Dell Security Management Server Virtual

Quick Start and Installation Guide v11.9

December 2023
Rev. A01

DELL Technologies

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Contents

1

Guide de démarrage rapide

Le présent Guide de démarrage rapide explique aux utilisateurs les plus expérimentés comment installer et configurer rapidement le Dell Server. En règle générale, Dell recommande d'installer d'abord le Dell Server, puis les clients.

Pour obtenir des instructions détaillées, reportez-vous au Guide d'installation de Security Management Server Virtual.

Pour plus d'informations sur les conditions préalables du Dell Server, consultez les Conditions préalables de Security Management Server Virtual, les Conditions préalables de la Console de gestion et les Conditions préalables du mode Proxy.

Pour savoir comment mettre à jour un Dell Server existant, reportez-vous à Mise à jour de Security Management Server Virtual.

Installation

1. Naviguez jusqu'au répertoire contenant les fichiers Dell Data Security. Cliquez deux fois dessus pour importer dans VMware le Security Management Server Virtual **v11.x.x Build x.ova**.

   REMARQUE : OVA est à présent signé SHA256 et ne peut pas être importé dans le client Thick VMware. Pour en savoir plus, voir https://kb.vmware.com/s/article/2151537.

2. Mettez en route Security Management Server Virtual.
3. Suivez les instructions à l'écran.

Configuration

Avant d'activer des utilisateurs, il est recommandé d'effectuer les tâches de configuration suivantes sur le terminal Security Management Server Virtual :

- Configurer les paramètres SMTP
- Importer un certificat existant ou inscrire un nouveau certificat de serveur
- Mettre à jour Security Management Server Virtual
- Installez un client FTP qui prend en charge SFTP sur le port 22 et Définir les utilisateurs FTP (Transfert de fichiers).

  Si votre organisation dispose de périphériques accessibles depuis l'extérieur, voir la section Installer et configurer le mode Proxy.

Ouverture de la Console de gestion

Ouvrez la console de gestion à cette adresse : https://server.domain.com:8443/webui/

Les références par défaut sont **superadmin/changeit**.

Pour obtenir la liste des navigateurs Web pris en charge, voir la rubrique Conditions préalables de la console de gestion.

Tâches administratives

Si vous n'avez pas démarré la Console de gestion, vous pouvez le faire maintenant. Les informations d'identification par défaut sont **superadmin/changeit**.

Dell Technologies vous recommande d'attribuer des rôles d'administrateur dès que possible. Pour effectuer cette tâche maintenant, reportez-vous à Attribuer le rôle d'administrateur Dell.

Cliquez sur « ? » dans le coin supérieur droit de la Console de gestion pour démarrer l'*Aide administrateur*. La page *Mise en route* s'affiche. Cliquez sur **Ajouter des domaines**.

Des règles de base ont été définies pour votre organisation, mais elles doivent être modifiées comme suit en fonction de vos besoins spécifiques (toutes les activations sont soumises à des licences et à des droits) :

- Le chiffrement basé sur des règles est activé avec un chiffrement à clé commun.
- Les ordinateurs équipés de disques à autochiffrement sont chiffrés.
- BitLocker Manager est désactivé.
- Advanced Threat Prevention est désactivé.
- La protection contre les menaces est désactivée.
- Les supports externes ne sont pas chiffrés.
- Les ports ne sont pas gérés par le contrôle des ports.
- Les appareils sur lesquels le chiffrement complet du disque est installé ne sont pas chiffrés.

Voir la rubrique AdminHelp *Gestion des règles* pour accéder à Groupes de technologie et à la description des règles.

Les tâches de démarrage rapide sont terminées.

2

Guide détaillé d'installation

Ce guide d'installation explique aux utilisateurs moins expérimentés comment installer et configurer Security Management Server Virtual. En règle générale, Dell recommande d'installer d'abord Security Management Server Virtual, puis les clients.

Pour savoir comment mettre à jour un Security Management Server Virtual existant, consultez Mettre à jour Security Management Server Virtual.

À propos de Security Management Server Virtual

La console de gestion permet aux administrateurs de surveiller l'état des points de terminaison, l'application des règles et la protection dans l'ensemble de l'entreprise. Le mode Proxy propose une option frontale (mode DMZ) à utiliser avec Security Management Server Virtual.

Security Management Server Virtual possède les caractéristiques suivantes :

- Gestion centralisée de 3 500 périphériques maximum
- Création et gestion de règles de sécurité basées sur des rôles
- Récupération de périphérique assistée par l'administrateur
- Division des tâches administratives
- Distribution automatique des règles de sécurité
- Chemins d'accès approuvés pour la communication entre les composants
- Génération de clés de chiffrement uniques et blocage automatique de clés sécurisées
- Audit et rapports de conformité centralisés
- Génération automatique de certificats auto-signés

Contactez Dell ProSupport for Software

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24x7 une assistance téléphonique concernant votre produit Dell.

Un support en ligne pour les produits Dell est en outre disponible à l'adresse dell.com/support. Le support en ligne englobe les pilotes, les manuels, des conseils techniques et des réponses aux questions fréquentes et émergentes.

Aidez-nous à vous mettre rapidement en contact avec l'expert technique approprié en ayant votre numéro de série ou votre code de service express à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez l'article Numéros de téléphone internationaux Dell ProSupport for Software.

Configuration requise

Security Management Server Virtual

Hardware

The recommended disk space for Security Management Server Virtual is 80 GB.

Virtualized Environment

Security Management Server Virtual v11.7 has been validated with the following virtualized environments.

Dell currently supports hosting the Dell Security Management Server or Dell Security Management Server Virtual within a Cloud-hosted Infrastructure as a Service (IaaS) environment, such as Amazon Web Services, Azure, and several other vendors. Support for these environments is only limited to the functionality of the application server hosted within these Virtual Machines, the administration and security of these Virtual Machines is up to the administrator of the IaaS solution.

Additional infrastructure requirements (Active Directory, as well as SQL Server for the Dell Security Management Server) are still required for proper functionality.

Virtualized Environments
• VMware Workstation 14.0 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 14.1 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 15.0 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 15.1 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware ESXi 6.0 ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware ESXi 6.5 ○ 64-bit x86 CPU required

Virtualized Environments
○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
● VMware ESXi 6.7 ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
● Hyper-V Server (Full or Core installation) ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An operating system is not required. ○ Hardware must conform to minimum Hyper-V requirements. ○ Must be run as a Generation 1 Virtual Machine. **NOTE:** For information about setting up Hyper-V, follow instructions for Endpoint Operating Systems: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v or for Server Operating Systems: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Console de gestion

Navigateurs Internet

REMARQUE :

Le navigateur doit accepter les cookies.

Le tableau suivant décrit les navigateurs Internet pris en charge.

Navigateurs Internet
● Mozilla Firefox 41.x ou supérieur ● Google Chrome 46.x ou version supérieure ● Microsoft Edge (Chromium) ● Microsoft Edge

Accès à la console de gestion

Comme Internet Explorer n'est plus pris en charge, vous devez installer un navigateur tiers pour accéder correctement à la console de gestion.

Si Internet Explorer est requis pour valider la console de gestion, vous devez désactiver la configuration de sécurité renforcée Internet Explorer pour le type de compte correspondant à l'administrateur connecté.

Mode Proxy

Matériel

Le tableau suivant détaille la configuration matérielle *minimale* requise.

Processeur CPU double cœur avancé (1,5 GHz minimum)
RAM 2 Go minimum de RAM dédiée / 4 Go de RAM dédiée recommandés
Espace disque disponible 1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel)
Carte réseau Carte d'interface réseau 10/100/1000
Divers IPv4, IPv6 ou une combinaison d'IPv4 et d'IPv6 sont pris en charge.

Logiciel

Le tableau suivant décrit les applications requises pour l'installation du serveur en mode Proxy.

Conditions préalables
• **Windows Installer 4.0 ou ultérieur** Windows Installer version 4.0 ou version ultérieure doit être installé sur le serveur cible de l'installation.
• **Package redistribuable Microsoft Visual C++ 2010** S'il n'est pas installé, le programme d'installation le fait pour vous.
• **Microsoft .NET Framework version 4.6.1** Microsoft a publié des mises à jour de sécurité pour .NET Framework version 4.6.1.

REMARQUE :

Le Contrôle de compte d'utilisateur (UAC) doit être désactivé lors de l'installation dans un répertoire protégé. Une fois l'UAC désactivé, vous devez redémarrer le serveur pour que cette modification prenne effet.

Emplacements dans le registre sous Windows Server : HKLM\SOFTWARE\Dell.

Le tableau suivant détaille la configuration logicielle requise pour le serveur en mode Proxy.

