Dell Security Management Server

Installation and Migration Guide v10.2.4

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

2019-05

Rev. A01

Contents

1

Introduction

À propos de Security Management Server

Security Management Server propose les fonctions suivantes :

- Gestion centralisée des périphériques, des utilisateurs et des règles de sécurité
- Audit et rapports de conformité centralisés
- Division des tâches administratives
- Création et gestion de règles de sécurité basées sur des rôles
- Application des règles de sécurité lors de la connexion de clients
- Récupération de périphérique assistée par l'administrateur
- Chemins d'accès approuvés pour la communication entre les composants
- Génération de clés de cryptage uniques et blocage automatique de clés sécurisées

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 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 service 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.

2

Configuration requise et architecture

Cette section présente en détail la configuration matérielle et logicielle requise et les recommandations de conception de l'architecture pour la mise en œuvre de Dell Security Management Server.

Conception de l'architecture de Security Management Server

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

Composants d'architecture

Les configurations matérielles suggérées ci-après conviennent à la plupart des environnements.

Security Management Server

- Système d'exploitation : Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter)
- Machine virtuelle/physique
- CPU : 4 cœurs
- RAM : 16,00 Go
- Disque C : 30 Go d'espace disque disponible pour les journaux et les bases de données d'applications

  REMARQUE : Jusqu'à 10 Go peuvent être consommés pour une base de données d'événements locale stockée dans PostgreSQL.

Serveur proxy

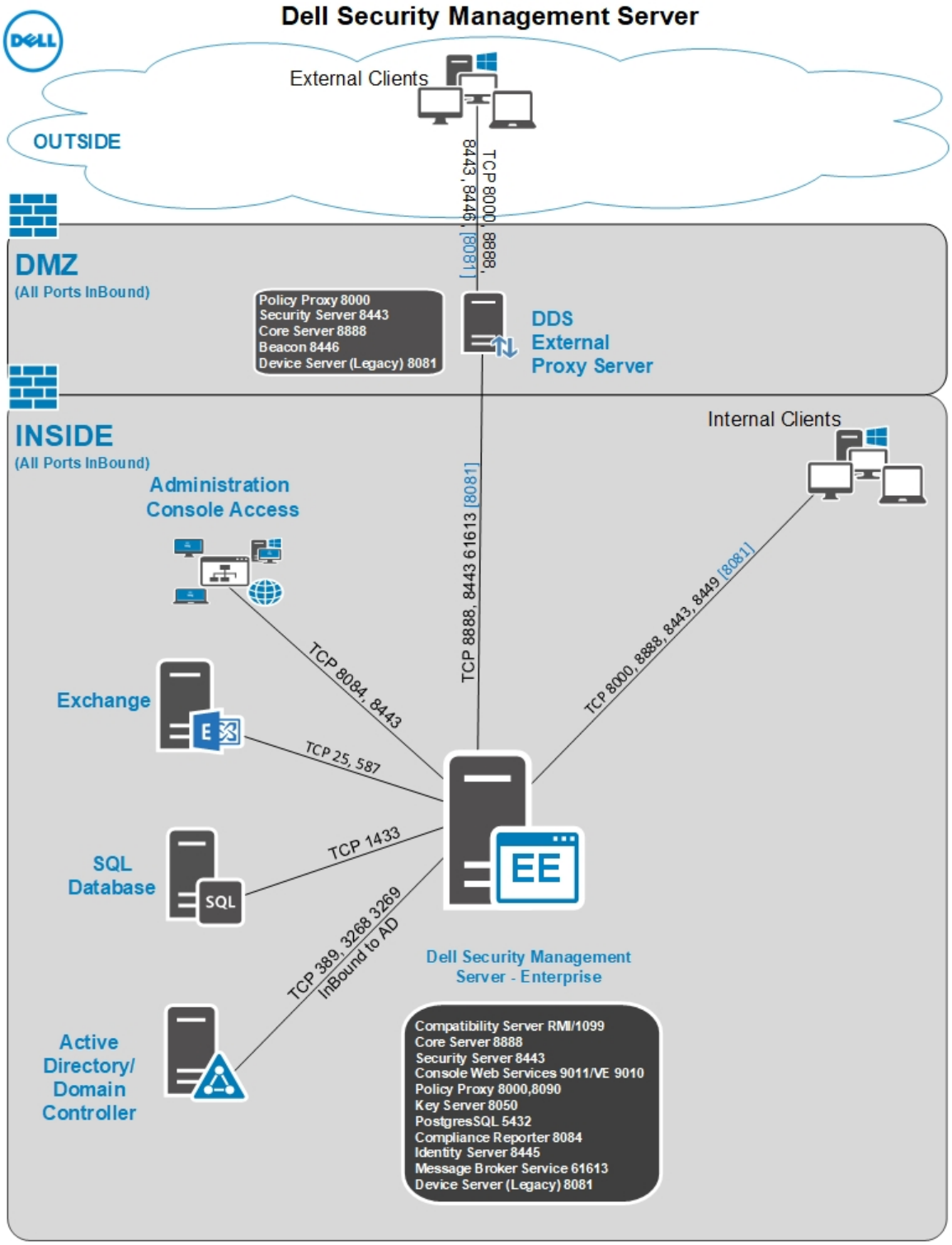
- Système d'exploitation : Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter)
- Machine virtuelle/physique
- CPU : 2 cœurs
- RAM : 8,00 Go
- Disque C : 20 Go d'espace disque disponible pour les journaux

Spécifications matérielles de SQL Server

- CPU : 4 cœurs
- RAM : 24,00 Go
- Lecteur de données : 100 à 150 Go d'espace disque disponible (cela peut varier en fonction de l'environnement)
- Lecteur de journaux : 50 Go d'espace disque disponible (cela peut varier en fonction de l'environnement)

  REMARQUE : Dell vous recommande de suivre Les meilleures pratiques relatives à SQL Server, bien que les informations ci-dessus doivent couvrir la majorité des environnements.

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



REMARQUE : Si l'entreprise compte plus de 20 000 points de terminaison, veuillez contacter Dell ProSupport pour obtenir une assistance.

Requirements

Les spécifications matérielles et logicielles pour l'installation du logiciel Security Management Server sont présentées ci-dessous.

Avant de commencer l'installation, assurez-vous que tous les correctifs et mises à jour sont appliqués aux serveurs utilisés pour l'installation.

Hardware

The following table details the *minimum* hardware requirements for Security Management Server see Security Management Server Architecture Design for additional information about scaling based on the size of your deployment.

Hardware Requirements
Processor
Modern Quad-Core CPU (1.5 GHz+)
RAM
16GB
Free Disk Space
20GB of free disk space
NOTE: Up to 10GB may be consumed for a local event database stored within PostgreSQL
Network Card
10/100/1000 or better
Miscellaneous
IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

The following table details the *minimum* hardware requirements for a Security Management Server Front - End / Proxy Server.

Hardware Requirements
Processor
Modern Dual-Core CPU
RAM
8GB
Free Disk Space
20GB of free disk space for log files
Network Card
10/100/1000 or better
Miscellaneous
IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

Virtualization

The Security Management Server can be installed in a virtual environment. Only the following environments are recommended.

Security Management Server v10.2.4 has been validated on the following platforms.

Hyper-V Server installed as a Full or Core installation or as a role in Windows Server 2012, Windows Server 2016, or Windows Server 2019.

- Hyper-V Server
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - Hardware must conform to minimum Hyper-V requirements
  - 4 GB minimum RAM for dedicated image resource
  - Must be run as a Generation 1 Virtual Machine
  - See https://technet.microsoft.com/en-us/library/hh923062.aspx for more information

Security Management Server v10.2.4 has been validated with VMware ESXi 5.5, VMware ESXi 6.0, and VMware ESXi 6.5.

NOTE: When running VMware ESXi and Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019, VMXNET3 Ethernet Adapters are recommended.

- VMware ESXi 5.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-55/index.jsp for more information
- VMware ESXi 6.0
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-60/index.jsp for more information
- VMware ESXi 6.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-65/index.jsp for more information

NOTE: The SQL Server database hosting the Security Management Server must be run on a separate computer for performance reasons.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run on a redundant system, such as a SQL Cluster, to ensure availability and data continuity. It is also recommended to perform daily full backups with transactional logging enabled to ensure that any newly generated keys through user/device activation are recoverable.

Database maintenance tasks should include rebuilding database indexes and collecting statistics.

Software

Le tableau ci-dessous répertorie la configuration logicielle requise pour Security Management Server et le serveur proxy.

REMARQUE : En raison de la nature critique des données présentes sur Security Management Server, et pour appliquer la règle du moindre privilège, Dell vous recommande d'installer Security Management Server sur son propre système d'exploitation dédié ou en tant qu'élément d'un serveur d'application associé à des rôles et privilèges limités pour s'assurer que l'environnement est sécurisé. Il ne faut donc pas installer Security Management Server sur des serveurs d'infrastructure disposant de privilèges. Voir https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models pour plus d'informations sur la mise en œuvre de la règle du moindre privilège.

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

REMARQUE : Emplacements dans le registre pour Policy Proxy (si installé) : HKLM\SOFTWARE\Wow6432Node\Dell

REMARQUE : Emplacement dans le registre pour les serveurs Windows : HKLM\SOFTWARE\Dell

Prérequis

- **Package redistribuable Visual C++ 2010**

  S'il n'est pas installé, le programme d'installation le fera pour vous.
- **Package redistribuable Visual C++ 2013**

  S'il n'est pas installé, le programme d'installation le fera pour vous.
- **Package redistribuable Visual C++ 2015**

  S'il n'est pas installé, le programme d'installation le fera pour vous.
- **.NET Framework version 3.5 SP1**
- **.NET Framework version 4.5**

  Microsoft a publié des mises à jour de sécurité pour .NET Framework version 4.5.
- **SQL Native Client 2012**

  Si vous utilisez SQL Server 2012 ou SQL Server 2016.

  S'il n'est pas installé, le programme d'installation le fera pour vous.

Security Management Server - Serveur principal et Serveur frontal Dell

- **Windows Server 2012 R2**

  - Édition Standard

  - Édition Datacenter
- **Windows Server 2016**

- Édition Standard

- Édition Datacenter

- **Windows Server 2019**

  - Édition Standard

  - Édition Datacenter

Référentiel LDAP

- Active Directory 2008 R2
- Active Directory 2012 R2
- Active Directory 2016

Console de gestion et Rapporteur de conformité

- Internet Explorer 11.x ou supérieur
- Mozilla Firefox 41.x ou supérieur
- Google Chrome 46.x ou version supérieure

REMARQUE : Votre navigateur doit accepter les cookies.

Environnements virtuels recommandés pour les composants de Security Management Server

Security Management Server peut être installé dans un environnement virtuel.

Dell prend actuellement en charge l'hébergement de Dell Security Management Server ou Dell Security Management Server Virtual au sein d'un environnement IaaS (Infrastructure en tant que service) hébergé dans le Cloud, tel qu'Amazon Web Services, Azure et d'autres fournisseurs. La prise en charge de ces environnements est limitée au fonctionnement de Security Management Server. L'administration et la sécurité de ces machines virtuelles sont assurées par l'administrateur de la solution IaaS.

Autres éléments de configuration requis pour l'infrastructure : pour assurer un fonctionnement correct, d'autres éléments (par exemple, Active Directory et SQL Server) sont toujours requis.

REMARQUE : La base de données SQL Server qui héberge Security Management Server doit être exécutée sur un ordinateur distinct.

Database

- **SQL Server 2008 R2 -** Standard Edition / Enterprise Edition
- **SQL Server 2012 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2014 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2016 -** Standard Edition / Enterprise Edition
- **SQL Server 2017 -** Standard Edition / Enterprise Edition

REMARQUE : Les versions Express Edition ne sont pas prises en charge pour les environnements de production. Leur utilisation doit uniquement se limiter à des fins de démonstration de faisabilité ou d'évaluation.

REMARQUE : Les conditions ci-dessous sont requises pour les autorisations SQL. L'utilisateur effectuant l'installation et fournissant les services doit disposer des droits d'administrateur local. En outre, les droits d'administrateur local sont requis pour le compte de service gérant les services de Dell Security Management Server.

Type	Action	Scénario	Privilège SQL requis
Back-end	Mise à niveau	De par leur nature, les mises à niveau possèdent déjà une base	db_owner

Type	Action	Scénario	Privilège SQL requis
		de données et une connexion/un utilisateur définis	
Back-end	Restauration de l'installation	La restauration implique une base de données et une connexion existantes.	db_owner
Back-end	Nouvelle installation	Utiliser la base de données existante	db_owner
Back-end	Nouvelle installation	Créer une base de données	dbcreator, db_owner
Back-end	Nouvelle installation	Utiliser une connexion existante	db_owner
Back-end	Nouvelle installation	Créer une connexion	securityadmin
Back-end	Désinstaller	S/O	S/O
Proxy frontal	N'importe lequel	S/O	S/O

REMARQUE : Si Contrôle de compte d'utilisateur (UAC) est activé, vous devez le désactiver avant l'installation sous Windows Server 2012 R2 lorsque l'installation a lieu dans C:\Program Files. Il faut redémarrer le serveur pour que cette modification prenne effet.

Au cours de l'installation, les identifiants d'authentification Windows ou SQL sont requis pour permettre la configuration de la base de données. Quel que soit le type d'identifiants utilisés, le compte doit disposer des privilèges appropriés pour l'action en cours d'exécution. Le tableau ci-dessus détaille les privilèges requis pour chaque type d'installation. De plus, le schéma par défaut du compte utilisé pour créer et configurer la base de données doit être défini sur dbo.

Ces privilèges sont uniquement requis lors de l'installation pour configurer la base de données. Une fois que Security Management Server est installé, le compte utilisé pour gérer l'accès à SQL peut être limité au propriétaire de la base de données et aux rôles publics.

Si vous n'êtes pas sûr des privilèges d'accès ou de la connectivité à la base de données, avant de lancer l'installation, demandez à votre administrateur de base de données de confirmer ces privilèges.

