

Dell Data Protection

Prise en main de
Dell Data Protection

v9.4



© 2016 Dell Inc.

Marques déposées et marques utilisées dans la suite de documents Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools et Dell Data Protection | Cloud Edition : Dell™ et le logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® et KACE™ sont des marques de Dell Inc. Cylance® et le logo Cylance sont des marques déposées de Cylance, Inc. aux États-Unis et dans d'autres pays. McAfee® et le logo McAfee sont des marques ou des marques déposées de McAfee, Inc. aux États-Unis et dans d'autres pays. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, et Xeon® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. Adobe®, Acrobat® et Flash® sont des marques déposées d'Adobe Systems Incorporated. Authen Tec® et Eikon® sont des marques déposées d'Authen Tec. AMD® est une marque déposée d'Advanced Micro Devices, Inc. Microsoft®, Windows® et Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® et Visual C++® sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. VMware® est une marque déposée ou une marque de VMware, Inc. aux États-Unis ou dans d'autres pays. Box® est une marque déposée de Box. DropboxSM est une marque de service de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® et Google™ Play sont des marques ou des marques déposées de Google Inc. aux États-Unis et dans d'autres pays. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloudSM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® et Siri® sont des marques de service, des marques ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. CO ID®, RSA®, et SecurID® sont des marques déposées d'EMC Corporation. EnCase™ et Guidance Software® sont des marques ou des marques déposées de Guidance Software. Entrust® est une marque déposée d'Entrust®, Inc. aux États-Unis et dans d'autres pays. InstallShield® est une marque déposée de Flexera Software aux États-Unis, en Chine, dans l'Union européenne, à Hong Kong, au Japon, à Taïwan et au Royaume-Uni. Micron® et RealSSD® sont des marques déposées de Micron Technology, Inc. aux États-Unis et dans d'autres pays. Mozilla® Firefox® est une marque déposée de Mozilla Foundation aux États-Unis et/ou dans d'autres pays. iOS® est une marque ou une marque déposée de Cisco Systems, Inc. aux États-Unis et dans certains autres pays et est utilisée sous licence. Oracle® et Java® sont des marques déposées d'Oracle et/ou de ses sociétés affiliées. Les autres noms peuvent être des marques de leurs propriétaires respectifs. SAMSUNG™ est une marque de SAMSUNG aux États-Unis ou dans d'autres pays. Seagate® est une marque déposée de Seagate Technology LLC aux États-Unis et/ou dans d'autres pays. Travelstar® est une marque déposée de HGST, Inc. aux États-Unis et dans d'autres pays. UNIX® est une marque déposée de The Open Group. VALIDITY™ est une marque de Validity Sensors, Inc. aux États-Unis et dans d'autres pays. VeriSign® et d'autres marques connexes sont des marques ou des marques déposées de VeriSign, Inc. ou de ses filiales ou sociétés affiliées aux États-Unis et dans d'autres pays et dont la licence est octroyée à Symantec Corporation. KVM on IP® est une marque déposée de Video Products. Yahoo!® est une marque déposée de Yahoo! Inc.

Ce produit utilise des parties du programme 7-Zip. Le code source est disponible à l'adresse www.7-zip.org. La licence est concédée sous forme de licence GNU LGPL + restrictions unRAR (www.7-zip.org/license.txt).

2016-07

Protégé par un ou plusieurs brevets U.S., notamment : numéro 7665125 ; numéro 7437752 ; et numéro 7665118.

Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

Table des matières

| | | |
|---|--|----|
| 1 | Phases de la mise en œuvre | 5 |
| 2 | Révision du lancement et des exigences | 7 |
| | Documents relatifs au client Dell Data Protection | 8 |
| | Documents Dell Data Protection Server | 9 |
| 3 | Liste de contrôle de la préparation - Mise en œuvre initiale | 11 |
| 4 | Liste de contrôle de préparation - Mise à niveau/ Migration | 17 |
| 5 | Architecture | 21 |
| | Dell Enterprise Server | 21 |
| | Jusqu'à 5 000 points finaux | 22 |
| | 5 000 - 20 000 points finaux | 23 |
| | 20 000 - 40 000 points finaux | 24 |
| | 40 000 - 60 000 points finaux | 25 |
| | Considérations relatives à la haute disponibilité | 26 |
| | Virtualisation | 27 |
| | Ports Dell Enterprise Server | 27 |
| | DDP Enterprise Server - Virtual Edition | 30 |
| | Spécifications matérielles | 30 |
| | Serveur frontal externe Dell | 30 |
| | Ports d'Virtual Edition | 31 |
| 6 | Exemple d'e-mail de notification client | 35 |

Phases de la mise en œuvre

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

- Effectuer une [Révision du lancement et des exigences](#)
- Compléter [Liste de contrôle de la préparation - Mise en œuvre initiale](#) ou [Liste de contrôle de préparation - Mise à niveau/Migration](#)
- Installer ou mettre à niveau/Migrer l'un des éléments suivants :
 - **Dell Enterprise Server**
 - Gestion centralisée des périphériques
 - S'exécute sur un serveur Microsoft Windows
 - **DDP Enterprise Server - VE**
 - Gestion centralisée de 3 500 périphériques maximum
 - S'exécute dans un environnement virtualisé

Pour en savoir plus sur les serveurs Dell Data Protection, voir l' *Enterprise Server Installation and Migration Guide* (Guide d'installation et de migration d'Enterprise Server) ou le *Virtual Edition Quick Start and Installation Guide* (Guide de démarrage rapide et d'installation de Virtual Edition) Pour vous procurer ces documents, consultez [Documents Dell Data Protection Server](#).

Pour des instructions concernant les conditions requises du client et l'installation du logiciel, sélectionnez les documents correspondant à votre déploiement :

- *Enterprise Edition Basic Installation Guide* (Guide d'installation de l'Édition Enterprise Basique) ou *Enterprise Edition Advanced Installation Guide* (Guide d'installation de l'Édition Enterprise Avancé)
- *Endpoint Security Suite Basic Installation Guide* (Guide d'installation d'Endpoint Security Suite Basique) ou *Endpoint Security Suite Advanced Installation Guide* (Guide d'installation d'Endpoint Security Suite Avancé)
- *Endpoint Security Suite Enterprise Basic Installation Guide* (Guide d'installation d'Endpoint Security Suite Enterprise Basique) ou *Endpoint Security Suite Enterprise Advanced Installation Guide* (Guide d'installation d'Endpoint Security Suite Enterprise Avancé)
- *Personal Edition Installation Guide* (Guide d'installation de l'Édition Personnelle)
- *Security Tools Installation Guide* (Guide d'installation des outils de sécurité)
- *Enterprise Edition for Mac Administrator Guide* (Guide de l'Édition Enterprise pour administrateur de Mac)
- *Mobile Edition Administrator Guide* (Guide de l'administrateur de l'Édition Mobile)

Pour obtenir ces documents, consultez [Documents relatifs au client Dell Data Protection](#).

