Devolutions

Devolutions Server

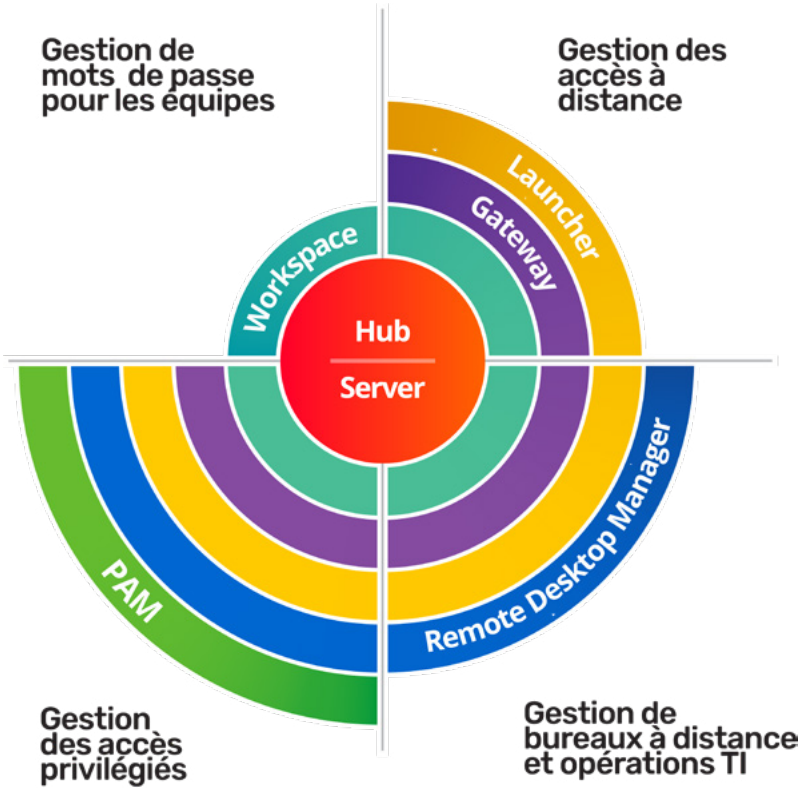
SPÉCIFICATIONS TECHNIQUES

Spécifications Techniques

Devolutions Server

Les organisations modernes font face à des défis croissants pour sécuriser les ressources TI, assurer la conformité et maintenir l'efficacité. **Devolutions Server (DVLS)** répond à ces besoins en centralisant la gestion des identifiants et des connexions à distance tout en renforçant la sécurité et en simplifiant l'accès des équipes.

DVLS s'intègre aux fournisseurs d'identité, applique une authentification forte et des contrôles d'accès rigoureux, et fournit un système de coffres évolutif pour les données sensibles. Il permet un accès sécurisé et audité grâce à des permissions basées sur les rôles, la rotation automatique des mots de passe, la gestion des sessions à distance et l'élévation des privilèges à la demande.



Exigences système

Recommandations de dimensionnement

Les recommandations suivantes fournissent des directives générales sur le matériel et l'infrastructure selon les habitudes d'utilisation et la charge utilisateur. Ces recommandations doivent être ajustées selon les caractéristiques de la charge de travail, les exigences de performance et la croissance anticipée.

- **Minimum :** 4 cœurs CPU, 8 Go de RAM (petites installations)
- **Recommandé :** 4 à 8 cœurs CPU, 8 Go de RAM (installations moyennes)
- **Entreprise :** 8+ cœurs CPU, 16+ Go de RAM (grandes installations)
- **Stockage :** SSD recommandé pour des performances optimales
- **Architecture :** x64

Taille de déploiement	Utilisateurs	Configuration recommandée
Basique	1-20	4 CPU cœurs, 8 GB RAM
Moyenne	21-75	4 CPU cœurs, 8 GB RAM
Grande	75 et plus	Configuration HA, 8+ CPU cœurs, 16+ GB RAM

Systèmes d'exploitation

Système d'exploitation	Versions prises en charge	Dépendances logicielles
Windows Server	Windows Server 2016 ou version ultérieure (Standard/Datacenter edition)	Microsoft IIS 10.0 ou supérieur, .NET 9.0 (.NET et ASP.NET Core)
Linux (prise en charge bêta)	Ubuntu 22.04 (autres distributions non testées)	Serveur web Kestrel intégré, .NET 9.0 (.NET et ASP.NET Core)

Exigences de base de données

Système de base de données	Versions prises en charge	Notes
Microsoft SQL Server	SQL Server 2016 ou supérieur (Express, Standard, or Enterprise editions)	Authentification SQL ou Windows prise en charge
Azure SQL	Version actuelle	Prend en charge uniquement les connexions SQL
AWS RDS for SQL Server	SQL Server 2016 ou supérieur	Disponible dans toutes les régions AWS

Composants supplémentaires

Composant	Exigence	Fonction
Devolutions Server Console	Windows uniquement, à installer sur Windows Server	Requise pour la gestion des instances du serveur
Windows Server	Niveau fonctionnel de domaine/forêt 2016 ou supérieur	Recommandé pour l'intégration Active Directory
Devolutions PowerShell Module	PowerShell 7.4+	Nécessaire pour le déploiement de DVLS sur Linux

Options de déploiement

DVLS propose des méthodes de déploiement flexibles pour répondre à divers besoins organisationnels, allant des exigences de sécurité strictes sur site à l'évolutivité basée sur le cloud. Ces options permettent aux organisations de mettre en œuvre DVLS de manière adaptée à leur infrastructure, leurs politiques de sécurité et leurs exigences opérationnelles spécifiques.