Support linguistique pour la Console de gestion

La Console de gestion est une interface utilisateur multilingue qui est conforme et qui prend en charge les langues suivantes :

Langues prises en charge	
EN : anglais	JA : japonais
ES : espagnol	KO : coréen
FR : français	PT-BR : portugais brésilien
IT : italien	PT-PT : portugais du Portugal (ibère)
DE : allemand	

3

Configuration préalable à l'installation

Avant de commencer, lisez les *Conseils techniques concernant Security Management Server* pour connaître les solutions palliatives ou problèmes connus relatifs à Security Management Server.

La configuration préalable à l'installation du ou des serveurs sur lesquels vous voulez installer Security Management Server est très importante. Lisez attentivement cette section pour installer correctement Security Management Server.

Configuration

1 Si elle est activée, désactivez la configuration de sécurité renforcée (ESC) d'Internet Explorer. Ajoutez l'URL de Dell Server aux sites de confiance dans les options de sécurité du navigateur. Redémarrez le serveur.

2 Ouvrez les ports suivants pour chaque composant :

Interne :

Communication Active Directory : TCP/389

Communication par courriel (facultatif) : 25

Vers le serveur frontal (si nécessaire) :

Communication entre Policy Proxy et courtier de messages : STOMP/61613

Communication avec le serveur back-end Security Server : HTTPS/8443

Communication avec le serveur back-end Core Server : HTTPS/8888

Communication avec les ports RMI - 1099

Communication avec le serveur back-end Device Server : HTTP(S)/8443 pour la version 7.7 ou ultérieure de Security Management Server HTTP(S)/8081 si vous utilisez un Serveur Dell antérieur à la version 7.7.

Serveur de balise : HTTP/8446 (Si vous utilisez Data Guardian)

Externe (si nécessaire) :

Base de données SQL : TCP/1433

Console de gestion : HTTPS/8443

LDAP : TCP/389/636 (contrôleur de domaine local), TCP/3268/3269 (catalogue global), TCP/135/49125+ (RPC)

Compatibility Server : TCP/1099

Rapporteur de conformité : HTTP(S)/8084 (configuré automatiquement à l'installation)

Identity Server : HTTPS/8445

Core Server : HTTPS/8888 (8888 est configuré automatiquement à l'installation)

Device Server : HTTP(S)/8443 (Security Management Server v7.7 ou version ultérieure) ou HTTP(S)/8081 (Serveur Dell antérieur à la version 7.7)

Key Server : TCP/8050

Policy Proxy : TCP/8000

Security Server : HTTPS/8443

Authentification client : HTTPS/8449 (si vous utilisez Server Encryption)

Communication du client, si vous utilisez Advanced Threat Prevention : HTTPS/TCP/443

Création d'une base de données Dell Server

3 Ces instructions sont facultatives. Le programme d'installation crée une base de données pour vous s'il n'en existe pas. Si vous préférez configurer une base de données avant d'installer Security Management Server, suivez les instructions ci-dessous pour créer la base de données SQL et l'utilisateur SQL dans SQL Management Studio.

Lorsque vous installez Security Management Server, suivez les instructions de la section Installation du serveur principal avec une base de données existante.

Security Management Server est préparé pour l'authentification SQL et Windows. La méthode d'authentification par défaut est l'authentification SQL.

Une fois que vous avez créé la base de données, créez un utilisateur de base de données Dell avec les droits db_owner. Le détenteur de droits db_owner peut attribuer des autorisations, sauvegarder et restaurer la base de données, créer et supprimer des objets, ou encore gérer les comptes utilisateurs et les rôles sans aucune restriction. En outre, veillez à ce que cet utilisateur dispose des autorisations / privilèges pour exécuter des procédures stockées.

Lorsque vous utilisez une instance de SQL Server autre que celle par défaut, après l'installation de Security Management Server, vous devez indiquer le port dynamique de l'instance sur l'onglet Base de données de l'outil de configuration de serveur. Pour en savoir plus, voir la section Outil de configuration de serveur. Vous pouvez également activer le service de navigateur SQL Server Browser et vous assurer que le port UDP 1434 est ouvert. Pour en savoir plus, consultez le document https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

Le classement attendu, autre que celui par défaut, pris en charge pour votre base de données SQL ou instance SQL est le classement « SQL_Latin1_General_CP1_CI_AS » .

Pour créer la base de données SQL et l'utilisateur SQL dans SQL Management Studio, choisissez une option :

Installation du package redistribuable Visual C++ 2010/2013/2015

4 *Si ce n'est pas déjà fait*, installez les packages redistribuables Visual C++ 2010, 2013, et 2015. Si vous le souhaitez, vous pouvez permettre au programme d'installation de Security Management Server d'installer ces composants.

Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 - https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads

Installation de .NET Framework 4.5

5 *Si ce n'est déjà fait*, installez .NET Framework 4.5.

Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 - https://www.microsoft.com/en-us/download/details.aspx?id=30653

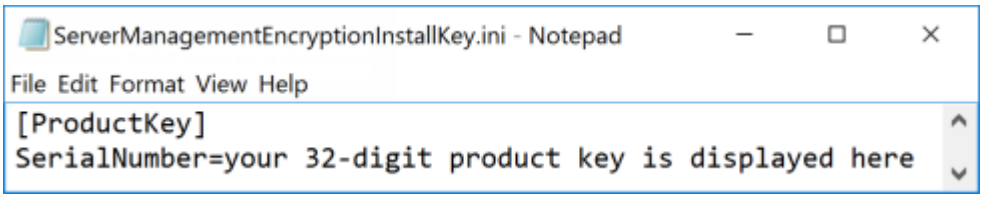
Installation de SQL Native Client 2012

6 *Si vous utilisez SQL Server 2012 ou SQL Server 2016)*, installez SQL Native Client 2012. Si vous le souhaitez, vous pouvez permettre au programme d'installation de Security Management Server d'installer ce composant.

http://www.microsoft.com/en-us/download/details.aspx?id=35580

Facultatif

7 **Pour une nouvelle installation** : copiez votre clé de produit (le nom du fichier est *EnterpriseServerInstallKey.ini*) vers **C:\Windows** pour renseigner automatiquement la clé de produit de 32 caractères dans le programme d'installation de Security Management Server.



La configuration préalable à l'installation du serveur est terminée. Passez à Installer ou mettre à niveau/Migrer.

4

Installer ou Mettre à niveau/Migrer

Ce chapitre fournit les instructions concernant :

- une nouvelle installation : pour installer un nouveau serveur Security Management Server.
- la mise à niveau et la migration : pour une mise à niveau à partir d'une version existante et fonctionnelle d'Enterprise Server v9.2 ou version ultérieure.
- la désinstallation de Security Management Server : pour supprimer l'installation actuelle, si nécessaire.

  Si votre installation doit comprendre plusieurs serveurs back-end, contactez votre représentant du service Dell ProSupport.

Avant de commencer l'installation ou la mise à niveau/migration

Avant de commencer, veillez à exécuter les étapes Configuration préalable à l'installation de configuration de préinstallation.

Lisez les *conseils techniques concernant Security Management Server* pour connaître les solutions palliatives ou les problèmes connus relatifs à l'installation de Security Management Server.

Pour raccourcir le temps d'installation sur Server 2016, ajoutez les exclusions suivantes à Windows Defender :

- C:\Program Files\Dell\Enterprise Edition
- C:\Windows\Installer
- Chemin de fichier depuis lequel le programme d'installation est exécuté

Dell recommande d'appliquer les meilleures pratiques pour les bases de données Dell Server et d'inclure le logiciel Dell dans le programme de reprise après sinistre de votre société.

Si vous prévoyez de déployer des composants Dell dans la zone DMZ, veillez à les protéger correctement contre les attaques.

Pour l'environnement de production, Dell recommande fortement d'installer SQL Server sur un serveur dédié.

La meilleure pratique consiste à installer le serveur back-end avant d'installer et de configurer tout serveur front-end.

Les fichiers journaux d'installation se trouvent dans ce répertoire : C:\Users\<UtilisateurConnecté>\AppData\Local\Temp

Nouvelle installation

Sélectionnez l'une des deux options d'installation du serveur back-end :

- Installer un serveur principal et une nouvelle base de données : permet d'installer un nouveau serveur Security Management Server et une nouvelle base de données.
- Installer un serveur principal avec une base de données existante : permet d'installer un nouveau serveur Security Management Server et de vous connecter à une base de données SQL créée au cours de la configuration préalable à l'installation, ou à une base de données SQL existante v9.x ou version ultérieure, lorsque la version de schéma correspond à celle du serveur Security Management Server à installer. Vous devez migrer une base de données v9.2 ou version ultérieure vers le dernier schéma à l'aide de la dernière version de Server Configuration Tool (Outil de configuration de serveur). Pour savoir comment migrer une base de données à l'aide de l'outil de configuration de serveur, reportez-vous à Migrer la base de données. Pour obtenir la dernière version de Server Configuration Tool (Outil de configuration de serveur), ou pour migrer une base de données antérieure à la version 9.2, contactez Dell ProSupport pour obtenir une assistance.

REMARQUE :

Si vous disposez d'un serveur Enterprise Server v9.2 ou version ultérieure fonctionnel, reportez-vous aux instructions figurant dans **Mettre à niveau/Migrer un serveur principal**.

Si vous installez un serveur front-end, effectuez l'installation une fois le serveur back-end installé :

- Installer un serveur front-end : instructions pour installer un serveur front-end pour communiquer avec un serveur back-end.

Installer le serveur principal et une nouvelle base de données

1 Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server. ***Les opérations de copier/coller ou glisser/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 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.

6 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

7 Si vous avez copié le fichier EnterpriseServerInstallKey.ini dans C:\Windows (opération facultative) comme indiqué dans la rubrique Configuration préalable à l'installation, cliquez sur **Suivant**. Sinon, saisissez la clé de produit de 32 caractères, puis cliquez sur **Suivant**. La clé du produit se trouve dans le fichier EnterpriseServerInstallKey.ini.

8 Sélectionnez **Installation principale**, puis cliquez sur **Suivant**.

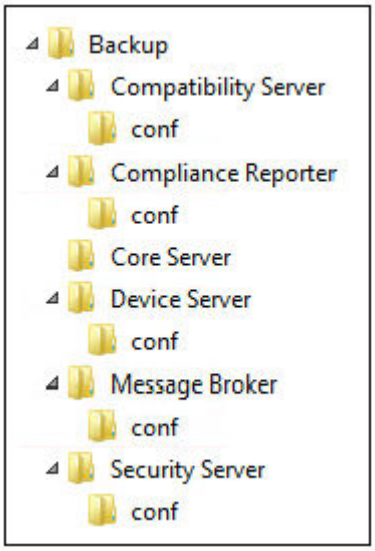
9 Pour installer Security Management Server dans l'emplacement par défaut C:\Program Files\Dell, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.

10 Pour sélectionner un emplacement où stocker les fichiers de configuration de sauvegarde, cliquez sur **Modifier**, naviguez vers le dossier de votre choix, puis cliquez sur **Suivant**.

Dell vous recommande de sélectionner un emplacement sur un réseau distant ou un disque externe pour la sauvegarde.

Après l'installation, tout changement apporté aux fichiers de configuration, y compris les changements effectués à l'aide de l'outil de configuration du serveur, doit être sauvegardé manuellement dans ces dossiers. Les fichiers de configuration sont un élément important de l'ensemble des informations utilisées pour restaurer manuellement le Dell Server, le cas échéant.

REMARQUE : La structure de dossiers créée par le programme d'installation lors de cette étape de l'installation (ci-dessous) doit rester inchangée.



11 Vous avez le choix entre différents types de certificats numériques. **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**.

Cliquez sur **Parcourir** pour saisir le chemin du certificat.

Saisissez le mot de passe associé au certificat. Le fichier de magasin de clés doit avoir le suffixe .p12 ou pfx. Pour obtenir des instructions, voir la section Exporter un certificat vers .PFX à l'aide de la console de gestion des certificats.

Cliquez sur **Suivant**.

> **REMARQUE :**
> Pour utiliser ce paramètre, le certificat de l'autorité de certification exporté qui est importé doit contenir la chaîne complète d'approbation. En cas de doute, ré-exportez le certificat de l'autorité de certification et vérifiez que les options suivantes sont sélectionnées dans l'« Assistant d'exportation de certificat » :
>
> - Échange d'informations personnelles - PKCS#12 (.PFX)
> - Inclure tous les certificats dans le chemin de certification, si possible
> - Exporter toutes les propriétés étendues

OU

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

Cliquez sur **Suivant**.

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

12 Pour Server Encryption, vous avez le choix entre différents types de certificats numériques. 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**.

Cliquez sur **Parcourir** pour saisir le chemin du certificat.

Saisissez le mot de passe associé au certificat. Le fichier de magasin de clés doit avoir le suffixe .p12 ou pfx. Pour obtenir des instructions, voir la section Exporter un certificat vers .PFX à l'aide de la console de gestion des certificats.

Cliquez sur **Suivant**.

REMARQUE :

Pour utiliser ce paramètre, le certificat de l'autorité de certification exporté qui est importé doit contenir la chaîne complète d'approbation. En cas de doute, ré-exportez le certificat de l'autorité de certification et vérifiez que les options suivantes sont sélectionnées dans l'« Assistant d'exportation de certificat » :

- Échange d'informations personnelles - PKCS#12 (.PFX)
- Inclure tous les certificats dans le chemin de certification, si possible
- Exporter toutes les propriétés étendues

OU

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

Cliquez sur **Suivant**.

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

13 Depuis la boîte de dialogue *Configuration de l'installation du serveur principal*, vous pouvez afficher ou modifier les noms d'hôte et les ports.