Système d'exploitation
• **Windows Server 2022** - Édition Standard - Édition Datacenter
• **Windows Server 2019** - Édition Standard - Édition Datacenter
• **Windows Server 2016**

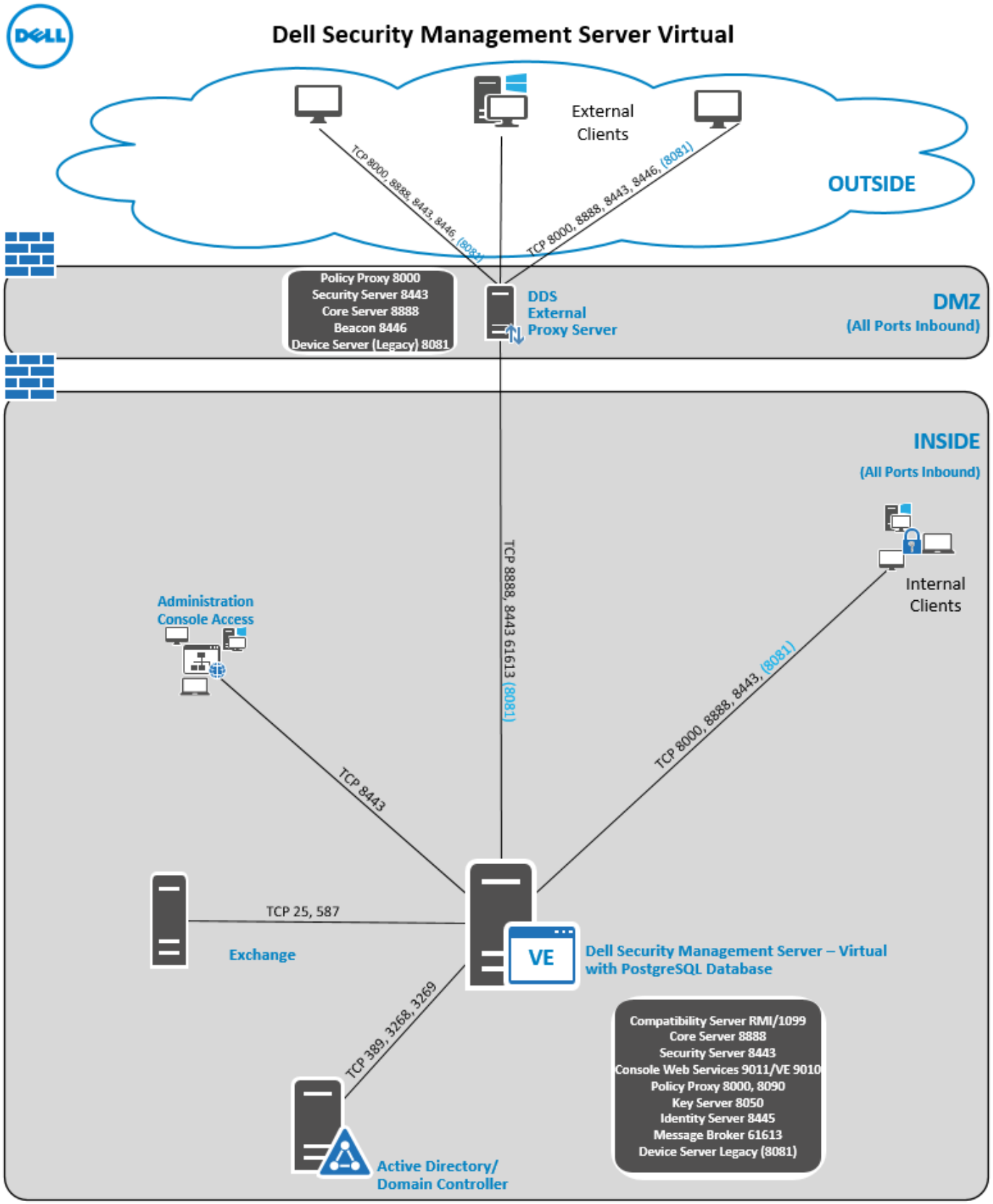
Système d'exploitation
- Édition Standard - Édition Datacenter
• **Windows Server 2012 R2** - Édition Standard - Édition Datacenter
• **Référentiel LDAP** - Active Directory 2008 R2 - Active Directory 2012 R2 - Active Directory 2016 - Azure Active Directory hybride

Conception d'architecture de Security Management Server Virtual

Les solutions Encryption Enterprise et Endpoint Security Suite Enterprise sont des produits hautement évolutifs, selon le nombre de points de terminaison ciblés pour le chiffrement dans votre entreprise.

Composants d'architecture

Le déploiement de base ci-dessous est celui de Dell Security Management Server Virtual.


Dell Security Management Server Virtual
External Clients
OUTSIDE
TCP 8000, 8888, 8443, 8446, (8081)
TCP 8000, 8888, 8443, 8446, (8081)
Policy Proxy 8000
Security Server 8443
Core Server 8888
Beacon 8446
Device Server (Legacy) 8081
DDS External Proxy Server
DMZ
(All Ports Inbound)
INSIDE
(All Ports Inbound)
Internal Clients
Administration Console Access
TCP 8888, 8443 61613 (8081)
TCP 8443
TCP 8000, 8888, 8443, (8081)
TCP 25, 587
Exchange
VE
Dell Security Management Server – Virtual with PostgreSQL Database
TCP 389, 3268, 3269
Compatibility Server RMI/1099
Core Server 8888
Security Server 8443
Console Web Services 9011/VE 9010
Policy Proxy 8000, 8090
Key Server 8050
Identity Server 8445
Message Broker 61613
Device Server Legacy (8081)
Active Directory/ Domain Controller

Téléchargement et installation du fichier OVA

Au cours de l'installation initiale, Security Management Server Virtual est livré sous la forme d'un fichier OVA, une application Open Virtual utilisée pour fournir un logiciel qui s' exécute sur une machine virtuelle. Le fichier OVA est disponible sur www.dell.com/support, sur les pages Support produit des produits Dell Data Security suivants :

- Chiffrement
- Endpoint Security Suite Enterprise

Pour télécharger le fichier OVA :

1. Accédez à la page *Pilotes et téléchargements* du produit approprié listé ci-dessus.
2. Cliquez sur **Pilotes et téléchargements**.
3. Sélectionnez la version de VMware ESXi appropriée.
4. Téléchargez le lot approprié.

Pour installer le fichier OVA :

Avant de commencer, assurez-vous que toutes les conditions requises du système et de l'environnement virtuel sont remplies.

1. Effectuez l'une des opérations suivantes :

VMware	Dans le support d'installation Dell, localisez le fichier *Security Management Server Virtual v11.x.x Build x.ova* et double-cliquez dessus pour l'importer dans VMware. Suivez les instructions à l'écran. **REMARQUE :** Si l'importation échoue lors de l'utilisation de VMWare, le client Web sera le chemin suggéré pour l'importation du fichier OVA. Pour en savoir plus, consultez le document https://kb.vmware.com/s/article/2151537.
Hyper-V Suivez les instructions pour Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/ .	Configuration requise : ● Machine virtuelle de la génération 1 ● Security Management Server Virtual est au format VHDX. Vous ne devez pas définir de disque. Il doit être ajouté à la machine virtuelle une fois qu'elle aura été créée dans Hyper-V. Voir https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v.
Systèmes d'exploitation du serveur	Suivez les instructions : https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.
ESXi Suivez les instructions :https://kb.vmware.com/s/article/2109708	Processus d'importation OVA : Voir https://docs.VMware.com/en/VMware-vSphere/6.7/com.VMware.vSphere.html.hostclient.doc/GUID-FBEED81C-F9D9-4193-BDCC-CC4A60C20A4E_copy.html.

2. Mettez en route Security Management Server Virtual.
3. Sélectionnez la langue du Contrat de licence et sélectionnez **Afficher le CLUF**.
4. Lisez le contrat et sélectionnez **Accepter le CLUF**.
5. Si une mise à jour est disponible, sélectionnez **Accepter**.
6. Sélectionnez **Mode Connecté** ou **Mode Déconnecté**.

REMARQUE :

Si vous sélectionnez le **Mode déconnecté**, vous ne pourrez jamais passer au mode Connecté.

Le mode Déconnecté isole le Dell Server d'Internet et d'un LAN ou autre réseau non sécurisé. Toutes les mises à jour doivent être effectuées manuellement. Pour plus d'informations sur le mode Déconnecté et les règles, voir l'*Aide administrateur*.

7. Sur l'écran *Définir le mot de passe delluser*, saisissez le mot de passe actuel (par défaut), **delluser**, saisissez un mot de passe unique, saisissez-le une deuxième fois, puis sélectionnez **Appliquer**.

   Les mots de passe doivent comprendre les éléments suivants :

   - Au moins 8 caractères
   - Au moins une lettre majuscule
   - Au moins 1 chiffre
   - Au moins un caractère spécial

   REMARQUE : il est possible de conserver le mot de passe par défaut en sélectionnant **Annuler** ou en appuyant sur la touche **Échap** du clavier.
8. Cliquez sur **Fermer** pour accéder à l'écran de configuration du nom d'hôte.
9. Dans la boîte de dialogue *Configurer le nom d'hôte*, utilisez la touche Retour arrière pour supprimer le nom d'hôte par défaut. Saisissez un nom d'hôte unique, puis sélectionnez **OK**.
10. Dans la boîte de dialogue *Configurer les paramètres de réseau*, choisissez l'une des deux options ci-après, puis sélectionnez **OK**.

    - (Par défaut) Utiliser DHCP (IPv4)
    - (Recommandée) Dans le champ *Utiliser DHCP*, appuyez sur la barre d'espacement pour supprimer le X et saisir manuellement ces adresses, le cas échéant :

      Static IP (Adresse IP statique)

      Masque de réseau

      Passerelle par défaut

      Serveur DNS 1

      Serveur DNS 2

      Serveur DNS 3

      Il est possible de sélectionner IPv6 ou IPv4 pour une configuration statique.

