Dell Data Protection

Enterprise Server Installation and Migration Guide v9.7

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.

Enterprise Server Installation and Migration Guide (Guide d'installation et de migration d'Enterprise Server)

2017 - 04

Rév. A01

Table des matières

Présentation de Dell Enterprise Server

À propos de Dell Enterprise Server

Enterprise Server est l'élément d'administration de la sécurité de la solution Dell. La console de gestion à distance permet aux administrateurs de surveiller l'état des points finaux, l'application des règles, et la protection dans l'ensemble de l'entreprise.

Enterprise Server présente les fonctions suivantes :

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

Contacter Dell ProSupport

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24h/24, 7j/7 une assistance téléphonique concernant votre produit Dell Data Protection.

Un support en ligne pour les produits Dell Data Protection 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 Code de service à portée de main lors de votre appel.

Pour les numéros de téléphone en dehors des États-Unis, consultez Numéros de téléphone internationaux Dell ProSupport .

2

Configuration requise pour le serveur Dell Enterprise Server et architecture

Cette section présente en détail la configuration matérielle et logicielle requise et les recommandations de conception de l'architecture de la mise en œuvre de Dell Data Protection.

Configuration requise pour Dell Enterprise Server

Outre le logiciel fourni sur le support d'installation , les composants de Dell Enterprise Server requièrent une configuration matérielle et logicielle spécifique. Avant de poursuivre toute opération d'installation ou de mise à niveau/migration, assurez-vous que l'environnement d'installation respecte les exigences suivantes.

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

Éléments prérequis pour Dell Enterprise Server

Le tableau suivant répertorie les logiciels qui doivent être déjà installé avant d'installer Dell Enterprise Server. Les liens et instructions d'installation de ces éléments prérequis sont décrits en détail dans Configuration de préinstallation.

Chaque élément logiciel applicable doit être installé préalablement à l'installation, à moins qu'il soit indiqué que le programme d'installation l'installera. Sinon, l'installation échouera.

Matériel pour Dell Enterprise Server

Pré-requis

- **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.

Pré-requis

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

Le tableau suivant décrit la configuration matérielle *minimale* requise pour Dell Enterprise Server. Reportez-vous à Conception de l'artichitecture Dell Enterprise Server pour obtenir des informations supplémentaires sur l'adaptation par rapport à la taille de votre déploiement.

Configuration matérielle requise

Processeur

UC double-cœur avancée au minimum (2 GHz ou +), tel que Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalents AMD

UC QuadCore avancée (2 GHz ou +) pour une configuration à serveur unique

RAM

8 Go minimum, en fonction de la configuration

16 Go pour une configuration à serveur unique

Espace disque disponible

Environ 1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel)

20 Go au moins d'espace disque disponible (outre l'espace de pagination virtuel) pour une configuration à serveur unique

Carte réseau

Carte d'interface réseau 10/100/1000

Divers

TCP/IPv4 installé et activé

Logiciel Dell Enterprise Server

Le tableau ci-dessous répertorie la configuration logicielle requise pour Dell Enterprise Server et Proxy Server.

REMARQUE : UAC doit être désactivé avant l'installation. Il faut redémarrer le serveur pour que cette modification prenne effet. Sur Windows Server 2012 R2 et Windows Server 2016, le programme d'installation désactive l'UAC.

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

REMARQUE : Emplacement dans le registre sous Windows Server : HKLM\SOFTWARE\Dell

Dell Enterprise Server - Serveur principal et Serveur frontal Dell

- **Windows Server 2008 R2 SP0-SP1 64 bits**
  - Édition Standard
  - Édition Enterprise
- **Windows Server 2008 SP2 64 bits**
  - Édition Standard

- Édition Enterprise

- **Windows Server 2012 R2**

  - Édition Standard

  - Édition Datacenter

- **Windows Server 2016**

  - Édition Standard

  - Édition Datacenter

Serveurs Exchange ActiveSync

Si vous prévoyez d'utiliser Mobile Edition, les serveurs Exchange ActiveSync suivants sont pris en charge. Ce composant est installé sur votre serveur Exchange frontal.

- Exchange ActiveSync 12.0 : un composant d'Exchange Server 2007
- Exchange ActiveSync 12.1 : un composant d'Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 : un composant d'Exchange Server 2010
- Exchange ActiveSync 14.1 : un composant d'Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) doit être installé/configuré sur le serveur Exchange.

Référentiel LDAP

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

Environnements virtuels recommandés pour les composants de Dell Enterprise Server

Dell Enterprise Server peut être également installé éventuellement dans un environnement virtuel. Seuls les environnements suivants sont recommandés.

Dell Enterprise Server v9.7 a été validé avec Hyper-V Server (installation complète ou minimale) et comme rôle dans Windows Server 2012 R2 ou Windows Server 2016.

- Hyper-V Server (installation complète ou minimale)

  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Le matériel doit être conforme à la configuration minimale requise par Hyper-V.
  - Au moins 4 Go de RAM pour la ressource d'image dédiée
  - Doit être exécutée en tant que machine virtuelle de première génération
  - Voir https://technet.microsoft.com/en-us/library/hh923062.aspx pour obtenir plus d'informations

Dell Enterprise Server v9.7 a été validé avec VMWare ESXi 5.5 et VMware ESXi 6.0. Assurez-vous que tous les correctifs et mises à jour sont appliqués immédiatement à VMware ESXi pour remédier aux vulnérabilités potentielles.

REMARQUE : Lors de l'exécution de VMware ESXi et Windows Server 2012 R2 ou Windows Server 2016, il est recommandé d'utiliser des adaptateurs Ethernet VMXNET3.

- VMware ESXi 5.5

  - UC 64 bits x86 requise

- Ordinateur hôte avec au moins deux cœurs
- Au moins 8 Go de RAM recommandés
- Un système d'exploitation n'est pas nécessaire
- Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
- Le matériel doit être conforme à la configuration minimale requise par VMware.
- Au moins 4 Go de RAM pour la ressource d'image dédiée
- Voir http://pubs.vmware.com/vsphere-55/index.jsp pour obtenir plus d'informations

- VMware ESXi 6.0
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
  - Le matériel doit être conforme à la configuration minimale requise par VMware.
  - Au moins 4 Go de RAM pour la ressource d'image dédiée
  - Voir http://pubs.vmware.com/vsphere-60/index.jsp pour en savoir plus.

REMARQUE : La base de données SQL Server qui héberge Dell Enterprise Server doit être exécutée sur un ordinateur séparé.

Database

- **SQL Server 2008 et SQL Server 2008 R2 -** Standard Edition / Enterprise Edition
- **SQL Server 2008 SP4 (avec KB3045311) -** 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

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.

Dell Data Protection Remote Management Console et Compliance Reporter

- 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.

Support linguistique pour Dell Enterprise Server

La Console de gestion à distance 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

Langues prises en charge

IT : italien

DE : allemand

PT-PT : portugais du Portugal (ibère)

Conception de l'architecture Dell Enterprise Server

Les solutions Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise et Data Guardian sont des produits hautement évolutifs, adaptés à la taille de votre entreprise et au nombre de points finaux ciblés pour le chiffrement. Cette section fournit un ensemble de consignes permettant de mettre l'architecture à l'échelle pour 5 000 à 60 000 points finaux.

REMARQUE : Si l'entreprise compte plus de 50 000 points d'extrémité, veuillez contacter Dell ProSupport pour obtenir une assistance.

REMARQUE :

Chacun des composants répertoriés dans chaque section comprend les spécifications matérielles minimales, requises pour garantir une performance optimale dans la plupart des environnements. Le fait de ne pas allouer des ressources adéquates à l'un ou plusieurs de ces composants risque de provoquer une dégradation des performances ou des problèmes de fonctionnement de l'application.

Jusqu'à 5 000 points finaux

Cette architecture est adaptée à la plupart des petites et moyennes entreprises comportant 1 à 5 000 points finaux. Tous les composants Dell Enterprise Server peuvent être installés sur un seul serveur. Éventuellement, un serveur frontal peut être placé dans la zone DMZ pour publier des règles et/ou activer des points finaux sur Internet.

Composants d'architecture

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Configuration à serveur unique

16 Go ; 20 Go ou plus d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne quadruple cœur (2 GHz+).

Configuration du serveur lorsqu'il est utilisé avec un serveur frontal

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur frontal externe Dell

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur SQL

SQL Server 2008, SQL Server 2008 R2 et SQL Server 2008 SP4 (avec KB3045311) 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

5 000 - 20 000 points finaux

Cette architecture est adaptée aux environnements comportant entre 5 000 et 20 000 points finaux. Un serveur frontal est ajouté pour distribuer la charge supplémentaire et conçu pour gérer environ 5 000 à 20 000 points finaux. Éventuellement, un serveur frontal peut être placé dans la zone DMZ pour publier des règles et/ou activer des points finaux sur Internet.

Composants d'architecture

Dell Enterprise Server

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur frontal interne Dell (1) et serveur frontal externe Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur SQL

SQL Server 2008, SQL Server 2008 R2 et SQL Server 2008 SP4 (avec KB3045311) 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

20 000 - 40 000 points finaux

Cette architecture est adaptée aux environnements comportant entre 20 000 et 40 000 points finaux. Un serveur frontal supplémentaire est ajouté pour distribuer la charge supplémentaire. Chaque serveur frontal est conçu pour gérer environ 15 000 à 20 000 points finaux. En option, un serveur frontal peut être placé dans la zone DMZ pour activer des points finaux et/ou publier des politiques sur Internet.