DVLS propose des méthodes de déploiement flexibles adaptées aux besoins organisationnels, allant des exigences de sécurité strictes sur site à l'évolutivité basée sur le cloud.

Topologies

Devolutions Server propose plusieurs topologies de déploiement pour s'adapter aux besoins organisationnels, aux exigences de sécurité et aux environnements d'infrastructure.

Topologie	Configuration	Description	Idéal pour
Serveur unique	DVLS et SQL Server sur la même machine	Déploiement le plus simple avec tous les composants sur un seul serveur	Petites équipes, environnements de test ou organisations avec des ressources TI limitées
Deux serveurs	DVLS et SQL Server sur des machines séparées	Sépare la couche application web de la base de données pour de meilleures performances	Organisations en croissance avec des besoins d'utilisation modérés
Haute disponibilité	DVLS avec un cluster SQL Server	Base de données SQL configurée en cluster actif-passif pour une protection en cas de panne	Organisations nécessitant un temps d'arrêt minimal et une protection des données
Répartition de charge	Plusieurs serveurs DVLS avec un répartiteur de charge et un cluster SQL	Un répartiteur de charge distribue le trafic entre plusieurs instances DVLS	Grandes entreprises avec de forts besoins de simultanéité
Basculement manuel	Serveurs DVLS dupliqués avec cluster SQL	Serveur DVLS secondaire disponible pour une connexion manuelle en cas de défaillance du serveur principal	Organisations ayant des exigences de reprise après sinistre avec peu de ressources d'automatisation

Types de déploiement

DVLS propose plusieurs types de déploiement afin de répondre aux différents besoins organisationnels et exigences d'infrastructure. Chaque modèle de déploiement offre des avantages uniques et peut être personnalisé pour satisfaire aux exigences spécifiques en matière de sécurité, de conformité et d'opérations.

Type de déploiement	Description	Idéal pour	Principaux avantages	Options de mise en œuvre
Sur site	Tous les composants sont hébergés dans votre infrastructure contrôlée	Organisations ayant des exigences strictes en matière de conformité réglementaire, de souveraineté des données ou des investissements existants en infrastructure	Contrôle total de la sécurité, des mises à jour et de la maintenance	Serveur unique, serveurs distribués
Basé sur le cloud	Déploiement dans Microsoft Azure (VM/App Services), AWS (EC2) ou autres plateformes cloud	Organisations recherchant l'évolutivité et l'accessibilité mondiale	Ressources élastiques, services gérés (Azure SQL/RDS), authentification intégrée	VM Azure, App Services, AWS EC2
Hybride	Combinaison stratégique de composants cloud et sur site	Organisations ayant des besoins mixtes	Options de déploiement flexibles	

Spécifications de sécurité

Devolutions Server offre des capacités de sécurité complètes grâce à des mécanismes de protection en couches, incluant la gestion des identités avec divers fournisseurs d'authentification, l'authentification multifacteur (MFA), un chiffrement robuste des données, des contrôles d'accès granulaires basés sur les rôles, ainsi qu'une journalisation d'audit étendue pour maintenir les normes de conformité et assurer une visibilité complète des activités du système.

Fournisseurs d'identité

DVLS prend en charge nativement divers fournisseurs d'identité, permettant aux utilisateurs de s'authentifier et d'accéder aux ressources de manière fluide tout en maintenant des standards de sécurité rigoureux à l'échelle de l'organisation. Ces intégrations permettent une gestion centralisée des identités, un accès utilisateur simplifié et une sécurité renforcée via des protocoles d'authentification standardisés.

Fournisseur d'identité	Fonctionnalités d'intégration entreprise
Microsoft Entra ID	Synchronisation de répertoires d'entreprise, gestion automatisée des accès basée sur les groupes Entra ID
Okta	Provisionnement automatique des utilisateurs, contrôle d'accès basé sur les rôles avec les groupes Okta
PingOne	Intégration avancée des répertoires, mappage personnalisable des attributs utilisateurs
Microsoft Active Directory	Synchronisation des utilisateurs de domaine, provisionnement automatique à partir d'Active Directory et mappage des appartenances aux groupes
Devolutions Server (built-in)	Attribution de rôles personnalisée, gestion granulaire des permissions, système d'authentification autonome

Prise en charge de l'authentification multifacteur (MFA)

DVLS offre des capacités complètes d'authentification multifacteur (MFA) afin de renforcer la sécurité au-delà de l'authentification par nom d'utilisateur et mot de passe. En mettant en œuvre plusieurs couches de vérification, les organisations peuvent réduire considérablement le risque d'accès non autorisé et d'attaques liées aux identifiants, garantissant ainsi que seuls les utilisateurs légitimes peuvent accéder aux informations et systèmes sensibles.

