Getting Started

Dell Data Security Implementation Services

December 2023
Rev. A01

DELL Technologies

Remarques, précautions et avertissements

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

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

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

Contents

1

Phases de la mise en œuvre

Le processus de mise en œuvre de base comprend les phases suivantes :

- Activer Révision du lancement et des exigences
- Terminer la Préparation de la check-list - Implémentation initiale ou Préparation de la check-list - Mise à niveau/Migration
- Installer ou mettre à niveau/Migrer ***l'une*** des options suivantes :
  - ***Security Management Server***
    - Gestion centralisée des périphériques
    - Application Windows s'exécutant sous un environnement physique ou virtualisé.
  - ***Security Management Server Virtual***
    - Gestion centralisée de 3 500 périphériques maximum
    - S'exécute dans un environnement virtualisé

    Pour obtenir des instructions d'installation / de migration pour Dell Server, consultez les documents suivants : *Guide d'installation et de migration de* Security Management Server ou *Guide d'installation et de démarrage rapide de Security Management Server Virtual*. Pour obtenir ces documents, reportez-vous aux documents sur le Dell Data Security Server.
- Configurer la règle initiale
  - ***Security Management Server*** : voir le document *Guide d'installation et de migration de Security Management Server, tâches administratives Security Management Server*, disponible sur support.dell.com et *Aide administrateur*, disponible dans la console de gestion.
  - ***Security Management Server Virtual*** : voir le document *Guide d'installation et de démarrage rapide de Security Management Server Virtual, tâches administratives de la console de gestion Security Management Server Virtual*, disponible sur support.dell.com et *Aide administrateur*, disponible dans la console de gestion.
- Emballage client

  Pour obtenir les documents sur les conditions requises du client et sur l'installation du logiciel, sélectionnez ceux qui correspondent à votre déploiement :
  - *Guide d'installation de base d'Encryption Enterprise* ou *Guide d'installation avancée d'Encryption Enterprise*
  - *Guide d'installation de base d'Endpoint Security Suite Enterprise* ou *Guide d'installation avancée d'Endpoint Security Suite Enterprise*
  - *Guide de l'administrateur d'Advanced Threat Prevention*
  - *Guide d'installation d'Encryption Personal*
  - *Guide de l'administrateur d'Encryption Enterprise pour Mac*
  - *Guide de l'administrateur d'Endpoint Security Suite Enterprise pour Mac*
  - Pour obtenir ces documents, reportez-vous aux documents client Dell Data Security.
- Participer au transfert de connaissances de base de l'administrateur de Dell Security
- Mettre en œuvre les pratiques d'excellence
- Coordonner l'assistance au pilote ou au déploiement avec Dell Client Services

2

Révision du lancement et des exigences

Avant l'installation, il est important de comprendre votre environnement ainsi que les objectifs professionnels et techniques de votre projet, de manière à mettre en œuvre avec succès Dell Data Security et atteindre ces objectifs. Veillez à bien comprendre les exigences générales de votre entreprise en terme de sécurité des données.

Vous trouverez ci-après quelques questions courantes qui aideront l'équipe Dell Client Services à comprendre votre environnement et vos besoins :

1. Dans quel secteur d'activité évolue votre entreprise (soins de santé, etc.) ?
2. Quelles sont les exigences réglementaires dont vous disposez (HIPAA/HITECH, PCI, etc.) ?
3. Quelle est la taille de votre entreprise (nombre d'utilisateurs, nombre de sites physiques, etc.) ?
4. Quel est le nombre ciblé de points d'extrémité pour le déploiement ? Existe-t-il des projets de développement au-delà de ce nombre à l'avenir ?
5. Les utilisateurs disposent-ils de privilèges d'administrateur local ?
6. Quels sont les données et les dispositifs que vous devez gérer et crypter (disques fixes locaux, clés USB, etc.) ?
7. Quels produits envisagez-vous de déployer ?
   - Encryption Enterprise
     - Encryption (Droit DE) : Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager et Mac Encryption.
     - Encryption External Media
   - Endpoint Security Suite Enterprise
     - Advanced Threat Prevention : avec ou sans les fonctions facultatives de protection Web et de pare-feu client (droit ATP).
     - Encryption (Droit DE) : Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager et Mac Encryption.
     - Encryption External Media
8. Quel type de connectivité utilisateur est pris en charge par votre entreprise ? Ces types peuvent comprendre :
   - Connectivité au réseau LAN local seulement
   - Utilisateurs sans fil basés sur un réseau virtuel VPN et/ou sur le réseau de l'entreprise
   - Utilisateurs distants/déconnectés (utilisateurs non connectés au réseau directement ou via un VPN pendant des périodes prolongées)
   - Postes de travail n'appartenant pas au domaine
9. Quelles données devez-vous protéger au point d'extrémité ? De quel type de données disposent les utilisateurs typiques au point d'extrémité ?
10. Quelles applications des utilisateurs peuvent contenir des informations sensibles ? Quels sont les types de fichiers d'application ?
11. De combien de domaines disposez-vous dans votre environnement ? Combien d'entre eux se prêtent au chiffrement ?
12. Quels systèmes d'exploitation et quelles versions du système d'exploitation sont ciblés pour le chiffrement ?
13. Des partitions d'amorçage alternatif sont-elles configurées sur vos points d'extrémité ?
    a. Partition de récupération du fabricant
    b. Postes de travail à double-amorçage

Documents relatifs au client

Pour connaître la configuration requise pour l'installation, les versions de système d'exploitation prises en charge, les disques à autocryptage pris en charge et les instructions sur les clients que vous envisagez de déployer, reportez-vous aux documents applicables, répertoriés ci-dessous.