- Configurer la règle initiale
 - **Dell Enterprise Server.** Voir le *Enterprise Server Installation and Migration Guide* (Guide d'installation et de migration du serveur), *Administrative Tasks* (Tâches administratives)
 - **DDP Enterprise Server - VE.** Voir le *Guide d'installation et de démarrage rapide de Virtual Edition, Tâches administratives de la console de gestion à distance VE*
- Exécuter un plan de test
- Emballage client
- Participer au transfert des connaissances de base de l'Administrateur de Dell Data Protection
- Mettre en œuvre les meilleures pratiques
- Coordonner l'assistance au pilote ou au déploiement avec Dell Client Services

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 Protection et atteindre ces objectifs. Veillez à bien comprendre les exigences générales de votre entreprise en termes 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 finaux pour le déploiement ? Existe-t-il des projets de développement au-delà de ce nombre à l'avenir ?
- 5 Les utilisateurs finaux disposent-ils de privilèges admin 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 ?
 - Édition Enterprise
 - Cryptage de disque (droits DE) – Cryptage Windows, Cryptage du serveur, Bouclier de support externe (EMS), Gestion SED, Authentification avancée, BitLocker Manager (BLM), et Cryptage Mac.
 - Édition External Media (droit EME)
 - Édition Cloud (droit CE)
 - Endpoint Security Suite
 - Threat Protection (droit TP)
 - Cryptage de disque (droits DE) – Cryptage Windows, Cryptage du serveur, Bouclier de support externe (EMS), Gestion SED, Authentification avancée, BitLocker Manager (BLM), et Cryptage Mac.
 - Édition External Media (droit EME)
 - Endpoint Security Suite Enterprise
 - Advanced Threat Protection (droits ATP)
 - Cryptage de disque (droits DE) – Cryptage Windows, Cryptage du serveur, Bouclier de support externe (EMS), Gestion SED, Authentification avancée, BitLocker Manager (BLM), et Cryptage Mac.
 - Édition External Media (droit EME)
 - Édition Mobile (droit ME) pour téléphones Android, iOS et Windows
- 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 ciblées pour le chiffrement ?
- 13 D'autres partitions d'amorçage sont-elles configurées sur vos points finaux ?
 - a Partition de récupération du fabricant
 - b Postes de travail à double-amorçage

Documents relatifs au client Dell Data Protection

Pour connaître les conditions requises d'installation, les versions du SE et les SED pris en charge, ainsi que les instructions d'utilisation des produits Dell Data Protection que vous envisager de déployer, référez-vous au(x) document(s) applicable(s) répertorié(s) ci-dessous.

Enterprise Edition (clients Windows) : voir les documents suivants à l'adresse ci-après :

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

- *Enterprise Edition Basic Installation Guide* : Guide d'installation de l'Édition Enterprise Basique.
- *Enterprise Edition Advanced Installation Guide* : Guide d'installation de l'Édition Enterprise Avancée, avec des commutateurs et paramètres avancés pour les installations personnalisées.
- *DDP Console User Guide* (Guide d'utilisation de DDP Console) : Instructions destinées aux utilisateurs finaux de Dell Data Protection | Advanced Authentication.
- *Cloud Edition User Guide* (Guide d'utilisation de Cloud Edition) : instructions destinées aux utilisateurs finaux de Dell Data Protection | Cloud Edition, concernant son installation, son activation et son fonctionnement.

Enterprise Edition (Mac clients) - Voir l'*Enterprise Edition for Mac Administrator Guide* (Guide de l'administrateur de l'Édition Enterprise pour Mac) à l'adresse

www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. L'*Administrator Guide* (Guide de l'administrateur) comporte les instructions relatives à l'installation et au déploiement).

Endpoint Security Suite (clients Windows) : voir les documents suivants à l'adresse ci-après :

www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.

- *Endpoint Security Suite Basic Installation Guide* : Guide d'installation d'Endpoint Security Suite Basic.
- *Endpoint Security Suite Advanced Installation Guide* : Guide d'installation d'Endpoint Security Suite Advanced, avec des commutateurs et paramètres avancés pour les installations personnalisées.
- *DDP Console User Guide* (Guide d'utilisation de DDP Console) : instructions destinées aux utilisateurs finaux de Dell Data Protection | Endpoint Security Suite.

Endpoint Security Suite Enterprise (clients Windows) - Voir les documents suivants à l'adresse :

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

- *Endpoint Security Suite Enterprise Basic Installation Guide* : Guide d'installation d'Endpoint Security Suite Enterprise Basic.
- *Endpoint Security Suite Enterprise Advanced Installation Guide* : Guide d'installation d'Endpoint Security Suite Enterprise Advanced, avec des commutateurs et paramètres avancés pour les installations personnalisées.
- *DDP Console User Guide* (Guide d'utilisation de DDP Console) : instructions destinées aux utilisateurs finaux de Dell Data Protection | Endpoint Security Suite Enterprise.

Mobile Edition pour téléphone Android, iOS et Windows

- Voir le *Mobile Edition Administrator Guide* (Guide de l'administrateur de l'Édition Mobile) à l'adresse www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. L'*Administrator Guide* (Guide de l'administrateur) explique le déploiement de Dell Data Protection | Mobile Edition.

Documents Dell Data Protection Server

Pour en savoir plus sur les conditions requises, les versions et les configurations de Dell Data Protection Server que vous envisagez de déployer, reportez vous aux documents pertinents ci-dessous.

Dell Enterprise Server

- Voir l'*Enterprise Server Installation and Migration Guide* (*Guide d'installation et de migration d'Enterprise 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/04/product-support/product/dell-dp-endpt-security-suite/manuals.
ou
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

DDP Enterprise Server - Virtual Edition

Voir le *Virtual Edition Quick Start Guide and Installation Guide* (Guide d'installation et de démarrage rapide de l'Virtual Edition) à l'adresse www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals
ou
www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals.
ou
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

Liste de contrôle de la préparation - Mise en œuvre initiale

Selon le serveur Dell Data Protection que vous déployez, utilisez la liste de contrôle appropriée pour vous assurer que vous avez répondu à toutes les exigences avant d'installer Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite ou Dell Data Protection | Endpoint Security Suite Enterprise.

- [Liste de contrôle de Dell Enterprise Server](#)
- [DDP Enterprise Server - Liste de contrôle de Virtual Edition](#)

Liste de contrôle de Dell Enterprise 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.
- Tout point d'extrémité de production utilisé pendant le test de Proof of Concept a été décrypté ou les ensembles clés ont été téléchargés.
- L'application Proof of Concept a été supprimée de l'environnement.

REMARQUE : Toute nouvelle mise en œuvre doit commencer par une nouvelle base de données et l'installation du logiciel Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise. Dell Client Services ne procédera pas à une nouvelle mise en œuvre en utilisant un environnement POC. Les éventuels points d'extrémité cryptés au cours d'une preuve de concept devront être décryptés ou reconstruits avant l'engagement d'installation avec Dell.

