

DDP Enterprise Server - Édition Virtuelle

Guide de démarrage rapide et Guide d'installation v9.7



Remarques, précautions et avertissements

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

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

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

© 2017 Dell Inc. Tous droits réservés. Dell, EMC et d'autres marques de commerce sont des marques de commerce de Dell Inc. ou de ses filiales. Les autres marques de commerce peuvent être des marques de commerce déposées par leurs propriétaires respectifs.

Marques déposées et marques commerciales utilisées dans Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise et dans la suite de documents Dell Data Guardian : Dell™ et le logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, et KACE™ sont des marques de Dell Inc. Cylance®, CylancePROTECT 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 commerciales ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. VMware® est une marque déposée ou une marque commerciale 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 commerciales 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™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® et Siri® sont des marques de service, des marques commerciales ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. GO ID®, RSA®, et SecurID® sont des marques déposées de Dell EMC. EnCase™ et Guidance Software® sont des marques commerciales 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 commerciale ou une marque déposée de Cisco Systems, Inc. aux États-Unis et dans certains autres pays et elle 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 commerciales 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 7-zip.org. L'octroi de licence est soumis à la licence GNU LGPL + aux restrictions unRAR (7-zip.org/license.txt). Virtual Edition utilise des bibliothèques tierces provenant de « urwid » selon les termes de la licence GNU Lesser General Public License. La notice de copyright et la licence GNU Lesser General Public License sont disponibles dans l'aide Admin, dans la page Attributions, Copyrights et Marques.

Guide de démarrage rapide et guide d'installation VE

2017 - 04

Rév. A01

Table des matières

| | |
|--|-----------|
| 1 Guide de démarrage rapide de Virtual Edition..... | 5 |
| Installer DDP Enterprise Server - VE..... | 5 |
| Configurer VE..... | 5 |
| Ouvrir la Console de gestion à distance VE..... | 5 |
| Tâches administratives..... | 6 |
| 2 Guide d'installation de Virtual Edition..... | 7 |
| À propos de DDP Enterprise Server - VE..... | 7 |
| Contacter Dell ProSupport..... | 7 |
| Configuration requise..... | 7 |
| Conditions préalables pour le DDP Enterprise Server - VE..... | 7 |
| Conditions préalables pour la Console de gestion à distance VE..... | 9 |
| Conditions préalables pour le mode Proxy..... | 9 |
| Télécharger DDP Enterprise Server - VE..... | 10 |
| Installer DDP Enterprise Server - VE..... | 11 |
| Ouvrir la Console de gestion à distance VE..... | 12 |
| (Installer un serveur frontal)Install and Configure Proxy Mode(Installer et configurer le mode Proxy)..... | 12 |
| Terminal VE - Tâches de configuration de base..... | 14 |
| Modifier le nom d'hôte..... | 14 |
| Modifier les paramètres réseau..... | 14 |
| Définir le nom d'hôte DMZ..... | 15 |
| Modifier le fuseau horaire..... | 15 |
| Mettre à jour DDP Enterprise Server - VE..... | 15 |
| Modifier les mots de passe utilisateur..... | 16 |
| Définir les utilisateurs FTP (Transfert de fichiers)..... | 17 |
| Activer SSH..... | 17 |
| Démarrer ou arrêter les services VE..... | 18 |
| Redémarrer le VE..... | 18 |
| Éteindre le VE..... | 18 |
| Terminal VE - Tâches de configuration avancée..... | 18 |
| Définir ou modifier le mot de passe de base de données..... | 18 |
| Configurer les paramètres SMTP..... | 19 |
| Importer un certificat existant ou inscrire un nouveau certificat de serveur..... | 19 |
| Configurer la rotation de rapport..... | 20 |
| Enregistrer et restaurer..... | 21 |
| Activer l'accès à distance à la base de données..... | 22 |
| Activer la prise en charge du serveur DMZ..... | 22 |
| 3 DDP Enterprise Server - Tâches d'administrateur VE..... | 23 |
| Définir ou modifier la langue du terminal DDP Enterprise Server - VE..... | 23 |
| Vérifier l'état du serveur..... | 23 |
| Rapports d'affichage..... | 24 |
| Ouvrir l'interface de ligne de commande..... | 24 |



| | |
|--|-----------|
| Générer le journal des instantanés du système..... | 24 |
| 4 Maintenance de DDP Enterprise Server - VE..... | 26 |
| 5 Dépannage de DDP Enterprise Server - VE..... | 27 |
| 6 Tâches de configuration après l'installation..... | 28 |
| Configurer VE pour Data Guardian..... | 28 |
| Installer et configurez la gestion EAS pour Mobile Edition..... | 28 |
| Activer la vérification de la chaîne d'approbation du gestionnaire..... | 30 |
| 7 Tâches d'administrateur de la console de gestion à distance VE..... | 31 |
| Assigner le rôle d'administrateur Dell..... | 31 |
| Se connecter avec le rôle d'administrateur Dell..... | 31 |
| Valider des règles..... | 32 |
| 8 Ports de solution..... | 33 |



Guide de démarrage rapide de Virtual Edition

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

Pour obtenir des instructions détaillées, reportez-vous au [Guide d'installation de Virtual Edition](#).

Pour plus d'informations sur les conditions préalables pour VE, voir [Conditions préalables de DDP Enterprise Server - VE](#), [Conditions préalables de la console de gestion à distance VE](#) et [Conditions préalables du mode proxy](#).

Pour plus d'informations sur la façon de mettre à jour un DDP Enterprise Server - VE existant, voir la section [Mettre à jour DDP Enterprise Server - VE](#).

Installer DDP Enterprise Server - VE

- 1 Naviguez jusqu'au répertoire contenant les fichiers Dell Data Protection et double-cliquez dessus pour importer les fichiers dans VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
- 2 Mettez sous tension DDP Enterprise Server - VE.
- 3 Suivez les instructions à l'écran.