Encryption Enterprise (Windows) : consultez les documents suivants à l'adresse : www.dell.com/support/home/fr/fr/04/product-support/product/dell-data-protection-encryption/manuals.

- Guide d'installation avancée d'*Encryption Enterprise* : guide d'installation avec des commutateurs et des paramètres avancés pour des installations personnalisées.
- *Guide de l'utilisateur de Dell Data Security Console* : instructions pour les utilisateurs.

Encryption Enterprise (Mac) : consultez le Guide de l'administrateur d'*Encryption Enterprise pour Mac* à l'adresse www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Inclut les instructions d'installation et de déploiement.

Endpoint Security Suite Enterprise (Windows) : consultez les documents suivants à l'adresse https://www.dell.com/support/home/fr/fr/frbsdt1/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- Guide d'installation avancée d'*Endpoint Security Suite Enterprise* : guide d'installation avec des commutateurs et des paramètres avancés pour des installations personnalisées.
- Guide de démarrage rapide de *Endpoint Security Suite Enterprise Advanced Threat Prevention* : instructions pour l'administration, comprenant des règles recommandées, l'identification et la gestion des menaces et le dépannage.
- Guide de l'utilisateur de *Dell Data Security Console* : instructions pour les utilisateurs.

Endpoint Security Suite Enterprise (Mac) : consultez le document suivant à l'adresse https://www.dell.com/support/home/fr/fr/frbsdt1/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- Guide de l'administrateur d'*Endpoint Security Suite Enterprise pour Mac* : guide d'installation

Pour en savoir plus sur les disques à chiffrement automatique pris en charge, voir https://www.dell.com/support/article/us/en/04/sln296720.

Documents relatifs au serveur

Pour connaître la configuration requise pour l'installation, les versions du système d'exploitation prises en charge et les configurations du Dell Server que vous envisagez de déployer, reportez-vous aux documents applicables, listés ci-dessous.

Security Management Server

- Voir le *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)* sur

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

Security Management Server Virtual

- Reportez-vous au *Guide de démarrage rapide et d'installation de Security Management Server Virtual* sur

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

3

Liste de contrôle de la préparation - Mise en œuvre initiale

Selon le Dell Server que vous déployez, utilisez la checklist appropriée pour vous assurer de remplir toutes les conditions préalables avant d'installer Dell Encryption ou Endpoint Security Suite Enterprise.

- Liste de contrôle de Security Management Server
- Liste de contrôle de Security Management Server Virtual

Check-list concernant la mise en œuvre initiale de Security Management Server

Le nettoyage de l'environnement Proof of Concept est-il terminé (le cas échéant) ?

☐	La base de données et l'application Proof of Concept ont été sauvegardées et désinstallées (si vous utilisez le même serveur) avant l'engagement d'installation avec Dell. Pour en savoir plus sur une désinstallation, voir https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us.
☐	Tout point de terminaison de production utilisé pendant le test de Proof of Concept a été déchiffré ou les ensembles clés ont été téléchargés. Pour en savoir plus sur les clients que vous envisagez de déployer, voir Documents relatifs au client.

REMARQUE :

Toute nouvelle mise en œuvre doit commencer par une nouvelle base de données et l'installation du logiciel Encryption ou Endpoint Security Suite Enterprise. Dell Services clients ne procédera pas à une nouvelle mise en œuvre en utilisant un environnement POC. Les éventuels points de terminaison chiffrés dans un environnement POC devront être déchiffrés ou reconstruits avant l'engagement d'installation avec Dell.

Les serveurs répondent-ils aux spécifications logicielles requises ?

☐	Consultez Conception de l'architecture de Dell Security Management Server.

Les serveurs répondent-ils aux spécifications logicielles requises ?

☐	Windows Server 2012 R2 (Standard ou Datacenter), 2016 (Standard ou Datacenter), Windows Server 2019 (Standard ou Datacenter) ou Windows Server 2022 (Standard ou Datacenter) est installé. Ces systèmes d'exploitation peuvent être installés sur du matériel physique ou virtuel.
☐	La version 4.0 (ou ultérieure) de Windows Installer est installée.
☐	.NET Framework 4.6.1 est installé.
☐	Microsoft SQL Native Client 2012 est installé, si vous utilisez Microsoft SQL Server 2012 ou SQL Server 2016. SQL Native Client 2014 peut être utilisé, le cas échéant. **REMARQUE :** SQL Express n'est pas pris en charge avec un déploiement de production de Security Management Server.

☐	Le pare-feu Windows est désactivé ou configuré de manière à autoriser les ports (entrants) 8 000, 8 050, 8 081, 8 888 et 61 613.
☐	La connectivité est disponible entre Security Management Server et Active Directory (AD) sur les ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (entrants vers AD).
☐	L'UAC est désactivé avant l'installation sur Windows Server 2012 R2 lors de l'installation dans C:\Program Files. Il faut redémarrer le serveur pour que cette modification prenne effet. (Voir le Panneau de configuration Windows > Comptes utilisateurs). • Windows Server 2012 R2 : le programme d'installation désactive UAC. • Windows Server 2016 R2 : le programme d'installation désactive UAC. **REMARQUE :** Le contrôle de compte d'utilisateur (UAC) n'est plus désactivé de force, sauf si un répertoire protégé est spécifié pour le répertoire d'installation.

Les comptes de service créés ont-ils été créés avec succès ?