Les serveurs répondent-ils aux spécifications logicielles requises ?

- Voir l'architecture du [Dell Enterprise Server](#).

Les serveurs répondent-ils aux spécifications logicielles requises ?

- Windows Server 2008 64 bits R2 (Standard ou Enterprise). 2008 R2 SP0-SP1 64 bits (Standard ou Enterprise) ; 2012 R2 (Standard) est installé.
- Le programme d'installation de Windows 4.0 ou version ultérieure est installé.
- .NET Framework 4.5 est installé.
- Microsoft SQL Native Client 2012 est installé, si vous utilisez Microsoft SQL Server 2012. SQL Native Client 2014 peut être utilisé, le cas échéant.

REMARQUE : SQL Express n'est pas pris en charge avec Dell Enterprise Server.

- Windows Firewall est désactivé ou configuré de sorte à accepter les ports (entrants) 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- La connectivité est disponible entre Dell Enterprise Server et Active Directory (AD) sur les ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (entrants vers AD).
- UAC est désactivé (voir le Panneau de configuration Windows > Comptes utilisateurs).
 - Windows Server 2008 SP2 64 bits/Windows Server 2008 R2 SP0-SP1 64 bits
 - Windows Server 2012 R2 : le programme d'installation désactive UAC.

Comptes de service créés avec succès ?

- Compte de service avec un accès en lecture seule à AD (LDAP) : un compte utilisateur/domaine de base est suffisant.
- Le compte de service doit disposer de droits d'administrateur local aux serveurs d'application Dell Enterprise 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 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 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 Protection et de Dell Enterprise Server se trouvent dans le dossier **Pilotes et téléchargements** sur www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research.
ou
www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y
ou
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals
Pour naviguer jusqu'au dossier depuis www.dell.com/support
 - 1 Sous **Rechercher un produit**, sélectionnez **Afficher les produits**, puis **Logiciel et sécurité** et **Endpoint Security Solutions**.
 - 2 Sélectionnez **Dell Data Protection | Encryption**, **Dell Data Protection | Endpoint Security Suite** ou **Dell Data Protection | Endpoint Security Suite Enterprise**, puis **Pilotes et téléchargements**.
 - 3 Dans la liste déroulante **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**.
 - 4 Sous le titre de logiciel applicable, sélectionnez **Télécharger le fichier**.
- Si vous avez acheté Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise intégré, le logiciel peut être téléchargé depuis www.dell.com. « Intégré » fait référence à un logiciel inclus avec l'image informatique créée par Dell en usine. Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise peut être préinstallé en usine sur tout ordinateur Dell.

OU

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

- Le logiciel se trouve à l'adresse <https://ddpe.credant.com> ou <https://cft.credant.com> sous le dossier **SoftwareDownloads**. (Téléchargements de logiciel)
- Si vous avez acheté Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise intégré, le logiciel peut être téléchargé depuis www.dell.com. « Intégré » fait référence à un logiciel inclus avec l'image informatique créée par Dell en usine. Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise peut être préinstallé en usine sur tout ordinateur Dell.

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 identifiants CFT. Voir [Exemple d'e-mail de notification client](#).
- Le fichier de licence est un fichier XML qui se trouve sur le site CFT 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, Endpoint Security Suite ou Endpoint Security Suite Enterprise.

La base de données est-elle créée ?

- (En option) 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 du serveur*. Le programme d'installation Enterprise 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 Dell Enterprise Server et/ou les Proxy de stratégies avec Split DNS pour le trafic interne et externe ?

Il est recommandé de créer des pseudonymes DNS, pour faciliter 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 :
 - Dell Enterprise Server : **ddpe-es.<domaine.com>**
 - Serveur frontal : **ddpe-fe.<domaine.com>**

REMARQUE : Split-DNS permet d'utiliser le même nom de DNS pour les services frontaux internes et externes et est nécessaire dans certains cas. Split-DNS permet d'utiliser une seule adresse pour vos clients et offre une grande flexibilité pour procéder à des mises à niveau ou mettre à jour la solution ultérieurement. Suggestion de nom CNAME pour les serveurs frontaux en cas d'utilisation de Split-DNS : ddpe-fe.<domaine.com>.

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. 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 de changement pour l'installation d'Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise à Dell Client Services 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 des clients.

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 systèmes actifs pour les tests. Les systèmes actifs 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.

DDP Enterprise Server - Liste de contrôle de Virtual Edition

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

- La base de données et l'application Proof of Concept (POC) ont été sauvegardées et désinstallées (si vous utilisez le même serveur) avant l'engagement d'installation avec Dell.
- Tout point d'extrémité de production utilisé pendant le test de Proof of Concept a été décrypté ou les ensembles clés ont été téléchargés.
- L'application Proof of Concept a été supprimée de l'environnement.

REMARQUE : Toute nouvelle mise en œuvre doit commencer par une nouvelle base de données et l'installation du logiciel Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise. Dell Client Services ne procédera pas à une nouvelle mise en œuvre en utilisant un environnement POC. Les éventuels points d'extrémité cryptés au cours d'une preuve de concept devront être décryptés 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 utilisateur/domaine de base est suffisant.

Le logiciel est-il téléchargé ?

- Les téléchargements de logiciel client Dell Data Protection et de l'Virtual Edition se trouvent dans le dossier **Pilotes et téléchargements** sur www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research.
ou
www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y
ou
www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

Pour naviguer jusqu'au dossier depuis www.dell.com/support

1 Sous **Rechercher un produit**, sélectionnez **Afficher les produits**, puis **Logiciel et sécurité** et **Endpoint Security Solutions**.

2 Sélectionnez **Dell Data Protection | Encryption**, **Dell Data Protection | Endpoint Security Suite** ou **Dell Data Protection | Endpoint Security Suite Enterprise**, puis **Pilotes et téléchargements**.

3 Dans la liste déroulante **Systèmes d'exploitation**, sélectionnez le système d'exploitation correspondant au produit que vous êtes en train de télécharger. Par exemple, pour télécharger Virtual Edition, sélectionnez **l'une des versions VMware**.

4 Sous le titre de logiciel applicable, sélectionnez **Télécharger le fichier**.

- Si vous avez acheté Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise intégré, le logiciel peut être téléchargé depuis www.dell.com. « Intégré » fait référence à un logiciel inclus avec l'image informatique créée par Dell en usine. Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise peut être préinstallé en usine sur tout ordinateur Dell.

Les fichiers de licence sont-ils disponibles ?

- Le fichier de licence est un fichier XML qui se trouve sur le site CFT sous 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, Endpoint Security Suite ou Endpoint Security Suite Enterprise.

Les serveurs répondent-ils aux spécifications logicielles requises ?

- Voir [DDP Enterprise Server - Virtual Edition](#).

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.