    - **REMARQUE :** Lorsque vous utilisez une adresse IP statique, vous devez également créer une entrée d'hôte dans le serveur DNS.
11. À l'invite de confirmation du fuseau horaire, cliquez sur **OK**.
12. Lorsque s'affiche le message indiquant que la configuration premier démarrage est terminée, sélectionnez **OK**.
13. Configurer les paramètres SMTP.
14. Importer un certificat existant ou inscrire un nouveau certificat de serveur.
15. Mettre à jour Security Management Server Virtual.
16. Installez un client FTP qui prend en charge SFTP sur le port 22 et Définir les utilisateurs FTP (Transfert de fichiers).

    Les tâches d'installation de Security Management Server Virtual sont terminées.

Ouverture de la Console de gestion

Ouvrez la console de gestion à cette adresse : https://server.domain.com:8443/webui/

Les références par défaut sont **superadmin/changeit**.

Pour obtenir la liste des navigateurs Web pris en charge, voir la rubrique Conditions préalables de la console de gestion.

Installer et configurer le mode Proxy

Le mode proxy fournit une option front-end (mode DMZ) à utiliser avec le Dell Server. Si vous prévoyez de déployer des composants Dell dans la zone DMZ, veillez à les protéger correctement contre les attaques.

Pour effectuer l'installation, vous aurez besoin du nom de l'hôte entièrement qualifié du serveur DMZ.

1. Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Extrayez** (SANS copier et coller ou glisser et déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server Virtual. ***Les opérations de copier et coller ou glisser et déposer produisent des erreurs et empêchent l'installation.***
2. Double-cliquez sur **setup.exe**.
3. Sélectionnez la langue de l'installation, puis cliquez sur **OK**.
4. Si les composants requis n'ont pas déjà été installés, un message s'affiche, vous informant des composants requis à installer. Cliquez sur **Installer**.
5. Cliquez sur **Suivant** sur l'écran Bienvenue.
6. Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
7. Entrez les 32 caractères composant la clé de produit, puis cliquez sur **Suivant**. La clé de produit se trouve dans le fichier `EnterpriseServerInstallKey.ini`.
8. Sélectionnez **Installation principale**, puis cliquez sur **Suivant**.
9. Pour installer le serveur front-end dans l'emplacement par défaut `C:\Program Files\Dell`, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.
10. Vous avez le choix entre différents types de certificats numériques.

    REMARQUE : Il est vivement recommandé d'utiliser un certificat numérique provenant d'une autorité de certification fiable.

    Sélectionnez l'option « a » ou « b » ci-dessous :

    a. Pour utiliser un certificat existant acheté auprès d'une autorité de certification, sélectionnez **Importer un certificat existant**, puis cliquez sur **Suivant**.
    b. Pour créer un certificat auto-signé, sélectionnez **Créer un certificat auto-signé et l'importer dans un magasin de clés, puis cliquez sur Suivant.**

       Dans la boîte de dialogue *Créer un certificat auto-signé*, saisissez les informations suivantes :

       Nom complet de l'ordinateur (par exemple : nomordinateur.domaine.com)

       Organisation

       Service (exemple : Sécurité)

       Ville

       État (nom complet)

       Pays : code de deux lettres du pays ou de la zone géographique

       Cliquez sur **Suivant**.

       REMARQUE : Par défaut, le certificat expire dans dix ans.

11. Dans la boîte de dialogue *Configuration du serveur front-end*, saisissez le nom de l'hôte complet ou l'alias DNS du serveur back-end, sélectionnez **Dell Security Management Server**, puis cliquez sur **Suivant**.
12. Depuis la boîte de dialogue *Configuration de l'installation du serveur frontal*, vous pouvez afficher ou modifier les noms de l'hôte et les ports.
    - Pour accepter les noms de l'hôte et les ports par défaut, dans la boîte de dialogue de *configuration de l'installation du serveur frontal*, cliquez sur **Suivant**.
    - Pour afficher ou modifier les noms de l'hôte, dans la boîte de *configuration du serveur frontal* cliquez sur **Modifier les noms de l'hôte**. Modifiez les noms d'hôte uniquement si nécessaire. Dell Technologies recommande l'utilisation des paramètres par défaut.

      REMARQUE :

      Un nom de l'hôte ne doit pas contenir de caractère de soulignement (« _ »).

      Supprimez un proxy uniquement si vous êtes certain de ne pas vouloir le configurer en vue de son installation. Si vous supprimez un proxy dans cette boîte de dialogue, il ne sera pas installé.

      Une fois que vous avez terminé, cliquez sur **OK**.
    - Pour afficher ou modifier les ports, dans la boîte de dialogue *Configuration du serveur frontal*, cliquez sur **Modifier les ports externes** ou **Modifier les ports de connexion internes**. Modifier les ports uniquement si nécessaire. Dell Technologies recommande l'utilisation des paramètres par défaut.

Si vous supprimez un proxy dans la boîte de dialogue *Modifier les noms de l'hôte frontaux*, le port correspondant ne s'affiche pas dans les boîtes de dialogue Ports externes ou Ports internes.

Une fois que vous avez terminé, cliquez sur **OK**.

13. Dans la boîte de dialogue *Prêt à installer le programme*, cliquez sur **Installer**.
14. Une fois l'installation terminée, cliquez sur **Terminer**.

Tâches de configuration de base du terminal

Les tâches de configuration de base sont accessibles à partir du menu principal.

Vérification du tableau de bord du système

Pour vérifier l'état des services de Dell Server, ouvrez le menu principal et cliquez sur **Tableau de bord du système**.

Le widget *Informations sur le système* affiche la version actuelle, le nom d'hôte et l'adresse IP, ainsi que l'utilisation de l'UC, de la mémoire et du disque.

Le widget *Historique des versions* affiche les modifications de schéma de la base de données par version. Les données proviennent du tableau d'informations et sont triées par date, avec la version la plus récente en haut.

Le tableau suivant décrit chaque service et sa fonction sous le widget *Santé du service*.

Nom	Description
Courtier de messages	Bus du serveur Enterprise
Serveur d'identité	Traite les demandes d'authentification de domaine.
Compatibility Server	Service de gestion de l'architecture d'entreprise.
Security Server	Mécanisme de contrôle des commandes et des communications avec Active Directory.
Core Server	Service de gestion de l'architecture d'entreprise. Ce service gère également l'ensemble de la collecte d'activations, de règles et d'inventaires des périphériques basés sur l'« Agent ».
Core Server HA (Haute disponibilité)	Un service de haute disponibilité qui permet d'augmenter la sécurité et la performance des connexions HTTPS lors de la gestion de l'architecture d'entreprise.
Serveur d'inventaire	Traite la file d'attente de l'inventaire.
Forensic Server	Fournit des services Web pour l'API Forensic.
Policy Proxy (Proxy de stratégie)	Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité.

Les services sont surveillés et redémarrés automatiquement si nécessaire.

REMARQUE : Si le processus de personnalisation de la base de données échoue, les serveurs passent à l'état Échec de l'exécution. Pour vérifier le rapport de personnalisation de la base de données, dans le menu principal, sélectionnez Afficher les rapports.

Modification du nom d'hôte

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser Security Management Server Virtual.

1. Dans le menu *Configuration de base*, sélectionnez **Nom d'hôte**.
2. Utilisez la touche RETOUR ARRIÈRE pour supprimer le nom d'hôte existant, puis remplacez-le par un nouveau nom d'hôte et sélectionnez **OK**.

Modifier les paramètres réseau

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser Security Management Server Virtual.

1. Dans le menu *Configuration de base*, sélectionnez **Réseau**.
2. À l'écran *Configurer les paramètres de réseau*, choisissez l'une des deux options ci-après, puis sélectionnez **OK**.
   - (Par défaut) Utiliser DHCP (IPv4)
   - (Recommandé) Dans le champ *Utiliser DHCP*, appuyez sur la barre d'espacement pour supprimer le X et entrer manuellement ces adresses, le cas échéant :

     Static IP (Adresse IP statique)

     Masque de réseau

     Passerelle par défaut

     Serveur DNS 1

     Serveur DNS 2

     Serveur DNS 3

     Il est possible de sélectionner IPv6 ou IPv4 pour une configuration statique.

     REMARQUE :

     Lorsque vous utilisez une adresse IP statique, vous devez créer une entrée d'hôte dans le serveur DNS.

Configuration de la prise en charge du serveur DMZ

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser Security Management Server Virtual.

1. Dans le menu *Configuration de base*, sélectionnez **Prise en charge du serveur DMZ**.
2. Utilisez la barre d'espacement pour saisir un **X** dans le champ Activer la prise en charge du serveur DMZ.
3. Entrez le nom de domaine complet du serveur DMZ, puis sélectionnez **OK**.

REMARQUE : Pour tirer le meilleur parti d'un serveur DMZ, veuillez vous reporter aux instructions d'installation ci-dessus pour un serveur Proxy, Installation et configuration du mode Proxy.

Modifier le fuseau horaire

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser Security Management Server Virtual.

1. Dans le *menu Configuration de base*, sélectionnez **Fuseau horaire**.
2. Dans l'écran *Fuseau horaire*, utilisez les touches fléchées pour mettre en surbrillance votre fuseau horaire, puis sélectionnez **Entrée**.