☐	Compte de service avec un accès en lecture seule à AD (LDAP) : un compte d'utilisateur/domaine de base est suffisant.
☐	Le compte de service doit disposer de droits d'administrateur local aux serveurs d'application Security Management Server.
☐	Pour utiliser l'authentification Windows pour la base de données, un compte de services de domaine doté de droits d'administrateur système. Le compte d'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.
☐	Pour utiliser l'authentification SQL, le compte SQL utilisé doit posséder des droits d'administrateur système sur SQL Server. Le compte d'utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

Le logiciel est-il téléchargé ?

Téléchargement à partir du site Web de support Dell.

☐	Les téléchargements de logiciel client Dell Data Security et de Security Management Server se trouvent dans le dossier **Pilotes et téléchargements** à l'adresse www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research ou www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research ou Sur la page Produit : http://www.dell.com/support 1. Sélectionnez **Pilotes et téléchargements**. 2. Dans la liste Systèmes d'exploitation, sélectionnez le système d'exploitation correspondant au produit que vous êtes en train de télécharger. Par exemple, pour télécharger Dell Enterprise Server, sélectionnez une des **l'une des options de Windows Server.** 3. Sous le titre de logiciel applicable, sélectionnez **Télécharger le fichier**.
☐	Si vous avez acheté Encryption ou Endpoint Security Suite Enterprise intégré, le logiciel peut être installé sur l'ordinateur cible à l'aide de Dell Digital Delivery.

OU

Effectuez le téléchargement depuis le site de transfert de fichiers (CFT) Dell Data Security.

☐	Le logiciel se trouve sur https://ddpe.credant.com dans le dossier **SoftwareDownloads**.

La clé d'installation et le fichier de licence sont-ils disponibles ?

☐	La clé de licence est incluse dans l'e-mail d'origine contenant les informations d'identification FTP. Voir Exemple d'email de notification au client. Cette clé est également incluse dans le téléchargement de l'application sur http://www.dell.com/support et https://ddpe.credant.com.
☐	Le fichier de licence est un fichier XML qui se trouve sur le site FTP dans le dossier **Licences client**.

REMARQUE :

Si vous avez acheté des licences intégrées, aucun fichier de licence n'est nécessaire. Le droit est téléchargé automatiquement depuis Dell lors de l'activation de tout nouveau client Encryption Personal, Encryption Enterprise ou Endpoint Security Suite Enterprise.

La base de données est-elle créée ?

☐	(Facultatif) Une nouvelle base de données est créée sur le serveur pris en charge. Voir la section Configuration requise et architecture dans le *Guide d'installation et de migration de Security Management Server*. Le programme d'installation de Security Management Server crée une base de données au cours de l'installation s'il n'en existe aucune.
☐	L'utilisateur de la base de données cible a reçu des droits **db_owner**.

Un pseudonyme DNS a-t-il été créé pour le Security Management Server et/ou des Proxy de stratégies avec Split DNS pour le trafic interne et externe ?

Il est recommandé de créer des pseudonymes DNS, pour facilité l'évolutivité. Cela vous permettra d'ajouter des serveurs supplémentaires par la suite ou de séparer des composants de l'application sans avoir besoin d'une mise à jour du client.

☐	Les alias DNS sont créés, le cas échéant. Alias DNS suggérés : • Security Management Server : dds.<domaine.com> • Serveur frontal : dds-fe.<domaine.com>

REMARQUE :

Split DNS permet à l'utilisateur d'employer le même nom DNS en interne et en externe. Cela signifie que nous pouvons fournir dds.<domaine.com> en interne comme nom c et le diriger vers Dell Security Management Server (back-end). En externe, nous pouvons fournir un enregistrement a pour dds.<domaine.com> et transmettre les ports concernés (voir Ports pour Security Management Server) au serveur frontal. Nous pouvons tirer profit de la permutation circulaire DNS ou d'un équilibreur de charge afin de répartir la charge sur les divers serveurs frontaux (s'il en existe plusieurs).

Envisagez-vous des certificats SSL ?

☐	Nous disposons d'une autorité de certification (CA) interne qui peut être utilisée pour signer des certificats et reconnue par tous les postes de travail de l'environnement **ou** nous prévoyons d'acheter un certificat signé en utilisant une autorité de certification publique telle que VeriSign ou Entrust. Si vous utilisez une autorité de certification, informez l'Ingénieur Services clients Dell. Le certificat contient l'intégrité de la chaîne de confiance (root et intermédiaire) avec les signatures de clés publiques et privées.
☐	Les SAN (Subject Alternate Names) de la Demande de certificat correspondent aux alias DNS octroyés à chaque serveur en cours d'utilisation pour l'installation du Dell Server. Ne s'applique pas aux demandes de certificats Wildcard ou Self-signed (autosignés).
☐	Le certificat est généré au format .pfx.

Modifier les exigences de contrôle identifiées et communiquées à Dell ?

☐	Envoyez toute exigence spécifique de contrôle des modifications pour l'installation d'Encryption ou Endpoint Security Suite Enterprise à Dell Services clients avant de lancer l'installation. Ces exigences peuvent comprendre des modifications du (des) serveur(s) d'application, de la base de données et des postes de travail du client.

Le matériel de test est-il préparé ?

☐	Préparez au moins trois ordinateurs avec votre image informatique d'entreprise à utiliser pour les tests. Dell recommande de **ne pas** utiliser les ordinateurs de production pour les tests. Ceux-ci doivent être utilisés pendant un pilote de production après que des politiques de chiffrement ont été définies et testées à l'aide du Plan de test fourni par Dell.