Méthode	Description
Email MFA	Codes de vérification temporels avec politiques d'expiration configurables
SMS Authentication	Vérification mobile en temps réel avec options de secours
Duo Security	Authentification par notification avec prise en charge biométrique
RADIUS	Authentification réseau de niveau entreprise
Authenticator (TOTP)	Les applications d'authentification génèrent des mots de passe à usage unique basés sur le temps
Backup Codes	Disponible en alternative à la MFA lorsqu'elle n'est pas accessible

Protection des données

DVLS applique une protection complète des données dans plusieurs domaines de sécurité à l'aide de techniques de chiffrement conformes aux normes de l'industrie. Devolutions Server utilise notre bibliothèque cryptographique open source : GitHub - Devolutions/devolutions-crypto: Devolutions Cryptographic Library

Contrôle d'accès

DVLS dispose de deux mécanismes de sécurité permettant de contrôler l'accès au système Devolutions Server ainsi qu'aux entrées et ressources qui y sont stockées. Ces mécanismes fonctionnent ensemble pour établir un cadre de sécurité complet protégeant le système et son contenu.

Accès applicatif

Contrôles permettant d'autoriser ou d'interdire les connexions à DVLS.

Type de contrôle	Configuration	Scénario
Accès applicatif	Liste d'applications approuvées avec contrôles spécifiques par plateforme pour Windows, Mac, Linux, iOS, Android, accès Web, accès CLI/scripts, Workspace, Launcher, extension navigateur Devolutions Workspace et PowerShell	Contrôle des applications clientes autorisées à accéder au système selon la plateforme et le type d'application
Restrictions IP	Configuration d'une IP unique, plages d'IP masquées, listes d'autorisation/interdiction	Restreint l'accès selon l'adresse IP du client, avec possibilité d'autoriser ou de bloquer des IP ou plages spécifiques
Accès basé sur le temps	Sélection des jours (semaine/weekend/personnalisé), définition de plages horaires, configuration du fuseau horaire, options de planification personnalisées	Restreint l'accès selon l'heure et le jour de la semaine
Restrictions GeoIP	Sélection de pays, listes d'autorisation/interdiction, intégration GeoIP de MaxMind	Restreint l'accès selon la localisation géographique de l'adresse IP du client
Blocage des nœuds de sortie Tor	Activation/désactivation du blocage Tor	Bloque l'accès depuis les nœuds de sortie Tor pour empêcher les connexions anonymes

Contrôles au niveau des ressources

Une fois connectés, les administrateurs peuvent contrôler de manière stricte l'accès aux ressources de plusieurs façons.

Type de contrôle	Implémentation	Configuration
Modèles personnalisés	Modèles de sécurité, modèles basés sur les rôles, modèles de groupes d'utilisateurs	Configurations de sécurité prédéfinies, héritage de modèles, règles de sécurité personnalisées
Accès temporaire	Octroi d'accès à durée limitée, flux de demandes d'accès	Paramètres de durée, flux d'approbation, configuration des heures de début et de fin
Politiques d'accès conditionnel	Contrôle d'accès basé sur des politiques gérant la connexion des utilisateurs	Combinaisons de règles (ET/OU), définitions d'actions (Autoriser/Refuser/MFA), ciblage des politiques
Accès basé sur les rôles	Hiérarchie des rôles, héritage des permissions, contrôles au niveau des dépôts	Attribution des rôles, ensembles de permissions, règles d'accès aux dépôts

Contrôle d'accès basé sur les rôles (RBAC)

DVLS met en œuvre un système de contrôle d'accès basé sur les rôles qui gère l'accès au système, les permissions et les périmètres de sécurité en fonction de rôles et responsabilités définis.

Rôle	Niveau d'accès	Permissions
Administrator	Accès complet au système	Toutes les permissions du système, y compris la configuration, la gestion des utilisateurs, les politiques de sécurité et l'accès aux coffres
Utilisateur	Accès standard	Créer/Modifier/Supprimer dans le périmètre assigné, lancer des connexions
LectureSeule	Accès en lecture seule	Voir les entrées et les connexions, sans droits de modification
Restreint	Accès limité	Permissions limitées définies de manière personnalisée

Journalisation

DVLS offre des capacités complètes de journalisation pour la surveillance opérationnelle, l'audit de sécurité et la production de rapports de conformité. La plateforme enregistre des informations détaillées sur les événements dans plusieurs domaines et propose des options de configuration flexibles pour la gestion, la rétention et la distribution des journaux vers diverses destinations.