Mettre à jour Security Management Server Virtual

Pour plus d'informations sur une mise à jour spécifique, voir *Security Management Server Virtual* sur dell.com/support. Pour consulter la version et la date d'installation d'une mise à jour déjà appliquée, vérifiez le *Tableau de bord du système*.

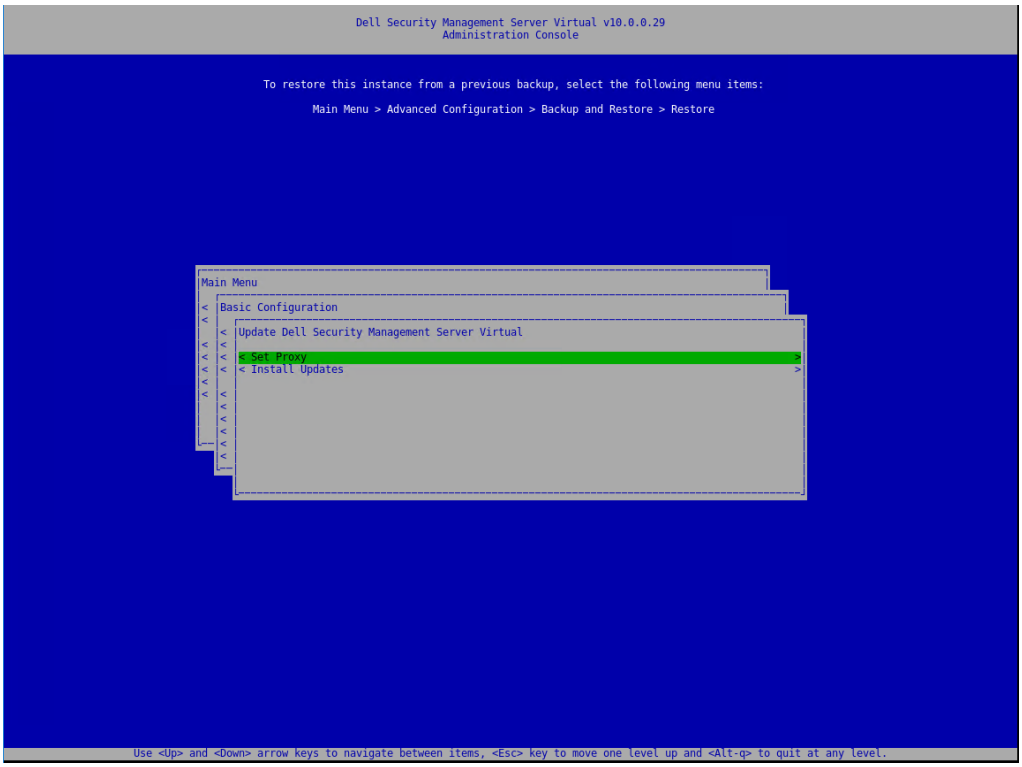
Pour recevoir des notifications par e-mail lorsque des mises à jour du Dell Server sont disponibles, voir Configurer les paramètres SMTP.

Si des modifications de règle ont été apportées mais non validées dans la console de gestion, appliquez ces modifications de règle avant la mise à jour du Dell Server :

1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le menu de gauche, cliquez sur **Gestion** > **Valider**.
3. Entrez la description de la modification dans le champ Commentaire.
4. Cliquez sur **Valider les règles**.
5. Une fois la validation effectuée, déconnectez-vous de la console de gestion.

Mettre à jour Security Management Server Virtual (mode Connecté)

1. Dell vous recommande d'effectuer une sauvegarde régulière. Avant la mise à jour, assurez-vous que le processus de sauvegarde fonctionne correctement. Consultez Sauvegarde et restauration.
2. Dans le menu **Configuration de base**, sélectionnez l'option de **mise à jour de Dell Security Management Server Virtual**.



REMARQUE : Le numéro de version peut être différent de celui sur la capture d'écran fournie.

3. Sélectionnez l'action souhaitée :
   - Définir les paramètres Proxy : sélectionnez cette option pour définir les paramètres Proxy de téléchargement des mises à jour.

     Dans l'écran *Configurer les paramètres Proxy*, appuyez sur la barre d'espacement pour saisir un **X** dans le champ *Utiliser Proxy*. Sélectionnez HTTPS et HTTP. Si une authentification pare-feu est requise, appuyez sur la barre d'espacement pour saisir un **X** dans le champ Authentification requise. Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur **OK**.

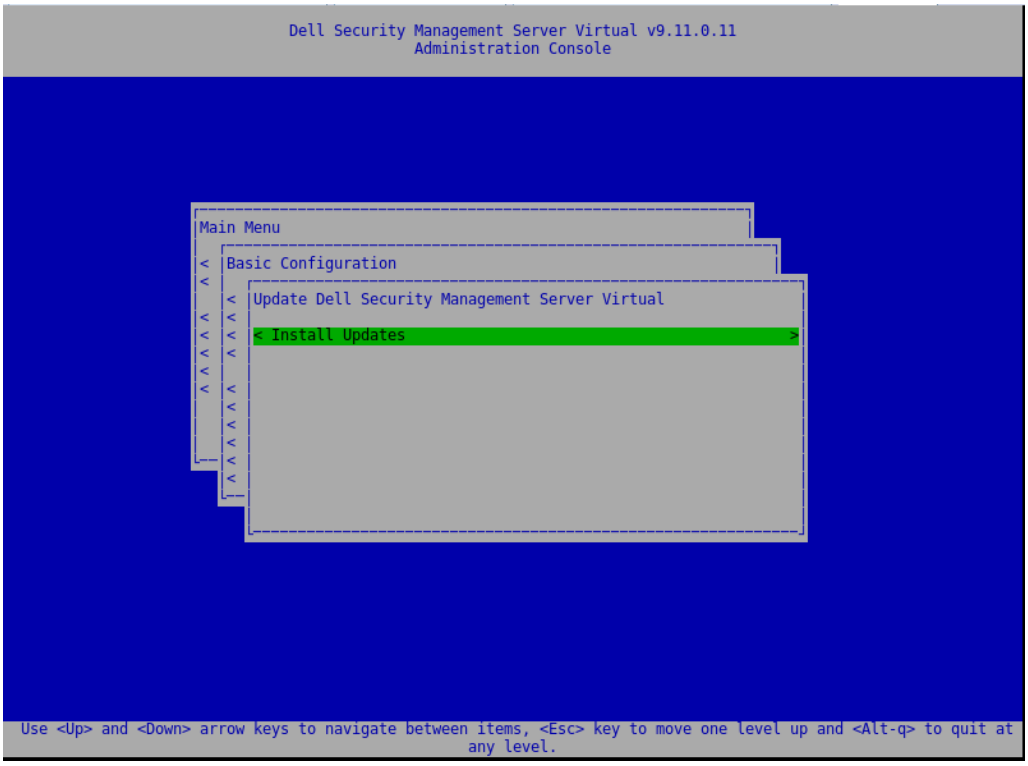
REMARQUE : L'option Définir les paramètres Proxy met désormais à jour les paramètres Proxy de diverses applications basées sur Java pour extraire les licences « intégrées », ainsi que la communication vers Endpoint Security Suite Enterprise SaaS et l'infrastructure back-end Dell/Credant.

- Lorsque vous sélectionnez **Installer les mises à jour**, Security Management Server Virtual interroge les logithèques Ubuntu intégrées par défaut ainsi que dist.ddspproduction.com, la logithèque personnalisée Dell qui contient les mises à jour de l'application.

  REMARQUE : Dell recherche toutes les mises à jour Ubuntu dans la logithèque dist.ddspproduction.com par le biais des ports 443 et 80. Toutes les mises à jour disponibles sont téléchargées. Les paramètres de proxy définis dans Définir le proxy sont utilisés pour les connexions aux ports 443 et 80 pour le téléchargement.

Mettre à jour Security Management Server Virtual (mode Déconnecté)