- Pour accepter les noms d'hôte et les ports par défaut, dans la boîte de dialogue *Configuration de l'installation du serveur frontal, cliquez sur* **Suivant**.
- Si vous utilisez un serveur front-end, sélectionnez **Fonctionne avec le serveur front-end pour communiquer avec les clients en interne dans votre réseau ou en externe dans le DMZ**, puis entrez le nom d'hôte du serveur de sécurité front-end (par exemple, serveur.domaine.com).
- Pour afficher ou modifier les noms d'hôtes, cliquez sur **Modifier les noms d'hôte**. Modifiez les noms d'hôte uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut.

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

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

- Pour afficher ou modifier les ports, cliquez sur **Modifier les ports**. Modifier les ports uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut. Une fois que vous avez terminé, cliquez sur **OK**.

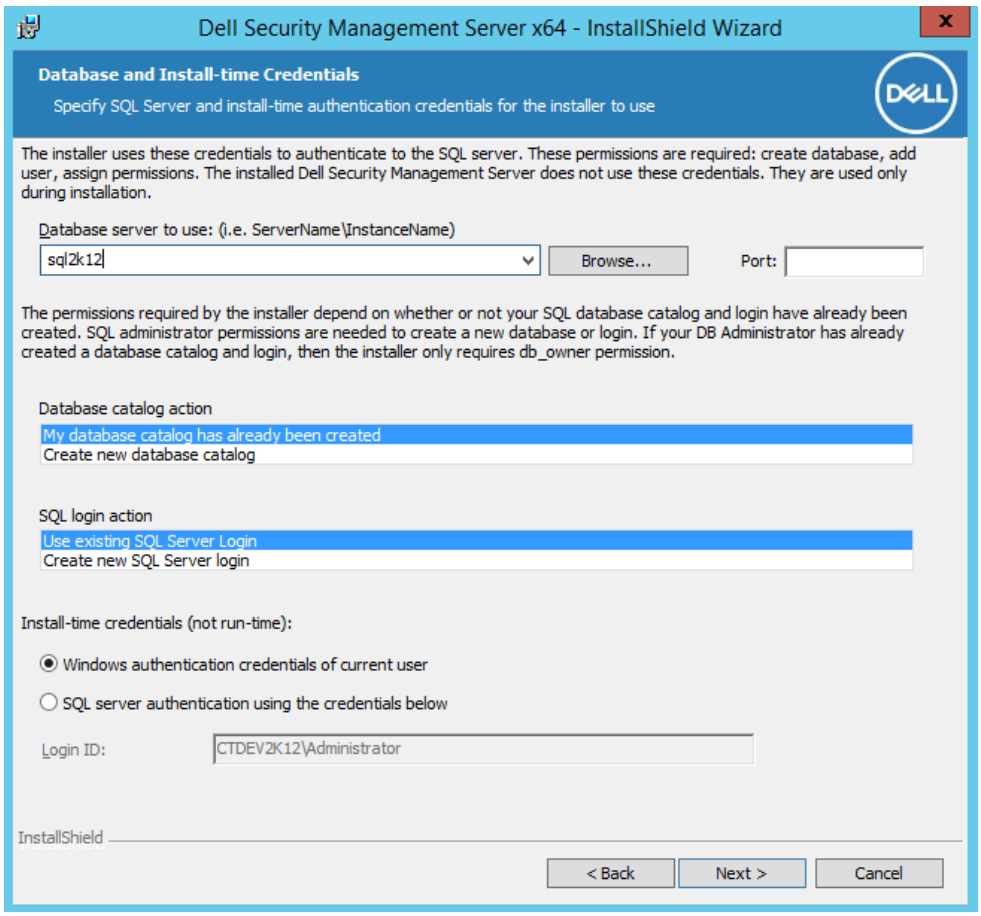
14 Pour créer une nouvelle base de données, procédez comme suit :

a Cliquez sur **Parcourir** pour sélectionner le serveur sur lequel installer la base de données.

b Sélectionnez la méthode d'authentification du programme d'installation à utiliser pour configurer la base de données Dell Server. Après l'installation, le produit installé n'utilise pas les données d'identification spécifiées ici.

- **Identifiants d'authentification Windows de l'utilisateur actuel**

  Si vous choisissez Authentification Windows, les identifiants utilisés pour vous connecter à Windows sont utilisés pour l'authentification (les champs *Nom d'utilisateur* et *Mot de passe* ne peuvent pas être modifiés). Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL.



OU

- **Authentification de SQL Server à l'aide des informations situées ci-dessous**

  Si vous utilisez l'authentification SQL, le compte SQL utilisé doit posséder des droits d'administrateur système sur SQL Server.

  Le programme d'installation doit s'authentifier sur le serveur SQL avec ces autorisations : création d'une base de données, ajout d'utilisateur, attribution d'autorisations.

c Identifiez le catalogue de bases de données :

Saisissez le nom d'un nouveau catalogue de bases de données. Vous êtes invité dans la boîte de dialogue suivante à créer le nouveau catalogue.

d Cliquez sur **Suivant**.

e Pour confirmer que vous voulez que le programme d'installation crée une base de données, cliquez sur **Oui**. Pour revenir à l'écran précédent pour effectuer des modifications, cliquez sur **Non**.

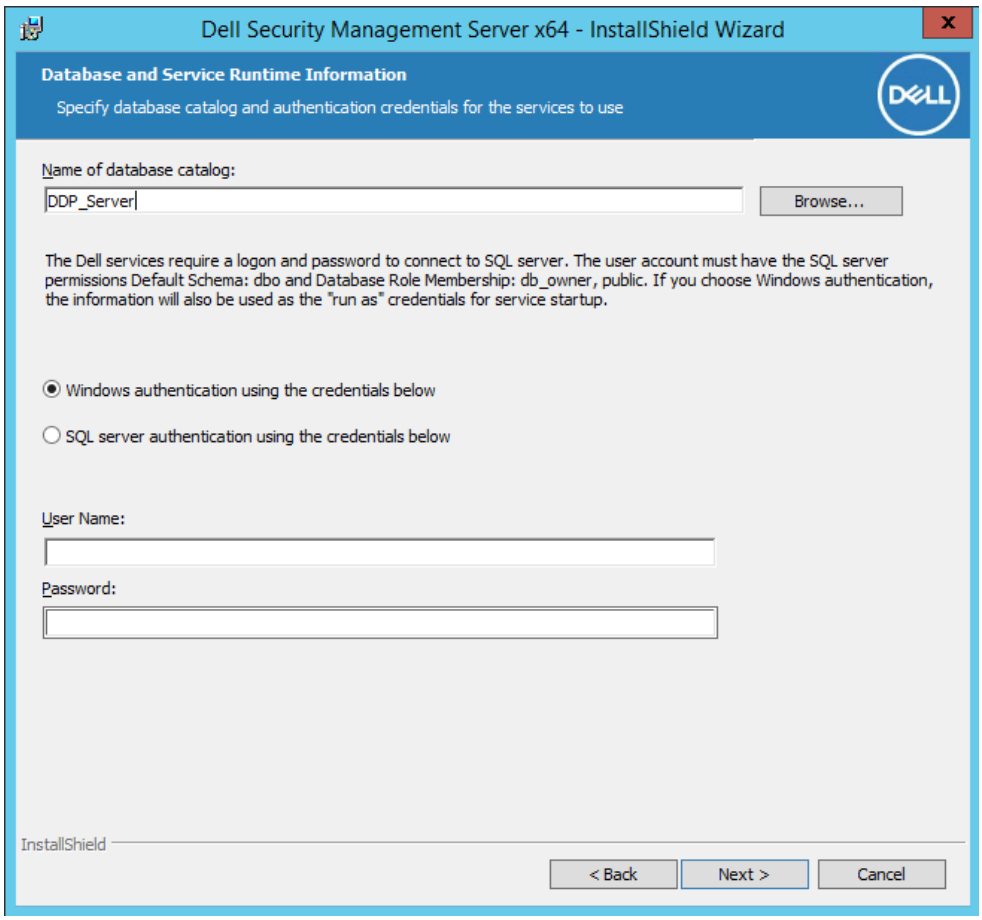
15 Sélectionnez la méthode d'authentification correspondant au produit à utiliser. Cette étape connecte un compte au produit.

- **Authentification Windows**

  Sélectionnez **Authentification Windows à l'aide des informations d'identification ci-dessous,** entrez les informations d'identification du produit à utiliser, puis cliquez sur **Suivant**.

  Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL. Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

  Ces informations d'identification sont également utilisées par les services Dell lorsqu'ils utilisent Security Management Server.



  OU

- **Authentification de SQL Server**

  Sélectionnez **Authentification de SQL Server à l'aide des données d'identification ci-dessous**, entrez les identifiants SQL Server que les services Dell utilisent lorsqu'ils travaillent avec Security Management Server, puis cliquez sur **Suivant**.

  Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

16 Dans la boîte de dialogue *Prêt à installer le programme*, cliquez sur **Installer**.
Une boîte de dialogue d'avancement affiche le statut pendant le processus d'installation.

17 Une fois l'installation terminée, cliquez sur **Terminer**.
Les tâches d'installation du serveur principal sont terminées.

Dell Services redémarre à la fin de l'installation. Il n'est pas nécessaire de redémarrer le Dell Server.

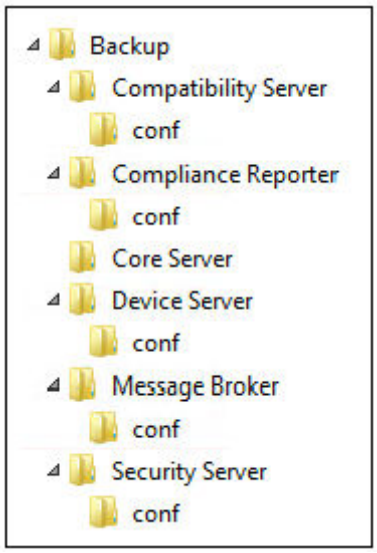
Installer le serveur frontal avec une base de données existante

REMARQUE :
Si vous disposez d'un serveur Dell Server v9.2 ou version ultérieure fonctionnel, reportez-vous aux instructions disponibles dans Mettre à niveau/Migrer un serveur principal.

Vous pouvez installer un nouveau serveur Security Management Server et vous connecter à une base de données SQL existante créée pendant la configuration préalable à l'installation, ou une base de données SQL existante v9.x ou version ultérieure, lorsque la version du schéma correspond à la version du serveur Security Management Server à installer.

Des privilèges de propriétaire de base de données sur la base de données SQL doivent être associés au compte d'utilisateur à partir duquel l'installation est effectuée. Si vous n'êtes pas sûr des privilèges d'accès ou de la connectivité à la base de données, avant de lancer l'installation, demandez à votre administrateur de base de données de confirmer ces privilèges.

Si la base de données existante a déjà été installée avec Security Management Server, avant de lancer l'installation, vérifiez que la base de données, les fichiers de configuration et le secretKeyStore sont sauvegardés et accessibles depuis le serveur sur lequel vous installez Security Management Server. L'accès à ces fichiers est nécessaire pour configurer Security Management Server et la base de données existante. La structure de dossiers créée par le programme d'installation lors de l'installation (ci-dessous) doit rester inchangée.



1 Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server. ***Les opérations de copier/coller ou glisser/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 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.

6 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

7 Si vous avez copié (facultatif) votre fichier EnterpriseServerInstallKey.ini sur C:\Windows comme indiqué dans la rubrique Configuration préalable à l'installation, cliquez sur **Suivant**. Sinon, saisissez la clé de produit de 32 caractères, puis cliquez sur **Suivant**. La clé du produit se trouve dans le fichier EnterpriseServerInstallKey.ini.

8 Sélectionnez **Installation principale** et **Installation de la récupération**, puis cliquez sur **Suivant**.

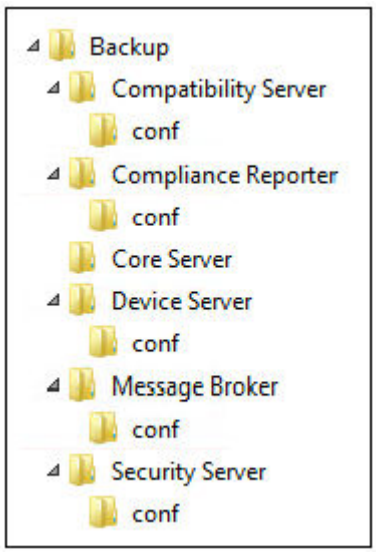
9 Pour installer Security Management Server dans l'emplacement par défaut C:\Program Files\Dell, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.

10 Pour sélectionner un emplacement où stocker les fichiers de récupération de la configuration de sauvegarde, cliquez sur **Modifier**, naviguez vers le dossier de votre choix, puis cliquez sur **Suivant**.

Dell vous recommande de sélectionner un emplacement sur un réseau distant ou un disque externe pour la sauvegarde.

Après l'installation, tout changement apporté aux fichiers de configuration, y compris les changements effectués à l'aide de l'outil de configuration du serveur, doit être sauvegardé manuellement dans ces dossiers. Les fichiers de configuration sont un élément important de l'ensemble des informations utilisées pour restaurer manuellement le serveur Dell Server.

REMARQUE : La structure de dossiers créée par le programme d'installation lors de l'installation (ci-dessous) doit rester inchangée.



11 Vous avez le choix entre différents types de certificats numériques. **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**.

Cliquez sur **Parcourir** pour saisir le chemin du certificat.

Saisissez le mot de passe associé au certificat. Le fichier de magasin de clés doit avoir le suffixe .p12 ou pfx. Pour obtenir des instructions, voir la section Exporter un certificat vers .PFX à l'aide de la console de gestion des certificats.

Cliquez sur **Suivant**.

REMARQUE :

Pour utiliser ce paramètre, le certificat de l'autorité de certification exporté qui est importé doit contenir la chaîne complète d'approbation. En cas de doute, ré-exportez le certificat de l'autorité de certification et vérifiez que les options suivantes sont sélectionnées dans l'« Assistant d'exportation de certificat » :

- Échange d'informations personnelles - PKCS#12 (.PFX)
- Inclure tous les certificats dans le chemin de certification, si possible
- Exporter toutes les propriétés étendues

OU

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

Cliquez sur **Suivant**.