Types d'événements

Type d'événement	Exemples d'événements
Syslog	Lorsque le serveur Syslog devient inaccessible, avec des messages d'échec et d'exception spécifiques.
Scheduler	Lorsque le service de planification passe hors ligne, bascule entre les modes actif et en attente, lorsqu'aucun planificateur de secours n'est disponible, ou lorsque le planificateur actif change.
Backup	Lorsque les sauvegardes système se terminent avec succès, échouent ou que la validation des sauvegardes échoue.
Gateway	Lorsqu'un Gateway est créé, mis à jour ou supprimé (ChangeManagement), ou lorsque son statut passe de « en ligne » à « hors ligne » (System).
Gateway Recording	Lorsque le nettoyage automatique des enregistrements de session s'effectue avec succès, avec avertissements ou lorsque l'espace de stockage des enregistrements est presque plein.
Gateway Farm	Lorsqu'un groupe de Gateway est créé, mis à jour ou supprimé du système.
Entry	Lorsque des entrées sont créées, modifiées, supprimées, consultées ou copiées, ou lorsque des mots de passe sont modifiés ou visualisés. Cela inclut le suivi détaillé des opérations sur les pièces jointes et les modifications de permissions.
Vault	Lorsque des données de coffres sont téléchargées pour le remplissage automatique (UserActivity), ou lorsque des coffres utilisateur sont transférés vers des coffres partagés (Administration).
Authentication Provider Sync	Lorsque la synchronisation des utilisateurs ou des groupes rencontre des erreurs ou se termine avec des avertissements, incluant des détails sur le processus de synchronisation.
Security	Lorsque des tâches du tableau de bord de sécurité sont ignorées ou restaurées, ou lorsque des entrées scellées sont descellées par les utilisateurs.
ServerCore	Lorsqu'un accès d'urgence est utilisé pour se connecter au système.
Expiration	Lorsque des entrées expirent ou approchent de leur date d'expiration, avec détails sur les entrées concernées.
Gateway Centralized Update	Lorsqu'une mise à jour de Gateway est demandée, démarrée, réussie, annulée, ou échoue avec des messages d'erreur spécifiques.
SMTP	Lorsque des opérations SMTP échouent, incluant des échecs généraux ou des erreurs spécifiques à l'envoi.

AdminLog	Lorsque des actions administratives sont enregistrées dans le système, avec détails sur l'action, l'utilisateur et les composants concernés.
DatasourceLog	Lors d'événements liés aux sources de données, incluant des détails sur la catégorie, le type de message et le contenu du journal.
PamPrivilegedAccount	Lorsque des comptes privilégiés sont créés, modifiés, supprimés, synchronisés ou que des opérations de mot de passe ont lieu, avec détails sur le compte et le fournisseur.
PAM Providers	Lorsque des fournisseurs PAM sont créés, modifiés, supprimés, synchronisés ou que des opérations de mot de passe ont lieu, avec détails sur la configuration du fournisseur.
PAM Checkout	Lorsque des emprunts de comptes privilégiés sont demandés, approuvés, refusés ou annulés, avec détails sur le processus et les approbateurs.
PAM Team Folder	Lorsque des dossiers PAM sont créés, modifiés ou supprimés, avec détails sur la configuration et les permissions.
PAM Checkout Policy	Lorsque des politiques d'emprunt sont créées, modifiées ou supprimées, avec détails sur la configuration de la politique.
PAM OTP Template	Lorsque des modèles OTP sont créés, modifiés ou supprimés, avec détails sur la configuration du modèle.
User	Lorsque des comptes utilisateurs sont créés, modifiés, supprimés ou que les permissions utilisateur changent, avec détails sur l'utilisateur concerné.
Role	Inclure les détails du rôle concerné lors de la création, modification ou suppression de rôles, ou lors de changements de permissions de rôles.

Options de conservation et de stockage des journaux

Type de politique	Description	Options
Périodes de rétention	Définit la durée de conservation des journaux dans le système	Personnalisée, 1 mois, 3 mois, 6 mois, 1 an, 2 ans, 7 ans, Jamais
Stratégies de nettoyage	Méthodes de gestion des journaux anciens	Archivage (déplacement vers des tables d'archives), Purge (suppression définitive)
Types de journaux gérés	Catégories de journaux avec politiques de rétention individuelles	Enregistrements de sauvegarde système, journaux d'activité de connexion, suivi des tentatives d'authentification, historique des sessions de connexion, messages d'événements système, journal d'audit de la gestion des accès privilégiés, historique des modifications des profils utilisateurs
Planification	Configuration des tâches de nettoyage automatisé	Activer/désactiver le nettoyage planifié, définir l'heure de nettoyage (par défaut : 2 h 00 UTC)
Options d'archivage	Rétention secondaire pour les journaux archivés	Période personnalisée, périodes prédéfinies, ne jamais supprimer

Alertes et notifications

DVLS offre un système complet d'alertes et de notifications permettant aux administrateurs et aux utilisateurs de rester informés des événements critiques du système, des incidents de sécurité et des activités opérationnelles. La plateforme propose plusieurs canaux de notification, des mécanismes de distribution configurables et des critères d'alerte personnalisables pour répondre aux besoins de l'organisation.