Composants d'architecture

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveurs frontaux internes Dell (2) et serveurs frontaux externes Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur SQL

SQL Server 2008, SQL Server 2008 R2 et SQL Server 2008 SP4 (avec KB3045311) 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

40 000 à 60 000 points finaux

Cette architecture est adaptée aux environnements comportant entre 40 000 et 60 000 points finaux. Un serveur frontal supplémentaire est ajouté pour distribuer la charge supplémentaire. Chaque serveur frontal est conçu pour gérer environ 15 000 à 20 000 points finaux. En option, un serveur frontal peut être placé dans la zone DMZ pour activer des points finaux et/ou publier des politiques sur Internet.

REMARQUE :
Si l'entreprise compte plus de 50 000 points d'extrémité, veuillez contacter Dell ProSupport pour obtenir une assistance.

Composants d'architecture

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveurs frontaux internes Dell (2) et serveurs frontaux externes Dell (1)

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

8 Go minimum, selon la configuration ; environ 1,5 Go d'espace disque libre (outre l'espace de pagination virtuel) ; UC moderne double cœur, minimum (2 GHz+), y compris Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalent AMD

Serveur SQL

SQL Server 2008, SQL Server 2008 R2 et SQL Server 2008 SP4 (avec KB3045311) 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

Considérations relatives à la haute disponibilité

Cette architecture représente une architecture hautement disponible prenant en charge jusqu'à 60 000 points finaux. Deux serveurs Dell Enterprise Servers sont configurés dans une configuration active/passive. Pour basculer sur le deuxième serveur Dell Enterprise Server, arrêtez les services sur le nœud principal et pointez l'alias DNS (CNAME) sur le second nœud. Démarrez les services sur le second nœud et lancez Remote Management Console (Console de gestion à distance) pour vous assurer que l'application fonctionne correctement. Les services sur le second nœud (passif) doivent être configurés comme « Manuel » afin d'éviter que ces services ne démarrent accidentellement au cours d'opérations d'entretien courantes et d'application de correctifs.

Une organisation peut également choisir d'installer un serveur de base de données SQL Cluster. Dans cette configuration, le serveur Dell Enterprise Server doit être configuré pour utiliser l'adresse IP ou le nom d'hôte du cluster.

REMARQUE :
Réplication de base de données non prise en charge.

Le trafic client est réparti sur trois serveurs frontaux internes. En option, plusieurs serveur frontaux peuvent être placés dans la zone DMZ pour activer des points finaux et/ou publier des politiques vers les points finaux sur Internet.

Virtualization

Dell Enterprise Server peut être également installé éventuellement dans un environnement virtuel. Seuls les environnements suivants sont recommandés.

Dell Enterprise Server v9.7 a été validé avec Hyper-V Server (installation complète ou minimale) et comme rôle dans Windows Server 2012 R2 ou Windows Server 2016.

- Hyper-V Server (installation complète ou minimale)
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Le matériel doit être conforme à la configuration minimale requise par Hyper-V.
  - Au moins 4 Go de RAM pour la ressource d'image dédiée
  - Doit être exécutée en tant que machine virtuelle de première génération
  - Voir https://technet.microsoft.com/en-us/library/hh923062.aspx pour obtenir plus d'informations

Dell Enterprise Server v9.7 a été validé avec VMWare ESXi 5.5 et VMware ESXi 6.0. Assurez-vous que tous les correctifs et mises à jour sont appliqués immédiatement à VMware ESXi pour remédier aux vulnérabilités potentielles.

REMARQUE : Lors de l'exécution de VMware ESXi et Windows Server 2012 R2 ou Windows Server 2016, il est recommandé d'utiliser des adaptateurs Ethernet VMXNET3.

- VMware ESXi 5.5
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
  - Le matériel doit être conforme à la configuration minimale requise par VMware.
  - Au moins 4 Go de RAM pour la ressource d'image dédiée

- Voir http://pubs.vmware.com/vsphere-55/index.jsp pour obtenir plus d'informations

- VMware ESXi 6.0
  - UC 64 bits x86 requise
  - Ordinateur hôte avec au moins deux cœurs
  - Au moins 8 Go de RAM recommandés
  - Un système d'exploitation n'est pas nécessaire
  - Reportez-vous à http://www.vmware.com/resources/compatibility/search.php pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
  - Le matériel doit être conforme à la configuration minimale requise par VMware.
  - Au moins 4 Go de RAM pour la ressource d'image dédiée
  - Voir http://pubs.vmware.com/vsphere-60/index.jsp pour en savoir plus.

REMARQUE : La base de données SQL Server qui héberge Dell Enterprise Server doit être exécutée sur un ordinateur séparé.

SQL Server

Dans les environnements plus volumineux, il est fortement recommandé de faire fonctionner le serveur SQL Database sur un système redondant, tel qu'un cluster SQL, pour garantir la disponibilité et la continuité des données. Il est également conseillé de procéder à des sauvegardes quotidiennes complètes avec la journalisation transactionnelle activée pour s'assurer que toute clé récemment générée par l'activation de l'utilisateur/du dispositif sera récupérable.

Les tâches de maintenance de la base de données doivent comprendre la reconstruction de tous les index de base de données et la collecte de statistiques.

3

Configuration préalable à l'installation

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

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

Configuration

1 Si elle est activée, désactivez la configuration de sécurité renforcée (ESC) d'Internet Explorer. Ajoutez l'URL du serveur 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 de Dell Policy Proxy vers Dell Message Broker : TCP/61616 et STOMP/61613

Communication avec le serveur principal Dell Security Server : HTTPS/8443

Communication vers le serveur principal Dell Core : HTTPS/8888 et 9000

Communication avec les ports RMI - 1099

Communication vers le serveur principal Dell Device Server : HTTP(S) /8443 : si votre serveur Dell Enterprise Server est v7.7 ou version ultérieure. Si Dell Enterprise Server est antérieur à la version 7.7, HTTP(S)/8081.

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

Externe (si nécessaire) :

Base de données SQL : TCP/1433

Remote Management Console: HTTPS/8443

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

Dell Compatibility Server : TCP/1099

Dell Compliance Reporter : HTTP(S)/8084 (configuré automatiquement à l'installation)

Dell Identity Server : HTTPS/8445

Dell Core Server : HTTPS/8888 et 9000 (8888 est configuré automatiquement à l'installation)

Dell Device Server : HTTP(S)/8443 (Dell Enterprise Server v7.7 ou version ultérieure) ou HTTP(S)/8081 (serveur Dell Enterprise Server antérieur à la version v7.7)

Dell Key Server : TCP/8050

Dell Policy Proxy : TCP/8000

Dell 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

REMARQUE :
Si les droits de vos clients Enterprise Edition sont activés depuis l'usine ou si vous achetez des licences de l'usine, définissez le GPO sur le contrôleur du domaine pour activer ces droits (il se peut que le serveur n'exécute pas Enterprise Edition). Assurez-vous que le port sortant 443 est disponible pour communiquer avec le serveur. Si le port 443 est bloqué pour une raison quelconque, les droits ne pourront pas être octroyés. Pour plus d'informations, voir le document Enterprise Edition Advanced Installation Guide.

Créer une base de données Dell

3 Si vous ne possédez pas encore une base de données SQL configurée pour Dell Enterprise Server, le programme d'installation crée la base de données automatiquement au cours de l'installation. Si vous préférez configurer une base de données avant d'installer Dell Enterprise Server, suivez les instructions ci-dessous pour créer la base de données SQL et l'utilisateur SQL dans SQL Management Studio. ***Ces instructions sont facultatives car le programme d'installation créera une base de données pour vous s'il n'en existe pas déjà une.***

Lorsque vous installez Dell Enterprise Server, suivez les instructions de la section Installer le serveur principal avec une base de données existante.

Dell Enterprise 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 par défaut, après l'installation de Dell Enterprise Server, vous devez indiquer le port dynamique de l'instance sur l'onglet Database (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, voir https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

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.

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

Création d'une nouvelle base de données Windows SQL Server à l'aide de l'authentification Windows :

a Cliquez sur **Démarrer** > **Tous les programmes** > **Microsoft SQL Server** > **Management Studio**.

b Effectuez un clic droit sur le dossier Bases de données, puis cliquez sur Nouvelle base de données. La boîte de dialogue Propriétés de la base de données s'affiche.

c Saisissez le nom de la base de données et cliquez sur **OK**.

d Développez le dossier *Sécurité*, et effectuez un clic droit sur **Connexions**.

e Cliquez sur **Nouvelle connexion** afin de créer le propriétaire de la nouvelle base de données.

f Saisissez un nom d'utilisateur dans le champ *Name* (Nom).

g Sélectionnez l'option d'authentification *Authentification Windows*.

h Sélectionnez **Mappage de l'utilisateur**, puis mettez en surbrillance la nouvelle base de données.

i Sélectionnez le rôle de la base de données (db_owner), puis cliquez sur **OK**.