Configurer VE

Avant d'activer les utilisateurs, vous devez effectuer les tâches de configuration suivantes sur le terminal DDP Enterprise Server - VE :

- [Définir ou modifier le mot de passe de base de données](#)
- [Configurer les paramètres SMTP](#)
- [Importer un certificat existant ou inscrire un nouveau certificat de serveur](#)
- [Mettre à jour DDP Enterprise Server - VE](#)
- Installez un client FTP qui prend en charge SFTP sur le port 22 et [Définir les utilisateurs FTP \(Transfert de fichiers\)](#).

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

REMARQUE : Si les droits de vos clients Enterprise Edition sont activés depuis l'usine ou si vous achetez des licences de l'usine, définissez le GPO sur le contrôleur du domaine pour activer ces droits (il se peut que le même serveur n'exécute pas l'Édition Enterprise). Assurez-vous que le port sortant 443 est disponible pour communiquer avec le serveur. Si le port 443 est bloqué (pour quelque raison que ce soit), les droits ne pourront pas être octroyés.

Ouvrir la Console de gestion à distance VE

Ouvrez la console de gestion à distance VE à cette adresse :

<https://server.domain.com:8443/webui/>

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

Pour obtenir la liste des navigateurs Web pris en charge, reportez-vous à [Conditions préalables de la console de gestion à distance VE](#).



Tâches administratives

Si vous n'avez pas démarré la Console de gestion à distance VE, vous pouvez le faire maintenant. Les références par défaut sont **superadmin/changeit**.

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

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

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

- Les ordinateurs Windows seront cryptés
- Les ordinateurs équipés de lecteurs à auto-cryptage seront cryptés
- La gestion BitLocker n'est pas activée
- Advanced Threat Protection n'est pas activé
- La protection contre les menaces est activée
- Les supports externes ne seront pas cryptés
- Les périphériques connectés à des ports ne seront pas cryptés
- Dell Data Guardian est activé
- Mobile Edition n'est pas activé

Reportez-vous à la rubrique Aide administrateur pour naviguer jusqu'à Groupes de technologie et la description des règles.

Les tâches de démarrage rapide sont terminées.



Guide d'installation de Virtual Edition

Ce guide d'installation explique aux utilisateurs moins expérimentés comment installer et configurer DDP Enterprise Server - VE. En règle générale, Dell recommande d'installer d'abord DDP Enterprise Server - VE, puis les clients.

Pour plus d'informations sur la façon de mettre à jour un DDP Enterprise Server - VE existant, voir la section [Mettre à jour DDP Enterprise Server - VE](#).

À propos de DDP Enterprise Server - VE

DDP Enterprise Server - VE est l'élément d'administration de la sécurité de la solution Dell. La VE Remote Management Console permet aux administrateurs de surveiller l'état des points finaux, de l'application des règles et de la protection dans l'ensemble de l'entreprise. Le mode Proxy propose une option frontale (mode DMZ) pour utilisation avec DDP Enterprise Server - VE.

DDP Enterprise Server - VE présente les fonctions suivantes :

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

Contacteur Dell ProSupport

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

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

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

Pour les numéros de téléphone en dehors des États-Unis, consultez [Numéros de téléphone internationaux Dell ProSupport](#).

Configuration requise

Conditions préalables pour le DDP Enterprise Server - VE

Matériel

L'espace disque recommandé pour DDP Enterprise Server - VE est 80 Go.



Environnement virtualisé

DDP Enterprise Server - VE v9.6 a été validé avec les environnements virtualisés suivants.

Environnements virtualisés

- VMware Workstation 12,5
 - UC 64 bits requise
 - 4 Go de RAM recommandés
 - Reportez-vous à <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
 - Le matériel doit être conforme à la configuration minimale requise par VMware
 - Au moins 4 Go de RAM pour la ressource d'image dédiée
 - Voir <http://pubs.vmware.com/workstation-11/index.jsp> pour plus d'informations

- VMware Workstation 11
 - UC 64 bits requise
 - 4 Go de RAM recommandés
 - Reportez-vous à <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
 - Le matériel doit être conforme à la configuration minimale requise par VMware
 - Au moins 4 Go de RAM pour la ressource d'image dédiée
 - Voir <http://pubs.vmware.com/workstation-11/index.jsp> pour plus d'informations

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

- VMware ESXi 5.5
 - UC 64 bits x86 requise
 - Ordinateur hôte avec au moins deux cœurs
 - Au moins 8 Go de RAM recommandés
 - Un système d'exploitation n'est pas nécessaire
 - Reportez-vous à <http://www.vmware.com/resources/compatibility/search.php> pour obtenir une liste complète des systèmes d'exploitation hôte pris en charge
 - Le matériel doit être conforme à la configuration minimale requise par VMware
 - Au moins 4 Go de RAM pour la ressource d'image dédiée
 - Voir <http://pubs.vmware.com/vsphere-55/index.jsp> pour obtenir plus d'informations

- Hyper-V Server (installation complète ou minimale)
 - UC 64 bits x86 requise
 - Ordinateur hôte avec au moins deux cœurs
 - Au moins 8 Go de RAM recommandés



Environnements virtualisés

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

Conditions préalables pour la Console de gestion à distance VE

Navigateurs Internet

① REMARQUE :

Votre navigateur doit accepter les cookies.

Le tableau suivant décrit les navigateurs Internet pris en charge.

Navigateurs Internet

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

Conditions préalables pour le mode Proxy

Matériel

Le tableau suivant décrit la configuration matérielle *minimale* requise pour le mode Proxy.