Événements

DVLS propose un système d'abonnement flexible aux événements, permettant aux administrateurs de configurer quels événements déclenchent des notifications et par quels canaux elles sont transmises. Les utilisateurs peuvent s'abonner à des types d'événements spécifiques en fonction de leur rôle et de leurs responsabilités, garantissant ainsi la réception d'alertes pertinentes en temps opportun sans être submergés par des notifications inutiles.

Catégorie d'événement	Type d'événement	Description	Niveau de gravité
Système	Changements de statut des services	Notifications lorsque les services passent en ligne/hors ligne	Information/Avertissement
Système	Défaillances et erreurs système	Erreurs critiques et défaillances du système	Erreur
Système	Événements d'authentification	Connexion d'urgence et activités d'authentification	Avertissement
Système	Modifications de configuration	Modifications des paramètres du système	Information
Système	Événements du planificateur	Succès/échec des tâches et état d'exécution	Information/Avertissement/Erreur
Gestion des utilisateurs	Création d'utilisateur	Création d'un nouveau compte utilisateur	Information
Gestion des utilisateurs	Modification d'utilisateur	Mises à jour du compte utilisateur	Information
Gestion des utilisateurs	Suppression d'utilisateur	Suppression d'un compte utilisateur	Information
Gestion des utilisateurs	Connexion/Déconnexion d'utilisateur	Activités de session utilisateur	Information
Gestion des utilisateurs	Modifications de permissions	Modifications des rôles et des permissions utilisateur	Information
Connexion	Création de connexion	Création d'une nouvelle connexion	Information
Connexion	Modification de connexion	Mises à jour de la connexion	Information
Connexion	Suppression de connexion	Suppression d'une connexion	Information
Connexion	Utilisation des connexions	Suivi du début et de la fin des sessions	Verbeux/Information
Connexion	Échecs de connexion	Tentatives de connexion échouées	Erreur
Connexion	Importation de connexions	Importations en masse de connexions	Information
Connexion	Consultation de mots de passe	Événements de visualisation de mots de passe	Information

Gateway	Changements de statut du Gateway	Statut en ligne/hors ligne du Gateway	Information/Avertissement
Gateway	Défaillances du Gateway	Défaillances des opérations du Gateway	Erreur
Gateway	Début/Interruption de session	Suivi des activités de session	Verbeux/Information
Gateway	Événements d'enregistrement	Limites de quota et avertissements d'espace disque faible	Avertissement
Communication	Succès/Échec de livraison de courriel	Statut des transmissions de courriels	Information/Erreur
Communication	Événements de traitement des messages	Statut du traitement des messages	Verbeux
PAM	Gestion des fournisseurs	Création, modification et suppression des fournisseurs PAM	Information
PAM	Gestion des comptes	Création, modification et suppression des comptes privilégiés	Information
PAM	Gestion des mots de passe	Réinitialisations et mises à jour des mots de passe	Information/Avertissement
PAM	Gestion des dossiers	Création, modification, suppression et exportation des dossiers PAM	Information
PAM	Gestion des modèles OTP	Création, modification et suppression des modèles OTP	Information
PAM	Gestion des politiques d'emprunt	Création, modification et suppression des politiques d'emprunt	Information
PAM	Activités d'emprunt	Création, approbation, refus, expiration des emprunts	Information/Avertissement
Demande d'accès	Création de demande	Soumission d'une nouvelle demande d'accès	Information
Demande d'accès	Approbation/Refus de demande	Décision sur les demandes d'accès	Information
Demande d'accès	Expiration de la demande	Expiration d'une demande d'accès	Information
Demande d'accès	Accès accordé	Fourniture d'un accès temporaire	Information

Canaux de notification

DVLS propose plusieurs canaux de notification permettant aux administrateurs de transmettre en temps opportun des alertes concernant des événements critiques du système, des incidents de sécurité et des activités opérationnelles aux parties prenantes concernées. Ces canaux peuvent être configurés indépendamment afin d'assurer une communication adaptée selon la gravité des événements, les rôles des destinataires et les préférences de l'organisation.

Canal	Configuration	Capacités
Notifications par courriel	Paramètres du serveur de courriel, modèles HTML, configuration des destinataires, options d'activation/désactivation	Modèles de courriels configurables avec prise en charge des destinataires individuels et en groupe, messages HTML avec détails sur les événements, personnalisation de l'objet et filtrage selon le niveau de notification
Notifications intégrées	Option d'activation/désactivation et préférences utilisateur	Notifications en temps réel disponibles dans l'interface web, avec centre de notifications pour consulter et gérer les alertes, indicateurs de statut (lu/non lu), tableau de bord des notifications et fonction « tout marquer comme lu »
Intégration Slack	Jeton OAuth du bot, nom du canal et option d'activation/désactivation	Publication des journaux d'activités dans des canaux Slack avec jetons de bot configurables et noms de canaux, messages formatés avec liens vers les ressources concernées, notifications d'événements de connexion et d'importation
Intégration syslog	Nom d'hôte/IP du serveur, numéro de port, protocole (TCP/UDP), option d'activation/désactivation, intervalle de battement	Transmission des événements vers des serveurs syslog avec format de journalisation standardisé, cibles syslog configurables, prise en charge de différents protocoles et surveillance de l'état du service
Notifications par message sécurisé	Option d'activation/désactivation et option de notification par courriel	Messagerie interne sécurisée pour les notifications sensibles, utilisée pour les demandes et approbations d'accès, prise en charge des pièces jointes, contenu localisé des messages et intégration des notifications push
Notifications push	Enregistrement de l'appareil, préférences par type de notification, options d'activation/désactivation	Notifications sur appareils mobiles configurables par appareil, avec prise en charge de divers types de notifications et ciblage spécifique selon l'appareil