OU

Création d'une base de données SQL Server à l'aide de l'authentification SQL Server :

a Cliquez sur **Démarrer** > **Tous les programmes** > **Microsoft SQL Server** > **Management Studio**.

b Effectuez un clic droit sur le dossier *Bases de données*, puis cliquez sur **Nouvelle base de données**. La boîte de dialogue *Propriétés de la base de données* s'affiche.

c Saisissez le nom de la base de données et cliquez sur **OK**.

d Développez le dossier *Sécurité*, et effectuez un clic droit sur **Connexions**.

e Cliquez sur **Nouvelle connexion** afin de créer le propriétaire de la nouvelle base de données.

f Saisissez un nom d'utilisateur dans le champ *Name* (Nom).

g Sélectionnez l'option d'authentification *Authentification SQL Server*. Saisissez et confirmez le mot de passe.

h Désélectionnez **Appliquer l'expiration du mot de passe**.

i Sélectionnez **Mappage de l'utilisateur**, puis mettez en surbrillance la nouvelle base de données.

j Sélectionnez le rôle de la base de données (db_owner), puis cliquez sur **OK**.

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 Dell Enterprise Server d'installer ces composants.

Windows Server 2008 et Windows Server 2008 R2 – http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555

Installation de .NET Framework 4.5

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

Windows Server 2008 et Windows Server 2008 R2 – https://www.microsoft.com/en-us/download/details.aspx?id=42643

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 Dell Enterprise Server d'installer ce composant.

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

Configurez l'autorité de certification Microsoft (MSCEP)

Cette étape n'est nécessaire sur votre serveur exécutant MSCEP que si vous prévoyez d'utiliser iOS avec Mobile Edition.

7 Configurez MSCEP.

Windows Server 2008 R2 doit correspondre à l'édition Enterprise Edition. ***Standard Edition ne permettra pas d'installer le rôle MSCEP***.

a Ouvrez le gestionnaire de serveur. Dans le menu de gauche, sélectionnez **Rôles de serveur** et cochez la case en regard de **Services de certificat Active Directory**. Cliquez sur **Suivant**. L'Assistant d'ajout de rôles vous fait passer aux étapes suivantes.

Dans *AD CS* > *Services de rôle*, cochez les cases en regard des services de rôle **Autorité de certification** et **Enregistrement Web de l'autorité de certification**. Sélectionnez **Ajouter les services de rôles requis pour le serveur Web (IIS)** (le cas échéant). Cliquez sur **Suivant**.

Dans *AD CS > Type de configuration*, sélectionnez **Autonome**. Cliquez sur **Suivant**.

Dans *AD CS > Type de CA*, sélectionnez **CA subordonnée**. Cliquez sur **Suivant**.

Dans *AD CS > Clé privée*, sélectionnez **Créer une nouvelle clé privée**. Cliquez sur **Suivant**.

Dans *AD CS > Clé privée > Cryptographie*, gardez les valeurs par défaut **RSA#Microsoft Software Key Storage Provider**, **2048** et **SHA1**. Cliquez sur **Suivant**.

Dans *AD CS > Clé privée > Nom de l'autorité de certification*, gardez toutes les valeurs par défaut. Cliquez sur **Suivant**.

Dans *AD CS > Clé privée > Demande de certificat.*, sélectionnez **Envoyer une demande de certificat à un parent : autorité de certification**. Sélectionnez **Parcourir par : nom d'autorité de certification**. Allez à et sélectionnez **Autorité de certification parent**. Cliquez sur **Suivant**.

Dans *AD CS > Base de données de certificats*, gardez les valeurs par défaut. Cliquez sur **Suivant**.

Dans *Serveur Web (IIS),* cliquez sur **Suivant**.

Dans Serveur Web (IIS) > *Services de rôle*, gardez les valeurs par défaut. Cliquez sur **Suivant**.

Dans *Confirmation*, cliquez sur **Installer**.

Dans *Résultats*, examinez les résultats et cliquez sur **Fermer**.

Dans *Gestionnaire de serveur > Rôles*, sélectionnez **Ajouter des services de rôle** sous *Services de certificat Active Directory*.

Lorsque la fenêtre *Sélectionnez les services de rôles* s'affiche, cochez la case en regard de **Service d'enregistrement de périphérique réseau**. Cliquez sur **Suivant**.

Ajoutez le compte utilisateur que le *Service d'enregistrement de périphérique réseau* doit utiliser lors de l'autorisation de demandes de certificat au Groupe d'utilisateurs IIS_IUSRS du serveur local. Le format est domaine\nom d'utilisateur. Cliquez sur **OK**.

Dans les fenêtres Spécifiez le compte d'utilisateur, sélectionnez l'utilisateur que vous venez d'ajouter au groupe IIS_IUSRS. Cliquez sur **Suivant**.

Dans la fenêtre *Spécifiez les informations de l'autorité d'enregistrement*, gardez les valeurs par défaut de *Informations requises* et *Ajoutez des informations facultatives* comme souhaité. Cliquez sur **Suivant**.

Dans la fenêtre *Configurer la cryptographie pour l'autorité d'enregistrement*, gardez les valeurs par défaut. Cliquez sur **Suivant**.

Dans la fenêtre *Confirmez les sélections d'installation*, cliquez sur **Installer**.

Dans la fenêtre *Résultats de l'installation*, examinez les résultats et cliquez sur **Fermer**.

Fermez le gestionnaire de serveur.

b Modifiez la clé de registre comme suit :

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c Ouvrez le gestionnaire des services Internet (IIS). Accédez à **\<ServerName > \Sites\Default Web Site\CertSrv \mscep_admin**.

Ouvrez *Authentification* et activez **Authentification anonyme**.

d Cliquez sur **Démarrer** > **Exécuter**. Saisissez *certsrv.msc* et cliquez sur **Entrée**.

Lorsque la fenêtre *certsrv* s'affiche, effectuez un clic droit sur le nom du serveur, sélectionnez **Propriétés** et cliquez sur l'onglet **Module de sratégie**.

Cliquez sur **Propriétés** et sélectionnez **Appliquer les paramètres du modèle de certificat, le cas échéant. Sinon, délivrer automatiquement le certificat.** Cliquez sur **OK**.

e Fermez le gestionnaire des services Internet (IIS).

f Redémarrez le serveur. Pour vérifier, ouvrez Internet Explorer et, dans la barre d'adresse, saisissez

http://server.domain.com/certsrv/mscep_admin/.

Fin de la configuration de Windows Server 2008 R2 pour MSCEP.

Windows Server 2012 R2 ou Windows Server 2016 :

a Suivez les instructions de configuration dans l'article, Services d'enregistrement de périphériques réseau (NDES) dans les services de certificat Active Directory (AD CS)..

b Modifiez la clé de registre comme suit :

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c Ouvrez le gestionnaire des services Internet (IIS). Accédez à **\<ServerName\Sites\Default Web Site\CertSrv\mscep_admin**.

Ouvrez *Authentification* et activez **Authentification anonyme**.

d Cliquez sur **Démarrer** > **Exécuter**. Saisissez *certsrv.msc* et cliquez sur **Entrée**.

Lorsque la fenêtre *certsrv* s'affiche, effectuez un clic droit sur le nom du serveur, sélectionnez **Propriétés** et cliquez sur l'onglet ***Module de stratégie***.

Cliquez sur **Propriétés** et sélectionnez **Appliquer les paramètres du modèle de certificat, le cas échéant. Sinon, délivrer automatiquement le certificat.** Cliquez sur **OK**.

e Fermez le gestionnaire des services Internet (IIS).

f Redémarrez le serveur. Pour vérifier, ouvrez Internet Explorer et, dans la barre d'adresse, saisissez

http://server.domain.com/certsrv/mscep_admin/.

Fin de la configuration de Windows Server 2012 R2/Windows Server 2016 pour MSCEP.

Installez/Configurez Microsoft Message Queuing (MSMQ)

Cette étape n'est nécessaire que si vous prévoyez d'utiliser Mobile Edition. Il s'agit d'une condition requise pour que EAS Device Manager et EAS Mailbox Manage puissent communiquer.

8 Sur Windows Server 2008 ou Windows Server 2008 R2 (sur le serveur hébergeant l'environnement Exchange) : http://msdn.microsoft.com/en-us/library/aa967729.aspx

OU

Sur Windows Server 2012 R2 :

a Ouvrez le gestionnaire de serveur.

b Accédez à **Gérer** > **Ajouter des rôles et fonctions.**

c Sur la page Before you Begin (Avant de commencer), cliquez sur **Suivant**.

d Sélectionnez **Installation à base de rôle ou de fonction**, puis cliquez sur **Suivant**.

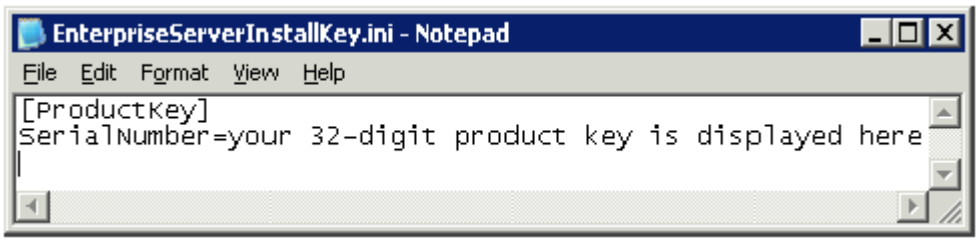
e Sélectionnez le serveur sur lequel installer la fonction, puis cliquez sur **Suivant** .

f Ne sélectionnez aucun rôle de serveur. Cliquez sur **Suivant**.

g Dans Fonctions, sélectionnez **File d'attente des messages**, puis cliquez sur **Installer**.