Processeur

2 GHz Core 2 Duo ou mieux

RAM

Environ 2 Go minimum de RAM dédiée / 4 Go de RAM dédiée recommandés

Espace disque disponible

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

Carte réseau

Carte d'interface réseau 10/100/1000

Divers

TCP/IP installé et activé

Logiciels

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



Pré-requis

- **Windows Installer 4.0 ou ultérieur**

Windows Installer version 4.0 ou version ultérieure doit être installé sur le serveur cible de l'installation.

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

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

- **Microsoft .NET Framework version 4.5**

Microsoft a publié des mises à jour de sécurité pour .NET Framework version 4.5.

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

① REMARQUE :

Désactivez toujours l'UAC lors de l'utilisation de Windows Server 2008. Une fois l'UAC désactivé, il faut redémarrer le serveur pour que cette modification prenne effet.

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

Systeme d'exploitation

- **Windows Server 2008 R2 SP0-SP1 64 bits**

- Édition Standard
- Édition Enterprise

- **Windows Server 2008 SP2 64 bits**

- Édition Standard
- Édition Enterprise

- **Windows Server 2012 R2**

- Édition Standard
- Édition Datacenter

- **Windows Server 2016**

- Édition Standard
- Édition Datacenter

Télécharger DDP Enterprise Server - VE

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

Cryptage

ou



ou

ou

Pour télécharger le fichier OVA :

- 1 Naviguez jusqu'à la page de support du produit pour [Encryption](#), [Endpoint Security Suite](#), [Endpoint Security Suite Enterprise](#) ou [Data Guardian](#).
- 2 Cliquez sur **Pilotes et téléchargements**.
- 3 En regard de « Afficher toutes les mises à jour disponibles pour <version du système d'exploitation> », cliquez sur **Changer de système d'exploitation**, et sélectionnez l'une des options suivantes : **VMware ESXi 6.0**, **VMware ESXi 5.5**, ou **VMware ESXi 5.1**.
- 4 Sous « Afficher par : », sélectionnez **Tout afficher**.
- 5 Sous Dell Data Protection, sélectionnez **Télécharger**.

Installer DDP Enterprise Server - VE

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

- 1 Identifiez les fichiers Dell Data Protection sur le support d'installation et double-cliquez pour les importer dans VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
- 2 Mettez sous tension DDP Enterprise Server - VE.
- 3 Sélectionnez la langue du Contrat de licence et sélectionnez **Afficher le CLUF**.
- 4 Lisez le contrat et sélectionnez **Accepter le CLUF**.
- 5 Si une mise à jour est disponible, sélectionnez **Accepter**.
- 6 Sélectionnez **Mode par défaut** ou **mode Déconnecté**.

REMARQUE :

Si vous sélectionnez le **Mode déconnecté**, le VE ne pourra jamais être modifié en mode par défaut.

Le mode Déconnecté isole VE d'Internet et d'un LAN ou autre réseau non sécurisé. Toutes les mises à jour doivent être effectuées manuellement. Pour plus d'informations sur les fonctionnalités et les stratégies du Mode déconnecté, voir l'[Aide administrateur](#).

- 7 À l'invite de modification du mot de passe par défaut, sélectionnez **Oui**.
- 8 Sur l'écran *Définir le mot de passe ddpuser*, saisissez le mot de passe actuel (par défaut), **ddpuser**, puis saisissez un mot de passe unique, saisissez-le une deuxième fois, puis sélectionnez **OK**.

Les mots de passe doivent comprendre les éléments suivants :

- Au moins 8 caractères
 - Au moins une lettre majuscule
 - Au moins 1 chiffre
 - Au moins un caractère spécial
- 9 Dans la boîte de dialogue *Configurer le nom d'hôte*, utilisez la touche Retour arrière pour supprimer le nom d'hôte par défaut. Saisissez un nom d'hôte unique, puis sélectionnez **OK**.
 - 10 Dans la boîte de dialogue *Configurer les paramètres de réseau*, choisissez l'une des deux options ci-après, puis sélectionnez **OK**.
 - (Par défaut) Utiliser le DHCP.
 - (Recommandé) dans le champ Utiliser DHCP, appuyez sur la barre d'espace pour retirer le X et saisissez manuellement ces adresses, le cas échéant : IP statique, masque de réseau, passerelle par défaut, serveur DNS 1, serveur DNS 2, serveur DNS 3



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

- 11 Dans l'écran *Fuseau horaire*, utilisez les touches fléchées pour mettre en surbrillance votre fuseau horaire, puis sélectionnez **Entrée**.
- 12 À l'invite de confirmation du fuseau horaire, cliquez sur **OK**.
- 13 Lorsque s'affiche le message indiquant que la configuration initiale est terminée, sélectionnez **OK**.
- 14 [Définir ou modifier le mot de passe de base de données](#).
- 15 [Configurer les paramètres SMTP](#).
- 16 [Importer un certificat existant ou inscrire un nouveau certificat de serveur](#).
- 17 [Mettre à jour DDP Enterprise Server - VE](#).
- 18 Installez un client FTP qui prend en charge SFTP sur le port 22 et [Définir les utilisateurs FTP \(Transfert de fichiers\)](#).

Les tâches d'installation de DDP Enterprise Server - VE sont terminées.

Ouvrir la Console de gestion à distance VE

Ouvrez la console de gestion à distance VE à cette adresse :

<https://server.domain.com:8443/webui/>

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

Pour obtenir la liste des navigateurs Web pris en charge, reportez-vous à [Conditions préalables de la console de gestion à distance VE](#).

(Installer un serveur frontal) Install and Configure Proxy Mode (Installer et configurer le mode Proxy)

L'option Proxy Mode (Installation du serveur frontal/Mode Proxy) est une option frontale (mode DMZ) à utiliser avec DDP Enterprise Server - VE. Si vous prévoyez de déployer des composants Dell dans la zone DMZ, veillez à les protéger correctement contre les attaques.