Intégration à l'écosystème Devolutions

Remote Desktop Manager

Remote Desktop Manager (RDM) se connecte de manière transparente à DVLS, offrant une solution multiplateforme complète pour la gestion des identifiants. Disponible sur Windows, Mac, Linux, iOS et Android, RDM permet un accès sécurisé aux identifiants stockés dans DVLS avec des contrôles de permissions détaillés pour garantir une gestion appropriée des accès au sein de l'organisation.

- **Authentification et contrôle d'accès**
  - Contrôles d'accès spécifiques à la plateforme configurables par utilisateur
  - Prise en charge de l'intégration avec l'authentification Windows
  - Fonctionnalités de gestion des comptes privilégiés
  - Contrôle d'accès basé sur les rôles (RBAC) pour des permissions granulaires
- **Synchronisation des données**
  - Prise en charge de l'importation et de l'exportation des données de coffres entre RDM et DVLS
  - Opérations multi-coffres et sélection de dépôts
  - Contrôle de version des fichiers exportés
  - Chiffrement des données lors du transfert avec options de clé maîtresse
- **Fonctionnalités de sécurité**
  - Stockage et transmission chiffrés des identifiants
  - Prise en charge de l'intégration des mots de passe à usage unique (OTP)
  - Intégration à la gestion des accès privilégiés (PAM)
  - Journalisation d'audit complète de tous les accès aux identifiants
- **Contrôles administratifs**
  - Paramètres d'accès aux applications granulaires par plateforme
  - Paramètres et permissions spécifiques à chaque utilisateur
  - Gestion de la propriété et de l'accès aux coffres
  - Surveillance des activités et génération de rapports
- **Fonctionnalités supplémentaires**
  - Gestion des favoris sur toutes les plateformes
  - Modèles et politiques de sécurité personnalisés
  - Journalisation et surveillance des connexions
  - Notifications push pour les plateformes mobiles (iOS/Android)

Devolutions Launcher

L'intégration de Devolutions Launcher avec DVLS permet une gestion centralisée des identifiants, un renforcement des contrôles de sécurité, un déploiement simplifié et une journalisation d'audit complète. Cette intégration transforme Launcher, outil de connexion de base, en solution d'accès à distance dotée de solides fonctionnalités de sécurité et de capacités administratives.

- **Sécurité centralisée :**
  gestion centralisée des identifiants, contrôle d'accès basé sur les rôles et application des politiques de sécurité
- **Gestion des identifiants :** accès sécurisé aux identifiants centralisés, y compris comptes privilégiés et OTP
- **Contrôle d'accès :** contrôle granulaire via les permissions utilisateur, organisation par coffres et journalisation d'audit
- **Conformité et audit :** traçabilité complète des connexions et de l'utilisation des identifiants

Extension navigateur Devolutions Workspace

L'intégration de l'extension navigateur Devolutions Workspace avec DVLS la fait évoluer d'un simple gestionnaire de mots de passe vers une solution de gestion des identifiants de niveau entreprise, avec des contrôles de sécurité complets et des fonctionnalités administratives robustes.

- **Gestion centralisée :** système de coffres unifié, politiques de sécurité à l'échelle de l'organisation, contrôle centralisé des accès utilisateurs
- **Sécurité d'entreprise :** gestion des accès basée sur les rôles, protection des comptes privilégiés, intégration MFA
- **Gouvernance des accès :** contrôles de permission granulaires, organisation par coffres, restrictions temporelles/géographiques
- **Conformité et audit :** suivi détaillé de l'utilisation des identifiants, pistes d'audit complètes, rapports de conformité
- **Contrôle administratif :** provisionnement simplifié des identifiants, procédures d'accès d'urgence, rotation automatisée des identifiants