Facultatif

9 **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 Dell Enterprise 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 :

- Nouvelle installation : permet d'installer un nouveau Dell Enterprise Server.
- Mise à niveau et de migration : pour une mise à niveau à partir d'une version existante, fonctionnelle de Dell Enterprise Server v8.0 ou version ultérieure.
- Désinstaller Dell Enterprise Server : pour supprimer l'installation actuelle, si nécessaire.

  Si votre installation doit comprendre plusieurs serveurs principaux, 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 Enterprise Server* pour connaître les solutions palliatives ou les problèmes connus relatifs à l'installation de Enterprise Server.

Si le contrôle de compte d'utilisateur (UAC) est activé, désactivez-le. Sur Windows Server 2012 R2, le programme d'installation désactive UAC. 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. Si vous sélectionnez l'authentification Windows, les identifiants de l'utilisateur connecté sont utilisés. L'utilisateur doit posséder des droits administrateurs pour le système ainsi que les droits de créer et de gérer la base de données SQL (création de base de données, ajout d'utilisateur, et attribution des permissions). Pour l'authentification SQL, le compte utilisé doit posséder les mêmes droits. Ces identifiants sont utilisés au cours de l'installation. Le produit installé n'utilise pas ces identifiants.

En outre, au cours de l'installation, les identifiants d'authentification du service Runtime doivent être précisés afin de permettre aux services Dell d'accéder au serveur SQL. Le compte utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

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 base de données Dell 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 vivement d'installer SQL Server sur un serveur dédié.

La meilleure pratique consiste à installer le serveur principal avant d'installer et de configurer tout serveur frontal.

Les fichiers journaux d'installation se trouvent dans le répertoire : **C:\ProgramData\Dell\Dell Data Protection\Installer Logs**.

Nouvelle installation

Sélectionnez l'une des deux options d'installation du serveur principal :

- Installer un serveur principal et une nouvelle base : permet d'installer un nouveau serveur Dell Enterprise Server et une nouvelle base de données.
- Installer un serveur principal avec une base de données existante : permet d'installer un nouveau serveur Dell Enterprise Server et de vous connecter à une base de données SQL créée au cours de la configuration de pré-installation, ou d'une base de données SQL existant v9.x ou ultérieure, lorsque la version de schéma correspond à celle du serveur Dell Enterprise Server à installer. Vous devez migrer une base de données v8.x 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 le dernier outil de configuration de serveur ou pour migrer une base de données antérieure à la version 8.0, contactez Dell ProSupport pour obtenir de l'aide.

REMARQUE :
Si vous disposez d'un serveur Dell Enterprise Server v8.x ou version suivante fonctionnel, consultez les instructions dans **Mettre à niveau/migrer un ou des serveurs principaux**.

Si vous installez un serveur frontal, effectuez l'installation une fois le serveur principal installé :

- Installer un serveur frontal : permet d'installer un serveur principal pour communiquer avec un serveur principal.

Installer le serveur principal et une nouvelle base de données

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

2 Double-cliquez sur **setup.exe**.

3 Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'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 effectué l'étape 9 facultative dans Configuration de préinstallation, 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**.

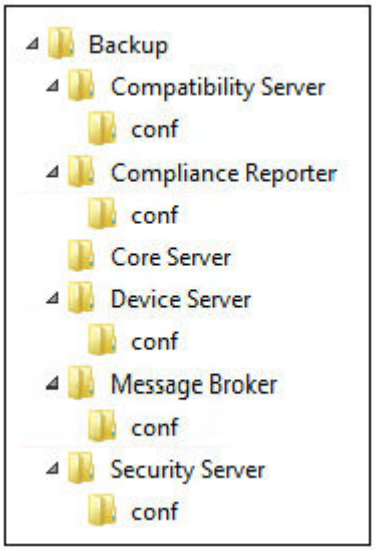
9 Pour installer Dell Enterprise Server dans l'emplacement par défaut **C: \Program Files\Dell**, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.

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 serveur.

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 Certificate Management Console.

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)

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

REMARQUE :
Par défaut, le certificat expire dans un an.

12 Pour Server Encryption (SE), 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)

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

REMARQUE :
Par défaut, le certificat expire dans un an.

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 frontal, sélectionnez **Fonctionne avec le serveur principal pour communiquer avec les clients en interne dans votre réseau ou en externe dans le DMZ**, puis saisissez le nom d'hôte du serveur de sécurité principal (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 Data Protection. 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 seront utilisés pour l'authentification (les champs Nom d'utilisateur et Mot de passe ne pourront 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 identifiants sont également utilisés par les services Dell lorsqu'ils utilisent Dell Enterprise 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 Dell Enterprise 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 redémarrer le serveur.

Installer le serveur frontal avec une base de données existante

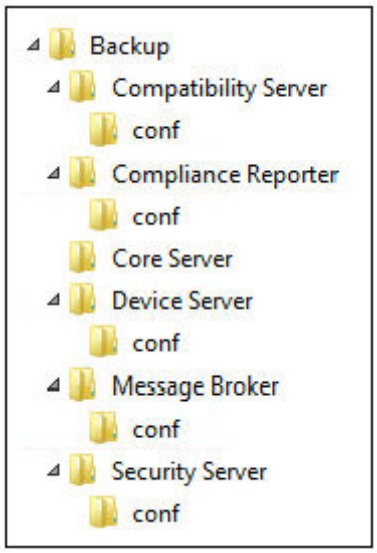
REMARQUE :
Si vous disposez d'un Dell Enterprise Server v8.x fonctionnel ou version ultérieure, voir les instructions qui se trouvent sous Mettre à niveau/Migrer un/des Serveur(s) principaux.

Vous pouvez installer un nouveau Dell Enterprise Server et vous connecter à une base de données SQL existante créée pendant la configuration de préinstallation, ou une base de données SQL existante v9.x ou ultérieure, lorsque la version du schéma correspond à la version de Dell Enterprise Server à installer.

Vous devez migrer une base de données v8.x 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 le dernier outil de configuration de serveur, ou **pour migrer une base de données antérieure à la version 8.0**, contactez Dell ProSupport pour obtenir une assistance**.**

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 Dell Enterprise 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 Dell Enterprise Server. L'accès à ces fichiers est nécessaire pour configurer Dell Enterprise 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 Dell Enterprise Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Dell Enterprise Server-x64 dans le répertoire racine du serveur où vous comptez installer Enterprise Server. ***Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.***
2 Double-cliquez sur **setup.exe**.
3 Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'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 effectué l'étape 9 facultative dans Configuration de préinstallation, 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**.

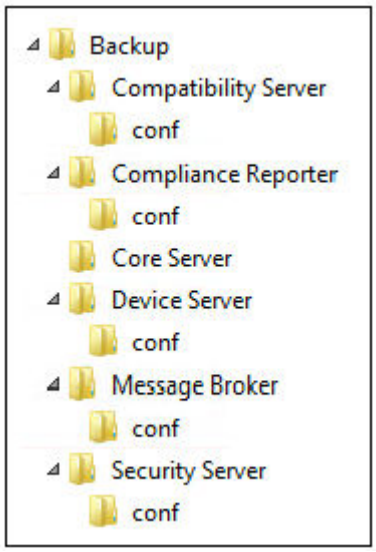
9 Pour installer Dell Enterprise Server dans l'emplacement par défaut **C: \Program Files\Dell**, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.

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 serveur.

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)

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

REMARQUE :

Par défaut, le certificat expire dans un an.

12 Pour Server Encryption (SE), 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

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)

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

> **REMARQUE :**
> **Par défaut, le certificat expire dans un an.**

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 frontal, sélectionnez **Fonctionne avec le serveur principal pour communiquer avec les clients en interne dans votre réseau ou en externe dans le DMZ**, puis saisissez le nom d'hôte du serveur de sécurité principal (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 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 seront utilisés pour l'authentification (les champs Nom d'utilisateur et Mot de passe ne pourront 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**.

15 Sélectionnez la méthode d'authentification correspondant au produit à utiliser. Il s'agit du compte utilisé par le produit pour travailler 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.

  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 doit être *uniquement* utilisée après avoir d'abord tenté de réinstaller la version correcte d'Enterprise Server, puis d'exécuter le dernier programme d'installation pour procéder à une mise à niveau.
  - L'option **Poursuivre sans migrer la base de données** installe les fichiers Enterprise 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 Dell Enterprise Server, il est considéré correspondre à une *récupération.* La boîte de dialogue suivante 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**.

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 redémarrer le serveur.

Install Front End Server(Installer un serveur frontal)(Installer et configurer le mode Proxy)

L'option Front End Server installation (Installation du serveur frontal/Mode Proxy) est une option frontale (mode DMZ) à utiliser avec Dell Enterprise 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'exécution du mode protégé Office. Ceci permet la communication entre n'importe quel périphérique à n'importe quel emplacement et sur le serveur frontal Dell. Assurez-vous que la sécurité réseau nécessaire est configurée avant d'utiliser la balise de rappel. La stratégie Activer une balise de rappel est activée par défaut.