REMARQUE : Le service de balise est installé dans le cadre de cette installation pour prendre en charge la balise de rappel de Data Guardian, qui insère une balise de rappel dans chaque fichier protégé par Data Guardian lors de l'exécution du mode protégé Office. Ceci permet la communication entre n'importe quel périphérique à n'importe quel emplacement et sur le serveur frontal Dell. Assurez-vous que la sécurité réseau nécessaire est configurée avant d'utiliser la balise de rappel. La stratégie Activer une balise de rappel est activée par défaut.

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

- 1 Sur le support d'installation Dell, accédez au répertoire Dell Enterprise Server. **Décompressez** (SANS copier/coller ou glisser/déposer) Dell Enterprise Server-x64 dans le répertoire racine du serveur où vous comptez installer VE. **Les opérations de copier/coller ou glisser/déposer produisent des erreurs et empêchent l'installation.**
- 2 Double-cliquez sur **setup.exe**.
- 3 Lorsque la boîte de dialogue *Assistant InstallShield* s'affiche, sélectionnez la langue d'installation, puis cliquez sur **OK**.
- 4 Si les composants requis n'ont pas déjà été installés, un message s'affiche, vous informant des composants requis à installer. Cliquez sur **Installer**.
- 5 Dans la boîte de dialogue *Accueil*, cliquez sur **Suivant**.
- 6 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
- 7 Entrez la clé de produit.
- 8 Sélectionnez **Installation principale**, puis cliquez sur **Suivant**.
- 9 Pour installer le serveur frontal dans l'emplacement par défaut C: \Program Files\Dell, cliquez sur **Suivant**. Sinon, cliquez sur **Modifier** pour sélectionner un autre emplacement, puis cliquez sur **Suivant**.
- 10 Vous avez le choix entre différents types de certificats numériques. **Il est vivement recommandé d'utiliser un certificat numérique provenant d'une autorité de certification fiable.**
Sélectionnez l'option « a » ou « b » ci-dessous :

- a Pour utiliser un certificat existant acheté auprès d'une autorité de certification, sélectionnez **Importer un certificat existant**, puis cliquez sur **Suivant**.

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

Saisissez le mot de passe associé au certificat. Le fichier de magasin de clés doit avoir le suffixe .p12 ou pfx.

Cliquez sur **Suivant**.

REMARQUE :

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

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

- b Pour créer un certificat auto-signé, sélectionnez **Créer un certificat auto-signé et l'importer dans un magasin de clés**, puis cliquez sur **Suivant**.

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

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

Entreprise

Service (exemple : Sécurité)

Ville

État (nom complet)

Pays : code de deux lettres du pays

Cliquez sur **Suivant**.

REMARQUE :

Par défaut, le certificat expire dans un an.

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

REMARQUE :

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

Désélectionnez un proxy uniquement si vous êtes certain de ne pas vouloir le configurer en vue de l'installation. Si vous désélectionnez un proxy dans cette boîte de dialogue, il ne sera pas installé.

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



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

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

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

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

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

Terminal VE - Tâches de configuration de base

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

Modifier le nom d'hôte

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Dans le *menu Configuration de base*, sélectionnez **Nom d'hôte**.
- 2 Utilisez la touche Retour arrière pour supprimer le nom d'hôte de DDP Enterprise Server - VE existant, puis remplacez-le par un nouveau nom d'hôte et sélectionnez **OK**.

Modifier les paramètres réseau

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

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

Adresse IP statique

Masque de réseau

Passerelle par défaut

Serveur DNS 1

Serveur DNS 2

Serveur DNS 3

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

Définir le nom d'hôte DMZ

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Dans le *menu Configuration de base*, sélectionnez **Nom d'hôte DMZ**.
- 2 Entrez le nom de domaine complet du serveur DMZ, puis sélectionnez **OK**.

REMARQUE : Pour utiliser le mode Proxy (mode DMZ), vous devez installer et configurer le mode Proxy.

Modifier le fuseau horaire

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Dans le *menu Configuration de base*, sélectionnez **Fuseau horaire**.
- 2 Dans l'écran *Fuseau horaire*, utilisez les touches fléchées pour mettre en surbrillance votre fuseau horaire, puis sélectionnez **Entrée**.
- 3 À l'invite de confirmation du fuseau horaire, cliquez sur **OK**.

Mettre à jour DDP Enterprise Server - VE

Pour plus d'informations sur une mise à jour spécifique, voir *Conseils techniques VE*, situé sur le site Web de support de Dell à l'adresse <http://www.dell.com/support>. Pour consulter la date de la version et l'installation d'une mise à jour qui s'applique déjà, à partir du menu **Configuration de base**, sélectionnez **Mettre à jour DDP Enterprise Server - VE > Dernière mise à jour appliquée avec succès**.

Pour recevoir des notifications par e-mail lorsque des mises à jour de VE sont disponibles, voir [Configurer les paramètres SMTP](#).

REMARQUE : En mode par défaut, une mise à jour doit être exécutée après l'installation initiale de DDP Enterprise Server - VE, et avant l'activation des clients.

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

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

Mise à jour VE (mode par défaut)

- 1 Dell vous recommande d'effectuer une sauvegarde régulière. Avant la mise à jour, assurez-vous que le processus de sauvegarde fonctionne correctement. Consultez [Sauvegarde et restauration](#).
- 2 Dans le menu **Configuration de base**, sélectionnez **Mettre à jour DDP Enterprise Server - VE**.
- 3 Sélectionnez l'action souhaitée :
 - Définir le serveur de mise à jour : sélectionnez cette option pour définir ou modifier l'emplacement des paquets de mise à jour de DDP Enterprise Server - VE. Dans l'écran *Définir le serveur de mise à jour*, utilisez la touche Retour arrière pour supprimer le nom d'hôte ou l'adresse IP du serveur existant. Entrez le nouveau nom de domaine complet ou la nouvelle adresse IP, puis sélectionnez **OK**.