Check-list de la mise en œuvre initiale de Security Management Server Virtual

Le nettoyage de l'environnement Proof of Concept est-il terminé (le cas échéant) ?

☐	La base de données et l'application Proof of Concept ont été sauvegardées et désinstallées (si vous utilisez le même serveur) avant l'engagement d'installation avec Dell. Pour en savoir plus sur une désinstallation, voir https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us
☐	Tout point de terminaison de production utilisé pendant le test de Proof of Concept a été déchiffré ou les ensembles clés ont été téléchargés. Pour en savoir plus sur les clients que vous envisagez de déployer, voir Documents relatifs au client.

REMARQUE :

Toute nouvelle mise en œuvre doit commencer par une nouvelle base de données et l'installation du logiciel Encryption ou Endpoint Security Suite Enterprise. Dell Services clients ne procédera pas à une nouvelle mise en œuvre en utilisant un environnement POC. Les éventuels points de terminaison chiffrés dans un environnement POC devront être déchiffrés ou reconstruits avant l'engagement d'installation avec Dell.

Les comptes de service créés ont-ils été créés avec succès ?

☐	Compte de service avec un accès en lecture seule à AD (LDAP) : un compte d'utilisateur/domaine de base est suffisant.

Le logiciel est-il téléchargé ?

☐	Les téléchargements de logiciel client Dell Data Security et de Security Management Server se trouvent dans le dossier **Pilotes et téléchargements** à l'adresse www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research ou www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research ou Sur la page Produit : http://www.dell.com/support 1. Sélectionnez **Pilotes et téléchargements**. 2. Dans la liste Systèmes d'exploitation, sélectionnez le système d'exploitation correspondant au produit que vous êtes en train de télécharger. Par exemple, pour télécharger Dell Enterprise Server, sélectionnez une des **l'une des options de Windows Server.**

	3. Sous le titre de logiciel applicable, sélectionnez **Télécharger le fichier**.
☐	Si vous avez acheté Encryption ou Endpoint Security Suite Enterprise intégré, le logiciel peut être installé sur l'ordinateur cible à l'aide de Dell Digital Delivery.

Les fichiers de licence sont-ils disponibles ?

☐	Le fichier de licence est un fichier XML qui se trouve sur le site ddpe.credant.com dans le dossier **Licenses client**.

REMARQUE :

Si vous avez acheté des licences intégrées, aucun fichier de licence n'est nécessaire. Le droit est téléchargé automatiquement depuis Dell lors de l'activation de tout nouveau client Encryption ou Endpoint Security Suite Enterprise.

Les serveurs répondent-ils aux spécifications logicielles requises ?

☐	Voir Conception de l'architecture de Security Management Server Virtual.

Un alias DNS a-t-il été créé pour Security Management Server Virtual et/ou des proxy de stratégies avec Split DNS pour le trafic interne et externe ?

Il est recommandé de créer des pseudonymes DNS, pour facilité l'évolutivité. Cela vous permettra d'ajouter des serveurs supplémentaires par la suite ou de séparer des composants de l'application sans avoir besoin d'une mise à jour du client.

☐	Les alias DNS sont créés, le cas échéant. Alias DNS suggérés : • Security Management Server : dds.<domaine.com> • Serveur frontal : dds-fe.<domaine.com>

REMARQUE :

Split DNS permet à l'utilisateur d'employer le même nom DNS en interne et en externe. Cela signifie que nous pouvons fournir dds.<domaine.com> en interne comme nom c et le diriger vers Dell Security Management Server (back-end). En externe, nous pouvons fournir un enregistrement a pour dds.<domaine.com> et transmettre les ports concernés (voir Ports pour Security Management Server Virtual) au serveur frontal. Nous pouvons tirer profit de la permutation circulaire DNS ou d'un équilibreur de charge afin de répartir la charge sur les divers serveurs frontaux (s'il en existe plusieurs).

Envisagez-vous des certificats SSL ?

☐	Nous disposons d'une autorité de certification (CA) interne qui peut être utilisée pour signer des certificats et reconnue par tous les postes de travail de l'environnement **ou** nous prévoyons d'acheter un certificat signé en utilisant une autorité de certification publique telle que VeriSign ou Entrust. En cas d'utilisation d'une autorité de certification, veuillez informer l'Ingénieur Dell Client Services.

Modifier les exigences de contrôle identifiées et communiquées à Dell ?

☐	Envoyez toute exigence spécifique de contrôle des modifications pour l'installation d'Encryption ou Endpoint Security Suite Enterprise à Dell Services clients avant de lancer l'installation. Ces exigences peuvent comprendre des modifications du (des) serveur(s) d'application, de la base de données et des postes de travail du client.

Le matériel de test est-il préparé ?

☐	Préparez au moins trois ordinateurs avec votre image informatique d'entreprise à utiliser pour les tests. Dell recommande de **ne pas** utiliser les ordinateurs de production pour les tests. Ceux-ci doivent être utilisés pendant un pilote de production après que des politiques de chiffrement ont été définies et testées à l'aide du Plan de test fourni par Dell.

4

Préparation de la check-list - Mise à niveau/ Migration

Cette check-list s'applique uniquement à Security Management Server.

REMARQUE :

Mettez à jour Security Management Server Virtual depuis le menu de configuration de base dans le terminal de votre Dell Server. Pour plus d'informations, reportez-vous au *Guide de démarrage rapide et d'installation de Security Management Server Virtual*.

