FICHE TECHNIQUE

Appliance de comptes à privilèges

Sécurité pour les solutions qui protègent vos comptes à privilèges

Avantages

- Installation aisée
- Protection contre contre les attaques externes et de réseau avec un pare-feu intégré
- Simplification de la sécurisation sécurisation du matériel de base
- Évolutivité permettant de répondre aux futurs besoins en matière de performances
- Optimisation de la disponibilité avec les options de reprise et continuité de l'activité
- Prise en charge des options de matériel redondant

Lorsque votre organisation déploie des solutions pour gérer les identifiants d'accès, surveiller les accès aux actifs de grande valeur et provisionner l'accès à des programmes, des tâches et des commandes spécifiques, il est également crucial de contrôler l'accès même à ces solutions.

L'appliance de comptes à privilèges One Identity offre la sécurité et la confiance dont les entreprises ont besoin lors du déploiement des solutions Privilege Password Manager (PPM) et Priviledge Session Manager (PSM).

En tant qu'appliance sans client et sans agent conçue spécialement pour héberger les applications PPM et PSM, l'appliance Priviledge Account est renforcée d'origine afin d'assurer un niveau de protection maximum pour les actifs les plus sensibles de votre organisation.

ONE IDENTITY

Fonctionnalités

Accès sécurisé, basé sur les rôles : en l'absence de port de console ou d'interface de niveau de console, l'appliance n'est accessible que par le biais d'une interface Web sécurisée, basée sur les rôles. Elle assure ainsi une protection contre les attaques d'administrateurs hôtes et les modifications du système d'exploitation, des bases de données ou autres changements au niveau du système.

Pare-feu interne : elle est également dotée d'un pare-feu interne qui vous protège contre les attaques réseau externes et offre des possibilités supplémentaires en termes d'audit.

Chiffrement des mots de passe enregistrés : le chiffrement AES-256 bit assure la bonne protection de tous les mots de passe enregistrés.

Chiffrement du disque dur complet : le disque dur de l'appliance est chiffré à l'aide de BitLocker™ Drive Encryption.

Communications sécurisées : toutes les connexions utilisateur sont sécurisées par le biais du protocole HTTPS/SSLv3 de niveau maximum disponible en fonction de la négociation avec le client. Le certificat initial est signé par One Identity. Il peut être remplacé par un certificat spécifique au client. Les connexions de proxy utilisateur sont sécurisée via le protocole SSH. Les proxys de sessions cibles se font via le protocole natif le plus sécurisé. Dans la plupart des cas, il s'agit du protocole SSH. La communication programmatique (CLI/API) est sécurisée par SSH2, en utilisant des clés DSS asymétriques à des fins d'authentification.

Sécurité des bases de données : les communications entre les applications Web basées sur les rôles et la base de données sous-jacente sont protégées en interdisant l'accès direct à tous les objets ou données de bases de données. Seules les procédures enregistrées sont autorisées à être appelées depuis l'application. Aucun appel SQL ad hoc n'est autorisé.

Sécurité de l'application : la séparation des tâches (SoD) est appliquée à travers le contrôle d'accès basé sur les rôles (RBAC), qui est intégré à l'application.

Appliance matérielle de comptes à privilèges

Nom du modèle	Appliance standard	Appliance standard
Processeur	Gamme de processeurs Intel® Xeon® E3-1220	Gamme de processeurs Intel® Xeon® E5-2600
Nombre de processeurs	1	2
Nombre de cœurs par processeur	Quatre	Six
Cache de niveau 2/ niveau 3	10 Mo	10 Mo
Jeu de puces	Intel® C236	Intel® série C610
Barrettes DIMM	R-DIMM DDR4	R-DIMM DDR4
Mémoire RAM	8 Go minimum	32 Go minimum
Baies de disque dur	4 x 3,5" enfichables à chaud	4 x 3,5" enfichables à chaud
Types de disques durs	SATA/SAS	Contrôleur SAS supplémentaire
Contrôleur interne de disque dur	Contrôleur RAID intégré H310	Contrôleur RAID intégré H710P ; cache NV de 1 Go
Espace disque	2 x 500 Go	4 x 300 Go 15 000 tr/min SAS
Disponibilité	Disque dur avec échange de mémoire ECC, bloc d'alimentation redondant, TPM	Disque dur enfichable à chaud, bloc d'alimentation redondant, mise en miroir de la mémoire, TPM
Emplacements d'E/S	2 x PCIe 3.0	2 x PCIe x16, mi-hauteur, mi-longueur
RAID	RAID 1 en miroir	RAID10
NIC/LOM	2 x GbE LOM	2 x GbE LOM
DRAC	iDRAC8 Entreprise	iDRAC8 Entreprise
USB	2 avants/2 arrières/2 internes	2 avants/2 arrières/2 internes
Blocs d'alimentation/ caractéristiques	Redondant, 350 W, auto-adaptable (100 V~240 V), compatible avec ACPI	Redondant, 550 W, auto-adaptable (100 V~240 V), compatible avec ACPI
Ventilateurs	3 non redondants, non enfichables à chaud	4 non redondants, non enfichables à chaud
Boîtier	Rack 1U	Rack 1U
Dimensions	42,8 x 434 x 625 mm (sans bordure) (1,68 x 17,08 x 24,6 pouces.)	42,8 x 434 x 607 mm (sans bordure ni patte) (1,68 x 17,08 x 23,9 pouces.)
Poids	13,8 kg maximum (30,42 livres)	19,9 kg maximum (43,87 livres)
Divers	Commutateur d'intrusion pour détecter l'ouverture du couvercle, fonctionnalité hyper-threading (8 fils), panneau d'état LCD de 128 x 120	Commutateur d'intrusion pour détecter l'ouverture du couvercle, multithreading simultané, module LCD d'état.
Température de fonctionnement	De 10 °C à 35 °C	De 10 °C à 35 °C
Certifications réglementaires	Classe A :	Classe A :
Les informations relatives aux certifications complémentaires par pays sont disponibles sur demande	Australie/Nouvelle-Zélande – AMCA ou C-Tick Canada – SCC, ICES Union européenne – CE Allemagne – TUV États-Unis – FCC, NRT	Australie/Nouvelle-Zélande – AMCA ou C-Tick Canada – SCC, ICES Union européenne – CE Allemagne – TUV États-Unis – FCC, NRT

Ce tableau indique les plateformes matérielles actuelles pour chaque configuration d'appliance de comptes à privilèges. Les composants répertoriés sont conformes aux unités sortant d'usine au moment de la publication de ce document. Cependant, ils peuvent être modifiés à tout moment sans préavis en raison de l'obsolescence des composants, de leur indisponibilité ou d'une notification de défaut.

À propos de One Identity

La gamme One Identity de solutions de gestion des accès et des identités (IAM) inclut une offre de solutions IAM concrètes de gouvernance des identités, de gestion des accès et de gestion des comptes à privilèges axées sur l'entreprise, modulaires, intégrées et tournées vers l'avenir.

Informations supplémentaires

Pour en savoir plus sur la solution Priviledge Password Manager, visitez oneidentity.com/privileged-password-manager