Les exigences de contrôle des modifications ont-elles été identifiées et communiquées à Dell ?

- Envoyez toute exigence spécifique concernant le contrôle des modifications de l'installation d'Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise aux services client Dell 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 systèmes actifs pour les tests. Les systèmes actifs 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.

Liste de contrôle de préparation - Mise à niveau/ Migration

Cette liste s'applique uniquement à Dell Enterprise Server.

REMARQUE : Mettez à jour DDP Enterprise Server - VE depuis le menu Configuration de base de votre terminal VE. Pour en savoir plus, voir le *Guide d'installation de démarrage rapide de Virtual Edition*.

Utilisez la liste de contrôle appropriée pour vous assurer que vous répondez à toutes les conditions préalables avant de démarrer la mise à niveau de Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, ou Dell Data Protection | Endpoint Security Suite Enterprise.

Les serveurs répondent-ils aux spécifications logicielles requises ?

- Windows Server 2008 64 bits R2 (Standard ou Enterprise) ; 2008 R2 SP0-SP1 64 bits (Standard ou Enterprise) ; 2012 R2 (Standard) est installé.
- Le programme d'installation de Windows 4.0 ou version ultérieure est installé.
- .NET Framework 4.5 est installé.
- Microsoft SQL Native Client 2012 est installé, si vous utilisez Microsoft SQL Server 2012. SQL Native Client 2014 peut être utilisé, le cas échéant.

REMARQUE : SQL Express n'est pas pris en charge avec Dell Enterprise Server.

- Le pare-feu Windows est désactivé ou configuré de sorte à accepter les ports (entrants) 80, 1099, 1433, 8000, 8050, 8081, 8084, 8443, 8445, 8888, 9000, 9011, 61613, 61616.
- La connectivité est disponible entre Dell Enterprise Server et Active Directory (AD) sur les ports 88, 135, 389, 636, 3268, 3269, 49125+ (RPC) (entrants vers AD).
- UAC est désactivé (voir le Panneau de configuration Windows > Comptes utilisateurs).
 - Windows Server 2008 SP2 64 bits/Windows Server 2008 R2 SP0-SP1 64 bits
 - Windows Server 2012 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 utilisateur/domaine de base est suffisant.
- Le compte de service doit disposer de droits d'administrateur local aux serveurs d'application Dell Enterprise 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 utilisateur doit être au format DOMAIN\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 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 identifiants CFT. Voir [Exemple d'e-mail de notification client](#).
- Le fichier de licence est un fichier XML qui se trouve sur le site CFT sous 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, Endpoint Security Suite ou Endpoint Security Suite Enterprise.

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

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

- Le logiciel se trouve à l'adresse <https://ddpe.credant.com> ou <https://cft.credant.com> sous le dossier **SoftwareDownloads**. (Téléchargements de logiciel)
- Si vous avez acheté Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise intégré, le logiciel peut être téléchargé depuis www.dell.com. « Intégré » fait référence à un logiciel inclus avec l'image informatique créée à l'usine et achetée auprès de Dell. Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise peut être préinstallé en usine sur tout ordinateur Dell.

Possédez-vous suffisamment de licences de point final ?

Avant la mise à niveau, assurez-vous que vous disposez d'un nombre suffisant de licences client pour couvrir tous les points finaux de votre environnement. Si vos installations dépassent actuellement votre nombre de licences, veuillez contacter votre représentant commercial Dell avant de procéder à une mise à niveau ou à une migration. Dell Data Protection procédera à la validation des licences et empêchera les validations si aucune licence n'est disponible.

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

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. 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 de changement pour l'installation d'Encryption, Endpoint Security Suite ou Endpoint Security Suite Enterprise à Dell Client Services 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 systèmes actifs pour les tests. Les systèmes actifs 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.

Architecture

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

- [Dell Enterprise Server](#)
- [DDP Enterprise Server - Virtual Edition](#)

Dell Enterprise Server

Les solutions Encryption; Endpoint Security Suite et Endpoint Security Suite Enterprise 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 votre entreprise compte plus de 50 000 points finaux, veuillez contacter Dell Client Services 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 de serveur DDP peuvent être installés sur un même serveur. En option, 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 Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

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

Configuration à un seul serveur

16 Go ; 20 Go au moins d'espace disque disponible (outre l'espace de pagination virtuel) ; Processeur Quad-Core avancé (2 GHz ou +)

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

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

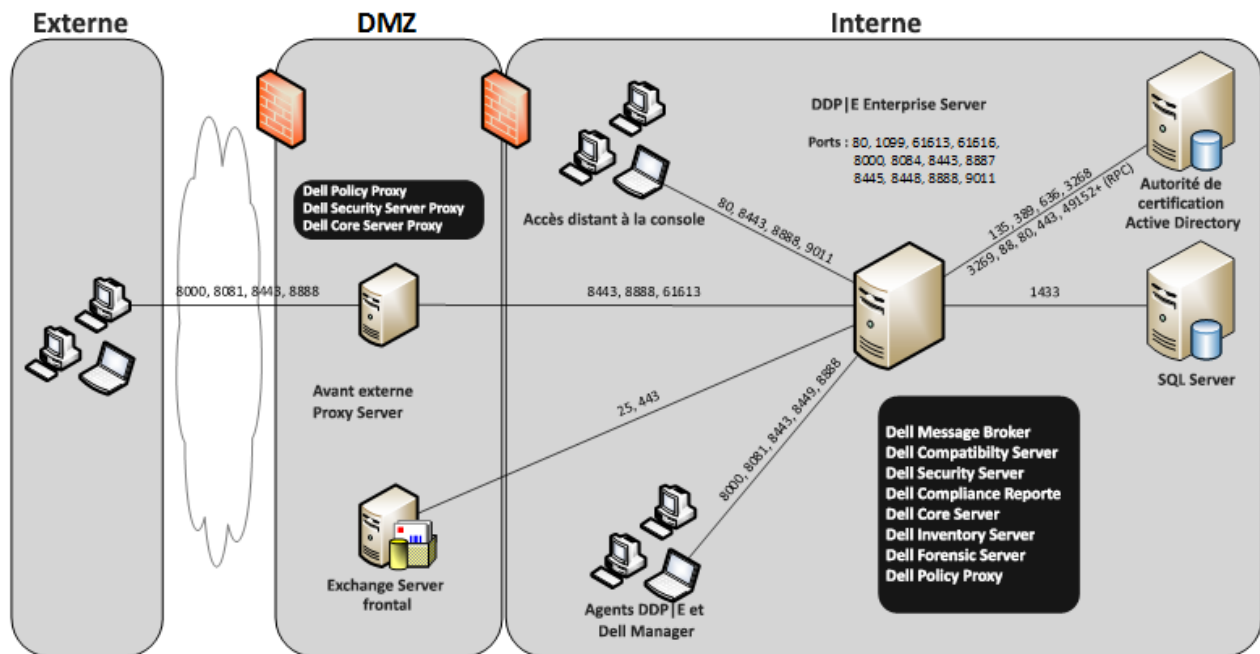
8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel) ; UC double-cœur avancée au minimum (2 GHz ou +), tel que Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalents AMD