Le serveur de mise à jour **act.credant.com**.

- Définir les paramètres Proxy : sélectionnez cette option pour définir les paramètres Proxy de téléchargement des mises à jour.

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

 **REMARQUE : Pour effectuer une mise à jour à partir d'un site FTP, saisissez le nom d'utilisateur et le mot de passe FTP, suivis de l'URL.**

- Rechercher les mises à jour : sélectionnez cette option pour rechercher un paquet de mise à jour de DDP Enterprise Server - VE auprès du serveur de mises à jour.
- Télécharger la mise à jour : sélectionnez cette option pour télécharger une mise à jour identifiée grâce à l'option Rechercher les mises à jour.
- Appliquer la mise à jour : sélectionnez cette option si vous voulez appliquer un paquet de mise à jour de DDP Enterprise Server - VE que vous avez téléchargé. Dans l'écran *Sélectionner un fichier de mise à jour (.deb)*, sélectionnez le paquet de mises à jour à installer, puis appuyez sur **Entrée**.
- Dernière mise à jour réussie appliquée : sélectionnez cette option pour afficher la version et la date d'installation de la version VE actuelle.

Mise à jour VE (mode déconnecté)

- 1 Dell vous recommande d'effectuer une sauvegarde régulière. Avant la mise à jour, assurez-vous que le processus de sauvegarde fonctionne correctement. Consultez [Sauvegarde et restauration](#).
- 2 Procurez-vous le fichier .deb qui contient la dernière mise à jour VE à partir du site Web de support de Dell. Les téléchargements VE 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/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/research

ou

www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

- 3 Stockez le fichier .deb dans le dossier /mises à jour sur le serveur FTP sécurisé du VE. Assurez-vous que le client FTP prend en charge SFTP sur le port 22 et qu'un utilisateur FTP est configuré. Consultez [Définir les utilisateurs FTP \(Transfert de fichiers\)](#).
- 4 Dans le menu **Configuration de base**, sélectionnez **Mettre à jour DDP Enterprise Server - VE**.
- 5 Sélectionnez **Appliquer la mise à jour** et appuyez sur **Entrée**.
Si le fichier .deb ne s'affiche pas, assurez-vous que [le fichier .deb est stocké au bon emplacement](#).
- 6 Sélectionnez le fichier de mise à jour .deb que vous souhaitez installer et appuyez sur **Entrée**.

Modifier les mots de passe utilisateur

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

Vous pouvez modifier les mots de passe pour ces utilisateurs :

- ddpuser (Administrateur de terminal DDP Enterprise Server - VE) : cet utilisateur a accès au terminal VE et à ses menus.

- ddpconsole (Accès shell de DDP Enterprise Server - VE) : cet utilisateur a accès au shell de VE. L'accès au shell permet à un administrateur réseau de vérifier et dépanner la connectivité réseau.
- ddpsupport (Administrateur Dell ProSupport) : cet utilisateur sert uniquement à Dell ProSupport. Pour des raisons de sécurité, vous contrôlez le mot de passe de ce compte.

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

Les mots de passe doivent comprendre les éléments suivants :

- Au moins 8 caractères
- Au moins 1 majuscule
- Au moins 1 chiffre
- Au moins 1 caractère spécial

Définir les utilisateurs FTP (Transfert de fichiers)

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

Vous pouvez donner accès au serveur FTP sécurisé de DDP Enterprise Server - VE à trois utilisateurs maximum pour les tâches de sauvegarde et de restauration. Le serveur FTP VE peut également servir à stocker ou charger des mises à jour vers DDP Enterprise Server - VE.

- 1 Depuis le menu *Configuration de base*, sélectionnez **Utilisateurs FTP (Transfert de fichiers)**.
- 2 Dans l'écran *Configurer les utilisateurs FTP*, appuyez sur la barre d'espace pour activer un Utilisateur FTP et entrer un **X** dans le champ État de cet utilisateur. Pour désactiver l'utilisateur FTP, appuyez sur la barre d'espace pour supprimer le **X** dans le champ État de cet utilisateur.
- 3 Saisissez un nom d'utilisateur et un mot de passe pour l'utilisateur SFTP.

Les mots de passe doivent comprendre les éléments suivants :

- Au moins 8 caractères
- Au moins 1 majuscule
- Au moins 1 chiffre
- Au moins 1 caractère spécial

- 4 Lorsque vous avez terminé de saisir les utilisateurs SFTP, sélectionnez **OK**.

Activer SSH

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

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

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



Démarrer ou arrêter les services VE

N'effectuez cette tâche qu'en cas de nécessité. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Pour démarrer ou arrêter simultanément tous les Services VE, dans le menu *Configuration de base*, sélectionnez **Démarrer l'application** ou **Arrêter l'application**.
- 2 À l'invite de confirmation, sélectionnez **Oui**.

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

Redémarrer le VE

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

- 1 Dans le menu *Configuration de base*, sélectionnez **Redémarrer l'appliance**.
- 2 À l'invite de confirmation, sélectionnez **Oui**.
- 3 Après le redémarrage, connectez-vous à DDP Enterprise Server - VE.

Éteindre le VE

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

- 1 Depuis le menu *Configuration de base*, faites défiler la page vers le bas et sélectionnez **Arrêter l'appliance**.
- 2 À l'invite de confirmation, sélectionnez **Oui**.
- 3 Après le redémarrage, connectez-vous à DDP Enterprise Server - VE.