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

12 Depuis la boîte de dialogue *Configuration de l'installation du serveur principal*, vous pouvez afficher ou modifier les noms d'hôte et les ports.

- Pour accepter les noms d'hôte et les ports par défaut, dans la boîte de dialogue *Configuration de l'installation du serveur frontal, cliquez sur* **Suivant**.
- Si vous utilisez un serveur front-end, sélectionnez **Fonctionne avec le serveur front-end pour communiquer avec les clients en interne dans votre réseau ou en externe dans le DMZ**, puis entrez le nom d'hôte du serveur de sécurité front-end (par exemple, serveur.domaine.com).
- Pour afficher ou modifier les noms d'hôtes, cliquez sur **Modifier les noms d'hôte**. Modifiez les noms d'hôte uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut.

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

  Une fois que vous avez terminé, cliquez sur **OK**.
- Pour afficher ou modifier les ports, cliquez sur **Modifier les ports**. Modifier les ports uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut. Une fois que vous avez terminé, cliquez sur **OK**.

13 Choisissez la méthode d'authentification correspondant au programme d'installation à utiliser.

a Cliquez sur **Parcourir** pour sélectionner le serveur où se trouve la base de données.

b Sélectionnez le type d'authentification.

- **Identifiants d'authentification Windows de l'utilisateur actuel**

  Si vous choisissez Authentification Windows, les identifiants utilisés pour vous connecter à Windows sont utilisés pour l'authentification (les champs *Nom d'utilisateur* et *Mot de passe* ne peuvent pas être modifiés). Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL.

  OU

- **Authentification de SQL Server à l'aide des informations situées ci-dessous**

  Si vous utilisez l'authentification SQL, le compte SQL utilisé doit posséder des droits d'administrateur système sur SQL Server.

  Le programme d'installation doit s'authentifier sur le serveur SQL avec ces autorisations : création d'une base de données, ajout d'utilisateur, attribution d'autorisations.

c Cliquez sur **Parcourir** pour sélectionnez le nom d'un catalogue de base de données existant.

d Cliquez sur **Suivant**.

14 Si la boîte de dialogue Erreur dans la base de données existante s'affiche, sélectionnez l'option appropriée.

Si le programme d'installation détecte un problème au niveau de la base de données, une boîte de dialogue *Erreur dans la base de données existante* s'affiche. Les options de la boîte de dialogue dépendent des circonstances :

- Le schéma de la base de données provient d'une version antérieure. (Reportez-vous à l'étape a.)
- La base de données dispose déjà d'un schéma de base de données qui correspond à la version actuellement installée. (Reportez-vous à l'étape b.)

a Lorsque le schéma de base est d'une version antérieure, sélectionnez **Quitter le programme d'installation pour mettre fin cette installation**. Vous devez ensuite sauvegarder la base de données.

Les options suivantes DOIVENT être utilisées uniquement avec l'aide de Dell ProSupport :

- l'option **Migrer cette base de données vers le schéma actuel** permet de récupérer une bonne base de données depuis une implémentation de serveur défectueux. Cette option utilise les fichiers de récupération dans le dossier \Backup pour se reconnecter à la base de données, puis migre la base de données vers le schéma actuel. Cette option ne doit être utilisée *qu'*après avoir d'abord tenté de réinstaller la version correcte de Security Management Server, puis exécuté le dernier programme d'installation pour procéder à une mise à niveau.
- L'option **Poursuivre sans migrer la base de données** installe les fichiers Security Management Server sans configurer complètement la base de données. La configuration de la base de données devra être terminée plus tard, manuellement, à l'aide de l'outil de configuration du serveur, et requiert d'autres changements manuels.

b Lorsque le schéma de base possède déjà la version actuelle du schéma et qu'il n'est pas connecté à un serveur principal Security Management Server, il est considéré correspondre à une *récupération*. Si **Installation de la récupération** n'a pas été sélectionnée lors de cette étape, cette boîte de dialogue s'affiche :

- Sélectionnez **Mode d'installation de récupération** pour poursuivre l'installation avec la base de données sélectionnée.
- Choisissez **Sélectionner une nouvelle base de données** pour choisir une autre base de données.
- Sélectionnez **Quitter le programme d'installation afin de mettre fin à cette installation**.

c Cliquez sur **Suivant**.

15 Sélectionnez la méthode d'authentification correspondant au produit à utiliser. Il s'agit du compte utilisé par le produit pour s'engager avec la base de données et les services Dell.

- **Pour utiliser l'authentification Windows**

  Sélectionnez **Authentification Windows à l'aide des identifiants ci-dessous,** saisissez les identifiants du compte que le produit peut utiliser, puis cliquez sur **Suivant**.

  Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL. Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

  OU

- **Pour utiliser l'authentification SQL Server**

  Sélectionnez **Authentification de SQL Server à l'aide des informations ci-dessous**, entrez les identifiants SQL Server, puis cliquez sur **Suivant.**

  Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

16 Dans la boîte de dialogue *Prêt à installer le programme*, cliquez sur **Installer**.

Une boîte de dialogue d'avancement affiche le statut pendant le processus d'installation.

Une fois l'installation terminée, cliquez sur **Terminer**.

Les tâches d'installation du serveur principal sont terminées.

Dell Services redémarre à la fin de l'installation. Il n'est pas nécessaire de redémarrer le serveur.

Installer un serveur frontal

L'installation du serveur front-end fournit une option front-end (mode DMZ) à utiliser avec Security Management Server. Si vous prévoyez de déployer des composants Dell dans la zone DMZ, veillez à les protéger correctement contre les attaques.

REMARQUE : Le service de balise est installé dans le cadre de cette installation pour prendre en charge la balise de rappel de Data Guardian, qui insère une balise de rappel dans chaque fichier protégé par Data Guardian lors de l'autorisation ou de l'application de documents Office protégés au sein de l'environnement. Ceci permet la communication entre n'importe quel périphérique à n'importe quel emplacement et le serveur front-end. Assurez-vous que la sécurité réseau nécessaire est configurée avant d'utiliser la balise de rappel.

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

1 Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server. ***Les opérations de copier/coller ou glisser/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 Si vous avez copié (facultatif) votre fichier EnterpriseServerInstallKey.ini sur C:\Windows comme indiqué dans la rubrique Configuration préalable à l'installation, cliquez sur **Suivant**. Sinon, saisissez la clé de produit de 32 caractères, puis cliquez sur **Suivant**. La clé du 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**.

Cliquez sur **Parcourir** pour saisir le chemin du certificat.

Saisissez le mot de passe associé au certificat. Le fichier de magasin de clés doit avoir le suffixe .p12 ou pfx. Pour obtenir des instructions, voir la section Exporter un certificat vers .PFX à l'aide de la console de gestion des certificats.

Cliquez sur **Suivant**.

REMARQUE :

Pour utiliser ce paramètre, le certificat de l'autorité de certification exporté qui est importé doit contenir la chaîne complète d'approbation. En cas de doute, ré-exportez le certificat de l'autorité de certification et vérifiez que les options suivantes sont sélectionnées dans l'« Assistant d'exportation de certificat » :

- Échange d'informations personnelles - PKCS#12 (.PFX)
- Inclure tous les certificats dans le chemin de certification, si possible
- Exporter toutes les propriétés étendues

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

Cliquez sur **Suivant**.

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

11 Dans la boîte de dialogue *Configuration du serveur front-end*, entrez le nom d'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 d'hôte et les ports.

- Pour accepter les noms d'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 d'hôtes, dans la boîte de *configuration du serveur frontal* cliquez sur **Modifier les noms d'hôte**. Modifiez les noms d'hôte uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut.

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

  Désélectionnez un proxy uniquement si vous êtes certain de ne pas vouloir le configurer en vue de son installation. Si vous désélectionnez 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 recommande l'utilisation des paramètres par défaut.

  Si vous déselectionnez un proxy dans la boîte de dialogue *Modifier les noms d'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**.
Une boîte de dialogue d'avancement affiche le statut pendant le processus d'installation.

14 Une fois l'installation terminée, cliquez sur **Terminer**.
Les tâches d'installation du serveur frontalsont terminées.

Mise à niveau/Migration

Vous pouvez mettre à niveau Enterprise Server v9.2 et les versions ultérieures vers Security Management Server v10.x. Si la version de votre Serveur Dell est antérieure à v9.2, vous devez d'abord effectuer une mise à niveau vers v9.2, puis vers les versions ultérieures.

Avant de commencer la mise à niveau/migration

Avant de commencer, veillez à exécuter toutes les étapes de configuration préalable à l'installation.

Lisez le document *Security Management Server Technical Advisories* (Conseils techniques concernant Security Management Server) pour connaître les solutions palliatives ou les problèmes connus relatifs à l'installation de Security Management Server.

Des privilèges de propriétaire de base de données sur la base de données SQL doivent être associés au compte d'utilisateur à partir duquel l'installation est effectuée. Si vous n'êtes pas sûr des privilèges d'accès ou de la connectivité à la base de données, avant de lancer l'installation, demandez à votre administrateur de base de données de confirmer ces privilèges.

Dell recommande d'appliquer les meilleures pratiques pour les bases de données Dell Server et d'inclure le logiciel Dell dans le programme de reprise après sinistre de votre société.

Si vous prévoyez de déployer des composants Dell dans la zone DMZ, veillez à les protéger correctement contre les attaques.

Pour l'environnement de production, Dell recommande d'installer SQL Server sur un serveur dédié.

Pour exploiter pleinement les fonctionnalités des règles, Dell recommande d'effectuer une mise à jour vers les dernières versions du serveur Security Management Server et des clients.

Security Management Server v9.x prend en charge :

- Encryption Enterprise :
  - Clients Windows v7.x/8.x
  - Clients Mac v7.x/8.x
  - Clients SED v8.x
  - Authentication v8.x
  - BitLocker Manager v7.2x+ et .v8.x
  - Data Guardian v1.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprise v1.x
- Mise à niveau/migration depuis Security Management Server v9.2 ou version ultérieure. (En cas de migration depuis un serveur Security Management Server antérieur à la version 9.2, contactez Dell ProSupport pour obtenir de l'aide.)

Lorsque vous mettez à niveau/migrez Security Management Server vers une version incluant de nouvelles règles qui lui sont propres, validez la règle mise à jour après la mise à niveau/migration afin de mettre en œuvre vos paramètres de règle préférentiels pour les nouvelles règles et non pas les valeurs par défaut.

En général, nous conseillons de commencer par mettre à niveau/migrer Security Management Server et ses composants, puis d'installer/mettre à niveau le client.

Appliquer les modifications de règles

1 Connectez-vous à la console de gestion en tant qu'administrateur Dell.

2 Dans le menu de gauche, cliquez sur **Gestion** > **Valider**.

3 Dans *Commentaire*, entrez une description de la modification.

4 Cliquez sur **Valider les règles**.

5 Une fois la validation effectuée, déconnectez-vous de la console de gestion.

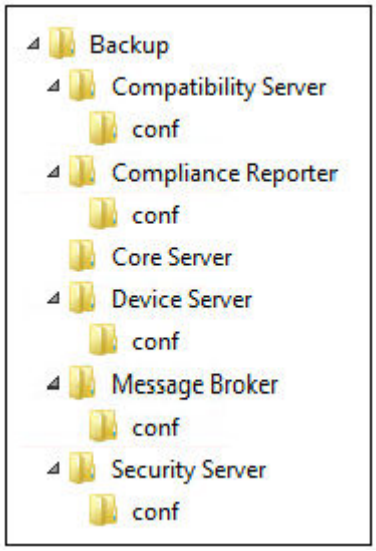
S'assurer que Dell Services est en cours d'exécution

6 Depuis le menu *Démarrer* de Windows, cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque *Services* s'ouvre, accédez à chaque service et, si nécessaire, cliquez sur **Démarrer le service**.

Sauvegarder l'installation existante

7 Sauvegardez l'ensemble de l'installation existante dans un autre emplacement. La sauvegarde doit comprendre la base de données SQL, secretKeyStore et les fichiers de configuration. Vous avez besoin de plusieurs fichiers de l'installation existante une fois le processus de mise à niveau/migration terminé.

> **REMARQUE :**
> La structure de dossiers créée par le programme d'installation lors de l'installation (ci-dessous) doit rester inchangée.



Mettre à niveau/Migrer un serveur principal

1 Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server. ***Les opérations de copier/coller ou glisser/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**.

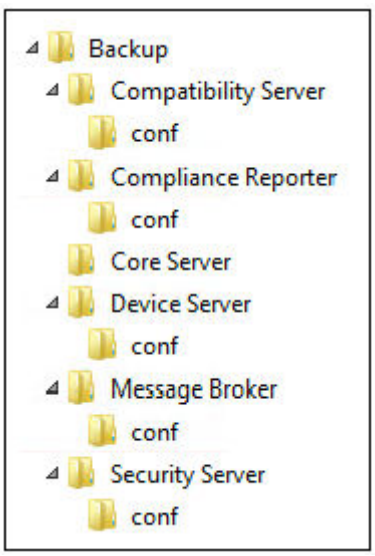
4 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.

5 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

6 Pour sélectionner un emplacement où stocker les fichiers de configuration de sauvegarde, cliquez sur **Modifier**, naviguez vers le dossier de votre choix, puis cliquez sur **Suivant**.

Dell vous recommande de sélectionner un emplacement sur un réseau distant ou un disque externe pour la sauvegarde.

La structure de dossiers créée par le programme d'installation lors de l'installation (ci-dessous) doit rester inchangée.



7 Lorsque le programme d'installation localise correctement la base de données existante, la boîte de dialogue est préremplie.