SQL Server

Microsoft SQL Server 2008 et Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

Microsoft SQL Server 2014 Standard Edition / Business Intelligence / 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. En option, 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 64 bits - Standard Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel) ; 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

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 Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

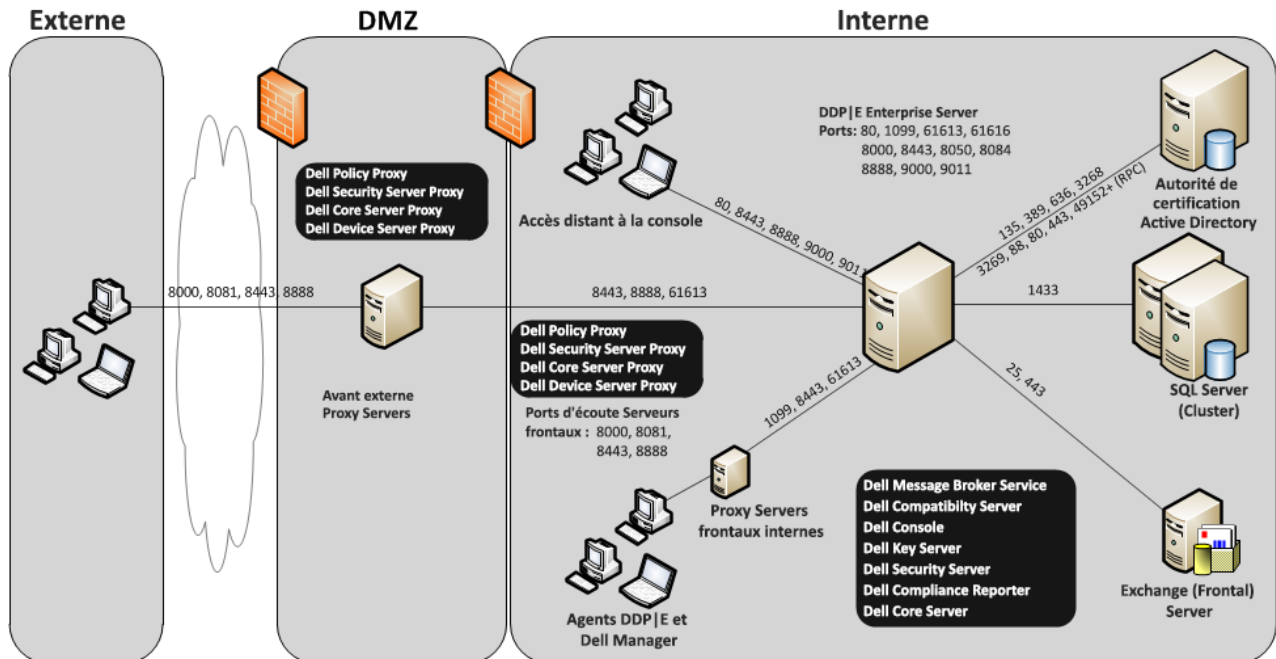
8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel) ; UC double-cœur avancée au minimum (2 GHz ou +), tel que Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalents AMD

SQL Server

Microsoft SQL Server 2008 et Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

Microsoft SQL Server 2014 Standard Edition / Business Intelligence / 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 règles sur Internet.

Composants d'architecture

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (autre l'espace de pagination virtuel) ; 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

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 Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

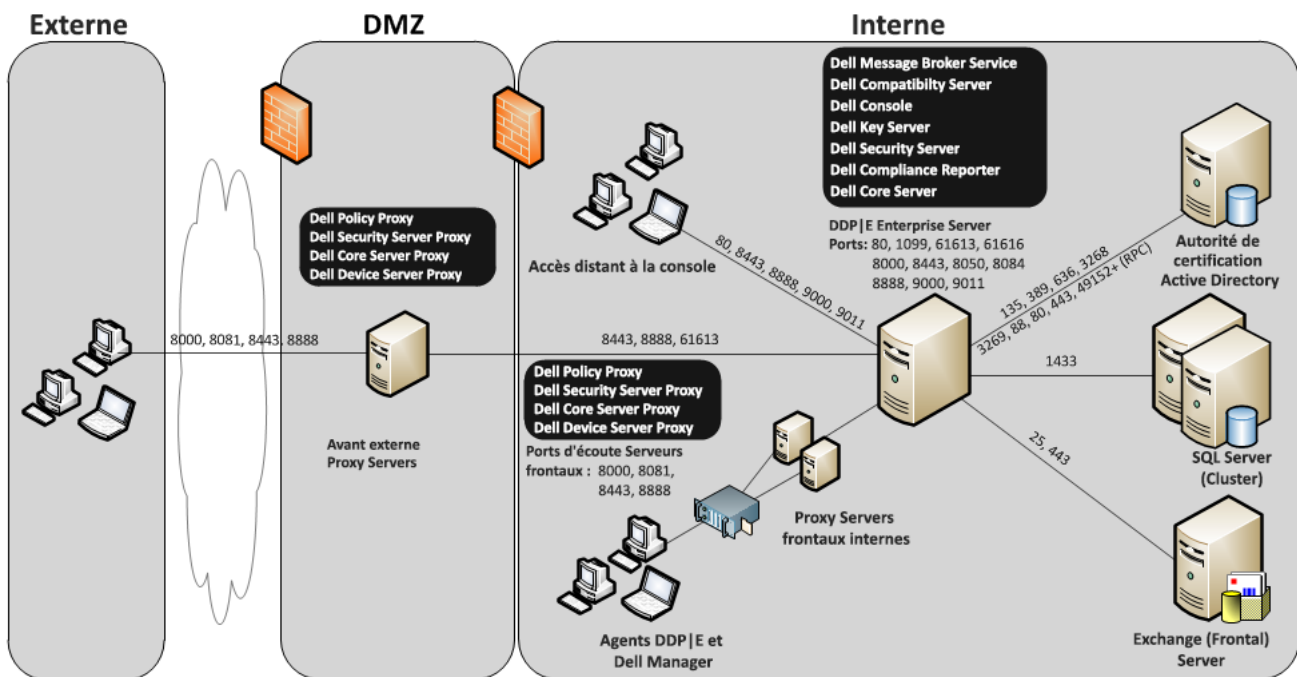
8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (autre l'espace de pagination virtuel) ; UC double-cœur avancée au minimum (2 GHz ou +), tel que Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalents AMD

SQL Server

Microsoft SQL Server 2008 et Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

Microsoft SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition



40 000 - 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 règles sur Internet.