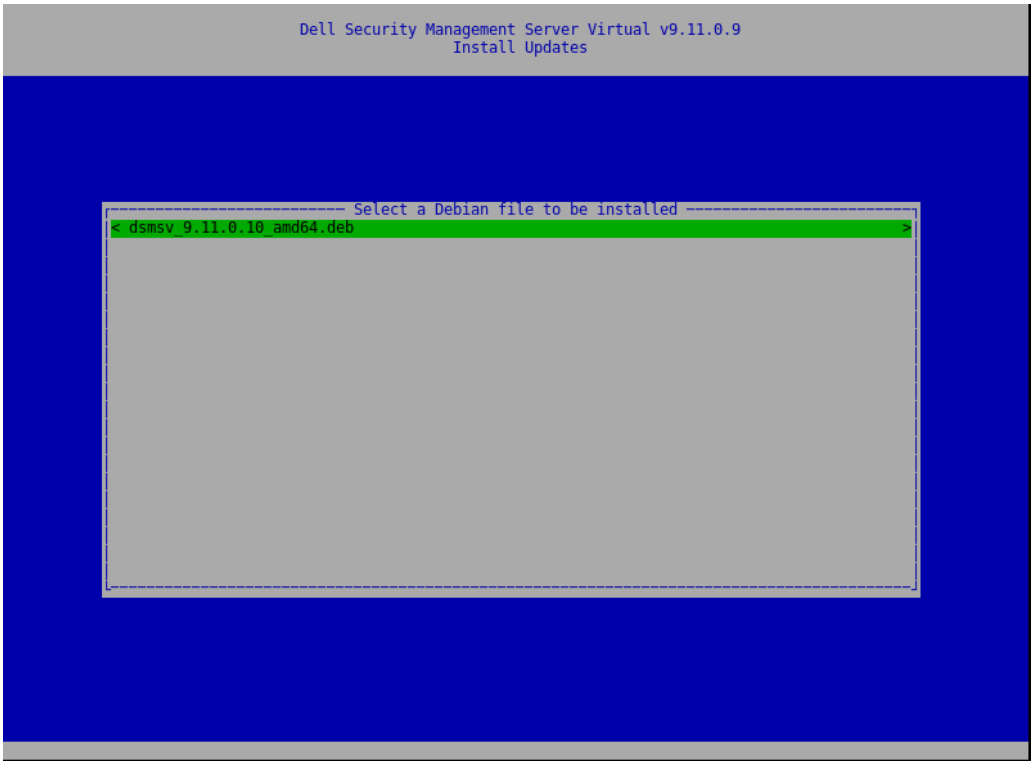
1. Dell vous recommande d'effectuer une sauvegarde régulière. Avant la mise à jour, assurez-vous que le processus de sauvegarde fonctionne correctement. Consultez Sauvegarde et restauration.
2. Procurez-vous le fichier .deb qui contient la dernière mise à jour pour Dell Server à partir de Dell ProSupport.
3. Stockez le fichier .deb dans le dossier /var/opt/dell/dsmsv/ftp/files/updates sur le serveur FTP sécurisé du Dell Server.
   Assurez-vous que le client FTP prend en charge SFTP sur le port 22 et qu'un utilisateur FTP est configuré. Consultez Définir les utilisateurs FTP (Transfert de fichiers).
4. Dans le menu **Configuration de base**, sélectionnez **Mettre à jour Security Management Server Virtual**.
5. Sélectionnez **Installer les mises à jour** et appuyez sur **Entrée**.



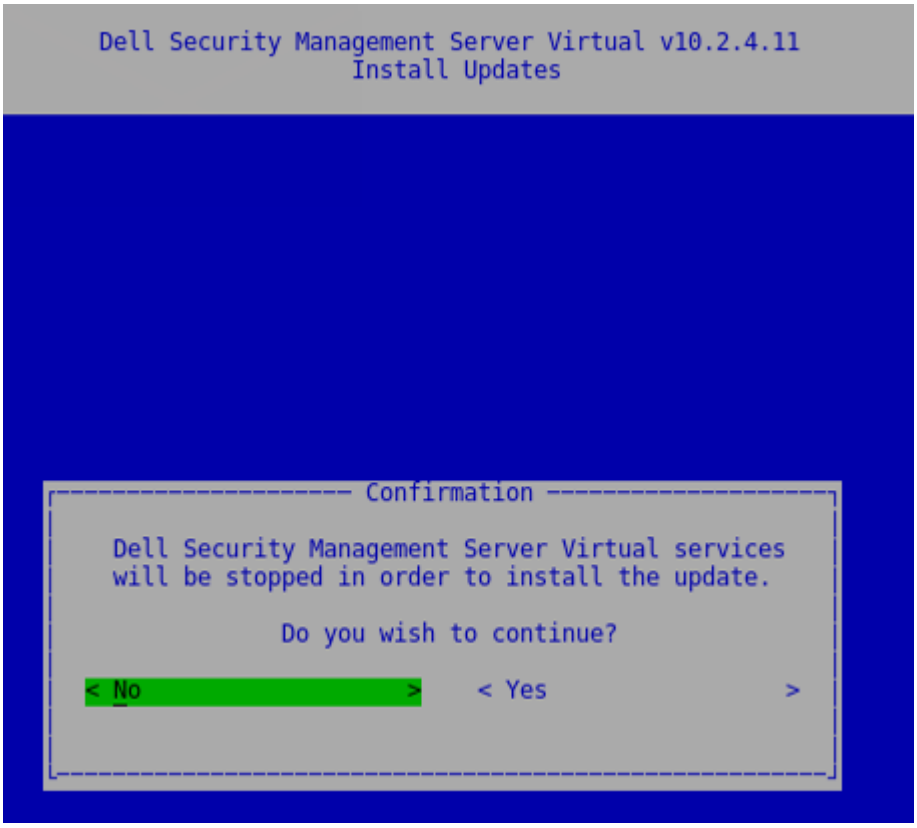
REMARQUE : Le numéro de version peut être différent de celui sur la capture d'écran fournie.

Si le fichier .deb ne s'affiche pas, assurez-vous que le fichier .deb est stocké au bon emplacement.

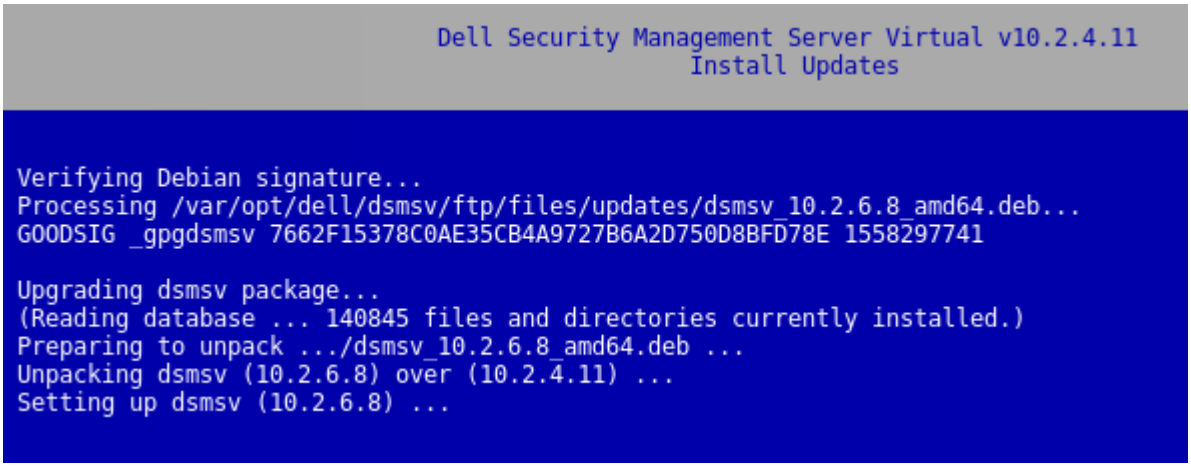
6. Sélectionnez le fichier de mise à jour .deb que vous souhaitez installer et appuyez sur **Entrée**.



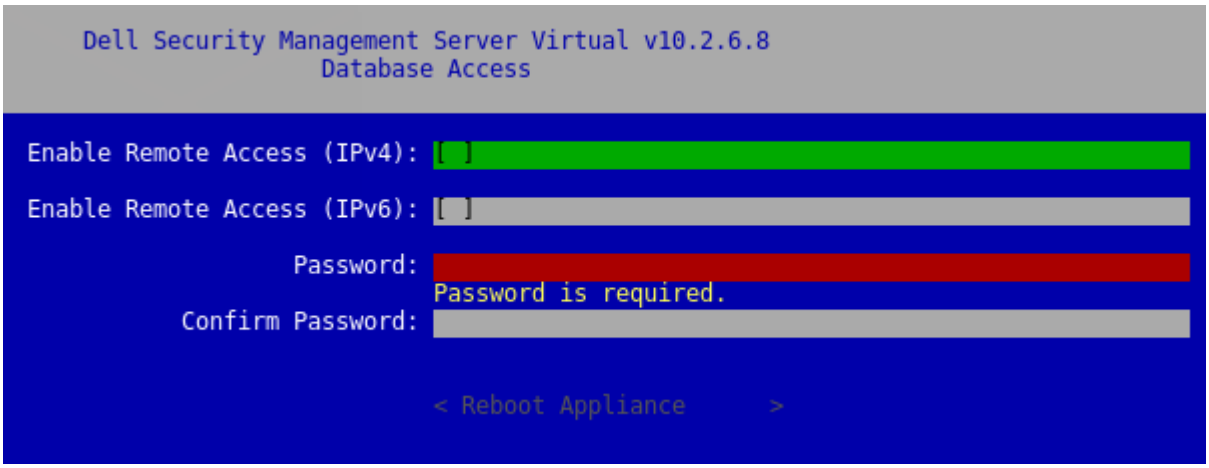
7. Sélectionnez **Oui** pour arrêter les services de Security Management Server Virtual.



8. Le package Debian est vérifié et mis à niveau.



9. Une fois la mise à jour effectuée, modifiez le mot de passe de la base de données.



REMARQUE : Le numéro de version peut être différent de celui sur la capture d'écran fournie.

Modifier les mots de passe utilisateur

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser Security Management Server Virtual.

Vous pouvez modifier les mots de passe pour ces utilisateurs :

- delluser (administrateur du terminal) : cet utilisateur a accès au terminal Dell Server et ses menus.
- dellconsole (accès au shell) : cet utilisateur a accès au shell de Dell Server. L'accès au shell permet à un administrateur réseau de vérifier et dépanner la connectivité réseau.
- dellsupport (administrateur Dell ProSupport) : cet utilisateur dispose des droits « sudo » et doit être utilisé avec modération. Pour des raisons de sécurité, vous contrôlez le mot de passe de ce compte.