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 Dell Enterprise Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Dell Enterprise Server-x64 dans le répertoire racine du serveur où vous comptez installer Enterprise Server. ***Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.***

2 Double-cliquez sur **setup.exe**.

3 Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'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 Entrez la clé de produit.

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

9 Pour installer le serveur frontal 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. **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)

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

> **REMARQUE :**
> **Par défaut, le certificat expire dans un an.**

11 Dans la boîte de dialogue *Configuration du serveur principal,* saisissez le nom d'hôte complet ou l'alias DNS du serveur principal, sélectionnez **Enterprise Edition**, 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 l'installation. Si vous déselectionnez 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 Dell Enterprise Server v8.0 et version ultérieure vers Dell Enterprise Server v9.x. Si la version de votre serveur est antérieure à v8.0, vous devez d'abord effectuez une mise à niveau vers v8.0, puis vers v9.x.

Avant de commencer la mise à niveau/migration

Avant de commencer, assurez-vous que toutes les tâches de configuration de préinstallation sont terminées. Cela est particulièrement important si vous déployez Mobile Edition.

Lisez les *conseils techniques concernant Enterprise Server* pour connaître les solutions palliatives ou les problèmes connus relatifs à l'installation de Dell Enterprise 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 base de données Dell 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, nous conseillons d'effectuer une mise à jour vers les dernières versions du serveur Dell Enterprise Server et des clients.

Prise en charge de Dell Enterprise Server v9.x :

- Enterprise Edition :
  - 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 v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Mise à niveau/migration depuis Dell Enterprise Server v8.x ou version ultérieure. (En cas de migration depuis un serveur Dell Enterprise Server antérieur à la version 8.x, contactez Dell ProSupport pour obtenir de l'aide.)

Lorsque vous mettez à niveau/migrez Dell Enterprise 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 oeuvre vos paramètres de règle préférentiels pour les nouvelles règles et non pas les valeurs par défaut.

En général, notre chemin de mise à niveau recommandé consiste à mettre à niveau/migrer Dell Enterprise Server et ses composants, puis à installer/mettre à niveau le client.

Appliquer les modifications de règles

1 Dans la Console de gestion à distance, connectez-vous en tant qu'administrateur Dell.

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

3 Entrez la description de la modification dans le champ Commentaire.

4 Cliquez sur **Valider les règles**.

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

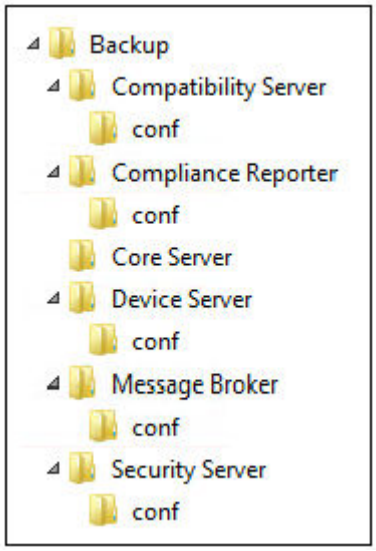
S'assurer que Dell Services est en cours d'exécution

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 aurez besoin de plusieurs fichiers de l'installation existante une fois le processus de mise à niveau/migration terminée.

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 Dell Enterprise Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Dell Enterprise Server-x64 dans le répertoire racine du serveur où vous comptez installer Enterprise Server. ***Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.***

2 Double-cliquez sur **setup.exe**.

3 Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'installation, puis cliquez sur **OK**.

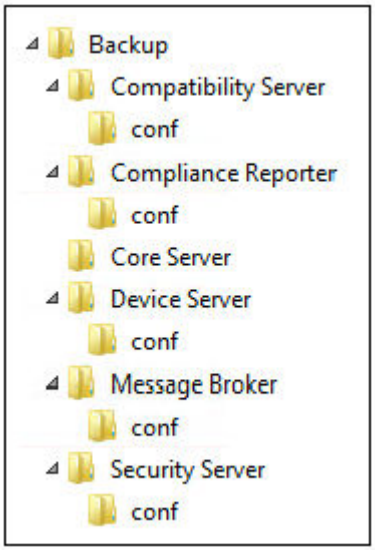
4 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.

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 seront utilisés pour l'authentification (les champs Nom d'utilisateur et Mot de passe ne pourront 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 redémarrer le serveur.

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

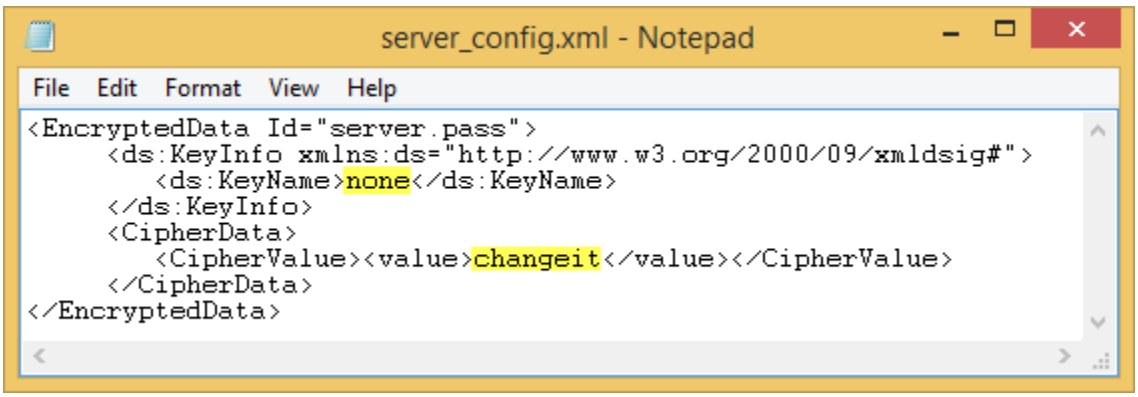
13 Dans la nouvelle installation, ouvrez le fichier <Compatibility Server install dir>\conf\server_config.xml, puis remplacez la valeur **server.pass** par celle du fichier sauvegardé <Compatibility Server install dir>\conf\server_config.xml, en procédant comme suit :

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 :

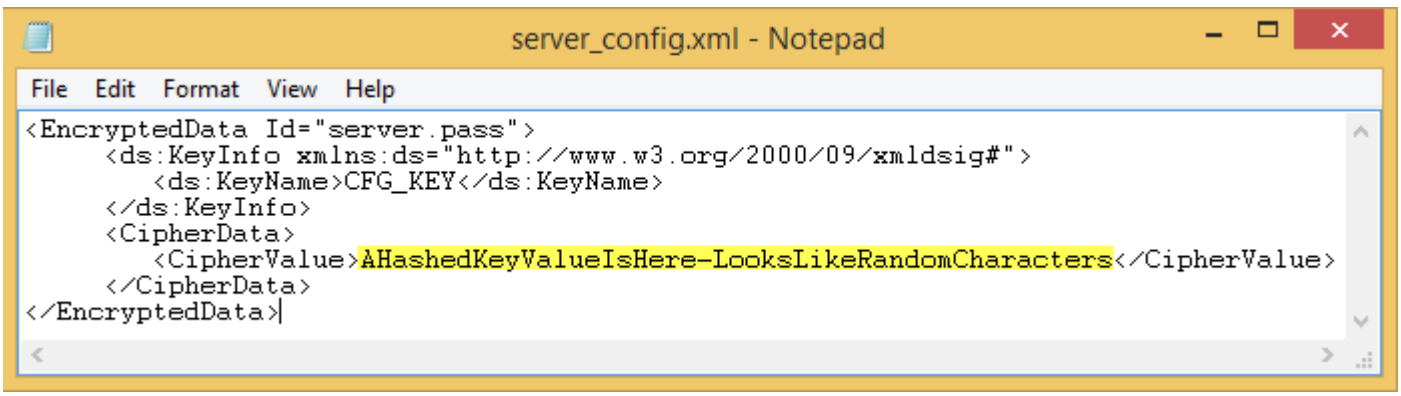
- Remplacez la valeur de *KeyName* **CFG_KEY** par **aucun**.
- Saisissez le mot de passe en clair et placez-le entre *<value> </value>*, par exemple, ici **<value>changeit</value>**.
- Lorsque Dell Enterprise Server démarre, le mot de passe en clair est crypté et la valeur cryptée remplace le texte 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 **Dell** Enterprise 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'exécution du mode protégé Office. Ceci permet la communication entre n'importe quel périphérique à n'importe quel emplacement et sur le serveur frontal Dell. La stratégie Activer une balise de rappel est activée par défaut. 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 Dell Enterprise Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Dell Enterprise Server-x64 dans le répertoire racine du serveur où vous comptez installer Enterprise Server. ***Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.***
2. Double-cliquez sur **setup.exe**.
3. Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'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 avant la fin des tâches de configuration post-installation.

Installation du mode déconnecté

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

Enterprise 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.
AIRGAP=1 : cette valeur doit être définie sur « 1 » pour installer Enterprise 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).