Consultez la check-list suivante pour vous assurer de remplir toutes les conditions préalables avant de commencer à mettre à niveau Encryption ou Endpoint Security Suite Enterprise.

Les serveurs répondent-ils aux spécifications logicielles requises ?

☐	Windows Server 2012 R2 (Standard ou Datacenter), Windows Server 2016 (Standard ou Datacenter), Windows Server 2019 (Standard ou Datacenter) ou Windows Server 2022 (Standard ou Datacenter) est installé. Une autre solution est d'installer un environnement virtualisé. **REMARQUE :** La mise à jour vers Dell Server v11.0 ou une version supérieure nécessite Windows Server 2019 ou une version supérieure.
☐	La version 4.0 (ou ultérieure) de Windows Installer est installée.
☐	.NET Framework 4.6.1 est installé.
☐	Microsoft SQL Native Client 2012 est installé, si vous utilisez Microsoft SQL Server 2012 ou SQL Server 2016. SQL Native Client 2014 peut être utilisé, le cas échéant. **REMARQUE :** SQL Express n'est pas pris en charge avec Security Management Server.
☐	Le pare-feu Windows est désactivé ou configuré de manière à autoriser les ports (entrants) 8 000, 8 050, 8 081, 8443, 8 888 et 61 613.
☐	La connectivité est disponible entre Security Management Server et Active Directory (AD) sur les ports 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (entrants vers AD).
☐	L'UAC est désactivé avant l'installation sur Windows Server 2012 R2 lors de l'installation dans C:\Program Files. Il faut redémarrer le serveur pour que cette modification prenne effet. (Voir le Panneau de configuration Windows > Comptes utilisateurs). • Windows Server 2012 R2 : le programme d'installation désactive UAC. • Windows Server 2016 R2 : le programme d'installation désactive UAC.

Les comptes de service créés ont-ils été créés avec succès ?

☐	Compte de service avec un accès en lecture seule à AD (LDAP) : un compte d'utilisateur/domaine de base est suffisant.
☐	Le compte de service doit disposer de droits d'administrateur local aux serveurs d'application Security Management Server.
☐	Pour utiliser l'authentification Windows pour la base de données, un compte de services de domaine doté de droits d'administrateur système. Le compte d'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.
☐	Pour utiliser l'authentification SQL, le compte SQL utilisé doit posséder des droits d'administrateur système sur SQL Server. Le compte d'utilisateur doit posséder le Schéma par défaut de permissions du serveur SQL : dbo et Database Role Membership : dbo_owner, public.

La base de données et tous les fichiers nécessaires sont-ils sauvegardés ?

☐	La totalité de l'installation existante est sauvegardée dans un autre emplacement. La sauvegarde doit comprendre la base de données SQL, secretKeyStore et les fichiers de configuration.
☐	Assurez-vous que ces fichiers critiques, qui stockent des informations nécessaires pour la connexion à la base de données, sont sauvegardés : <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

La clé d'installation et le fichier de licence sont-ils disponibles ?

☐	La clé de licence est incluse dans le courriel d'origine avec les informations d'indentification CFT. Voir Exemple d'email de notification au client. Cette clé est également incluse dans le téléchargement de l'application sur http://www.dell.com/support et https://ddpe.credant.com.
☐	Le fichier de licence est un fichier XML qui se trouve sur le site CFT dans le dossier **Client Licences**.

REMARQUE :

Si vous avez acheté des licences intégrées, aucun fichier de licence n'est nécessaire. Le droit est téléchargé automatiquement depuis Dell lors de l'activation de tout nouveau client Encryption ou Endpoint Security Suite Enterprise.

Les logiciels (nouveaux et existants) de Dell Data Security sont-ils téléchargés ?

Effectuez le téléchargement depuis le site de transfert de fichiers (CFT) Dell Data Security.

☐	Le logiciel se trouve sur https://ddpe.credant.com dans le dossier **SoftwareDownloads**.
☐	Si vous avez acheté Encryption Enterprise ou Endpoint Security Suite Enterprise version « intégrée », le logiciel peut être installé à l'aide de Dell Digital Delivery. Le logiciel peut également être téléchargé depuis www.dell.com/support ou ddpe.credant.com.

Possédez-vous suffisamment de licences de point de terminaison ?

Avant la mise à niveau, assurez-vous que vous disposez d'un nombre suffisant de licences client pour couvrir tous les points de terminaison de votre environnement. Si vos installations dépassent actuellement votre nombre de licences, contactez votre agent commercial Dell avant de procéder à une mise à niveau ou à une migration. Dell Data Security procède à la validation des licences et empêche les activations si aucune licence n'est disponible.

☐	Je dispose d'un nombre suffisant de licences pour couvrir mon environnement.

Les enregistrements DNS sont-ils documentés ?

☐	Assurez-vous que les enregistrements DNS sont documentés et préparés pour la mise à jour si le matériel a été modifié.

Envisagez-vous des certificats SSL ?

☐	Nous disposons d'une autorité de certification (CA) interne qui peut être utilisée pour signer des certificats et reconnue par tous les postes de travail de l'environnement **ou** nous prévoyons d'acheter un certificat signé en utilisant une autorité de certification publique telle que VeriSign ou Entrust. Si vous utilisez une autorité de certification, informez l'Ingénieur Services clients Dell. Le certificat contient l'intégrité de la chaîne de confiance (root et intermédiaire) avec les signatures de clés publiques et privées.
☐	Les SAN (Subject Alternate Names) de la Demande de certificat correspondent aux pseudonymes DNS octroyés à chaque serveur en cours d'utilisation pour l'installation du Dell Enterprise Server. Ne s'applique pas aux demandes de certificats Wildcard ou Self-signed (autosignés).
☐	Le certificat est généré au format .pfx.