Terminal VE - Tâches de configuration avancée

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

Définir ou modifier le mot de passe de base de données

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Dans le menu *Configuration avancée*, sélectionnez l'option **Mot de passe de base de données**.
- 2 Saisissez un mot de passe pour accéder à la base de données, puis sélectionnez **OK**.

Les mots de passe doivent comprendre les éléments suivants :

- Au moins 8 caractères
- Au moins 1 majuscule
- Au moins 1 chiffre
- Au moins 1 caractère spécial

 **REMARQUE** : Dell vous recommande de sauvegarder les mots de passe une fois l'installation terminée.

Configurer les paramètres SMTP

Pour recevoir des notifications DDP Enterprise Server - VE par e-mail **ou** pour utiliser Data Guardian, suivez les étapes de cette section pour configurer les paramètres SMTP. Les notifications par e-mail de DDP Enterprise Server - VE informent les destinataires des états d'erreur du statut des serveurs DDP Enterprise Server - VE server, des mises à jour des mots de passe, de la disponibilité des mises à jour de DDP Enterprise Server - VE et des problèmes relatifs aux licences des clients.

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

Pour configurer les paramètres SMTP, suivez ces étapes :

- 1 Dans le menu *Configuration avancée*, sélectionnez **Notifications par e-mail**.
- 2 Dans l'écran *Configurer les notifications par e-mail*, pour activer les alertes par e-mail, appuyez sur la barre d'espace pour saisir un **X** dans le champ Activer les alertes par e-mail.
- 3 Saisissez le nom de domaine complet du serveur SMTP.
- 4 Saisissez le port SMTP.
- 5 Dans le champ de l'expéditeur, saisissez l'identifiant du compte e-mail qui enverra les notifications par e-mail.
- 6 Dans le champ Entrer l'utilisateur, saisissez un identifiant de compte e-mail pour modifier les notifications par e-mail configurées.
- 7 Dans le champ Mot de passe, saisissez un mot de passe pour modifier les notifications par e-mail configurées.
- 8 Dans les champs ID d'adresses e-mail pour l'état VE, les mises à jour de mot de passe et la disponibilité des mises à jour, saisissez une liste de destinataires pour chaque type de notification. Suivez les conventions ci-après lorsque vous répertoriez les destinataires :
 - Le format de l'adresse e-mail est destinataire@dell.com.
 - Les destinataires sont séparés par des virgules ou des points-virgules.
- 9 Dans le champ Rappel d'alerte de service, pour activer les rappels, appuyez sur la barre d'espace pour saisir un **X** dans le champ, puis définissez l'intervalle entre les rappels en minutes. Un rappel d'alerte de service est déclenché lorsque l'intervalle est dépassé, malgré l'envoi d'une notification concernant un problème d'intégrité du système ou bien lorsque l'état du service n'est pas modifié.
- 10 Dans le champ Rapport récapitulatif, pour activer le rapport des notifications, sélectionnez l'intervalle souhaité (Quotidien, Hebdomadaire ou Mensuel), puis appuyez sur la barre d'espace pour entrer un **X** dans le champ.
- 11 Sélectionnez **OK**.

Importer un certificat existant ou inscrire un nouveau certificat de serveur

Les certificats doivent être en place avant que vous puissiez activer des utilisateurs pour DDP Enterprise Server - VE.

Vous pouvez importer un certificat existant ou créer une requête de certificat par l'intermédiaire de DDP Enterprise Server - VE.

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

Importation d'un certificat de serveur existant

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

REMARQUE : Conservez le mot de passe d'exportation car vous en aurez besoin lorsque vous importerez le certificat dans DDP Enterprise Server - VE.

- 2 Sur le serveur FTP de DDP Enterprise Server - VE, stockez le certificat dans **/opt/dell/vsftpd/files/certificates**.
- 3 À partir du menu *Configuration avancée* de DDP Enterprise Server - VE, sélectionnez **Certificats de serveur**.
- 4 Sélectionnez l'option **Importer un certificat existant**.
- 5 Sélectionnez un fichier de certificat à installer sur DDP Enterprise Server - VE.
- 6 Lorsque vous y êtes invité, saisissez le mot de passe d'exportation du certificat, puis sélectionnez **OK**.



7 Une fois l'importation terminée, sélectionnez **OK**.

Enregistrer un nouveau certificat de serveur

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

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

Créez et installez un certificat auto-signé

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

Les services redémarrent automatiquement.

Configurer la rotation de rapport

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

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

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

Pour activer la rotation de rapport, suivez ces étapes :

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

Enregistrer et restaurer

Les sauvegardes peuvent être configurées ou effectuées à tout moment. Elles ne sont pas nécessaires pour commencer à utiliser DDP Enterprise Server - VE. Dell vous recommande de configurer un processus de sauvegarde régulière.

Vous pouvez stocker les sauvegardes sur un serveur FTP sécurisé externe (recommandé) ou sur DDP Enterprise Server - VE. En cas de stockage sur le Serveur VE, lorsque le disque fonctionne à 90 pour cent de sa capacité, aucune nouvelle sauvegarde ne sera stockée. Vous recevrez une notification par e-mail vous indiquant que l'espace disque est faible.

REMARQUE :

Pour conserver l'espace partition de disque et prévenir la suppression automatique des sauvegardes, supprimez les sauvegardes inutiles faites sur DDP Enterprise Server - VE.

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

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

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

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

REMARQUE :

Tous les services de serveur VE doivent être en cours d'exécution avant le démarrage d'une opération de Restauration. **Vérifier l'état du serveur**. Si tous les serveurs ne sont pas en cours d'exécution, redémarrez les services. Pour plus d'informations, reportez-vous à **Démarrer ou arrêter les services VE**. Commencez à restaurer **uniquement** lorsque **tous les** services sont en cours d'exécution.

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

VE s'amorce et la sauvegarde est restaurée.