1. Dans le menu *Configuration de base*, sélectionnez **Modifier les mots de passe utilisateur**.
2. Dans l'écran *Modifier les mots de passe utilisateur*, sélectionnez le mot de passe utilisateur à modifier, puis sélectionnez **Entrée**.
3. Dans l'écran *Définir le mot de passe*, entrez le mot de passe actuel, saisissez le nouveau mot de passe, saisissez-le une deuxième fois, puis cliquez sur **OK**.

   Les mots de passe doivent comprendre les éléments suivants :

   - Au moins 8 caractères
   - Au moins une lettre majuscule
   - Au moins 1 chiffre
   - Au moins un caractère spécial

   REMARQUE :

Si vous souhaitez sélectionner plusieurs comptes d'utilisateur, utilisez la touche Espace du clavier pour afficher la liste de sélection.

Configurer des utilisateurs SFTP (Secure File Transfer)

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser Security Management Server Virtual.

1. Dans le menu *Configuration de base*, sélectionnez **SFTP**.
2. Dans l'écran *SFTP*, pour ajouter un utilisateur SFTP et définir un mot de passe, appuyez sur la touche **Entrée** ou la touche de direction bas dans le champ *État* de l'utilisateur. Appuyez sur la barre d'espacement pour afficher des options qui permettent de mettre à jour ou de supprimer un utilisateur existant. Pour désactiver un utilisateur SFTP, sélectionnez **Supprimer** après avoir sélectionné l'utilisateur, puis sélectionnez **Oui** dans l'écran de confirmation SFTP.
3. Saisissez un nom d'utilisateur et le mot de passe de l'utilisateur SFTP.

   Les mots de passe doivent comprendre les éléments suivants :

   - Au moins 8 caractères
   - Au moins une lettre majuscule
   - Au moins 1 chiffre
   - Au moins un caractère spécial
4. Lorsque vous avez terminé de saisir les utilisateurs SFTP, sélectionnez **Appliquer**.

Activer SSH

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser Security Management Server Virtual.

Vous pouvez activer SSH pour la connexion de l'administrateur de support, l'accès shell et l'interface de ligne de commande du terminal.

1. Dans le menu *Configuration de base*, sélectionnez **SSH**.
2. Mettez en surbrillance l'utilisateur pour lequel vous souhaitez activer SSH, appuyez sur la barre d'espacement pour saisir un **X**, puis cliquez sur **OK**.

Démarrer ou arrêter les services

N'effectuez cette tâche qu'en cas de nécessité.

1. Pour démarrer ou arrêter simultanément tous les services, dans le menu *Configuration de base*, sélectionnez **Démarrer l'application** ou **Arrêter l'application**.
2. Dans l'invite de commande, cliquez sur **Oui**.

   REMARQUE :

   Les modifications de l'état du serveur peuvent prendre jusqu'à deux minutes.

Redémarrer l'appliance

N'effectuez cette tâche qu'en cas de nécessité.

1. Dans le menu *Configuration de base*, sélectionnez **Redémarrer l'appliance**.
2. Dans l'invite de commande, cliquez sur **Oui**.
3. Après le redémarrage, connectez-vous au serveur Security Management Server Virtual.

Arrêter l’appliance

N'effectuez cette tâche qu'en cas de nécessité.

1. Depuis le menu *Configuration de base*, faites défiler la page vers le bas et sélectionnez **Arrêter l'appliance**.
2. Dans l'invite de commande, cliquez sur **Oui**.
3. Après le redémarrage, connectez-vous au serveur Security Management Server Virtual.

Tâches de configuration avancée du terminal

Les tâches de configuration avancée sont accessibles à partir du menu principal.

Configurer la rotation de rapport

REMARQUE : Les instructions ci-dessous définissent la rotation du journal des applications sur Dell Security Management Server Virtual prenant en charge la rotation de journal.

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser Security Management Server Virtual.

Par défaut, la rotation de rapport quotidienne est sélectionnée. Pour modifier la rotation par défaut des rapports, depuis le menu *Configuration avancée*, sélectionnez **Configuration Logrotate**.

Pour désactiver la rotation des rapports, utilisez la barre d'espacement pour saisir un **X** dans le champ *Aucune rotation*, puis cliquez sur **OK**.

Pour activer la rotation de rapport, suivez ces étapes :

1. Pour activer la rotation quotidienne, hebdomadaire ou mensuelle, utilisez la barre d'espacement pour saisir un **X** dans le champ approprié. Pour la rotation hebdomadaire, utilisez le menu déroulant pour sélectionner le jour de la semaine souhaité. Pour la rotation mensuelle, saisissez le jour du mois souhaité.
2. Saisissez une heure de rotation dans le champ *Heure de la rotation de rapport*.
3. Sélectionnez **OK**.

Enregistrer et restaurer

Les sauvegardes peuvent être configurées ou effectuées à tout moment. Elles ne sont pas nécessaires pour commencer à utiliser Security Management Server Virtual. Dell vous recommande de configurer un processus de sauvegarde régulière. Pour en savoir plus, voir http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

En cas de stockage sur le Dell Server, lorsque le disque fonctionne à 90 % de sa capacité, aucune nouvelle sauvegarde ne sera stockée. Si vous avez configuré les notifications par e-mail, vous recevrez une notification par e-mail vous indiquant que l'espace disque est faible.

REMARQUE :

Pour conserver l'espace partition de disque et prévenir la suppression automatique des sauvegardes, supprimez les sauvegardes inutiles stockées.

Les sauvegardes sont exécutées quotidiennement, par défaut. La société Dell vous recommande de stocker vos sauvegardes sur un serveur FTP externe sécurisé à une fréquence qui répond aux exigences de l'entreprise en ce qui concerne les sauvegardes et l'utilisation appropriée de l'espace de stockage.

Pour configurer un programme de sauvegarde, ouvrez le menu Configuration avancée, sélectionnez *Sauvegarde et restauration > Configuration*, puis appliquez les étapes suivantes :

1. Pour activer la sauvegarde quotidienne, hebdomadaire ou mensuelle, utilisez la barre d'espacement pour saisir un **X** dans le champ approprié. Pour les sauvegardes hebdomadaires ou mensuelles, saisissez le jour de la semaine ou du mois approprié sous forme de chiffre, où Lundi=1. Pour désactiver les sauvegardes, utilisez la barre d'espacement pour saisir un **X** dans le champ *Aucune sauvegarde* et sélectionnez **OK**.
2. Saisissez une heure de sauvegarde dans le champ *Heure de la sauvegarde*.
3. Sélectionnez **OK**.

Pour effectuer une sauvegarde immédiate, depuis le menu *Configuration avancée*, sélectionnez **Sauvegarde et restauration > Sauvegarder maintenant**. Lorsque la confirmation de la sauvegarde s'affiche, sélectionnez **OK**.

REMARQUE :

Avant le lancement d'une opération de restauration, tous les services du Dell Server doivent être en cours d'exécution. Vérifier l'état du serveur. Si tous les services ne sont pas en cours d'exécution, redémarrez-les. Pour plus d'informations, reportez-vous à Démarrer ou arrêter les services. Commencez à restaurer ***uniquement*** lorsque ***tous*** les services sont en cours d'exécution.

Pour effectuer une restauration à partir du menu *Configuration avancée*, sélectionnez **Sauvegarde et restauration > Restauration**, puis sélectionnez le fichier de sauvegarde à restaurer. Dans l'écran de confirmation, sélectionnez **Oui**.

La sauvegarde est restaurée après le redémarrage.

Stockez les sauvegardes sur un serveur FTP sécurisé

Pour stocker des sauvegardes sur un serveur FTP, le client FTP doit prendre en charge SFTP sur le port 22.

Selon des exigences de sauvegarde de l'entreprise, les sauvegardes doivent se télécharger de la manière suivante :

- Manuellement
- au moyen d'un script automatisé
- au moyen d'une solution de sauvegarde autorisée par l'entreprise

Pour télécharger des sauvegardes au moyen de la solution de sauvegarde de l'entreprise, procurez-vous des instructions détaillées de votre fournisseur de solution de sauvegarde.

REMARQUE :

Le Dell Server se base sur Linux Debian Ubuntu x64.

Connectez-vous au Dell Server en tant que dellsupport et utilisez la commande **sudo** pour configurer votre solution de sauvegarde :

sudo <instructions du vendeur de solution de sauvegarde>

Contenu de sauvegarde des dossiers suivants :

/backup (requis)

/certificates (fortement recommandé)

/support (facultatif)

À la fin du processus sudo, saisissez **Quitter** et appuyez sur **Saisir** jusqu'à l'affichage de l'invite de connexion.

Configurer les paramètres SMTP

Pour recevoir des notifications par e-mail, suivez les étapes de cette section pour configurer les paramètres SMTP. Les notifications par e-mail informent les destinataires des états d'erreur du Dell Server, des mises à jour de mots de passe, de la disponibilité des mises à jour du Dell Server et des problèmes de licence des clients.

Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

Pour configurer les paramètres SMTP, suivez ces étapes :

1. Dans le menu *Configuration avancée*, sélectionnez **Notifications par e-mail**.
2. Dans l'écran Notifications par e-mail, pour activer les alertes par e-mail, appuyez sur la barre d'espacement afin de saisir un **X** dans le champ *Activer les alertes par e-mail*.
3. Saisissez le nom de domaine complet du serveur SMTP.
4. Saisissez le port SMTP.
5. Saisissez l'utilisateur SMTP.
6. Saisissez le mot de passe SMTP.
7. Dans le champ *Expéditeur des notifications*, saisissez l'identifiant du compte e-mail qui enverra les notifications par e-mail.
8. Dans le champ *Destinataire des notifications d'état du serveur*, saisissez l'identifiant du compte e-mail auquel envoyer les notifications d'état du serveur. Les destinataires sont séparés par des virgules ou des points-virgules.
9. Dans le champ *Destinataire des changements de mot de passe*, saisissez l'identifiant du compte e-mail auquel envoyer les notifications de changements de mot de passe.

10. Dans le champ *Destinataire des mises à jour logicielles*, saisissez l'identifiant du compte e-mail auquel envoyer les notifications de mises à jour logicielles.
11. Dans le champ *Rappel d'alerte de service*, pour activer les rappels, appuyez sur la barre d'espacement pour saisir un **X** dans le champ, puis définissez l'intervalle entre les rappels en minutes. Un rappel d'alerte de service est déclenché lorsque l'intervalle est dépassé, malgré l'envoi d'une notification concernant un problème d'intégrité du système ou bien lorsque l'état du service n'est pas modifié.
12. Dans le champ *Rapport récapitulatif*, pour activer le rapport des notifications, sélectionnez l'intervalle souhaité (Quotidien, Hebdomadaire ou Mensuel), puis appuyez sur la barre d'espacement pour saisir un **X**.
13. Sélectionnez **OK**.

Importer un certificat existant ou inscrire un nouveau certificat de serveur

Vous pouvez importer un certificat existant ou créer une requête de certificat par l'intermédiaire de Security Management Server Virtual .

Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

Importation d'un certificat de serveur existant

1. Exportez le certificat existant et sa chaîne d'approbation complète à partir de son magasin de clés.

   REMARQUE : Conservez le mot de passe d'exportation car vous en aurez besoin lorsque vous importerez le certificat dans Security Management Server Virtual .
2. Sur le serveur FTP du Dell Server, stockez le certificat dans **/certificates**.
3. Dans le menu *Configuration avancée*, sélectionnez **Notifications par e-mail**.
4. Sélectionnez l'option **Importer un certificat existant**.
5. Sélectionnez un fichier de certificat à installer sur le Dell Server .
6. Lorsque vous y êtes invité, saisissez le mot de passe d'exportation du certificat, puis sélectionnez **OK**.
7. Une fois l'importation terminée, sélectionnez **OK**.

   REMARQUE : Pour plus d'informations, voir http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en

Enregistrer un nouveau certificat de serveur

1. Dans le menu *Configuration avancée*, sélectionnez **Notifications par e-mail**.
2. Sélectionnez **Nouveau certificat de serveur**.
3. Sélectionnez **Créer une requête de certificat**.
4. Remplissez les champs de l'écran *Générer une requête de certificat* comme suit :
   - Nom du pays : code de pays à deux lettres.
   - *État/province* : entrez le nom non abrégé de l'État ou de la province (par exemple, Texas).
   - *Nom de la localité/ville.* Entrez la valeur appropriée (exemple, Dallas).
   - *Organisation* : entrez la valeur appropriée (exemple, Dell).
   - *Unité organisationnelle* : entrez la valeur appropriée (exemple, Sécurité).
   - *Nom commun* : saisissez le nom de domaine complètement qualifié du Dell Server . Ce nom complet comprend le nom d'hôte et le nom de domaine (par exemple, serveur.domaine.com).
   - *ID d'e-mail* : entrez l'adresse e-mail à laquelle votre requête de signature de certificat (CSR) doit être envoyée.
5. Suivez votre processus organisationnel pour l'acquisition d'un certificat de serveur SSL auprès d'une autorité de certification. Envoyez le contenu du fichier CSR pour signature.
6. Lorsque vous recevez le certificat signé, exportez le certificat sous forme de fichier .p7b et téléchargez la chaîne d'approbation complète au format .der.
7. Faites des copies de sauvegarde du certificat et de la chaîne d'approbation.
8. Chargez le fichier de certificat et sa chaîne d'approbation complète sur le serveur FTP du Dell Server .

9. Dans le menu *Configuration avancée*, sélectionnez **Notifications par e-mail**.
10. Sélectionnez **Nouveau certificat de serveur**.
11. Sélectionnez **`Terminer l'inscription du certificat`**.
12. Sélectionnez le fichier de certificat à installer sur le Dell Server .
13. Si vous y êtes invité, entrez le mot de passe de certificat : **changeit**.

Pour activer la validation d'approbation sur les clients Encryption Windows, voir Activer la vérification de la chaîne d'approbation du gestionnaire.

Créez et installez un certificat auto-signé

REMARQUE : Les certificats auto-signés générés par défaut le sont pour 10 ans.

1. Dans le menu de configuration avancée Dell Server *Advanced Configuration*, sélectionnez **Certificats de serveur**.
2. Sélectionnez **Créez et installez un certificat auto-signé.**
3. Pour confirmer que vous souhaitez remplacer le certificat pré-installé par un nouveau certificat, cliquez sur **Yes**.
4. Entrez le mot de passe du certificat : **changeit**.
5. Une fois le nouveau certificat est installé, sélectionnez **OK** et attendez que les services redémarrent.

Les services redémarrent automatiquement.

Activation de l'accès à la base de données

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser Security Management Server Virtual.

REMARQUE : Dell vous recommande d'activer l'accès à la base de données uniquement si cela est nécessaire et de le désactiver lorsque vous n'en avez plus besoin.

1. Dans le menu *Configuration avancée*, sélectionnez **Accès à la base de données**.
2. Utilisez la barre d'espacement pour entrer un **X** dans le champ *Activer l'accès à la base de données*, puis sélectionnez **OK**. Si le mot de passe de la base de données n'a pas encore été configuré, une invite de saisie du mot de passe s'affiche.
3. Saisissez le mot de passe de la base de données.
4. Saisissez de nouveau le mot de passe de la base de données.

   Les composants de l'application Dell Data Security s'arrêtent automatiquement.

Définir ou modifier la langue du terminal

Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

1. Dans le menu principal, sélectionnez **Définir la langue**.
2. Utilisez les touches fléchées pour sélectionner la langue voulue.

Afficher les journaux

Pour consulter les journaux suivants, dans le menu principal, sélectionnez **Afficher les journaux**.

- Rapports système
  - Rapport Syslog
  - Rapport e-mail
  - Rapport auth. (SSH)
  - Rapport PostgreSQL
  - Rapport de surveillance
- Rapports de serveur

- Courtier de messages
- Serveur d'identité
- Compatibility Server
- Security Server
- Core Server
- Core Server HA
- Serveur d'inventaire
- Forensic Server
- Policy Proxy (Proxy de stratégie)

- Console Administration
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Rapport de personnalisation de la base de données

REMARQUE : Pour parcourir cet écran, procédez comme suit :

- Pour accéder à la fin du journal, vous pouvez maintenir la touche Alt de droite enfoncée, puis appuyer sur la touche « / » du clavier
- Pour quitter le journal, maintenez la touche Ctrl de gauche enfoncée et appuyez sur « x » sur le clavier.
- Touches fléchées pour la navigation.
- Page précédente et page suivante pour passer à la page précédente ou suivante.
- Barre d'espacement pour parcourir les journaux page par page.

Ouverture de l'interface de ligne de commande

Pour ouvrir l'interface de ligne de commande, ouvrez le menu principal, puis sélectionnez **Lancer Shell**.

Pour quitter l'interface de ligne de commande, saisissez **quitter** et appuyez sur **Entrée**.

Générer le journal des instantanés du système

Pour générer un journal des instantanés du système pour Dell Pro Support, ouvrez le menu principal et sélectionnez **Outils de support**.

1. Dans le menu Outils de support, sélectionnez *Générer le journal des instantanés du système*.
2. Lorsque le système signale que le fichier a été créé, sélectionnez **OK**.

3

Entretien de

Supprimez les sauvegardes inutiles de Security Management Server Virtual .

Seules les dix sauvegardes les plus récentes sont conservées. Si l'espace disponible sur les partitions de disque est de 10 % ou moins, aucune nouvelle sauvegarde ne sera enregistrée. Si cela se produit, vous recevrez une notification par e-mail vous indiquant que l'espace disque est faible.

4

Résolution des problèmes

Si une erreur se produit et que vous avez configuré les notifications par e-mail, vous recevrez une notification par e-mail. En fonction des informations fournies dans cette notification par e-mail, suivez ces étapes :

1. Vérifiez les rapports concernés.
2. Redémarrez les services, le cas échéant. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.
3. Générer un journal des instantanés du système.
4. Contacter Dell ProSupport Pour plus d'informations, reportez-vous à contacter Dell ProSupport.

5

Configuration postérieure à l'installation

Après l'installation, certains composants de votre environnement peuvent avoir besoin d'être configurés, selon la solution Dell Data Security utilisée par votre entreprise.