Modifier les exigences de contrôle identifiées et communiquées à Dell ?

☐	Envoyez toute exigence spécifique de contrôle des modifications pour l'installation d'Encryption ou Endpoint Security Suite Enterprise à Dell Services clients avant de lancer l'installation. Ces exigences peuvent comprendre des modifications du (des) serveur(s) d'application, de la base de données et des postes de travail du client.

Le matériel de test est-il préparé ?

☐	Préparez au moins trois ordinateurs avec votre image informatique d'entreprise à utiliser pour les tests. Dell recommande de **ne pas** utiliser les ordinateurs de production pour les tests. Ceux-ci doivent être utilisés pendant un pilote de production après que des politiques de chiffrement ont été définies et testées à l'aide du Plan de test fourni par Dell.

5

Architecture

Cette section présente en détail les recommandations de conception de l'architecture pour la mise en œuvre de Dell Data Security. Sélectionnez le Dell Server que vous allez déployer :

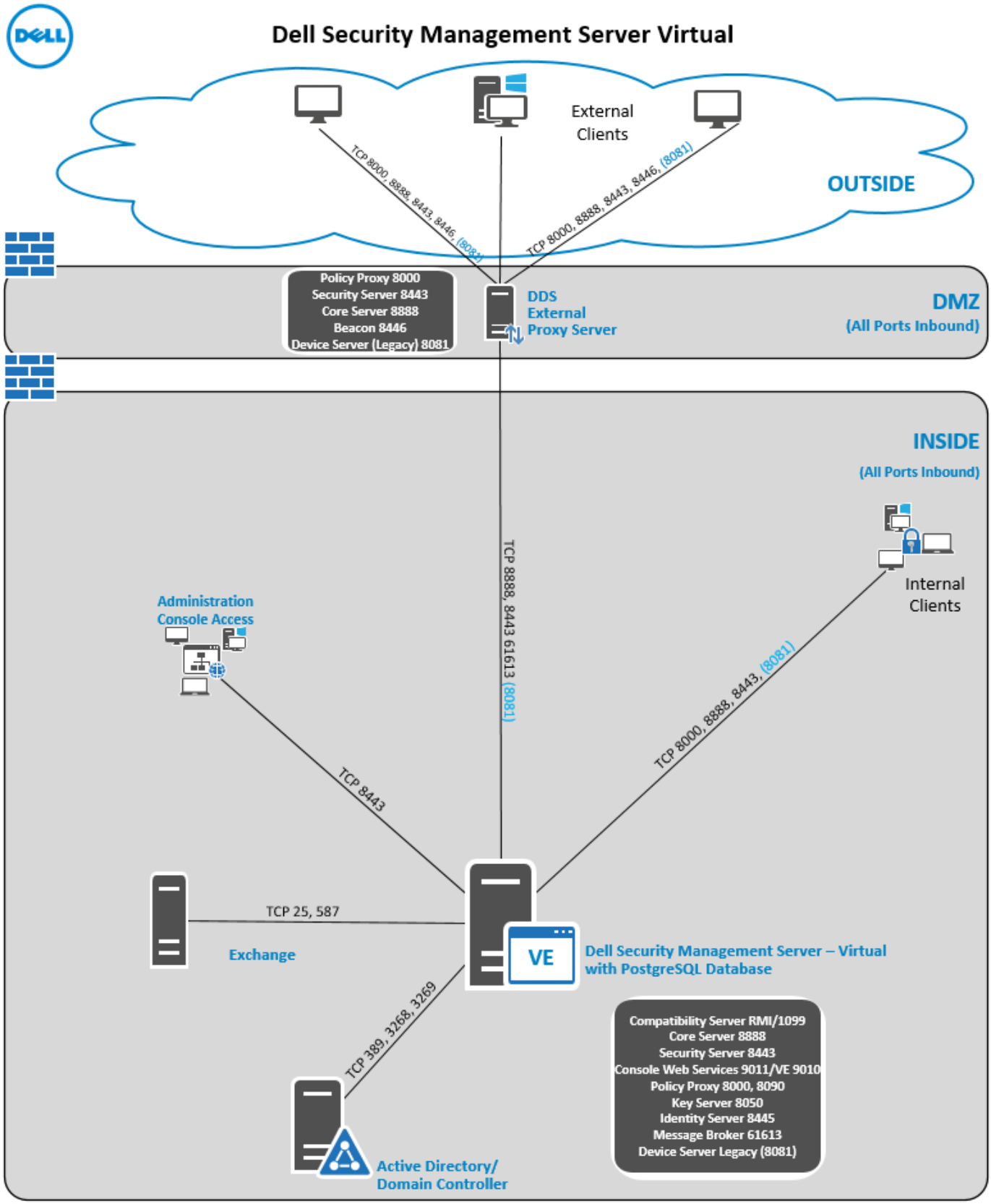
- Conception de l'architecture de Security Management Server
- Conception de l'architecture de Security Management Server Virtual

Conception d'architecture de Security Management Server Virtual

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

Composants d'architecture

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



Ports

Le tableau suivant décrit chaque composant et sa fonction.