Stockez les sauvegardes sur un serveur FTP sécurisé

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

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

- manuellement



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

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

REMARQUE :

Virtual Edition se base sur Linux Debian Ubuntu x64.

Connectez-vous sur VE en tant que ddpsupport et utilisez la commande sudo pour configurer votre solution de sauvegarde :

```
sudo <instructions du vendeur de solution de sauvegarde>
```

Contenu de sauvegarde des dossiers suivants :

/opt/dell/vsftpd/fichiers/sauvegarde (requis)

/opt/dell/vsftpd/fichiers/certificats (fortement recommandé)

/opt/dell/vsftpd/fichiers/support (facultatif)

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

Activer l'accès à distance à la base de données

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

REMARQUE : Dell vous recommande de n'activer l'accès à distance à la base de données qu'en cas de nécessité.

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

Activer la prise en charge du serveur DMZ

Cette tâche peut être réalisée à tout moment. Elle n'est pas obligatoire pour commencer à utiliser DDP Enterprise Server - VE. Le redémarrage des services lors de chaque modification des paramètres fait partie des meilleures pratiques.

- 1 Dans le menu *Configuration avancée*, sélectionnez **Activer la prise en charge du serveur DMZ**.
- 2 Utilisez la barre d'espace pour saisir un **X** dans le champ Activer la prise en charge du serveur DMZ, puis sélectionnez **OK**.

REMARQUE : Pour utiliser le mode Proxy (mode DMZ), vous devez installer et configurer le mode Proxy.

DDP Enterprise Server - Tâches d'administrateur VE

Définir ou modifier la langue du terminal DDP Enterprise Server - VE

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

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

Vérifier l'état du serveur

Pour vérifier l'état des services DDP Enterprise Server - VE, dans le menu principal, sélectionnez **État du serveur**.

Le tableau suivant décrit chaque service et sa fonction.

| Nom | Description |
|--|---|
| Dell Message Broker | Bus du serveur Enterprise |
| Dell Identity Server | Traite les demandes d'authentification de domaine. |
| Dell Compatibility Server | Service de gestion de l'architecture de l'entreprise. |
| Dell Security Server | Mécanisme de contrôle des commandes et des communications avec Active Directory. Permet de communiquer avec Dell Policy Proxy. |
| Dell Compliance Reporter | Aperçu complet de l'environnement de contrôle et de rapports de conformité. |
| Dell Core Server | Service de gestion de l'architecture de l'entreprise. |
| Dell Core Server HA (Haute disponibilité) | Un service de haute disponibilité qui permet d'augmenter la sécurité et la performance des connexions HTTPS lors de la gestion de la architecture d'entreprise. |
| Dell Inventory Server | Traite la file d'attente de l'inventaire. |
| Dell Forensic Server | Fournit des services Web pour l'API Forensic. |
| Dell Policy Proxy | Fournit un chemin de communication réseau pour les mises à jour de l'inventaire et des règles de sécurité. |

DDP Enterprise Server - VE surveille et redémarre ses services, si nécessaire.



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

Rapports d'affichage

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

Journal Syslog Journal e-mail Journal auth (SSH) Journal Postgres Journal de surveillance

- Rapports système
 - Rapport Syslog
 - Rapport e-mail
 - Rapport auth. (SSH)
 - Rapport PostgreSQL
 - Rapport de surveillance
- Rapports de serveur
 - Compatibility Server
 - Security Server
 - Courtier de messages
 - Core Server
 - Core Server HA
 - Compliance Reporter (Rapporteur de conformité)
 - Identity Server (Serveur d'identité)
 - Inventory Server (Serveur d'inventaire)
 - Forensic Server
 - Policy Proxy (Proxy de stratégie)
- Rapport de personnalisation de la base de données

Ouvrir l'interface de ligne de commande

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

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

Générer le journal des instantanés du système

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

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

Si l'utilisateur ddpsupport est activé, Dell ProSupport peut récupérer le journal à partir du serveur SFTP de DDP Enterprise Server - VE. Si l'utilisateur ddpsupport n'est pas activé, contactez Dell ProSupport. Pour plus d'informations, reportez-vous à [contacter Dell ProSupport](#).



Maintenance de DDP Enterprise Server - VE

Vous devez supprimer les sauvegardes inutiles de DDP Enterprise Server - VE.

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

Dépannage de DDP Enterprise Server - VE

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

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



Tâches de configuration après l'installation

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

Configurer VE pour Data Guardian

Pour que configurer VE pour prendre en charge Data Guardian, ouvrez la console de gestion à distance VE et définissez la stratégie de chiffrement Cloud sur Activé. Pour activer le mode documents Office protégés Data Guardian, définissez la stratégie de documents Office protégés sur Activé.

Pour obtenir des instructions pour installer le client Data Guardian, reportez-vous au *Guide d'installation avancée Enterprise Edition*, *Guide d'installation basique Enterprise Edition* ou *Guide d'utilisation Data Guardian*.

Installer et configurez la gestion EAS pour Mobile Edition

Pour utiliser Mobile Edition, vous devez installer et configurer la gestion EAS. Si vous n'avez pas l'intention d'utiliser Mobile Edition, ignorez cette section.