REMARQUE : Si l'entreprise compte plus de 50 000 points finaux, veuillez contacter Dell Client Services 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 Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (autre l'espace de pagination virtuel) ; 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

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 Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition

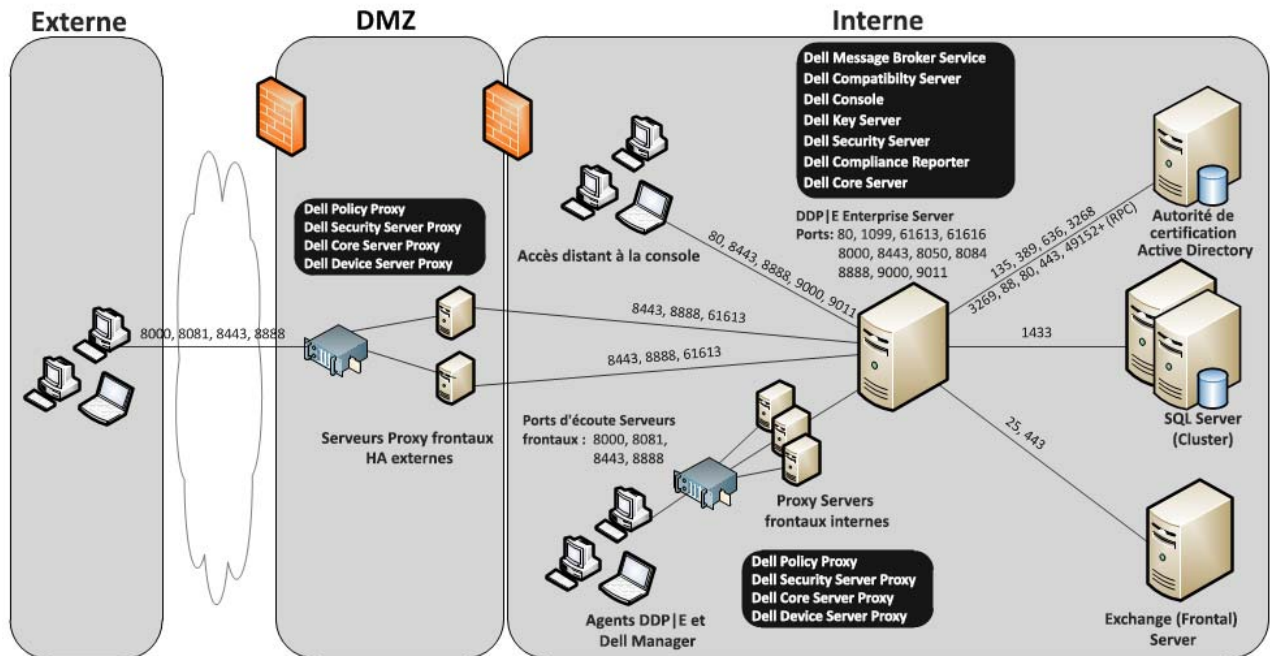
8 Go minimum, en fonction de la configuration ; +/-1,5 Go d'espace disque disponible (autre l'espace de pagination virtuel) ; UC double-cœur avancée au minimum (2 GHz ou +), tel que Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou équivalents AMD

SQL Server

Microsoft SQL Server 2008 et Microsoft SQL Server 2008 R2 Standard Edition / Enterprise Edition

Microsoft SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

Microsoft SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition



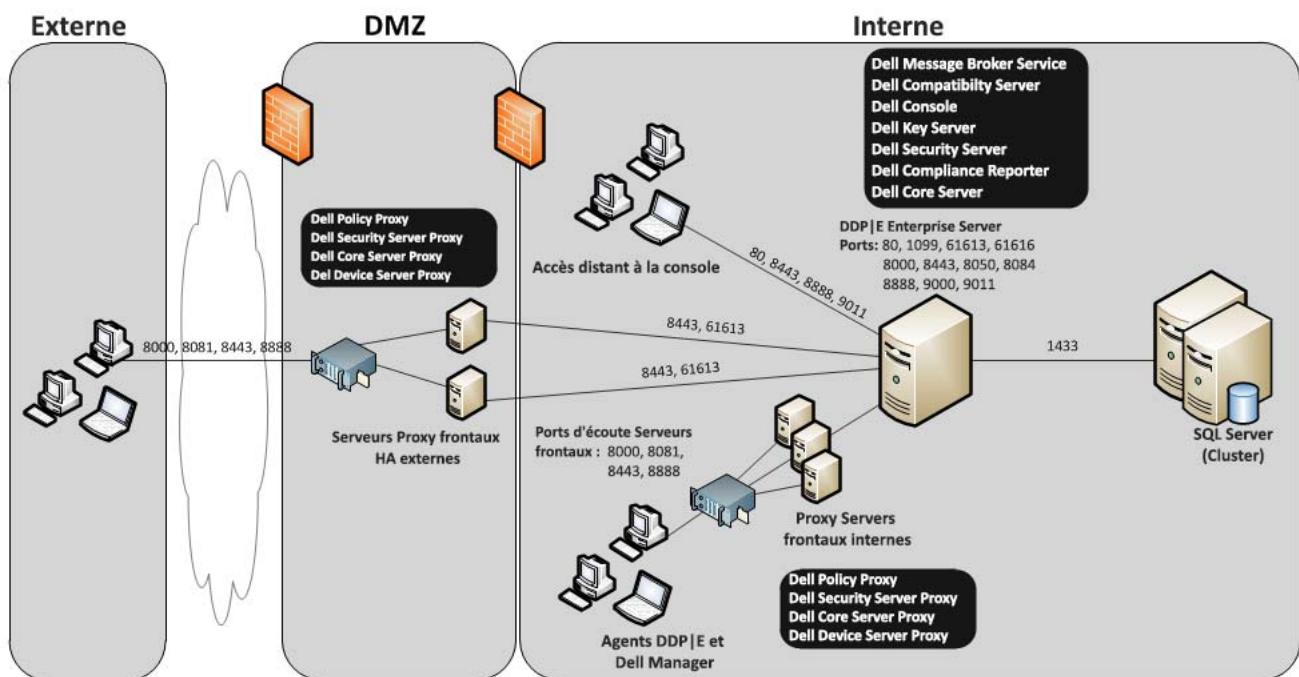
Considérations relatives à la haute disponibilité

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 règles vers les points finaux sur Internet.



Virtualisation

Serveurs d'application Dell Data Protection

La vitesse du disque sur le matériel hébergeant le serveur virtuel, l'allocation de mémoire RAM à l'hôte et la configuration du stockage peuvent affecter considérablement la performance. Cet impact est particulièrement notable pendant l'activation, le traitement des politiques et de l'inventaire et le triage. Dell recommande de réserver autant de mémoire RAM que possible pour l'hôte virtuel, et de donner la priorité à ce dernier dans l'allocation des ressources. Si vous rencontrez des problèmes de performances, Dell recommande d'effectuer le déploiement vers un environnement de serveur non virtuel.

Serveur SQL

Dans les environnement plus volumineux, il est fortement recommandé de faire fonctionner le serveur SQL Database sur un matériel physique et 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.