Nom	Port par défaut	Description
Access Group Service	TCP/ 8006	Gère diverses autorisations et accès de groupe pour divers produits de sécurité Dell. **REMARQUE :** Le port 8006 n'est pas sécurisé pour le moment. Assurez-vous que ce port est correctement filtré par le biais d'un pare-feu. Ce port est interne uniquement.
Console de gestion	HTTPS/ 8443	Console de gestion et centre de commande pour le déploiement à toute l'entreprise.
Core Server	HTTPS/ 8887 (fermé)	Gère le flux des stratégies, les licences et l'enregistrement de Preboot Authentication, SED Management, BitLocker Manager, Threat Protection et Advanced Threat Prevention. Traite les données d'inventaire pour l'utilisation par la Console de gestion. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles.
Core Server HA (Haute disponibilité)	HTTPS/ 8888	Un service à haute disponibilité qui permet la sécurité et les performances augmentées des connexions HTTPS avec la Console de gestion, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection et Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Communique avec Policy Proxy, gère les extractions de clé de détection, les activations de client et les communications SED-PBA et Full Disk Encryption-PBA.
Compatibility Server	TCP/ 1099 (fermé)	Service de gestion de l'architecture d'entreprise. Collecte et stocke les données d'inventaire initiales lors de l'activation et les données des stratégies lors des migrations. Traite les données en fonction des groupes d'utilisateurs. **REMARQUE :** Le port 1099 doit être filtré via un pare-feu. Dell recommande que ce port soit uniquement interne.
Service Courtier de messages	TCP/ 61616 (fermé) et STOMP/	Gère les communications entre les services du Dell Server. Organise les informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des règles.

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

Nom	Port par défaut	Description
		peuvent être retournés. Par exemple, un service utilisateur n'a pas pu être retourné à l'aide du port 3268 dans la mesure où cet attribut n'est pas répliqué sur le catalogue global.
Authentification client	HTTPS/ 8449	Permet aux serveurs client de s'authentifier auprès du Dell Server. Requis pour Server Encryption.

Conception de l'architecture de Security Management Server

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

Composants d'architecture

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

Security Management Server

- Système d'exploitation : Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard ou Datacenter)
- Machine virtuelle ou physique
- CPU : 4 cœurs
- RAM : 16,00 Go
- Disque C : 30 Go d'espace disque disponible pour les journaux et les bases de données d'applications

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

Serveur proxy

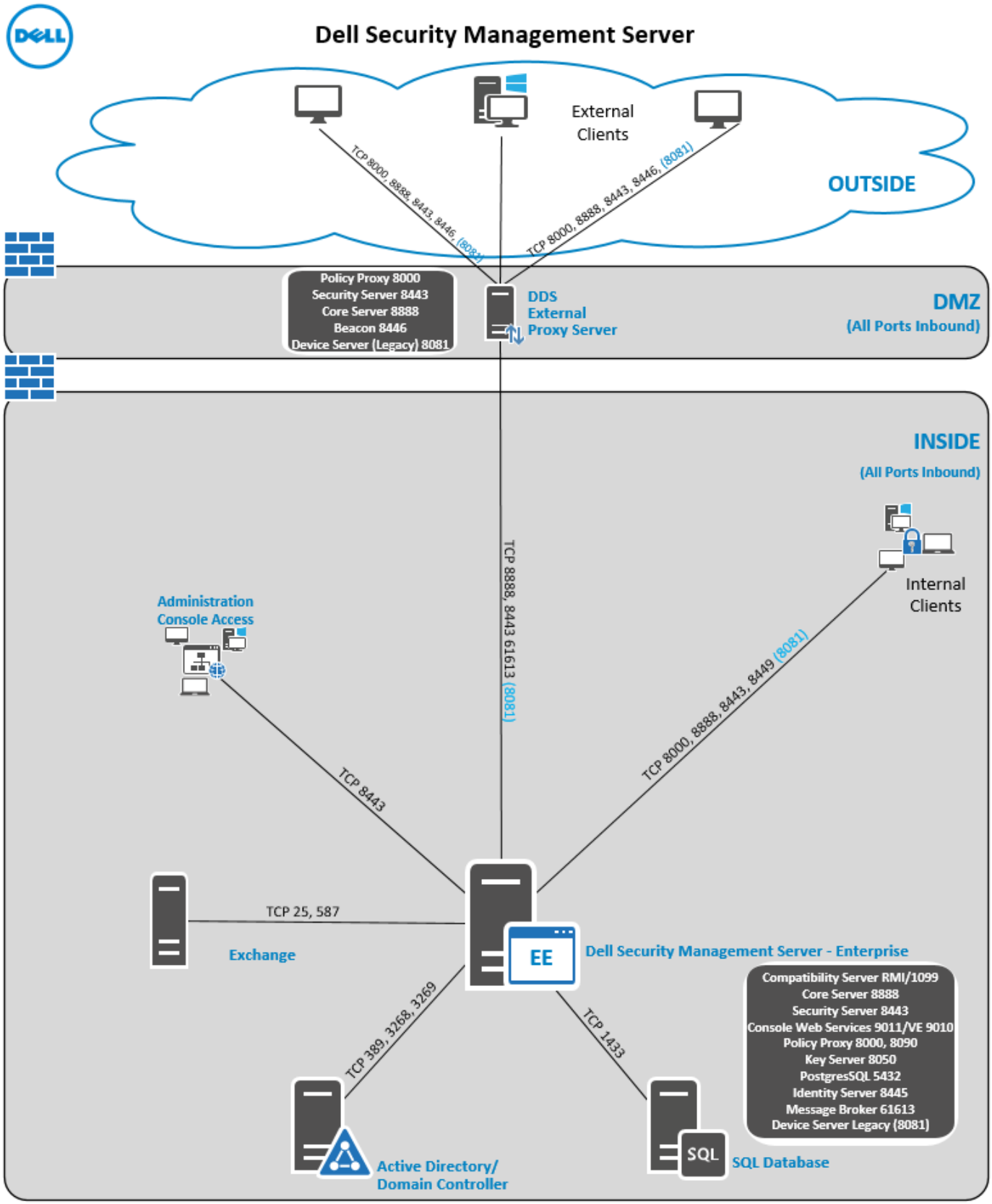
- Système d'exploitation : Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard ou Datacenter)
- Machine virtuelle
- CPU : 2 cœurs
- RAM : 8,00 Go
- Disque C : 20 Go d'espace disque disponible pour les journaux

Spécifications matérielles de SQL Server

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

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

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



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

Ports

Le tableau suivant décrit chaque composant et sa fonction.