Pour vous connecter à la base de dialogue existante, spécifiez la méthode d'authentification à utiliser. Après l'installation, le produit installé n'utilise pas les données d'identification spécifiées ici.

a Sélectionnez le type d'authentification de la base de données :

- **Identifiants d'authentification Windows de l'utilisateur actuel**

  Si vous choisissez Authentification Windows, les identifiants utilisés pour vous connecter à Windows sont utilisés pour l'authentification (les champs *Nom d'utilisateur* et *Mot de passe* ne peuvent pas être modifiés).

  Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL. Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

  OU

- **Authentification de SQL Server à l'aide des informations situées ci-dessous**

  Si vous utilisez l'authentification SQL, le compte SQL utilisé doit posséder des droits d'administrateur système sur SQL Server.

  Le programme d'installation doit s'authentifier sur le serveur SQL avec ces autorisations : création d'une base de données, ajout d'utilisateur, attribution d'autorisations.

b Cliquez sur **Suivant**.

8 Si la boîte de dialogue « Informations concernant le compte Service Runtime » n'est pas pré-renseignée, spécifiez la méthode d'authentification du produit à utiliser après installation.

a Sélectionnez le type d'authentification.

b Saisissez le nom d'utilisateur et le mot de passe du compte du service de domaine qu'utiliseront les services Dell pour accéder à SQL Server, puis cliquez sur **Suivant**.

Le compte utilisateur doit être au format DOMAINE\Nomd'utilisateur et doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

9 Si la base de données n'est pas sauvegardé, vous ***devez*** la sauvegarder avant de continuer l'installation. ***L'opération de mise à niveau de la base de données ne peut pas être annulée.*** Sélectionnez **Oui**, **la base de données a été sauvegardée** après avoir sauvegardée la base de données, puis cliquez sur **Suivant**.

10 Cliquez sur **Installer** pour démarrer l'installation.

Une boîte de dialogue de progression affiche le statut pendant le processus de mise à niveau.

11 Une fois l'installation terminée, cliquez sur **Terminer**.

Dell Services redémarre à la fin de la migration. Il n'est pas nécessaire de redémarrer le Serveur Dell.

Le programme d'installation effectue les étapes 12 et 13 pour vous. Une bonne pratique consiste à vérifier ces valeurs afin de vous assurer que les modifications ont été correctement effectuées.

12 Dans votre installation de sauvegarde, copiez/collez : <Rép. d'installation de Compatibility Server>\conf\secretKeyStore vers la nouvelle installation :

<Compatibility Server install dir>\conf\secretKeyStore

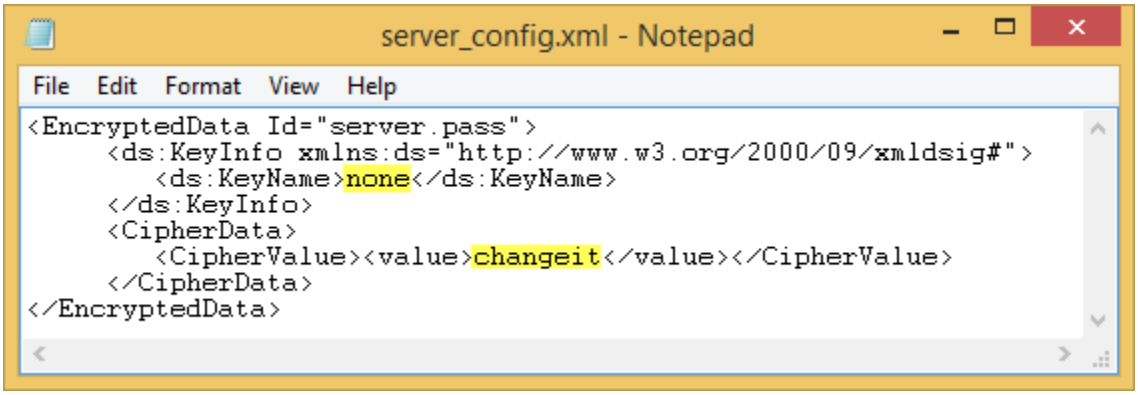
13 Dans la nouvelle installation, ouvrez le fichier <Compatibility Server install dir>\conf\server_config.xml, puis remplacez la valeur **server.pass** par celle du fichier sauvegardé <Compatibility Server install dir>\conf\server_config.xml, en procédant comme suit :

Instructions pour server.pass :

Si vous connaissez le mot de passe, reportez-vous au fichier d'exemple server_config.xml de et apportez les modifications suivantes :

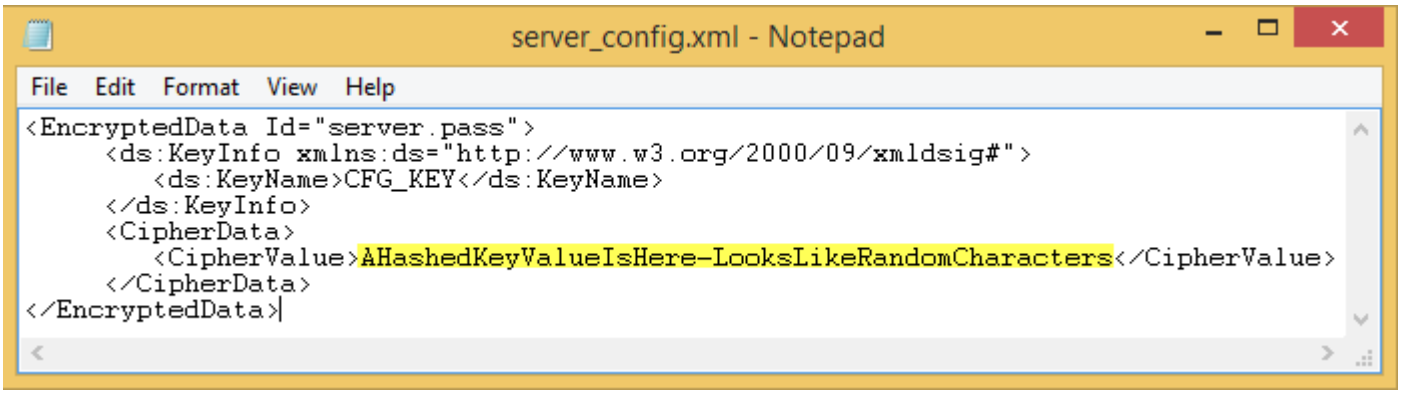
- Remplacez la valeur de *KeyName* **CFG_KEY** par **aucun**.
- Saisissez le mot de passe en clair et placez-le entre *<value> </value>*, par exemple, ici **<value>changeit</value>**.
- Lorsque Security Management Server démarre, le mot de passe en clair est crypté et la valeur cryptée remplace le texte en clair.

Mot de passe connu



Si vous ne connaissez pas le mot de passe, coupez et collez la section similaire à la section de la figure 4-2, du fichier sauvegardé sauvegardé <Compatibility Server install dir>\conf\server_config.xml file vers la section correspondante dans le nouveau fichier *server_config.xml*.

Mot de passe inconnu



Enregistrez le fichier, puis fermez-le.

REMARQUE :
N'essayez pas de changer le mot de passe de Security Management Server en modifiant la valeur server.pass dans le fichier server_config.xml à tout autre moment. Si vous modifiez cette valeur, vous n'aurez plus accès à la base de données.

Les tâches de migration du serveur principal sont terminées.

Mettre à niveau/Migrer un serveur frontal

REMARQUE : À partir de la version 9.5, le service de balise est installé dans le cadre de cette mise à niveau à l'aide du nom d'hôte par défaut et du port 8446. Le service de balise prend en charge la balise de rappel de Data Guardian, qui insère une balise de rappel dans chaque fichier protégé par Data Guardian lors de l'autorisation ou de l'application de documents Office protégés au sein de l'environnement. Ceci permet la communication entre n'importe quel périphérique à n'importe quel emplacement et le serveur front-end. Assurez-vous que la sécurité réseau nécessaire est configurée avant d'utiliser la balise de rappel.

1. Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez installer Security Management Server. ***Les opérations de copier/coller ou glisser/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 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.

6 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.

7 Dans la boîte de dialogue *Prêt à installer le programme*, cliquez sur **Installer**.

Une boîte de dialogue d'avancement affiche le statut pendant le processus d'installation.

8 Une fois l'installation terminée, cliquez sur **Terminer**.

9 Définissez le serveur principal pour communiquer avec le serveur avant.

a Sur le serveur principal, allez à <Rép. d'installation de Security Server>\conf\ et ouvrez le fichier application.properties.

b Localisez publicdns.server.host et configurez le nom en un nom d'hôte résolvable en externe.

c Localisez publicdns.server.port et configurez le port (le port par défaut est 8443).

Dell Services redémarre à la fin de l'installation. Il n'est pas nécessaire de redémarrer le Serveur Dell avant la fin des tâches de configuration post-installation.

Installation du mode déconnecté

Le mode Déconnecté isole Security Management Server d'Internet et d'un LAN ou autre réseau non sécurisé. Une fois Security Management Server installé en mode Déconnecté, il reste dans ce mode et ne peut pas revenir au mode Connecté.

Security Management Server est installé en mode Déconnecté sur la ligne de commande.

Le tableau suivant répertorie les commutateurs disponibles.

Commutateur	Signification
/v	Transmission des variables au fichier .msi dans le fichier .exe
/s	Mode Silencieux

Le tableau suivant répertorie les options d'affichage disponibles.

Option	Signification
/q	Boîte de dialogue Aucune progression, se réinitialise après la fin du processus
/qb	Boîte de dialogue de progression dotée du bouton **Annuler**
/qn	Pas d'interface utilisateur

Le tableau suivant indique les paramètres disponibles dans le cadre de l'installation. Vous pouvez spécifier ces paramètres dans la ligne de commande ou les appeler à partir d'un fichier à l'aide de la propriété suivante :

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

Paramètres
AGREE_TO_LICENSE=Yes : cette valeur doit être définie sur « Oui ».
PRODUCT_SN=xxxxx : facultatif si les informations de licence figurent dans un emplacement de stockage standard; sinon saisissez cette propriété.
INSTALLDIR=<chemin d'accès> : facultatif.
BACKUPDIR=<chemin d'accès> : emplacement de stockage du fichier de récupération.

REMARQUE : La structure de dossiers créée par le programme d'installation lors de cette étape de l'installation (ci-dessous) doit rester inchangée.

Paramètres

AIRGAP=1 : cette valeur doit être définie sur « 1 » pour installer Security Management Server en mode Déconnecté.

SSL_TYPE=n : où n est défini sur 1 pour importer un certificat existant acheté auprès d'une autorité de certification et sur 2 pour créer un certificat auto-signé. La valeur SSL_TYPE détermine les propriétés SSL requises.

Les éléments suivants sont requis avec la valeur SSL_TYPE=1 :

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

Les éléments suivants sont requis avec la valeur SSL_TYPE=2 :

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY : facultatif (« US » par défaut).

SSL_STATENAME

SSOS_TYPE=n : où n est défini sur 1 pour importer un certificat existant acheté auprès d'une autorité de certification et sur 2 pour créer un certificat auto-signé. La valeur SSOS_TYPE détermine les propriétés SSOS requises.

Les éléments suivants sont requis avec la valeur SSOS_TYPE=1 :

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

Les éléments suivants sont requis avec la valeur SSOS_TYPE=2 :

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY : facultatif (« US » par défaut).

SSOS_STATENAME

DISPLAY_SQLSERVER : cette valeur est analysée afin d'obtenir les informations d'instance et de port de SQL Server.

Exemple :

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE : facultatif. La valeur par défaut est FALSE, ce qui signifie que la base de données n'est pas créée. La base de données doit déjà exister sur le serveur.

Pour créer une nouvelle base de données, définissez cette valeur sur TRUE.

IS_SQLSERVER_AUTHENTICATION=0 : facultatif. La valeur par défaut est 0 ; elle indique que les informations d'authentification Windows de l'utilisateur actuellement connecté servent à authentifier SQL Server. Pour utiliser l'authentification SQL, définissez cette valeur sur 1.

Paramètres

REMARQUE : Le programme d'installation doit s'authentifier auprès du serveur SQL avec ces permissions : création d'une base de données, ajout d'utilisateur, attribution de permissions. Les informations d'identification sont définies au moment de l'installation, et non au moment de l'exécution.

Les éléments suivants sont requis pour l'authentification SQL :

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION : obligatoire. Choisissez la méthode d'authentification correspondant au produit à utiliser. Cette étape connecte un compte au produit. Ces informations d'identification sont également utilisées par les services Dell lorsqu'ils impliquent Security Management Server. Pour l'authentification Windows, définissez cette valeur sur 0. Pour l'authentification SQL, définissez la valeur sur 1.

REMARQUE : Assurez-vous que le compte dispose de droits d'administrateur sur le système et de la possibilité de gérer le serveur SQL. Le compte d'utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

SQL_EE_USERNAME : obligatoire. Avec l'authentification Windows, utilisez le format suivant : DOMAINE/Nomd'utilisateur. Avec l'authentification SQL, spécifiez le nom d'utilisateur.

SQL_EE_PASSWORD : obligatoire. Spécifiez le mot de passe associé au nom d'utilisateur Windows ou SQL.

Les éléments suivants sont valides pour l'authentification SQL (EE_SQLSERVER_AUTHENTICATION=1) :

RUNAS_KEYSERVER_USER : définissez le nom d'utilisateur Windows « run as » du Key Server en utilisant le format Domaine\Utilisateur. Il doit s'agit d'un compte d'utilisateur Windows.

RUNAS_KEYSERVER_PSWD : définissez le mot de passe Windows « run as » du Key Server qui est associé au compte d'utilisateur Windows.

SQL_ADD_LOGIN=T : facultatif. La valeur par défaut est nulle (cette session n'est pas ajoutée). Lorsque la valeur est définie sur T, si la valeur SQL_EE_USERNAME n'est pas une session ou un utilisateur de la base de données, le programme d'installation tente d'ajouter les informations d'authentification SQL de l'utilisateur et de définir les privilèges afin que les informations d'authentification puissent être utilisées par le produit.