Paramètres

SSOS_STATENAME

DISPLAY_SQLSERVER : cette valeur sera analysée afin d'obtenir les informations de serveur, d'instance et de port.

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 le serveur SQL. Pour utiliser l'authentification SQL, définissez cette valeur sur 1.

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 utilisent Dell Enterprise 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/nomutilisateur. 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. 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.

Paramètres

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 de Message Broker.

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

SERVERPORT_CLIENTAUTH : facultatif.

REPORTERPORT : facultatif.

DEVICEPORT : facultatif.

KEYSERVERPORT : facultatif.

GKPORT : facultatif.

TIGAPORT : facultatif.

SMTP_PORT : facultatif.

ACTIVEMQ_TCP : facultatif.

ACTIVEMQ_STOMP : facultatif.

Installation d'Enterprise Server en mode Déconnecté

Dans l'exemple suivant, Enterprise 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\" "
```

Désinstaller Dell Enterprise Server

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

Configuration postérieure à l'installation

Lisez les *conseils techniques concernant Entreprise Server* pour connaître les solutions palliatives ou les problèmes connus relatifs à la configuration de Dell Enterprise Server.

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

Installation et configuration de la gestion EAS

Cette section doit être appliquée si vous prévoyez d'utiliser Mobile Edition. Dans le cas contraire, ignorez la section et passez à Configuration de Dell Secrurity Server en mode DMZ.

Pré-requis

- Le compte de connexion du service de gestionnaire de boîtes aux lettres EAS doit être un compte autorisé à créer/modifier des règles Exchange ActiveSync, à attribuer des règles aux boîtes aux lettres des utilisateurs et à rechercher des informations sur les périphériques ActiveSync.
- Vous devez exécuter l'utilitaire de configuration EAS avec les droits d'administrateur pour pouvoir modifier les fichiers et redémarrer les services.
- La connexion réseau à Dell Policy Proxy est requise.
- Munissez-vous du nom de domaine complet de Dell Policy Proxy.
- Munissez-vous du numéro de port de Dell Policy Proxy.
- La file d'attente MSMQ doit déjà être installée et configurée sur le serveur hébergeant l'environnement Exchange. Si tel n'est pas le cas,, reportez-vous à Installer/Configurer Microsoft Message Queuing (MSMQ)

Pendant le processus de déploiement

Si vous avez l'intention d'utiliser Exchange ActiveSync pour gérer les périphériques mobiles via Mobile Edition, votre environnement Exchange Server doit être configuré.

Installer le gestionnaire de périphériques EAS

1 Sur le support d'installation Dell , accédez au dossier Gestion EAS. À partir du dossier de gestionnaire de périphérique EAS, copiez le fichier setup.exe sur votre ou vos *serveur(s) d'accès au client Exchange*.

2 Double-cliquez sur le fichier **setup.exe** pour démarrer l'installation. Si votre environnement comprend plusieurs *serveurs d'accès au client Exchange*, exécutez ce programme d'installation sur chacun d'entre eux.

3 Sélectionnez la langue d'installation, puis cliquez sur **OK**.

4 Cliquez sur **Suivant** lorsque l'écran d'*accueil* s'affiche.

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

6 Cliquez sur **Suivant** pour installer EAS Device Manager dans l'emplacement par défaut **C: \inetpub\wwwroot\Dell\EAS Device Manager\.**

7 Cliquez sur **Installer** dans l'écran *Prêt pour commencer l'installation*.

Une fenêtre affichant l'avancée de l'installation apparaît.

8 Si vous le souhaitez, cochez la case pour afficher le journal Windows Installer, puis cliquez sur **Terminer**.

Installer le gestionnaire de boîtes aux lettres EAS

1 Sur le support d'installation Dell, accédez au dossier Gestion EAS. À partir du dossier de gestionnaire de boîtes aux lettres EAS, copiez le fichier setup.exe vers votre ou vos *Serveur(s) de boîtes aux lettres Exchange*.

2 Double-cliquez sur le fichier **setup.exe** pour démarrer l'installation. Si votre environnement comprend plusieurs *Serveurs de boîtes aux lettres Exchange*, exécutez ce programme d'installation sur chacun d'entre eux.

3 Sélectionnez la langue d'installation, puis cliquez sur **OK**.

4 Cliquez sur **Suivant** lorsque l'écran d'*accueil* s'affiche.

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

6 Cliquez sur **Suivant** pour installer EAS Mailbox Manager dans l'emplacement par défaut **C:\Program Files\Dell\EAS Mailbox Manager\.**

7 Dans l'écran Informations de connexion, saisissez les identifiants du compte d'utilisateur qui se connectera pour utiliser ce service.

Nom d'utilisateur : DOMAINE\Nom d'utilisateur

Mot de passe : mot de passe associé à ce nom d'utilisateur

Cliquez sur **Suivant**.

8 Cliquez sur **Installer** dan l'écran *Prêt pour commencer l'installation*.

Une fenêtre affichant l'avancée de l'installation apparaît.

9 Si vous le souhaitez, cochez la case pour afficher le journal Windows Installer, puis cliquez sur **Terminer**.

Utiliser l'utilitaire de configuration EAS

1 Sur le même ordinateur, accédez à **Démarrer** > **Utilitaire** > **de configuration EAS Dell** > **Configuration EAS** pour exécuter l'utilitaire de configuration EAS.

2 Cliquez sur **Configurer** pour configurer les paramètres de gestion EAS.

3 Saisissez les informations suivantes :

Nom de domaine complet de Dell Policy Proxy

Port de Dell Policy Proxy (le port par défaut est 8090)

Fréquence d'interrogation de Dell Policy Proxy (la valeur par défaut est 1 minute)

Cochez la case permettant d'exécuter le Gestionnaire de périphérique EAS en mode rapport uniquement (recommandé pendant le déploiement).

> **REMARQUE :**
> Le mode Rapport uniquement permet aux périphériques/utilisateurs inconnus d'avoir accès à Exchange ActiveSync tout en continuant à vous fournir des rapports sur le trafic. Une fois votre déploiement terminé, vous pouvez modifier ce paramètre pour renforcer la sécurité.

Cliquez sur **OK**.

4 Un message de confirmation s'affiche. Cliquez sur **Oui** pour redémarrer les services de gestion de boîtes aux lettres EAS et IIS.

5 Cliquez sur **Quitter** lorsque vous avez terminé.

Configurer les paramètres de gestion EAS

Une fois que votre déploiement est terminé et que vous êtes prêt à renforcer la sécurité, suivez les étapes ci-dessous.

1 Accédez à **Démarrer** > **Dell** > **Utilitaire de configuration EAS** > **Configuration EAS** afin d'exécuter l'utilitaire de configuration EAS.
2 Cliquez sur **Configurer** pour configurer les paramètres de gestion EAS.
3 Saisissez les informations suivantes :
Nom de domaine complet de Dell Policy Proxy

Port de Dell Policy Proxy (le port par défaut est 8090)

Fréquence d'interrogation de Dell Policy Proxy (la valeur par défaut est 1 minute)

Décochez la case correspondant à l'exécution du gestionnaire de périphérique EAS en mode rapport.

Cliquez sur **OK**.
4 Un message de confirmation s'affiche. Cliquez sur **Oui** pour redémarrer les services de gestionnaire de boîtes aux lettres EAS et IIS.
5 Cliquez sur **Quitter** lorsque vous avez terminé.

Configuration de Dell Security Server en mode DMZ

Si Dell 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 Dell Security Server dans le réseau privé.

Si un certificat approuvé est utilisé, ignorez cette section et passez à Enregistrement des notifications APN.

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

Utilisez Keytool pour importer le certificat de domaine DMZ

IMPORTANT:
Sauvegardez le fichier cacerts existant de **Dell** Security Server avant de suivre les instructions de Keytool. En cas d'erreur de configuration, vous pourrez revenir au fichier sauvegardé.

Hypothèses

- Dell Security Server a été installé avec un certificat non approuvé.
- Dell Security Server en mode DMZ a été installé à l'aide d'un certificat signé (Entrust, Verisign, etc.)
- Un fichier de certificat .pfx est disponible. Si votre certificat a besoin d'être convertie au format .pfx, reportez-vous à l'exportation d'un certificat vers .PFX à l'aide de Certificate Management Console.

Processus

1 Ajouter Keytool au chemin d'accès au système.

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

2 Utilisez Keytool pour lister le contenu du certificat de domaine approuvé que vous souhaitez importer. Prenez note du Nom d'alias indiqué.

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

3 Utilisez Keytool pour importer le contenu du certificat signé dans le fichier cacerts de Dell Security Server :

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

Pour -srcalias, vous devez recueillir cette information à partir du contenu exporté du certificat signé.

Pour -destalias, cela peut être tout emplacement de votre choix.

4 Sauvegardez et remplacez le fichier cacerts actuel dans le répertoire <Security Server install dir>\conf\ par le nouveau fichier cacerts créé sur Dell Security Server.

Modifiez le fichier application.properties

Modifiez le fichier application.properties pour spécifier l'alias du cert. de signature.

1 Allez à <Rép. d'installation de Security Server>\conf\application.properties
2 Modifiez les informations suivantes :

Keystore.alias.signing=<remplacer cette valeur par la valeur de l'étape 3 ci-dessus pour `-destalias`>

3 Redémarrez Dell Security Server Service.

Enregistrement d'APN

Si vous avez l'intention d'utiliser Mobile Edition for Mobile Device Security avec des périphériques iOS, vous devez utiliser l'assistant d'enregistrement des notifications APN pour :

- Créer une CSR
- Créer un certificat Apple Push
- Charger un certificat Push

Si vous n'avez pas l'intention d'utiliser Mobile Edition for Mobile Device Security avec des périphériques iOS, ignorez cette section et passez à Server Configuration Tool (Outil de configuration de serveur).

Le service Apple Push Notification (APN) permet d'avoir des communications sans fil sécurisées avec les appareils iOS. Les notifications APN servent à envoyer une notification à un appareil iOS pour qu'il s'enregistre dans Dell Enterprise Server. APN envoie uniquement une notification à l'appareil, aucune donnée n'est envoyée.

Processus

1 Ouvrez un navigateur et rendez-vous sur https://<FQDN-of-security-server>:8443/csrweb.