Nom	Port par défaut	Description
Service ACL	TCP/ 8006	Gère diverses autorisations et accès de groupe pour divers produits de sécurité Dell. **REMARQUE :** Le port 8006 n'est pas sécurisé. Assurez-vous que ce port est correctement filtré par le biais d'un pare-feu. Ce port est interne uniquement.
Console de gestion	HTTP(S)/ 8443	Console de gestion et centre de commande pour le déploiement à toute l'entreprise.
Core Server	HTTPS/ 8888	Gère le flux des stratégies, les licences et l'enregistrement de Preboot Authentication, SED Management, BitLocker Manager, Threat Protection et Advanced Threat Prevention. Traite les données d'inventaire pour l'utilisation par la Console de gestion. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles.
Device Server	HTTPS/ 8081	Prend en charge les activations et la récupération de mot de passe. Composant de Security Management Server. Requis pour Encryption Enterprise (Windows et Mac)
Security Server	HTTPS/ 8443	Communique avec Policy Proxy, gère les extractions de clé de détection, les activations de client, les communications SED-PBA et Full Disk Encryption-PBA, et Active Directory pour l'authentification ou le rapprochement. Cela inclut la validation d'identité pour l'authentification dans la console de gestion. Exige l'accès à la base de données SQL.
Compatibility Server	TCP/ 1099	Service de gestion de l'architecture d'entreprise. Collecte et stocke les données d'inventaire initiales lors de l'activation et les données des stratégies lors des migrations. Traite les données en fonction des groupes d'utilisateurs. **REMARQUE :** Le port 1099 doit être filtré via un pare-feu.

Nom	Port par défaut	Description
		Dell Technologies recommande que ce port soit uniquement interne.
Service Courtier de messages	TCP/ 61616 et STOMP/ 61613	Gère les communications entre les services du Dell Server. Organise les informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des règles. Exige l'accès à la base de données SQL. **REMARQUE :** Le port 61616 doit être filtré via un pare-feu. Dell Technologies recommande que ce port soit uniquement interne. **REMARQUE :** N'ouvrez le port 61613 que sur les serveurs Security Management configurés en mode front-end.
Key Server	TCP/ 8050	Négocie, authentifie et crypte une connexion client grâce aux interfaces API Kerberos. Exige l'accès à la base de données SQL pour récupérer les données des clés.
Policy Proxy (Proxy de stratégie)	TCP/ 8000	Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité.
PostGres	TCP/ 5432	Base de données locale utilisée pour les données d'événement. **REMARQUE :** Le port 5432 doit être filtré via un pare-feu. Dell Technologies recommande que ce port soit uniquement interne.
LDAP	TCP/ 389/636 (contrôleur de domaine local), 3268/3269 (catalogue global) TCP/ 135/49125 + (RPC)	Port 389 : ce port est utilisé pour la demande d'informations auprès du contrôleur de domaine local. Les requêtes LDAP envoyées au port 389 peuvent être utilisées pour la recherche d'objets uniquement à l'intérieur du domaine d'accueil du catalogue global. Cependant, l'application de requête peut obtenir tous les attributs de ces objets. Par exemple, une requête au port 389 peut être utilisée pour obtenir un service utilisateur. Port 3268 : ce port est utilisé pour les requêtes ciblées spécifiquement sur le catalogue global. Les requêtes LDAP envoyées au port 3268 peuvent être utilisées pour la recherche d'objets dans l'ensemble de la forêt. Cependant, seuls les attributs marqués pour réplication sur le catalogue global

Nom	Port par défaut	Description
		peuvent être retournés. Par exemple, un service utilisateur n'a pas pu être retourné à l'aide du port 3268 dans la mesure où cet attribut n'est pas répliqué sur le catalogue global.
Base de données Microsoft SQL	TCP/ 1433	Le port de Serveur SQL par défaut est 1433 et une valeur aléatoire comprise entre 1 024 et 5 000 est attribuée aux ports du client.
Authentification client	HTTPS/ 8449	Permet aux serveurs client de s'authentifier auprès du Dell Server. Requis pour Server Encryption.

6

Meilleures pratiques SQL Server

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

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

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

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 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

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

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

   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

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

5. Vérifiez que les autorisations et les fonctionnalités sont adaptées à la base de données utilisée par Security Management Server. Pour plus d'informations, reportez-vous à l'article de la base de connaissances 124909.

7

Exemple d'e-mail de notification client

Après l'achat de Dell Data Security, vous recevrez un e-mail de DellDataSecurity@Dell.com. L'exemple ci-dessous montre un e-mail qui contient vos identifiants CFT et vos informations de clé de licence.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - U.S. & Canada Only
- Outside the U.S., click here for a list of numbers

Need Support? CHAT NOW! Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options