Les paramètres des noms d'hôte sont les suivants. Modifiez les noms d'hôte uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut. Le format doit être le suivant : `serveur.domaine.com`.

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

CORESERVERHOST : facultatif. Nom d'hôte du Core Server.

RMIHOST : facultatif. Nom d'hôte du Compatibility Server.

REPORTERHOST : facultatif. Nom d'hôte du Compliance Reporter.

DEVICEHOST : facultatif. Nom d'hôte du Device Server.

KEYSERVERHOST : facultatif. Nom d'hôte du Key Server.

TIGAHOST : facultatif. Nom d'hôte du Security Server.

SMTP_HOST : facultatif. Nom d'hôte du serveur SMTP.

ACTIVEMQHOST : facultatif. Nom d'hôte du Message Broker.

Les paramètres des ports sont les suivants. Modifier les ports uniquement si nécessaire. Dell recommande l'utilisation des paramètres par défaut.

Paramètres
SERVERPORT_CLIENTAUTH : facultatif.
REPORTERPORT : facultatif.
DEVICEPORT : facultatif.
KEYSERVERPORT : facultatif.
GKPORT : facultatif.
TIGAPORT : facultatif.
SMTP_PORT : facultatif.
ACTIVEMQ_TCP : facultatif.
ACTIVEMQ_STOMP : facultatif.

Installation de Security Management Server en mode Déconnecté

Dans l'exemple suivant, Security Management Server est installé en mode silencieux avec une boîte de dialogue de progression, à l'aide des paramètres d'installation indiqués dans le fichier `C:\mysetups\eeoptions.txt\" "`

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

Désinstallation de Security Management Server

1. Sur le support d'installation Dell, accédez au répertoire Security Management Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Security Management Server-x64 dans le répertoire racine du serveur où vous comptez désinstaller Security Management Server. ***Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.***
2. Double-cliquez sur **setup.exe**.
3. Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.
4. Dans la boîte de dialogue *Supprimer le programme*, cliquez sur **Supprimer**.
   Une boîte de dialogue de progression affiche le statut pendant le processus de désinstallation.
5. Une fois la désinstallation terminée, cliquez sur **Terminer**.

5

Configuration postérieure à l'installation

Lisez le document *Conseils techniques concernant Security Management Server* pour connaître les solutions palliatives ou les problèmes connus relatifs à la configuration de Security Management Server.

Que vous installiez Security Management Server pour la première fois ou que vous mettiez à niveau une installation existante, certains composants de votre environnement doivent être configurés.

Après avoir installé Security Management Server, 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.

Configuration en mode DMZ

Si Security Server est déployé dans une zone DMZ et un réseau privé, et que seul le serveur DMZ possède un certificat de domaine d'une autorité de certification (CA) approuvée, certaines étapes manuelles sont nécessaires pour ajouter le certificat approuvé dans le magasin de clés Java de Security Server du réseau privé.

Si un certificat approuvé est utilisé, ignorez cette section.

REMARQUE : Dell vous recommande vivement d'utiliser des certificats de domaine d'une autorité de certification approuvée pour les serveurs DMZ et de réseau privé.

Pour plus d'informations sur la mise à jour du certificat de Dell Encryption avec un certificat existant dans le magasin de clés Microsoft, voir http://www.dell.com/support/article/us/en/19/sln297240/.

Outil de configuration serveur

Lorsqu'il devient nécessaire de configurer votre environnement, une fois l'installation terminée, utilisez l'outil de configuration de serveur pour apporter les modifications.

Le Server Configuration Tool vous permet d'effectuer les tâches suivantes :

- Ajouter des certificats nouveaux ou mis à jour

- Importer un certificat Dell Manager.
- Importer un certificat d'identité
- Configuration des paramètres de certificat SSL du serveur
- Configurer les paramètres SMTP pour Data Guardian ou les services de messagerie
- Changer le nom de la base de données, l'emplacement, ou les informations d'identification
- Migrer la base de données

Les services Dell Core Server et Compatibility Server ne peuvent pas s'exécuter en même temps que l'outil de configuration serveur. Arrêtez le service Core Server et le service Compatibility Server dans *Services* (**Démarrer > Exécuter**. Tapez ***services.msc***) avant de démarrer l'outil de configuration serveur.

Pour lancer l'outil de configuration de serveur, accédez à **Démarrer** > **Dell** > **Exécuter l'outil de configuration de serveur**.

Les journaux de l'outil de configuration de serveur sont sauvegardés dans **C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs**.

Ajouter des certificats nouveaux ou mis à jour

Vous pouvez choisir le type de certificats à utiliser : auto-signé ou signé :

- Les certificats **auto-signés** sont signés par leur propre créateur. Les certificats auto-signés conviennent aux projets pilotes, aux démonstrations de faisabilité, etc. Dans un environnement de production, Dell recommande d'utiliser des certificats signés par une autorité de certification publique ou un domaine.
- Les certificats **signés** (qu'il s'agisse de certificats signés par une autorité de certification publique ou un domaine) sont signés par une autorité de certification publique ou un domaine. Si les certificats sont signés par une autorité de certification publique (CA), le certificat de l'autorité de certification signataire existera généralement déjà dans le magasin de certificats Microsoft. Par conséquent, la chaîne d'approbation est automatiquement établie. En ce qui concerne les certificats signés par une autorité de certification de domaine, si la station de travail a été associée au domaine, le certificat de l'autorité de certification signataire du domaine aura été ajouté au magasin de certificats Microsoft de la station de travail, créant ainsi également une chaîne d'approbation.

Composants concernés par la configuration de certificats :

- Services Java (par exemple, Device Server, etc.)
- Applications .NET (Core Server)
- Validation de cartes à puce utilisées pour l'authentification de préamorçage (Security Server)
- Importation de clés de cryptage privées destinée à la signature d'ensembles de stratégies envoyés à Dell Manager. Dell Manager effectue la validation SSL pour les clients Encryption gérés avec des disques à cryptage automatique, ou Gestionnaire BitLocker.
- Postes de travail client :
  - Postes de travail exécutant Gestionnaire BitLocker
  - Postes de travail exécutant Encryption Enterprise (Windows)
  - Postes de travail exécutant Endpoint Security Suite Enterprise

Informations concernant le type de certificats à utiliser :

L'authentification de préamorçage à l'aide de cartes à puce exige une validation SSL avec le Security Server. Dell Manager effectue la validation SSL lors de la connexion au Dell Core Server. Pour ces types de connexions, l'autorité de certification signataire doit se trouver dans le magasin de clés (c'est-à-dire le magasin de clés Java ou Microsoft, selon le composant Serveur Dell concerné). Si vous choisissez les certificats auto-signés, vous disposerez des options suivantes :

- Validation de cartes à puce utilisées pour Preboot Authentication (authentification de préamorçage) :
  - Importez le certificat de signature « Root Agency » et la chaîne de confiance complète dans le magasin de clés Java de Security Server. La chaîne de confiance complète doit être importée.

Dell Manager :

- Insérez le certificat de signature « Root Agency » (à partir du certificat auto-signé généré) dans la rubrique « Autorités de certification racines d'approbation » du poste de travail (pour l'« ordinateur local ») dans le magasin de clés Microsoft.
- Modifiez le comportement de la validation SSL du côté serveur. Pour désactiver la validation d'approbation SSL du côté serveur, sélectionnez **Désactiver la vérification de la chaîne d'approbation** dans l'onglet Paramètres.

Il existe deux méthodes pour créer un certificat : *Expresse* et *Avancée*.

Choisissez **une** méthode :

- Expresse : choisissez cette méthode pour générer un certificat auto-signé pour tous les composants. Il s'agit de la méthode la plus simple, mais les certificats auto-signés conviennent aux projets pilotes, aux démonstrations de faisabilité, etc, uniquement Dans un environnement de production, Dell recommande d'utiliser des certificats signés par une autorité de certification publique ou un domaine.
- Avancée : choisissez cette méthode pour configurer chaque composant séparément.

Express

1 Dans le menu supérieur, sélectionnez **Actions** > **Configurer les certificats**.

2 Au lancement de l'Assistant Configuration, sélectionnez **Express**, puis cliquez sur **Suivant**. Les informations du certificat auto-signé qui a été créé lors de l'installation de Security Management Server sont utilisées, si disponibles.

3 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

La configuration du certificat est terminée. Le reste de cette section décrit la méthode avancée de création d'un certificat.

Avancé

Deux chemins d'accès sont disponibles pour créer un certificat : *Générer un certificat auto-signé* et *Utiliser les paramètres actuels*. Choisissez **une** seule méthode :

- Méthode 1 : Générer un certificat auto-signé
- Méthode 2 : Utiliser les paramètres actuels

Méthode 1 : Générer un certificat auto-signé

1 Dans le menu supérieur, sélectionnez **Actions** > **Configurer les certificats**.

2 Lors du démarrage de l'assistant de configuration, sélectionnez **Avancée** et cliquez sur **Suivant**.

3 Sélectionnez **Générer un certificat auto-signé** et cliquez sur **Suivant**. Les informations du certificat auto-signé qui a été créé lors de l'installation de Security Management Server sont utilisées, si disponibles.

4 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

La configuration du certificat est terminée. Le reste de cette section décrit l'autre méthode de création d'un certificat.

Méthode 2 : Utiliser les paramètres actuels

1 Dans le menu supérieur, sélectionnez **Actions** > **Configurer les certificats**.

2 Lors du démarrage de l'assistant de configuration, sélectionnez **Avancée** et cliquez sur **Suivant**.

3 Sélectionnez **Utiliser les paramètres actuels** et cliquez sur **Suivant**.

4 Dans la fenêtre *Certificat SSL du Compatibility Server*, sélectionnez **Générer un certificat auto-signé** et cliquez sur **Suivant**. Les informations du certificat auto-signé qui a été créé lors de l'installation de Security Management Server sont utilisées, si disponibles.

Cliquez sur **Suivant**.

5 Dans la fenêtre *Certificat SSL de Core Server*, sélectionnez l'une des options suivantes :

- *Sélectionner un certificat* : sélectionnez cette option pour utiliser un certificat existant. Cliquez sur **Suivant**.

  Accédez à l'emplacement du certificat existant, saisissez le mot de passe associé du certificat existant et cliquez sur **Suivant**.

Cliquez sur **Terminer** lorsque vous avez terminé.

- *Générer un certificat auto-signé* : les informations du certificat auto-signé qui a été créé lors de l'installation de Security Management Server sont utilisées, si disponibles. Si vous sélectionnez cette option, la fenêtre Certificat de sécurité des messages ne s'affiche pas (la fenêtre ne s'affiche que si vous sélectionnez l'option *Utiliser les paramètres actuels*) et que le certificat créé pour Compatibility Server est utilisé.

  Vérifiez que le nom complet de l'ordinateur est correct. Cliquez sur **Suivant**.

  Un message d'avertissement vous indique qu'il existe déjà un certificat du même nom. Lorsqu'un message vous demande si vous voulez l'utiliser, cliquez sur **Oui**.

  Cliquez sur **Terminer** lorsque vous avez terminé.
- *Utiliser les paramètres actuels* : sélectionnez cette option pour modifier le paramètre d'un certificat à tout moment après la configuration initiale de Security Management Server. Cette option ne modifie pas le certificat que vous avez déjà configuré. Sélectionnez cette option pour accéder à la fenêtre Certificat de sécurité des messages.

  Dans la fenêtre Certificat de Sécurité des messages, sélectionnez **l'une** des options suivantes :

  – *Sélectionner un certificat* : sélectionnez cette option pour utiliser un certificat existant. Cliquez sur **Suivant**.

    Accédez à l'emplacement du certificat existant, saisissez le mot de passe associé du certificat existant et cliquez sur **Suivant**.

    Cliquez sur **Terminer** lorsque vous avez terminé.

  – *Générer un certificat auto-signé* : les informations du certificat auto-signé qui a été créé lors de l'installation de Security Management Server sont utilisées, si disponibles.

    Cliquez sur **Suivant**.

    Cliquez sur **Terminer** lorsque vous avez terminé.

La configuration du certificat est terminée.

Lorsque les modifications sont terminées :

1. Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.
2. Fermez l'outil de configuration du Serveur Dell.
3. Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

Importer un certificat Dell Manager.

Si votre déploiement comprend des clients Security Management Server gérés à distance avec des instances d'Encryption Management Agent, vous devez importer votre certificat nouvellement créé (ou existant). Le certificat Dell Manager sert à protéger la clé privée utilisée pour signer les ensembles de règles envoyés aux clients Security Management Server gérés à distance, ainsi qu'à Encryption Management Agent. Ce certificat peut être indépendant des autres certificats. Par ailleurs, si cette clé est compromise, elle peut être remplacée par une nouvelle clé et Dell Manager demandera une nouvelle clé publique s'il ne peut pas décrypter les ensembles de règles.

1. Ouvrez la console de gestion Microsoft (MMC).
2. Cliquez sur **Fichier** > **Ajouter/Supprimer un snap-in** (composant logiciel enfichable).
3. Cliquez sur **Ajouter**.
4. Dans la fenêtre *Ajouter un composant logiciel enfichable autonome*, sélectionnez **Certificats** et cliquez sur **Ajouter**.
5. Sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.
6. Dans la fenêtre *Sélectionner un ordinateur*, sélectionnez **Ordinateur local (l'ordinateur sur lequel s'exécute cette console)**, puis cliquez sur **Terminer**.

7 Cliquez sur **Fermer**.

8 Cliquez sur **OK**.

9 Dans le dossier *Racine de la console*, développez *Certificats (Ordinateur local)*.

10 Accédez au dossier *Personnel* et localisez le certificat voulu.

11 Mettez en surbrillance le certificat voulu, puis, avec le bouton droit de la souris, cliquez sur **Toutes les tâches** > **Exporter**.