2 Dans la boîte de dialogue de connexion de l'assistant d'enregistrement des APN, saisissez vos identifiants d'administrateur et cliquez sur **Connexion**.
3 Une boîte de dialogue décrivant les étapes à suivre s'affiche. Cliquez sur **Suivant**.

Étape I : Créez un CSR

4 Saisissez les informations suivantes :

E-mail : l'adresse e-mail peut être n'importe quel UPN, mais nous vous recommandons d'utiliser un compte pour l'administrateur qui maintiendra le certificat APN.

Nom courant : saisissez le nom courant associé à cette adresse e-mail.

Cliquez sur **Générer une CSR**.

5 Après avoir généré un CSR, enregistrez le fichier à un emplacement facilement accessible.
6 Cliquez sur **Suivant**.

Étape II : Créez un certificat Apple Push

7 Cliquez sur le lien vers le **Portail de certificats Apple Push**. Connectez-vous avec votre ID et mot de passe Apple.

8 Lisez les conditions d'utilisation, indiquez votre acceptation, et cliquez sur **Accepter**.

9 Cliquez sur **Parcourir** et **Envoyez** la demande de signature de certificat (CSR) que vous venez de créer.

10 Sur la page *Certificats pour serveurs tiers*, cliquez sur **Télécharger**. Enregistrez le fichier à un emplacement facilement accessible.

11 Revenez à l'Assistant Enregistrement d'APN et cliquez sur **Suivant**.

Étape III : Chargez le certificat Push

12 Saisissez les informations suivantes (utilisez les mêmes identifiants que dans). Étape I : Créer un CSR

E-mail :

Nom commun :

Téléverser le fichier de cert. : cliquez sur **Parcouri**r pour localiser le fichier enregistré dans l'**étape 7** Cliquez sur **Télécharger**.

13 Un message de confirmation s'affiche. Cliquez sur **Terminer**.

L'enregistrement du certificat des APN dans Dell Enterprise Server est terminée.

Outil de configuration serveur

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

L'outil de configuration de serveur Dell 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
- Configurer les paramètres de certificat SSL du serveur ou Mobile Edition
- 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

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

Pour lancer Dell Server Configuration Tool, accédez à **Démarrer** > **Programmes** > **Dell** > **Enterprise Edition** > **Server Configuration Tool** > **Exécuter Server Configuration Tool.**.

L'outil de configuration de serveur Dell se connecte à **C:\Program Files\Dell\Enterprise Edition\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 sera 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, Dell Device Server, etc.)
- Applications .NET (Dell Core Server)
- Validation de cartes à puce utilisées pour Preboot Authentication (Authentification de préamorçage) (Dell 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 Enterprise Edition gérés à distance avec des disques à cryptage automatique, ou BitLocker Manager.
- Postes de travail client :
  - Stations de travail exécutant BitLocker Manager
  - Postes de travail exécutant Enterprise Edition (clients Windows)
  - Postes de travail exécutant Endpoint Security Suite
  - 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 Dell 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 de 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 Dell Security Server. Pour en savoir plus, voir la section Créer un certificat auto-signé et générer une demande de signature de certificat (CSR). 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, cochez **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 d'Enterprise Server seront 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 d'Enterprise Server seront 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 d'Enterprise Server seront 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 d'Enterprise Server seront 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 Dell Enterprise 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 d'Enterprise Server seront 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 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**.

Importer un certificat Dell Manager.

Si votre déploiement comprend des clients Enterprise Edition gérés à distance avec des disques à auto-chiffrement ou BitLocker Manager, 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 gérés à distance, ainsi qu'à BitLocker Manager. 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 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 cliquez-droit 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 le champ `Nom de fichier`, saisissez 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 Dell Server Configuration Tool.

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

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 terminée.

Lorsque les modifications sont terminées :

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

2 Fermez Dell Server Configuration Tool.

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

Importer un certificat d'identité

Si votre déploiement le Cryptage du serveur, vous devez importer votre nouveau certificat (ou certificat existant). Le certificat d'identité sert à protéger la clé privée utilisée pour signer les ensembles de règles envoyés aux serveurs client. Ce certificat peut être indépendant des autres certificats.

1 Dans le menu supérieur, sélectionnez **Actions > Importer un certificat d'identité**.

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.

Configurer les paramètres de certificat SSL du serveur ou Mobile Edition

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

Dell Manager :

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

SCEP :

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

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**.

Configuration des paramètres SMTP pour Data Guardian ou les services de messagerie

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

Cet onglet permet de configurer les paramètres SMTP pour Data Guardian. Si les paramètres SMTP doivent être configurés à d'autres fins que pour Data Guardian, voir la rubrique d'aide à l'administrateur « Activation des notifications de licence par e-mail sur le serveur SMTP ».

Saisissez les informations suivantes :

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

2 Dans le champ Nom d'utilisateur, saisissez le nom de l'utilisateur qui se connectera au serveur de messagerie. Le format peut être DOMAINE\jdupont, jdupont ou toute autre formulation requise par votre société.

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

4 Dans le champ Adresse, saisissez 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 le champ Port, saisissez le numéro de port (en général, 25).

6 Dans le menu Authentification, sélectionnez Vrai ou 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 le Server Configuration Tool, cliquez sur l'onglet **Base de données**.

1 Dans le champ `Nom du serveur`, saisissez 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 recommande d'utiliser un nom de domaine complet, mais il est possible d'utiliser une adresse IP.

2 Dans le champ `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 le champ *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 le champ `Base de données`, entrez le nom de la base de données.

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

5 Dans le champ `Nom d'uitilisateur`, saisissez le nom d'utilisateur approprié associé à cette base de données.

6 Dans le champ `Mot de passe`, saisissez le mot de passe correspondant au nom d'utilisateur indiqué dans le champ 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 Dans la fenêtre *Test de la configuration*, lisez les informations concernant le test, puis cliquez sur **Suivant**.

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

11 Les résultats des tests des paramètres de connexion, de compatibilité et de migration de la base de données s'affichent dans la fenêtre *Tester la configuration*.

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 doit respecter la casse. Pour obtenir la liste des classements et la sensibilité à la casse, reportez-vous à 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 Dell Server Configuration Tool

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque *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 v8.x vers le dernier schéma avec la dernière version du Server Configuration Tool. Pour obtenir le dernier outil de configuration de serveur ou pour migrer une base de données antérieure à la version 8.0, contactez Dell ProSupport pour obtenir de l'aide.

Dans le Server Configuration Tool, cliquez sur l'onglet **Base de données**.

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

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

3 Un avertissement s'affiche dans la fenêtre *Migrer la base de données Enterprise*. 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 base de données et reprenez 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 Dell Server Configuration Tool.

3 Cliquez sur **Démarrer** > **Exécuter**. Tapez *services.msc* et cliquez sur **OK**. Lorsque *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 Dell, connectez-vous à l'adresse https://server.domain.com:8443/webui/. Les identifiants par défaut de 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 n'apparaît 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 Remote Management Console, Enterprise Server.
2 Connectez-vous à Remote Management Console Enterprise Server et 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 Entrez la description de la modification dans le champ Commentaire.
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*.
3 Deux méthodes d'authentification différentes sont prises en charge. Pour configurer, sélectionnez l'une des options suivantes :

- Configurer l'authentification SQL avec Compliance Reporter
- Configurer l'authentification Windows avec Compliance Reporter

Configurer l'authentification SQL avec Compliance Reporter

Depuis la version 8.1, la source de données est fournie préconfigurée. Aucune configuration n'est nécessaire. Suivez les étapes ci-dessous pour modifier la Source de données, si nécessaire.

1 Pour définir la Source de données, dans le menu supérieur, cliquez sur **Paramètres**. Dans le menu de gauche, cliquez sur **Source de données**.
2 Saisissez le nom d'utilisateur pour vous connecter à la base de données Dell.
3 Saisissez le mot de passe pour vous connecter à la base de données Dell.