Devolutions Gateway

- **Contrôle d'accès centralisé**
  - DVLS gère les permissions d'accès à Gateway à l'aide de la sécurité basée sur les rôles
  - Les administrateurs contrôlent l'accès aux ressources Gateway
  - Intégration avec le système d'authentification DVLS pour une gestion unifiée
- **Sécurité renforcée**
  - Authentification par jeton via JWT (JSON Web Tokens)
  - Génération et validation sécurisées des jetons
  - Journalisation des accès et activités Gateway
- **Gestion automatisée des sessions**
  - Génération et validation automatiques des jetons de session
  - Surveillance et interruption des sessions
  - Révocation des jetons en cas d'incident
- **Administration simplifiée**
  - Configuration centralisée de Gateway et mises à jour à distance via DVLS
  - Intégration avec la gestion des utilisateurs DVLS
  - Journalisation et surveillance unifiées
  - Surveillance de l'état de Gateway et notifications
- **Fonctionnalités d'entreprise**
  - Prise en charge de plusieurs méthodes d'authentification (Windows, Azure AD, etc.)
  - Intégration à la gestion des accès privilégiés (PAM)
  - Journalisation détaillée des activités et rapports

Devolutions Workspace

L'intégration de Devolutions Workspace avec DVLS transforme l'accès via navigateur en solution complète de gestion de coffres, avec des contrôles de sécurité avancés et une intégration transparente.

- **Gestion centralisée des identifiants –**
  accès unifié aux coffres DVLS, comptes privilégiés et mots de passe sécurisés via une interface web intuitive
- **Intégration à la sécurité d'entreprise**
  - Intégration transparente aux contrôles d'accès basés sur les rôles de DVLS
  - Prise en charge de l'authentification multifacteur
  - Fonctionnalités PAM pour les identifiants sensibles
  - Notifications push en temps réel pour les événements de sécurité
- **Contrôles d'accès avancés**
  - Permissions granulaires sur les coffres et politiques d'accès
  - Restrictions d'accès temporelles et géographiques
  - Filtrage IP et blocage des nœuds de sortie Tor
  - Flux de demandes d'accès temporaire
- **Efficacité opérationnelle**
  - Intégration à l'extension navigateur pour le remplissage automatique des mots de passe
  - Synchronisation en temps réel avec les coffres DVLS
  - Messagerie sécurisée intégrée pour les demandes et approbations d'accès
  - Mode hors ligne pour un accès continu
- **Conformité et audit**
  - Journalisation complète des activités intégrée à DVLS
  - Suivi détaillé de l'utilisation des identifiants
  - Pistes d'audit des demandes d'accès
  - Gestion sécurisée des pièces jointes avec chiffrement

Méthodes d'accès client

DVLS propose plusieurs méthodes permettant aux clients d'accéder au système et d'interagir avec lui, assurant ainsi flexibilité et compatibilité avec divers cas d'usage et besoins organisationnels. Ces méthodes offrent un accès sécurisé et efficace tout en maintenant des contrôles de sécurité rigoureux et des capacités de journalisation complètes.

Interface Web

L'interface Web permet un accès complet à DVLS via des navigateurs standard :

- **Fonctionnalités principales**
  - Gestion des identifiants et des connexions
  - Administration des utilisateurs et des permissions
  - Accès et gestion des coffres
  - Configuration de la gestion des accès privilégiés (PAM)
  - Journalisation détaillée des activités et génération de rapports
- **Fonctionnalités de sécurité**
  - Contrôle d'accès basé sur les rôles (RBAC)
  - Prise en charge de l'authentification multifacteur
  - Gestion des sessions
  - Restrictions d'accès basées sur l'adresse IP
  - Filtrage par géolocalisation

API REST

DVLS propose une API REST complète pour un accès programmatique.

- **Authentification**
  - Authentification par jeton OAuth 2.0
  - Prise en charge de l'autorisation par jeton porteur
  - Intégration optionnelle avec l'authentification Windows
  - Prise en charge du proxy de pré-authentification
- **Fonctionnalités**
  - Format JSON pour les requêtes/réponses
  - Gestion complète des erreurs
  - Contrôles d'accès
  - Prise en charge des opérations synchrones et asynchrones

Intégration PowerShell

- **Fonctionnalités du module PowerShell**
  - Opérations de gestion des identifiants
  - Administration des utilisateurs et permissions
  - Configuration du système
  - Rotation automatisée des mots de passe
  - Gestion des politiques de sécurité
  - Opérations sur les coffres
- **Fonctionnalités de sécurité**
  - Gestion sécurisée des identifiants via SecureString
  - Prise en charge de l'authentification Windows intégrée
  - Contrôle d'accès basé sur les rôles
  - Journalisation des opérations PowerShell
- **Opérations courantes**
  - Gestion des utilisateurs
  - Réinitialisation des mots de passe
  - Configuration des accès
  - Gestion des coffres
  - Surveillance de l'état du système
  - Tâches de sauvegarde et de maintenance

Sauvegardes

Devolutions Server offre une fonctionnalité de sauvegarde robuste afin de protéger et préserver vos données. Ces sauvegardes garantissent la sécurité de vos informations critiques et permettent leur restauration fiable en cas de besoin.