12 Lorsque l'assistant d'exportation de certificat démarre, cliquez sur **Suivant**.

13 Sélectionnez **Oui, exporter la clé privée** et cliquez sur **Suivant**.

14 Sélectionnez **Échange d'informations personnelles - PKCS #12 (.PFX)**, puis sélectionnez les sous-options **Inclure tous les certificats dans le chemin de certification si possible** et **Exporter toutes les propriétés étendues**. Cliquez sur **Suivant**.

15 Saisissez et confirmez le mot de passe. Il peut s'agir de n'importe quel mot de passe de votre choix. Choisissez un mot de passe facile à retenir pour vous, mais difficile à deviner pour un tiers. Cliquez sur **Suivant**.

16 Cliquez sur **Parcourir** pour accéder à l'emplacement où vous souhaitez enregistrer le fichier.

17 Dans *Nom de fichier*, entrez un nom d'enregistrement du fichier. Cliquez sur **Enregistrer**.

18 Cliquez sur **Suivant**.

19 Cliquez sur **Terminer**.

20 Un message indiquant que l'exportation a réussi s'affiche. Fermez le MMC.

21 Revenez dans l'outil de configuration du Serveur Dell.

22 Dans le menu supérieur, sélectionnez **Actions** > **Importer un certificat DM**.

23 Naviguez jusqu'à l'emplacement d'enregistrement du fichier exporté. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.

24 Saisissez le mot de passe associé à ce fichier, puis cliquez sur **OK**.

L'importation du certificat Dell Manager est à présent terminée.

Lorsque les modifications sont terminées :

1 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

2 Fermez l'outil de configuration du Serveur Dell.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

Importer un certificat SSL/TLS bêta

Si votre déploiement le Cryptage du serveur, vous devez importer votre nouveau certificat (ou certificat existant). Le certificat SSL/TLS bêta sert à protéger la clé privée utilisée pour signer les ensembles de règles envoyés aux serveurs client.

1 Dans le menu supérieur, sélectionnez **Actions** > **Importer un certificat SSL/TLS bêta**.

2 Parcourez pour sélectionner un certificat et cliquez sur **Suivant**.

3 En réponse à l'invite de *Mot de passe de certificat*, entrez le mot de passe associé au certificat existant.

4 Dans la boîte de dialogue Compte Windows, choisissez une option :

   a Pour modifier les données d'identification associées au certificat d'identité, sélectionnez **Utiliser différentes informations d'identification Windows avec le certificat d'identité**.

   b Pour continuer à utiliser les informations d'identité du compte connecté, cliquez sur **Suivant**.

5 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

Configuration des paramètres de certificat SSL du serveur

Dans Server Configuration Tool, cliquez sur l'onglet **Paramètres**.

Dell Manager :

Pour désactiver la validation d'approbation SSL de Dell Manager côté serveur, sélectionnez **Désactiver la vérification de la chaîne d'approbation**.

SCEP :

Si vous utilisez Mobile Edition, saisissez l'URL du serveur hébergeant le protocole SCEP.

REMARQUE : À partir de la version 9.8, Mobile Edition n'est plus pris en charge.

Lorsque les modifications sont terminées :

1 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

2 Fermez l'outil de configuration du Serveur Dell.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

Configurer les paramètres SMTP

Dans Server Configuration Tool, cliquez sur l'onglet **SMTP**.

Cet onglet permet de configurer les paramètres SMTP pour Data Guardian, les bulletins produit, les notifications et les messages Advanced Threat Prevention Threat Relay.

Une fois les modifications apportées à la configuration, redémarrez le service Security Server. Le service Security Server doit être redémarré pour que les paramètres soient mis à jour.

Saisissez les informations suivantes :

1 Dans *Nom d'hôte*, entrez le nom de domaine complet de votre serveur SMTP, par exemple nomserveursmtp.domaine.com.

2 Dans *Nom d'utilisateur*, entrez le nom d'utilisateur pour vous connecter au serveur de courrier. Le format peut être DOMAINE \jdupont, jdupont ou toute autre formulation requise par votre société.

3 Dans *Mot de passe*, entrez le mot de passe associé à ce nom d'utilisateur.

4 Dans *Adresse*, entrez l'adresse e-mail qui générera les e-mails. Il peut s'agir du même compte que celui du nom d'utilisateur (jdupont@domaine.com). Il peut également s'agir d'un autre compte auquel l'utilisateur concerné a accès pour l'envoi d'e-mails (EnregistrementCloud@domaine.com).

5 Dans *Port*, entrez le numéro de port (en général, 25).

6 Dans le menu *Authentification*, sélectionnez *Vrai* ou *Faux*.

REMARQUE : Le nom d'utilisateur et le mot de passe doit être laissés vides si l'authentification est définie sur Faux.

Lorsque les modifications sont terminées :

1 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

2 Fermez l'outil de configuration de Serveur Dell.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

Changer le nom de la base de données, l'emplacement, ou les informations d'identification

Dans l'outil de configuration de serveur, cliquez sur l'onglet **Base de données**.

1 Dans *Nom du serveur*, entrez le nom de domaine complet (s'il existe un nom d'instance, incluez-le) du serveur hébergeant la base de données. Par exemple, SQLTest.domaine.com\DellDB.

   Dell vous recommande d'utiliser un nom de domaine complet bien que vous puissiez utiliser une adresse IP.

2 Dans *Port du serveur*, entrez le numéro de port.

   Lorsque vous n'utilisez pas une instance SQL Server par défaut, vous devez définir le port dynamique de l'instance dans *Port :*. Vous pouvez également activer le service de navigateur SQL Server Browser et vous assurer que le port UDP 1434 est ouvert. Pour en savoir plus, voir https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

3 Dans *Base de données*, entrez le nom de la base de données.

4 Dans *Authentification*, sélectionnez **Authentification Windows** ou **Authentification SQL Server**. Si vous choisissez Authentification Windows, les identifiants déjà utilisés pour vous connecter à Windows sont utilisés pour l'authentification (les champs *Nom d'utilisateur* et *Mot de passe* ne peuvent pas être modifiés).

5 Dans *Nom d'utilisateur :*, entrez le nom d'utilisateur approprié associé à cette base de données.

6 Dans *Mot de passe :*, entrez le mot de passe de l'utilisateur spécifié dans *Nom d'utilisateur*.

7 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

8 Pour tester la configuration de la base de données, dans le menu supérieur, sélectionnez **Actions** > **Tester la configuration de la base de données**. L'Assistant Configuration se lance.

9 Lorsqu'elles s'affichent, lisez les informations de la fenêtre *Test de la configuration*, puis cliquez sur **Suivant**.

10 Si vous avez choisi l'authentification Windows dans l'onglet *Base de données*, vous pouvez entrer d'autres identifiants pour autoriser l'utilisation des mêmes identifiants utilisés pour exécuter Security Management Server. Cliquez sur **Suivant**.

11 Dans la fenêtre *Test de la configuration*, les résultats des tests des paramètres de connexion, de compatibilité et de migration de la base de données s'affichent.

12 Cliquez sur **Terminer**.

REMARQUE :
Si la base de données SQL ou l'instance SQL est configurée selon un classement autre que par défaut, ce classement ne doit pas respecter la casse. Pour obtenir la liste des classements et la sensibilité à la casse, voir https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Lorsque les modifications sont terminées :

1 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

2 Fermez l'outil de configuration du Serveur Dell.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

Migrer la base de données

Vous pouvez migrer une base de données v9.2 ou version ultérieure vers le dernier schéma avec la dernière version du serveur.

Dans l'outil de configuration de serveur, cliquez sur l'onglet **Base de données**.

1 Si vous n'avez pas encore effectué de sauvegarde de votre base de données Dell Server existante, **faites-le maintenant**.

2 Dans le menu supérieur, sélectionnez **Actions** > **Migration de la base de données**. L'Assistant Configuration se lance.

3 Dans la fenêtre *Migration de la base de données Enterprise*, un avertissement s'affiche. Confirmez soit que vous avez sauvegardé la totalité de la base de données, soit que la sauvegarde de votre base de données actuelle n'est pas nécessaire. Cliquez sur **Suivant**.

Dans la fenêtre *Migration de la base de données en cours*, des messages à caractère informatif affichent l'état de la migration.

Une fois que vous avez terminé, vérifiez s'il y a des erreurs.

REMARQUE : Un message d'erreur signalé par  **signifie qu'une tâche de la base de données a échoué et qu'une action corrective doit être effectuée pour que la base de données puisse être correctement migrée. Cliquez sur Terminer, corrigez les erreurs de la base de données et recommencez les instructions de cette section.**

4 Cliquez sur **Terminer**.

Lorsque la migration est terminée :

1 Dans le menu supérieur, sélectionnez **Configuration** > **Enregistrer**. Confirmez l'enregistrement si vous y êtes invité.

2 Fermez l'outil de configuration du Serveur Dell.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque la page *Services* s'ouvre, accédez à chaque service Dell et cliquez sur **Démarrer le service**.

6

Tâches administratives

Assigner le rôle d'administrateur Dell

1 En tant qu'administrateur de Security Management Server Virtual, connectez-vous à la console de gestion à l'adresse suivante : https://server.domain.com:8443/webui/. Les références 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 et connectez-vous avec les identifiants d'utilisateur de domaine.

Chargement des licences d'accès client

Vous avez reçu des licences d'accès client séparément des fichiers d'installation, lors de l'achat initial ou ultérieurement si vous avez ajouté des licences d'accès client supplémentaires.

1 Dans le volet de gauche, cliquez sur **Gestion**
2 Cliquez sur **Gestion des licences**.
3 Cliquez sur **Choisir un fichier** à localiser, puis sélectionnez le fichier Licence du client.

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**.

Configurer Dell Compliance Reporter

1 Dans le volet de gauche, cliquez sur **Compliance Reporter**.
2 Lorsque Dell Compliance Reporter démarre, connectez-vous à l'aide des identifiants par défaut *superadmin/changeit*.

Réaliser des sauvegardes

À des fins de reprise après sinistre, assurez-vous que les emplacements suivants sont sauvegardés chaque semaine, avec les différentiels nocturnes : Pour plus d'informations sur la planification de la reprise après sinistre, consultez l'article http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en. Pour plus d'informations sur la sauvegarde des données du Rapporteur de conformité, consultez l'article http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en.

Sauvegardes relatives à Security Management Server

Sauvegardez régulièrement les fichiers stockés dans l'emplacement que vous avez sélectionné pour la sauvegarde des fichiers de configuration au cours de l'installation (étape 10, page 27) ou mise à niveau/migration (étape 6, page 68). Les sauvegardes hebdomadaires de ces données sont acceptables, car elles évoluent normalement assez peu et peuvent être reconfigurées manuellement si nécessaire. Les fichiers les plus critiques stockent les informations nécessaires pour la connexion à la base de données :

<Dossier d'installation>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Dossier d'installation>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Dossier d'installation>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

Sauvegardes de SQL Server

Effectuez chaque soir des sauvegardes complètes avec connexion transactionnelle activée et effectuez des sauvegardes des bases de données différentielles toutes les 3 ou 4 heures. Si une sauvegarde de base de données est disponible, il est alors recommandé d'effectuer des enregistrements de transaction et des tâches d'expédition toutes les 15 minutes (ou plus fréquemment si possible). Comme toujours, Dell recommande d'appliquer les meilleures pratiques pour les bases de données Dell Server et d'inclure le logiciel Dell dans le programme de reprise après sinistre de votre société.

Pour obtenir des informations supplémentaires sur les meilleures pratiques relatives à SQL Server, reportez-vous à la liste suivante pour les mettre en œuvre lorsque Dell Security est installé et si elles ne sont pas encore mises en œuvre.

Sauvegardes de PostgreSQL Server

Les événements d'audit sont stockés sur le PostgreSQL Server, qui doit être régulièrement sauvegardé. Pour consulter les instructions de sauvegarde, voir la section https://www.postgresql.org/docs/9.5/static/backup.html.

Dell recommande d'appliquer les meilleures pratiques pour les base de données PostgreSQL et d'inclure le logiciel Dell dans le programme de reprise après sinistre de votre société.

7

Ports

Le tableau suivant décrit chaque composant et sa fonction.

Nom	Port par défaut	Description
Rapporteur de conformité	HTTP(S)/ 8084	Fournit un aperçu complet de l'environnement d'audit et de génération de rapports de conformité.
Console de gestion	HTTP(S)/ 8443	Console de gestion et centre de commande pour le déploiement à toute l'entreprise.
Core Server	HTTPS/ 8888	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 Rapporteur de conformité et la Console de gestion. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles.
Device Server	HTTPS/ 8081	Prend en charge les activations et la récupération de mot de passe. Composant de Security Management Server. Requis pour Encryption Enterprise (Windows et Mac)
Security Server	HTTPS/ 8443	Communique avec Policy Proxy, gère les extractions de clé de détection, les activations de client, Data Guardian, les communications SED-PBA et Active Directory pour l'authentification ou le rapprochement, y compris la validation d'identité pour l'authentification dans la console de gestion. Exige l'accès à la base de données SQL.
Compatibility Server	TCP/ 1099	Service de gestion de l'architecture de l'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.
Service Courtier de messages	TCP/ 61616 et STOMP/ 61613	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. Exige l'accès à la base de données SQL.
Key Server	TCP/ 8050	Négocie, authentifie et crypte une connexion client grâce aux interfaces API Kerberos. Exige l'accès à la base de données SQL pour récupérer les données des clés.

Nom	Port par défaut	Description
Proxy de stratégie	TCP/ 8000	Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité.
LDAP	TCP/ 389/636 (contrôleur de domaine local), 3268/3269 (catalogue global)	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 objets. Par exemple, une requête au port 389 peut être utilisée pour obtenir un service utilisateur.
	TCP/ 135/49125+ (RPC)	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.
Base de données Microsoft SQL	TCP/ 1433	Le port de Serveur SQL par défaut est 1433 et une valeur aléatoire comprise entre 1 024 et 5 000 est attribuée aux ports du client.
Authentification client	HTTPS/ 8449	Permet aux serveurs client de s'authentifier auprès du Dell Server. Requis pour Server Encryption.
Balise de rappel	HTTP/TCP 8446	Permet d'insérer une balise de rappel dans chaque fichier Office protégé lors de l'exécution du mode protégé Office Data Guardian.