Après avoir installé Security Management Server Virtual, les paramètres par défaut suivants doivent être modifiés :

- Modifiez le mot de passe du serveur principal à l'emplacement suivant :

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- Modifiez le mot de passe de chaque serveur frontal dans votre environnement à l'emplacement suivant :

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

Le mot de passe s'affiche comme suit : `proxy-server.password=ENC(<texthere>)`

Pour modifier le mot de passe :

1. Sélectionnez : `ENC(<texthere>)`
2. Remplacez le texte sélectionné par : `CLR(<newpasswordhere>)`

   Après le redémarrage du service, la ligne modifiée passe de `ENC` à `CLR` et le mot de passe est chiffré.

Remarque : proxy-server.username peut également être modifié, mais cette modification doit avoir une correspondance dans le fichier application.properties du courtier de messages et tous les serveurs frontaux actifs.

Validation de la vérification de la chaîne d'approbation du gestionnaire

Si un certificat auto-signé est utilisé sur Security Management Server Virtual pour SED ou le gestionnaire BitLocker, la validation d'approbation SSL/TLS doit être ***désactivée*** sur l'ordinateur client. Les conditions suivantes doivent être remplies avant l'activation de la validation d'approbation SSL/TLS sur l'ordinateur client :

- Un certificat signé par une autorité racine (par ex. Entrust ou Verisign), doit être importé dans le Dell Server. Voir Importer un certificat existant ou inscrire un nouveau certificat de serveur.
- La chaîne d'approbation complète du certificat doit être stockée dans le magasin de clés Microsoft de l'ordinateur client.

Pour désactiver la validation d'approbation SSL/TLS, modifiez la valeur d'entrée de registre suivante sur 1 sur l'ordinateur client :

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

Propriétés du délai d'expiration pour la console de gestion

Pour modifier la propriété du délai d'expiration de la console de gestion, accédez au fichier application.properties et modifiez les valeurs par défaut :

- `idle.warn.seconds=1080`
- `idle.timeout.seconds=1200`

6

Tâches d'administrateur de la console de gestion

Assigner le rôle d'administrateur Dell

1. En tant qu'administrateur de Security Management Server, connectez-vous à la console de gestion à l'adresse suivante : https://server.domain.com:8443/webui/. Les informations d'identification par défaut sont **superadmin/changeit**.
2. Dans le volet de gauche, cliquez sur **Populations** > **Domaines**.
3. Cliquez sur un domaine auquel vous souhaitez ajouter un utilisateur.
4. Sur la page Détails du domaine, cliquez sur l'onglet **Membres**.
5. Cliquez sur **Ajouter un utilisateur**.
6. Entrez un filtre pour rechercher le nom d'utilisateur par Nom courant, Nom principal universel ou NomdeComptesAMA. Le caractère de remplacement est *.

   Un Nom courant, Nom principal universel et NomdeCompteSAM doivent être définis sur le serveur d'annuaire d'entreprise pour chaque utilisateur. Si un utilisateur est membre d'un domaine ou d'un groupe et qu'il ne s'affiche pas dans la liste des membres de ce domaine ou de ce groupe dans la gestion, assurez-vous que les trois noms sont correctement définis pour l'utilisateur sur le serveur d'annuaire d'entreprise.

   La requête effectuera automatiquement une recherche par nom courant, puis UPN, puis NomdeCompteSAM, jusqu'à ce qu'une correspondance soit trouvée.

7. Sélectionnez les membres de la *Liste des utilisateurs d'annuaire* à ajouter au domaine. Utilisez <Maj><clic> ou <Ctrl><clic> pour sélectionner plusieurs utilisateurs.
8. Cliquez sur **Ajouter**.
9. Depuis la barre de tâches, cliquez sur l'onglet **Détails et actions** de l'utilisateur spécifié.
10. Déplacez-vous dans la barre de tâches, puis sélectionnez l'onglet **Admin**.
11. Sélectionnez les rôles d'administrateur à assigner à cet utilisateur.
12. Cliquez sur **Enregistrer**.

Se connecter avec le rôle d'administrateur Dell

1. Déconnectez-vous de la Console de gestion.
2. Connectez-vous à la Console de gestion avec les informations d'identification d'utilisateur de domaine.

   Cliquez sur « ? » dans le coin supérieur droit de la Console de gestion pour démarrer l'*Aide administrateur*. La page *Mise en route* s'affiche. Cliquez sur **Ajouter des domaines**.

   Des règles de base ont été définies pour votre entreprise, mais elles doivent être modifiées comme suit en fonction de vos besoins spécifiques (toutes les activations sont soumises à des licences et à des droits) :

   - Policy Based Encryption est activé avec un chiffrement à clé commun
   - Les ordinateurs équipés de lecteurs à auto-cryptage seront cryptés
   - La gestion BitLocker n'est pas activée
   - Advanced Threat Prevention n'est pas activé.
   - La protection contre les menaces est désactivée
   - Les supports externes ne seront pas cryptés
   - Les ports ne sont pas gérés par le contrôle des ports
   - Les périphériques sur lesquels le cryptage complet du disque est installé ne sont pas cryptés

   Reportez-vous à la rubrique de l'Aide administrateur intitulée *Gestion des règles* pour obtenir une description des règles.

Valider des règles

Validez les règles lorsque l'installation est terminée.

Pour les valider après l'installation ou plus tard après la sauvegarde des modifications de règles, procédez comme suit :

1. Dans le volet de gauche, cliquez sur **Gestion** > **Valider**.
2. Dans le champ *Commentaire*, entrez une description de la modification.
3. Cliquez sur **Valider les règles**.

7

Ports

Le tableau suivant décrit chaque composant et sa fonction.

Nom	Port par défaut	Description
Access Group Service	TCP/ 8006	Gère diverses autorisations et accès de groupe pour divers produits de sécurité Dell. **REMARQUE :** Le port 8006 n'est pas sécurisé pour le moment. Assurez-vous que ce port est correctement filtré par le biais d'un pare-feu. Ce port est interne uniquement.
Console de gestion	HTTPS/ 8443	Console de gestion et centre de commande pour le déploiement à toute l'entreprise.
Core Server	HTTPS/ 8887 (fermé)	Gère le flux des stratégies, les licences et l'enregistrement de Preboot Authentication, SED Management, BitLocker Manager, Threat Protection et Advanced Threat Prevention. Traite les données d'inventaire pour l'utilisation par la Console de gestion. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles.
Core Server HA (Haute disponibilité)	HTTPS/ 8888	Un service à haute disponibilité qui permet la sécurité et les performances augmentées des connexions HTTPS avec la Console de gestion, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection et Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Communique avec Policy Proxy, gère les extractions de clé de détection, les activations de client et les communications SED-PBA et Full Disk Encryption-PBA.
Compatibility Server	TCP/ 1099 (fermé)	Service de gestion de l'architecture d'entreprise. Collecte et stocke les données d'inventaire initiales lors de l'activation et les données des stratégies lors des migrations. Traite les données en fonction des groupes d'utilisateurs.

Nom	Port par défaut	Description
		REMARQUE : Le port 1099 doit être filtré via un pare-feu. Dell recommande que ce port soit uniquement interne.
Service Courtier de messages	TCP/ 61616 (fermé) et STOMP/ 61613 (fermé ou, si configuré pour DMZ, port 61613 ouvert)	Gère les communications entre les services du Dell Server. Organise les informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des règles. **REMARQUE :** Le port 61616 doit être filtré via un pare-feu. Dell recommande que ce port soit uniquement interne. **REMARQUE :** Le port 61613 doit être uniquement accessible via les serveurs de gestion de sécurité configurés en mode front-end.
Serveur d'identité	8445 (fermé)	Gère les demandes d'authentification de serveur pour l'authentification de SED Management.
Forensic Server	HTTPS/ 8448	Permet aux administrateurs dotés des privilèges appropriés d'obtenir des clés de chiffrement de la Console de gestion pour l'utilisation dans les déverrouillages de données ou les tâches de déchiffrement. Requis pour l'API Forensic.
Serveur d'inventaire	8887	Traite la file d'attente de l'inventaire.
Policy Proxy (Proxy de stratégie)	TCP/ 8000	Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité. Requis pour Encryption Enterprise (Windows et Mac)
PostGres	TCP/ 5432	Base de données locale utilisée pour les données d'événement. **REMARQUE :** Le port 5432 doit être filtré via un pare-feu. Dell recommande que ce port soit uniquement interne.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Port 389 : ce port est utilisé pour la demande d'informations auprès du contrôleur de domaine local. Les requêtes LDAP envoyées au port 389 peuvent être utilisées pour la recherche d'objets uniquement à l'intérieur du domaine d'accueil du catalogue global. Cependant, l'application de requête peut obtenir tous les attributs de ces

Nom	Port par défaut	Description
		objets. Par exemple, une requête au port 389 peut être utilisée pour obtenir un service utilisateur. Port 3268 : ce port est utilisé pour les requêtes ciblées spécifiquement sur le catalogue global. Les requêtes LDAP envoyées au port 3268 peuvent être utilisées pour la recherche d'objets dans l'ensemble de la forêt. Cependant, seuls les attributs marqués pour réplication sur le catalogue global peuvent être retournés. Par exemple, un service utilisateur n'a pas pu être retourné à l'aide du port 3268 dans la mesure où cet attribut n'est pas répliqué sur le catalogue global.
Authentification client	HTTPS/ 8449	Permet aux serveurs client de s'authentifier auprès du Dell Server. Requis pour Server Encryption.