Pour en savoir plus sur les meilleures pratiques concernant SQL Server, voir l'*Enterprise Server Installation and Migration Guide* (Guide d'installation et de migration d'Enterprise Server)

Ports Dell Enterprise Server

Le tableau suivant décrit chaque composant et sa fonction.

| Nom | Port par défaut | Description | Obligatoire pour |
|---|--|--|---|
| Compliance Reporter (Rapporteur de conformité) | HTTP(S)/ 8084 | Aperçu complet de l'environnement de contrôle et de rapports de conformité. Un composant du Dell Enterprise Server. | Rapports |
| Console de gestion à distance | HTTP(S)/ 8443 | Console de gestion et centre de commande pour le déploiement à toute l'entreprise. Un composant du Dell Enterprise Server. | Tous |
| Core Server | HTTPS/ 8888 et 9000 | 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 les rôles. Un composant du Dell Enterprise Server. | Tous |
| Device Server | HTTPS/ 8443 HTTPS/ 8081 (vers Dell Device Server principal) | Prend en charge les activations et la récupération de mot de passe. Un composant du DellEnterprise Server. | Dell Data Protection I Enterprise Edition pour Mac Dell Data Protection I Enterprise Edition pour Windows CREDActivate |

| Nom | Port par défaut | Description | Obligatoire pour |
|------------------------------|-------------------------------------|---|---|
| Security Server | HTTPS/ 8443 | Communique avec Policy Proxy ; gère les récupérations de clés légal, activations de clients, produits Cloud Edition, communications SED-PBA et Active Directory pour l'authentification ou la réconciliation, dont la validation d'identité pour l'authentification dans la Console de gestion à distance. Exige l'accès à la base de données SQL. Un composant du Dell Enterprise Server. | Tous |
| Compatibility Server | TCP/ 1099 | Service de gestion de l'architecture de l'entreprise. Collecte et stocke les données d'inventaire initiales lors de l'activation et les données des stratégies lors des migrations. Traite les données en fonction des groupes d'utilisateurs de ce service. Un composant du Dell Enterprise Server. | Tous |
| Service Courtier de messages | TCP/ 61616 et STOMP/ 61613 | Gère les communications entre les services du Dell 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. Un composant du Dell Enterprise Server. | Tous |
| Identity Server | HTTPS/ 8445 | Gère les demandes d'authentification de serveur, dont l'authentification du SED Manager. Exige un compte Active Directory. Doit être le compte utilisé pour accéder à SQL lorsque l'Authentification Windows est utilisée. Un composant du Dell Enterprise Server. | Tous |
| 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. Un composant du Dell Enterprise Server. | Utilitaires d'administration Dell |
| Dell Policy Proxy | TCP/ 8000 | Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité. Un composant du Dell Enterprise Server. | Dell Data Protection I Enterprise Edition pour Mac Dell Data Protection I Enterprise Edition pour Windows Dell Data Protection I Mobile Edition |

| Nom | Port par défaut | Description | Obligatoire pour |
|--|---|--|--|
| LDAP | TCP/ 389/636 (contrôleur de domaine local), 3268/3269 (catalogue global) TCP/ 135/ 49125+ (RPC) | <p>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.</p> <p>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 réplique sur le catalogue global peuvent être retournés. Par exemple, un service utilisateur n'a pas pu être retourné à l'aide du port 3268 dans la mesure où cet attribut n'est pas répliqué sur le catalogue global.</p> | Tous |
| Base de données Microsoft SQL | TCP/ 1433 | Le port de serveur SQL par défaut est 1433 et une valeur aléatoire comprise entre 1024 et 5000 est attribuée aux ports du client. | Tous |
| Authentification du client | HTTPS/ 8449 | Permet aux serveurs client de s'authentifier auprès de l'Enterprise Server Dell. | Dell Data Protection Server Encryption (SE) |
| Communication par e-mail | 25 | Fournit des notifications d'événements. | Facultatif |
| 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. |
| 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. |

DDP Enterprise Server - Virtual Edition

Cette architecture est adaptée à la plupart des petites et moyennes entreprises comportant 1 à 3500 points finaux. En option, un serveur frontal peut être placé dans la zone DMZ pour publier des règles et/ou activer des points finaux sur Internet.

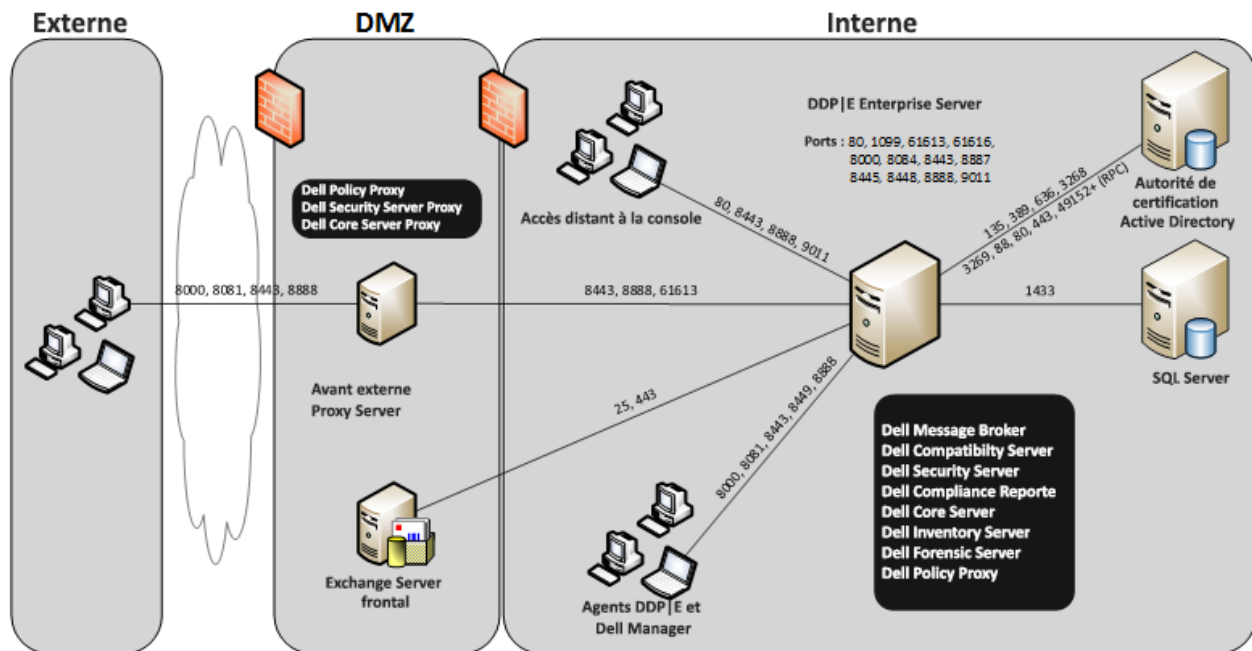
Spécifications matérielles

- DDP Enterprise Server - Virtual Edition (VE)
- VMWare Workstation 9, 10 ou 11 ; VMware ESXi 5.1, ESXi 5.5 ou ESXi 6.0
- RAM 4 Go avec VMWare Workstation 9, 10 ou 11 ; RAM 8 Go avec ESXi 5.1, 5.5 ou 6.0 ;
- 80 Go d'espace disque disponible
- Processeur 2+ Ghz, Double cœur ou supérieur