Types de sauvegardes

Type de sauvegarde	Fonctionnalités	Description
Sauvegarde de base de données	Protection par mot de passe, chiffrement AES256/ZipCrypto, délai configurable	Crée des sauvegardes sécurisées de la base de données SQL Server à l'aide des mécanismes SQL natifs, avec chiffrement et compression optionnels. Prend en charge les stratégies de sauvegarde complètes ou différentielles.
Sauvegarde des fichiers web	Protection par mot de passe, chiffrement et validation d'intégrité	Crée des sauvegardes chiffrées des fichiers de l'application web, en conservant les configurations, personnalisations et paramètres système pour une restauration complète.

Déclencheurs de sauvegarde

Type de déclencheur	Description	Options de configuration
Manuel	Sauvegarde lancée manuellement par l'utilisateur via l'interface web	Exécution à la demande pour des scénarios de maintenance ou de mise à jour
Planifié	Sauvegarde automatisée selon un calendrier défini	Date/heure de début, intervalle en jours/heures, période de rétention

Gestion des sauvegardes

- **Politiques de rétention**
  - Historique configurable (nombre de sauvegardes à conserver)
  - Nettoyage automatique des anciens fichiers de sauvegarde
  - Rétention personnalisée selon le type de sauvegarde
- **Validation**
  - Vérifications automatisées de l'intégrité après la création des sauvegardes
  - Vérification de l'accessibilité des fichiers de sauvegarde
  - Validation de la cohérence des sauvegardes de bases de données

Rapports

DVLS (Devolutions Server) offre des capacités de génération de rapports complètes qui aident les organisations à surveiller l'activité du système, assurer la conformité en matière de sécurité et gérer efficacement les accès privilégiés. Ces rapports détaillés fournissent des informations exploitables sur les activités des utilisateurs, les événements de sécurité, les actions administratives et les opérations sur les coffres.

Catégories de rapports

Les rapports DVLS sont organisés en cinq grandes catégories afin d'aider les administrateurs à accéder efficacement aux informations dont ils ont besoin :

Rapports d'administration

Surveillez les modifications administratives et les opérations du système pour assurer la gouvernance et la conformité :

- Journaux d'administration
- Permissions système
- Permissions des administrateurs
- Configuration de la sécurité Gateway

Rapports d'activité

Suivez les interactions des utilisateurs et les comportements du système pour un audit complet :

- Journaux d'activité
- Activité des utilisateurs
- Historique de connexion
- Tentatives de connexion
- Dernière connexion
- Journaux de source de données

Rapports de sécurité

Évaluez la posture de sécurité et les contrôles d'accès :

- Analyseur de mots de passe
- Permissions des coffres
- Permissions des connexions
- Permissions non par défaut
- Permissions Gateway centrées utilisateur

Rapports PAM

Surveillez les activités liées à la gestion des accès privilégiés :

- Activités récentes PAM
- Journal de la dernière mise à jour de mot de passe PAM

Rapports d'entrées

Suivez la gestion des connexions et des entrées :

- Entrées de connexion expirées
- Entrées supprimées

Types d'événements et activités

Le système de rapports capture des informations détaillées dans divers domaines opérationnels :

Catégorie	Activités suivies
Événements système	Événements syslog, opérations du planificateur, processus de sauvegarde, changements de statut des services
Gestion des Gateway	Statut des Gateway (création/mises à jour/suppressions), opérations d'enregistrement, configuration des fermes
Gestion des entrées	Création, modification, suppression, accès aux identifiants, modifications des permissions
Activités des coffres	Opérations sur les données, changements de permissions, transferts entre coffres
Événements de sécurité	Modifications de configuration, activités d'authentification, utilisation des accès d'urgence
Opérations PAM	Gestion des comptes, processus d'emprunt, application des politiques
Activité utilisateur	Événements de connexion, actions administratives, modifications des permissions

Configuration des rapports

DVLS offre des options de configuration de rapports flexibles :

Options de planification

- Rapports ponctuels ou récurrents
- Modèles de récurrence multiples (quotidien, hebdomadaire, mensuel, personnalisé)
- Conditions de fin configurables

Méthodes de livraison

- Exportation au format CSV
- Distribution automatique par courriel
- Génération à la demande
- Archivage des rapports historiques

Contrôles de permission

- Accès aux rapports basé sur les rôles
- Droits administratifs requis
- Capacités de délégation pour la génération de rapports

À PROPOS DE DEVOLUTIONS

Devolutions aide les équipes TI à sécuriser les accès, les identifiants et les connexions à distance grâce à une plateforme intégrée conçue pour la complexité du monde réel.

De la gestion des mots de passe d'entreprise à la gestion des accès privilégiés et au contrôle des connexions à distance, nos solutions sont adaptées aux besoins des professionnels TI, des utilisateurs métier et des partenaires externes. Basée au Québec, au Canada, Devolutions reste fièrement indépendante et déterminée à rendre les solutions TI avancées accessibles, conviviales et abordables — pour les organisations de toutes tailles.

Documentations Devolutions:
https://docs.devolutions.net/fr/server/overview/what-is-server/

Forum: https://forum.devolutions.net/

Contactez nos experts :

Courriel: sales@devolutions.net

Téléphone: +1 (844) 463-0419

Du lundi au vendredi de 8 h à 17 h HNE (UTC-4)