4 Saisissez le nom d'hôte pour vous connecter à la base de données Dell.
5 Saisissez le nom de la base de données pour vous connecter à la base de données Dell.
6 Saisissez le nombre maximum de connexions inactives autorisées. La valeur par défaut est 2.
7 Saisissez le nombre maximum de connexions (actives) autorisées. La valeur par défaut est 10.
8 Entrez la valeur d'attente maximale (nombre maximum de millisecondes d'attente de connexion). -1 est indéfiniment.
9 Pour vérifier l'URL de la base de données et tester la connectivité entre Dell Compliance Reporter et la base de données Dell , cliquez sur **Tester la connexion**.
10 Cliquez sur **Mettre à jour**. Pour rejeter les informations, cliquez sur Annuler.

Les tâches administratives sont terminées. Le reste de ce chapitre porte sur l'authentification Windows et peut être ignoré si l'authentification SQL est utilisée pour Dell Compliance Reporter.

Si nécessaire, passez à Créer un certificat autosigné et Générer une requête de signature de certificat, ou Exporter un certificat vers .PFX à l'aide de Certificate Management Console.

Configurer l'authentification Windows avec Compliance Reporter

Depuis la version 8.1, la source de données est fournie préconfigurée. Aucune configuration n'est nécessaire. Suivez les étapes ci-dessous pour modifier la Source de données, si nécessaire.

1 Saisissez le nom d'utilisateur pour vous connecter à la base de données Dell.
2 Laissez le champ du mot de passe vide. Lorsque l'utilisateur du domaine se connecte, son mot de passe est enregistré dans la base de données.
3 Saisissez le nom d'hôte pour vous connecter à la base de données Dell.
4 Saisissez le nom de la base de données pour vous connecter à la base de données Dell.
5 Saisissez le nombre maximum de connexions inactives autorisées. La valeur par défaut est 2.
6 Saisissez le nombre maximum de connexions (actives) autorisées. La valeur par défaut est 10.

7 Entrez la valeur d'attente maximale (nombre maximum de millisecondes d'attente de connexion). -1 est indéfiniment.

8 Pour vérifier l'URL de la base de données et tester la connectivité entre Dell Compliance Reporter et la base de données Dell, cliquez sur **Tester la connexion**.

9 Cliquez sur **Mettre à jour**. Pour rejeter les informations, cliquez sur Annuler.

Les tâches administratives sont terminées. **Si nécessaire**, continuer pour créer un certificat autosigné et générer une requête de signature de certificat, ou exporter un certificat vers .PFX à l'aide de Certificate Management Console.

Réaliser des sauvegardes

À des fins de reprise après sinistre, assurez-vous que les emplacements suivants sont sauvegardés chaque semaine, avec les différentiels nocturnes :

Sauvegardes d'Enterprise 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\gkresource.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, il est recommandé d'appliquer les meilleures pratiques en matière de bases de données pour la base de données Dell et d'inclure le logiciel Dell au programme de reprise après sinistre de votre société.

Pour des informations supplémentaires sur les meilleures pratiques SQL, veuillez vous reporter àLa liste suivante explique les meilleures pratiques SQL server qui doivent être mises en œuvre lorsque Dell Data Protection est installé si celles ne le sont pas déjà.

Sauvegardes de PostgreSQL Server

Les événements d'audit sont stockés sur le serveur PostgreSQL, 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.

Descriptions des composants Dell

Le tableau suivant décrit chaque composant et sa fonction.

Nom	Description	Requis pour
Compliance Reporter (Rapporteur de conformité)	Fournit un aperçu complet de l'environnement d'audit et de génération de rapports de conformité. Composant de Dell Enterprise Server.	Rapports
Key Server	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. Composant de Dell Enterprise Server.	Utilitaires d'administration Dell
Outil de configuration serveur	Configure les communications de base de données avec Core Server et Compatibility Server/Security Server. Sert à initialiser la base de données à l'installation ou à la migrer vers un schéma plus récent. Utilisé pour les services Dell. Composant de Dell Enterprise Server.	Tous
Certificate Management Console, Enterprise Server Console	Console de gestion et centre de commande pour le déploiement à toute l'entreprise. Composant de Dell Enterprise Server.	Tous
Core Server	Gère le flux des stratégies, les licences et l'enregistrement de Preboot Authentication, SED Management, BitLocker Manager, Threat Protection et Advanced Threat Protection. Traite les données d'inventaire pour l'utilisation par Compliance Reporter (Rapporteur de conformité) et la Console de gestion à distance. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles. Composant de Dell Enterprise Server.	Tous
Security Server	Communique avec Policy Proxy, gère les extractions de clé de détection, les activations de clients, les produits Data Guardian, les communications SED-PBA et les communications Active Directory pour l'authentification ou le rapprochement, y compris la validation d'identité pour l'authentification dans la console de gestion	Tous

Nom	Description	Requis pour
	à distance. Exige l'accès à la base de données SQL. Composant de Dell Enterprise Server.	
Compatibility Server	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 de ce service. Composant de Dell Enterprise Server.	Tous
Service Courtier de messages	Gère les communications entre les services d'Enterprise Server. Organise les informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des stratégies. Exige l'accès à la base de données SQL. Composant de Dell Enterprise Server.	Tous
Device Server	Prend en charge les activations et la récupération de mot de passe. Composant de Dell Enterprise Server.	Édition Entreprise pour Mac Édition Entreprise pour Windows Handheld Shields CREDActivate
Mod. d'extension Device Server	Prend en charge divers composants. Composant de Dell Enterprise Server.	Tous
Identity Server (Serveur d'identité)	Traite les demandes d'authentification de domaine. Exige un compte Active Directory. Doit être le compte utilisé pour accéder à SQL lorsque l'Authentification Windows est utilisée. Composant de Dell Enterprise Server.	Tous
Policy Proxy (Proxy de stratégie)	Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité. Composant de Dell Enterprise Server.	Édition Entreprise pour Mac Édition Entreprise pour Windows Mobile Edition for Mobile Device Security
Security Token Services (STS)	Utilisé pour créer un canal d'authentification sécurisé entre l'interface utilisateur Dell Enterprise Server et les services principaux Dell.	Tous
Gestionnaire de périphériques EAS	Permet une fonctionnalité sans fil. Installé sur l'Exchange Client Access Server (Serveur d'accès au client Exchange).	Gestion d'appareils mobiles par Exchange ActiveSync.

Nom	Description	Requis pour
Gestionnaire de boîtes aux lettres EAS	L'agent de boîtes aux lettres qui est installé sur le serveur de boîtes aux lettres Exchange.	Gestion d'appareils mobiles par Exchange ActiveSync.

8

Meilleures pratiques SQL Server

La liste suivante explique les meilleures pratiques SQL server, qui doivent être mises en œuvre lorsque Dell Data Protection est installé 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 SQL Storage) 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 - http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29
   - 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 « Options de configuration de la mémoire des serveurs » dans les articles TechNet de Microsoft.

   - Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29
   - 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)

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 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29
   - 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

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

Certificats

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.

Nous vous recommandons 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 devrez 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 Dell Compliance Reporter, Dell Security Server ou Dell 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 pourront être résolus sans procéder à une réinstallation de **Dell** Enterprise 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 :

  <Compliance Reporter install dir>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =

<Device Server install dir>\conf\eserver.properties. Définissez la valeur eserver.keystore.password =

<Security Server install dir>\conf\eserver.properties. Définissez la valeur eserver.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 (par exemple, Sécurité).
- *Entreprise* : entrez la valeur appropriée (par exemple,).
- *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 de 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.

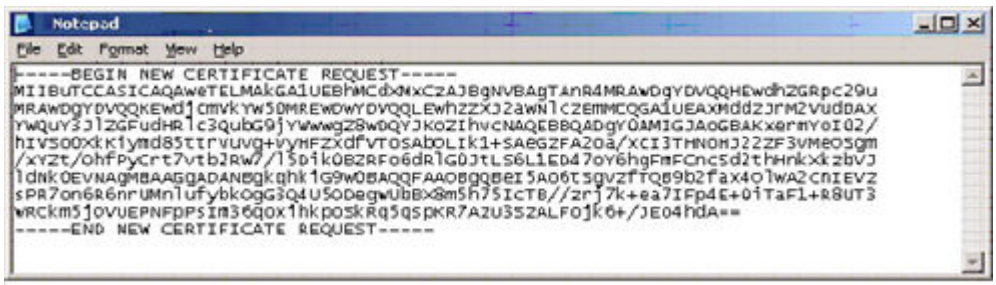
1 Substituez la même valeur utilisée précédemment pour <**certificatealias**>:

```
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 contiendra une paire BEGIN/END qui sera utilisée 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 pourra 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 Dell Compliance Reporter, Dell Security Server ou Dell Device Server, accédez au répertoire composant **conf**.
- Si vous activez SSL entre Dell Enterprise Server et le serveur d'annuaire d'entreprise, accédez à <**Dell install dir>\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 sera mis en place en interne par votre entreprise.

1 Naviguez jusqu'au serveur CA Microsoft. L'adresse IP sera 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. Renvoie à la fenêtre DOS. 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 montrera 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 Dell Security Server est utilisé en mode DMZ *et* lors de l'importation d'un certificat Dell Manager vers Dell Server Configuration Tool.

1 Ouvrez la console de gestion Microsoft (MMC).
2 Cliquez sur **Fichier** > **Ajouter/Supprimer un 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 cliquez-droit 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 d'enregistrement du fichier.
17 Dans le champ *Nom de fichier*, saisissez 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.