Pour connaître les exigences plus en détail, voir le *DDP Enterprise Server - Virtual Edition Quick Start Guide and Installation Guide* (Guide de démarrage rapide et d'installation de DDP Enterprise Server - Virtual Edition)

Serveur frontal externe Dell

- Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard Edition ou Enterprise Edition/Windows Server 2012 R2 - Standard Edition
- 2 Go minimum de RAM dédiée / 4 Go de RAM dédiée recommandés
- 1,5 Go d'espace disque disponible (outre l'espace de pagination virtuel)
- Double cœur 2 GHz ou mieux



Ports d'Virtual Edition

Le tableau suivant décrit chaque composant et sa fonction.

| Nom | Port par défaut | Description | Obligatoire pour |
|---|---------------------|--|------------------|
| Compliance Reporter (Rapporteur de conformité) | HTTP(S)/ 8084 | Aperçu complet de l'environnement de contrôle et de rapports de conformité. Un composant du DDP Enterprise Server - VE. | Rapport |
| Console de gestion à distance | | Console de gestion et centre de commande pour le déploiement à toute l'entreprise. Un composant du DDP Enterprise Server - VE. | Tous |
| 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 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 les rôles. Un composant du DDP Enterprise Server - VE. | Tous |
| 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 à distance, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection et Advanced Threat Protection. Un composant du DDP Enterprise Server - VE. | Tous |
| Security Server | HTTPS/ 8443 | Communique avec Policy Proxy ; gère les récupérations des clés légales, les activations de clients, les produits Cloud Edition et les communications SED-PBA. Un composant du DDP Enterprise Server - VE. | Tous |
| Compatibility Server | TCP/1099 (fermé) | 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. Un composant du DDP Enterprise Server - VE. | Tous |

| Nom | Port par défaut | Description | Obligatoire pour |
|-----------------------------------|--|--|---|
| Service Courtier de messages | TCP/61616 et STOMP/61613 (fermé ou, si configuré pour DMZ, le port 61613 est ouvert) | Gère les communications entre les services du DDP Enterprise Server - VE. Organise les informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des stratégies. Un composant du DDP Enterprise Server - VE. | Tous |
| Identity Server | 8445 | Gère les demandes d'authentification de serveur, dont l'authentification du SED Manager. Exige un compte Active Directory. Un composant du DDP Enterprise Server - VE. | Tous |
| Forensic Server | HTTPS/8448 | Permet aux administrateurs dotés des privilèges appropriés d'obtenir des clés de chiffrement de la Console de gestion à distance pour l'utilisation dans les déverrouillages de données ou les tâches de déchiffrement. Un composant du DDP Enterprise Server - VE. | API Forensic |
| Inventory Server | 8887 | Traite la file d'attente de l'inventaire. Un composant du DDP Enterprise Server - VE. | Tous |
| Policy Proxy (Proxy de stratégie) | TCP/8000/8090 | Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité. Un composant du DDP Enterprise Server - VE. | Dell Data Protection I Enterprise Edition pour Mac Dell Data Protection I Enterprise Edition pour Windows Dell Data Protection I Édition mobile |

| Nom | Port par défaut | Description | Obligatoire pour |
|--|---|---|--|
| LDAP | 389/636, 3268/3269 RPC - 135, 49125+ | <p>Port 389 : ce port est utilisé pour la demande des informations à partir 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.</p> <p>Port 3268 : ce port est utilisé pour les requêtes ciblées spécifiquement sur le catalogue global. Les requêtes LDAP envoyées au port 3268 peuvent être utilisées pour la recherche d'objets dans l'ensemble de la forêt. Cependant, seuls les attributs marqués pour réplication sur le catalogue global peuvent être retournés. Par exemple, un service utilisateur n'a pas pu être retourné à l'aide du port 3268 dans la mesure où cet attribut n'est pas répliqué sur le catalogue global.</p> | Tous |
| Authentification du client | HTTPS/ 8449 | Permet aux serveurs client de s'authentifier auprès de DDP Enterprise Server - VE. | Dell Data Protection I Server Encryption |
| 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. |
| 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. |

Exemple d'e-mail de notification client

Après l'achat de Dell Data Protection, vous recevrez un e-mail de DellDataProtectionEncryption@Dell.com. L'exemple ci-dessous montre un e-mail Dell Data Protection | Encryption. Il contient vos identifiants CFT et vos informations de clé de licence.

Dell

Dell Data Protection | Encryption

Dear [Redacted],

Thank you for purchasing Dell Data Protection | Encryption to quickly and easily protect your critical business data.

The following is the information you need to download your software and installation instructions for Dell Order # [Redacted]

| | |
|-------------------------------------|---|
| Download Server: | https://ddpe.credant.com |
| Username: | [Redacted] |
| Password: | l1oFqQe |
| Required to change password: | No |
| Account Expiration Date: | Never |
| License Key: | [Redacted] |

Support

Your **Dell Data Protection | Encryption Solution** is entitled to Dell service and maintenance. For extending your service, contact your Dell sales representative or ask your support representative about an upgrade. For **Dell Data Protection | Encryption Solution** support, call **1-877-459-7304**.

This email was generated at: 14 Feb 12 07:31:26

© 2010 Dell Inc and CREDANT Technologies, Inc. All rights reserved.

L'exemple ci-dessous montre un e-mail envoyé par Dell Data Protection | Endpoint Security Suite.

Dell Data Protection | Endpoint Security Suite

Dear **XXXXX**,

Thank you for purchasing Dell Data Protection | Endpoint Security Suite to quickly and easily protect your end users, data and reputation. The following is the information you need to download your software and installation instructions for Dell Order #**XXXXXXXX**

| | |
|------------------------------|---|
| Download Server: | https://XXXXXXXXXX.com |
| Username: | XXXXXXXXXXXX |
| Password: | XXXXX |
| Required to change password: | No |
| License Key: | XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX |

Support

Your Dell Data Protection | Endpoint Security Suite includes Dell support and maintenance. To extend your support, contact your Dell sales representative or ask your support representative about an upgrade. For Dell Data Protection | Endpoint Security Suite support.

This email was generated at: 06 Feb 15 10:25:01
© 2015 Dell Inc. All rights reserved.

Dell and the Dell logo are trademarks of Dell Inc. All other trademarks used herein are the property of their respective owners and are used for identification purposes only.



0XXXXXA0X