8

Meilleures pratiques SQL Server

La liste suivante explique les meilleures pratiques relatives à SQL Server, qui doivent être mises en œuvre lorsque la sécurité Dell est installée et si elles ne sont pas encore mises en œuvre.

1 Assurez-vous que la taille de blocs NTFS où résident le fichier de données et le fichier journal est de 64 Ko. Les extensions SQL Server (unité de base de stockage SQL) sont de 64 Ko.

   Pour plus d'informations, recherchez la rubrique « Comprendre les pages et les extensions » dans les articles TechNet de Microsoft.

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 D'une manière générale, définissez la quantité de mémoire SQL Server sur 80 pour cent de la mémoire installée.

   Pour plus d'informations, recherchez la rubrique *Server Memory Server Configuration Options* (Options de configuration de la mémoire des serveurs) dans les articles TechNet de Microsoft.

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3 Définissez -t1222 sur les propriétés au démarrage de l'instance pour vous assurer que les informations sur le blocage seront capturées le cas échéant.

   Pour plus d'informations, recherchez « Indicateurs de trace (Transact-SQL) » dans les articles TechNet de Microsoft.

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4 Assurez-vous que tous les index sont couverts par une tâche de maintenance hebdomadaire pour reconstituer les index.

9

Certificats

Ce chapitre explique comment obtenir les certificats permettant d'utiliser Security Management Server.

Pour plus d'informations sur la façon de configurer l'authentification avec carte à puce, voir http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en.

Pour plus d'informations sur la configuration minimum requise pour demander des certificats SSL/TLS à des fins d'utilisation par le serveur Dell Data Security, voirhttp://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en.

Pour plus d'informations sur la mise à jour du certificat de Dell Encryption avec un certificat existant dans le magasin de clés Microsoft, voir http://www.dell.com/support/article/us/en/19/sln297240/.

Créer un certificat auto-signé et générer une demande de signature de certificat (CSR)

Cette section décrit les étapes à suivre pour créer un certificat auto-signé pour des composants Java. Ce processus ne **peut pas** être utilisé pour créer un certificat auto-signé pour les composants .NET.

Dell recommande d'utiliser un certificat auto-signé *uniquement* dans un environnement hors production.

Si votre entreprise nécessite un certificat de serveur SSL, ou si vous avez besoin de créer un certificat pour d'autres raisons, cette section décrit le processus de création d'un magasin de clés Java à l'aide de l'outil Keytool.

Si votre entreprise prévoit d'utiliser des cartes à puce pour l'authentification, vous devez utiliser Keytool pour importer la chaîne complète d'approbation des certificats qui sont utilisés dans le certificat de l'utilisateur de la carte à puce.

Keytool crée les clés privées qui sont transmises sous le format d'une demande de signature de certificat (CSR) à une autorité de certification (CA), telle que VeriSign® ou Entrust®. Sur la base de cette CSR, l'autorité de certification créera ensuite un certificat de serveur signé. Le certificat de serveur est ensuite téléchargé sur un fichier avec le certificat de l'autorité de signature. Les certificats sont ensuite importés dans le fichier cacerts.

Générer une nouvelle paire de clés et un certificat auto-signé

1 Accédez au répertoire **conf** de Compliance Reporter, Security Server ou Device Server.

2 Sauvegardez la base de données de certificats par défaut :

Cliquez sur **Démarrer** > **Exécuter**, puis saisissez `move cacerts cacerts.old`.

3 Ajouter Keytool au chemin d'accès au système. Tapez la commande suivante dans une invite de commande :

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 Pour générer un certificat, exécutez Keytool comme indiqué :

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Saisissez les informations suivantes, quand l'outil keytool vous invite à le faire.

REMARQUE :

Faites une copie de sauvegarde des fichiers de configuration avant de les modifier. Modifiez uniquement les paramètres spécifiés. Vous risquez de corrompre ou d'endommager le système si vous modifiez les autres données contenues dans ces fichiers, notamment les balises. Dell ne garantit pas que les problèmes résultant de modifications non autorisées de ces fichiers puissent être résolus sans procéder à une réinstallation de Security Management Server.

- *Mot de passe de magasin de clés* : saisissez un mot de passe (les caractères non pris en charge <>;&" ') et définissez la variable dans le fichier de composant **conf** en lui affectant la même valeur, comme suit :

  <rép. d'installation de Compliance Reporter>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =

  <rép. d'installation de Device Server>\conf\application.properties. Définissez la valeur keystore.password =

  <rép. d'installation de Security Server>\conf\application.properties. Définissez la valeur keystore.password =
- *Nom complet du serveur* : saisissez le nom complet du serveur où est installé le composant que vous utilisez. Ce nom complet comprend le nom d'hôte et le nom de domaine (par exemple, serveur.domaine.com).
- *Unité organisationnelle* : entrez la valeur appropriée (exemple, Sécurité).
- *Organisation* : entrez la valeur appropriée (exemple, Dell).
- *Ville ou localité* : saisissez la valeur appropriée (par exemple, Dallas).
- *État ou province* : entrez le nom non abrégé de l'État ou de la province (par exemple, Texas).
- Code à deux lettres du pays.
- L'utilitaire demande confirmation que l'information est correcte. Si c'est le cas, saisissez `oui`.

  Sinon, tapez `non`. Le Keytool affiche toutes les valeurs saisies précédemment. Cliquez sur **Entrée** pour accepter la valeur ou modifiez la valeur et cliquez sur **Entrée**.
- *Mot de passe de clé pour alias* : si vous ne saisissez pas un autre mot de passe ici, ce mot de passe sera par défaut celui du magasin de clés.

Demander un certificat signé par une autorité de certification

Utilisez cette procédure pour générer une requête de signature de certificat pour le certificat auto-signé créé dans Générer une nouvelle paire de clés et un certificat autosigné.

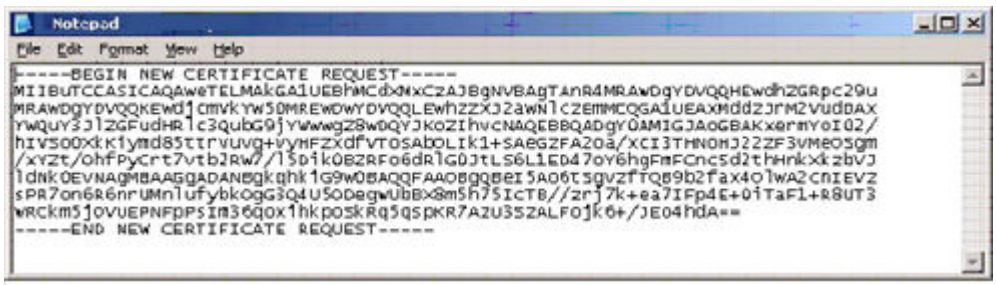
1 Substituez la même valeur utilisée précédemment pour <**certificatealias**>:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

Par exemple, `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

Le fichier .csr contient une paire BEGIN/END à utiliser lors de la création du certificat de l'autorité de certification.

Exemple de fichier CSR



2 Suivez votre processus organisationnel pour l'acquisition d'un certificat de serveur SSL auprès d'une autorité de certification. Envoyer le contenu de <csr-filename> pour la signature.

> **REMARQUE :**
> Il existe plusieurs méthodes de demande d'un certificat valide. Un exemple de méthode est figure dans**Exemple de méthode pour demander un certificat**.

3 Lorsque le certificat signé est reçu, enregistrez-le dans un fichier.

4 La méthode recommandée consiste à sauvegarder ce certificat dans le cas où une erreur se produirait pendant le processus d'importation. Cette sauvegarde peut vous éviter d'avoir à reprendre le processus depuis le début.

Importer un certificat racine

Si l'Autorité de certification du certificat racine est Verisign (mais pas Verisign Test), passez à la procédure suivante et importez le certificat signé.

Le certificat racine de l'autorité de certification valide les certificats signés.

1 Effectuer l'**une** des opérations suivantes :

- Téléchargez le certificat racine de l'autorité de certification et enregistrez-le dans un fichier.
- Obtenez le certificat racine du serveur de l'annuaire d'entreprise.

2 Effectuer l'**une** des opérations suivantes :

- Si vous activez SSL pour Compliance Reporter, Security Server ou Device Server, accédez au répertoire composant **conf**.
- Si vous activez SSL entre Security Management Server et le serveur d'annuaire d'entreprise, accédez à <**rép. d'installation de Dell>\Java Runtimes\jre1.x.x_xx\lib\security** (le mot de passe par défaut de JRE cacerts est **changeit**).

3 Exécutez Keytool comme suit pour installer le certificat racine :

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

Par exemple, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Exemple de méthode de demande de certificat

Exemple de méthode pour demander un certificat : utiliser un navigateur web pour accéder au Serveur CA Microsoft, qui est mis en place en interne par votre entreprise.

1 Naviguez jusqu'au serveur CA Microsoft. L'adresse IP est fournie par votre entreprise.

2 Sélectionnez **Demander un certificat** et cliquez sur **Suivant**.

Services de certificats Microsoft

3 Sélectionnez **Demande avancée** et cliquez sur **Suivant**.

Choisissez le type de requête

4 Sélectionnez l'option pour **Soumettre une demande de certificat avec un fichier PKCS #10 à encodage base64** et cliquez sur **Suivant**.

Requête de certificat avancée

5 Collez le contenu de la demande CSR dans la zone de texte. Sélectionnez un modèle de certificat de **serveur Web** et cliquez sur **Envoyer**.

Envoyer une requête enregistrée

6 Enregistrez le certificat. Sélectionnez **encodage DER** et cliquez sur **Télécharger le certificat de l'autorité de certification**.

Télécharger le certificat CA

7 Enregistrez le certificat. Sélectionnez **encodage DER** et cliquez sur **Télécharger le chemin de certification de l'autorité de certification**.

Télécharger le chemin d'accès à la certification CA

8 Importer les certificats d'autorité de signature convertis. Revenez à l'invite de commandes. Type :

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Une fois le certificat de l'autorité de signature importé, le certificat du serveur peut être importé (la chaîne de confiance peut être établie). Type :

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Utilisez l'alias du certificat auto-signé pour combiner la demande CSR avec le certificat du serveur.

10 Un listing du fichier cacerts montre que le certificat du serveur a une **longueur de chaîne de certificats** égale à **2**, ce qui indique que le certificat n'est pas auto-signé. Type :

```
keytool -list -v -keystore cacerts
```

L'empreinte de certificat du deuxième certificat de la chaîne est le certificat d'autorité de signature importé (qui est également répertorié sous le certificat du serveur dans le listing).

Exporter un certificat vers .PFX à l'aide de Certificate Management Console

Une fois que vous disposez d'un certificat sous la forme d'un fichier .crt dans la console MMC, il doit être converti en un fichier .pfx pour l'utiliser avec Keytool quand Security Server est utilisé en mode DMZ *et* lors de l'importation d'un certificat Dell Manager vers l'outil de configuration de serveur.

1 Ouvrez la console de gestion Microsoft (MMC).
2 Cliquez sur **Fichier** > **Ajouter/Supprimer un snap-in** (composant logiciel enfichable).
3 Cliquez sur **Ajouter**.
4 Dans la fenêtre *Ajouter un composant logiciel enfichable autonome*, sélectionnez **Certificats** et cliquez sur **Ajouter**.
5 Sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**.
6 Dans la fenêtre *Sélectionner un ordinateur*, sélectionnez **Ordinateur local (l'ordinateur sur lequel s'exécute cette console)**, puis cliquez sur **Terminer**.
7 Cliquez sur **Fermer**.
8 Cliquez sur **OK**.
9 Dans le dossier *Racine de la console*, développez *Certificats (Ordinateur local)*.
10 Accédez au dossier *Personnel* et localisez le certificat voulu.
11 Mettez en surbrillance le certificat voulu, puis, avec le bouton droit de la souris, cliquez sur **Toutes les tâches** > **Exporter**.
12 Lorsque l'assistant d'exportation de certificat démarre, cliquez sur **Suivant**.
13 Sélectionnez **Oui, exporter la clé privée** et cliquez sur **Suivant**.
14 Sélectionnez **Échange d'informations personnelles - PKCS #12 (.PFX)**, puis sélectionnez les sous-options **Inclure tous les certificats dans le chemin de certification si possible** et **Exporter toutes les propriétés étendues**. Cliquez sur **Suivant**.
15 Saisissez et confirmez le mot de passe. Il peut s'agir de n'importe quel mot de passe de votre choix. Choisissez un mot de passe facile à retenir pour vous, mais difficile à deviner pour un tiers. Cliquez sur **Suivant**.

16 Cliquez sur **Parcourir** pour accéder à l'emplacement où vous souhaitez enregistrer le fichier.

17 Dans *Nom de fichier*, entrez un nom d'enregistrement du fichier. Cliquez sur **Enregistrer**.

18 Cliquez sur **Suivant**.

19 Cliquez sur **Terminer**.

Un message indiquant que l'exportation a réussi s'affiche. Fermez le MMC.

Ajouter un certificat de signature approuvé à Security Server quand un certificat non approuvé a été utilisé pour SSL

1 Arrêtez le service Security Server, s'il est exécuté.

2 Sauvegardez le fichier cacerts dans <Rép. d'installation de Security Server>\conf\.

Utilisez Keytool pour effectuer ce qui suit :

3 Exportez le PFX approuvé dans un fichier texte et documentez l'Alias :

```
keytool -list -v -keystore "
```

4 Importez le PFX dans le fichier cacerts dans <Rép. d'installation de Security Server>\conf\.

```
keytool -importkeystore -v -srckeystore "
```

5 Modifiez la valeur keystore.alias.signing dans <Rép. d'installation de Security Server>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

Démarrez le service Security Server.