Pré-requis

- Le compte de connexion du service de gestionnaire de boîtes aux lettres EAS doit être un compte autorisé à créer/modifier des règles Exchange ActiveSync, à attribuer des règles aux boîtes aux lettres des utilisateurs et à rechercher des informations sur les périphériques ActiveSync.
- Vous devez exécuter l'utilitaire de configuration EAS avec les droits d'administrateur pour pouvoir modifier les fichiers et redémarrer les services.
- Une connexion réseau à DDP Enterprise Server - VE est requise.
- Vous devez avoir à portée de main le nom d'hôte ou l'adresse IP de DDP Enterprise Server - VE.
- La file d'attente MSMQ doit déjà être installée et configurée sur le serveur hébergeant l'environnement Exchange. Si tel n'est pas le cas, installez MSMQ 4.0 sous Windows Server 2008 ou Windows Server 2008 R2 (sur le serveur qui héberge l'environnement Exchange) – <http://msdn.microsoft.com/en-us/library/aa967729.aspx>

Pendant le processus de déploiement

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

Installer le gestionnaire de périphériques EAS

- 1 Sur le support d'installation Mobile Edition, accédez au dossier Gestion EAS. À partir du dossier de gestionnaire de périphérique EAS, copiez le fichier **setup.exe** sur votre ou vos serveur(s) d'accès au client Exchange.
- 2 Double-cliquez sur le fichier **setup.exe** pour démarrer l'installation. Si votre environnement comprend plusieurs serveurs d'accès au client Exchange, exécutez ce programme d'installation sur chacun d'entre eux.
- 3 Sélectionnez la langue de l'installation, puis cliquez sur **OK**.
- 4 Cliquez sur **Suivant** lorsque l'écran de *Bienvenue* s'affiche.

- 5 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
- 6 Cliquez sur **Suivant** pour installer le Gestionnaire de périphériques EAS à l'emplacement par défaut, à savoir `C:\inetpub\wwwroot\Dell\EAS Device Manager\`.
- 7 Cliquez sur **Installer** dans l'écran *Prêt à lancer l'installation*.

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

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

Installer le gestionnaire de boîtes aux lettres EAS

- 1 Sur le support d'installation Mobile Edition, accédez au dossier Gestion EAS. À partir du dossier de gestionnaire de boîtes aux lettres EAS, copiez le fichier `setup.exe` vers votre ou vos *Serveur(s) de boîtes aux lettres Exchange*.
- 2 Double-cliquez sur le fichier **setup.exe** pour démarrer l'installation. Si votre environnement comprend plusieurs *Serveurs de boîtes aux lettres Exchange*, exécutez ce programme d'installation sur chacun d'entre eux.
- 3 Sélectionnez la langue de l'installation, puis cliquez sur **OK**.
- 4 Cliquez sur **Suivant** lorsque l'écran de *Bienvenue* s'affiche.
- 5 Lisez le contrat de licence, acceptez-en les termes, puis cliquez sur **Suivant**.
- 6 Cliquez sur **Suivant** pour installer le gestionnaire de boîtes aux lettres EAS à l'emplacement par défaut, à savoir `C:\Program Files\Dell\EAS Mailbox Manager\`.
- 7 Dans l'écran *Informations de connexion*, entrez les références du compte d'utilisateur qui se connectera pour utiliser ce service.

Nom d'utilisateur : `DOMAINE\Nom d'utilisateur`

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

Cliquez sur **Suivant**.

- 8 Cliquez sur **Installer** dans l'écran *Prêt à lancer l'installation*.

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

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

Utiliser l'utilitaire de configuration EAS

- 1 Sur le même ordinateur, accédez à **Démarrer > Dell > Utilitaire de configuration EAS > Configuration EAS** afin d'exécuter l'utilitaire de configuration EAS.
- 2 Cliquez sur **Configurer** pour configurer les paramètres de gestion EAS.
- 3 Saisissez les informations suivantes :

Nom d'hôte de DDP Enterprise Server - VE

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

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

REMARQUE :

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

Cliquez sur **OK**.

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

Après le processus de déploiement



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

Sur votre ou vos serveur(s) de boîte aux lettres Exchange

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

Nom d'hôte de DDP Enterprise Server - VE

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

Décochez la case permettant d'exécuter le gestionnaire de périphérique EAS en mode rapport

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

Activer la vérification de la chaîne d'approbation du gestionnaire

Si un certificat auto-signé est utilisé sur VE Server pour SED ou Bitlocker Manager, la validation d'approbation SSL/TLS doit être *désactivée* sur l'ordinateur client. Avant l'activation de la validation d'approbation SSL/TLS sur l'ordinateur client, les conditions suivantes doivent être remplies :

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

Pour activer la validation d'approbation SSL/TLS, modifiez la valeur d'entrée de registre suivante sur 0 sur l'ordinateur client :

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

DisableSSLCertTrust=REG_DWORD (32-bit):0



Tâches d'administrateur de la console de gestion à distance VE

Assigner le rôle d'administrateur Dell

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

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

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

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

Se connecter avec le rôle d'administrateur Dell

- 1 Déconnectez-vous de la Console de gestion à distance Enterprise Server.
- 2 Connectez-vous à Console de gestion à distance Enterprise Server et connectez-vous avec les données d'identification de l'utilisateur de domaine.

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

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

- Les ordinateurs Windows seront cryptés
- Les ordinateurs équipés de lecteurs à auto-cryptage seront cryptés
- Les ordinateurs Windows avec accélérateur de cryptage matériel seront cryptés
- La gestion BitLocker n'est pas activée
- Advanced Threat Protection n'est pas activé



- La protection contre les menaces est activée
- Les supports externes ne seront pas cryptés
- Les périphériques connectés à des ports ne seront pas cryptés
- Data Guardian est activé
- Mobile Edition n'est pas activé

Reportez-vous à la rubrique Aide administrateur pour naviguer jusqu'à Groupes de technologie et la description des règles.

Valider des règles

Validez les règles lorsque l'installation est terminée.

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

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



Ports de solution

Le tableau suivant décrit chaque composant et sa fonction.

| Nom | Port par défaut | Description | Requis pour |
|---|------------------|--|-------------|
| Rapporteur de conformité | HTTP(S)/8084 | Fournit un aperçu complet de l'environnement d'audit et de génération de rapports de conformité. Un composant de DDP Enterprise Server - VE. | Rapports |
| Console de gestion à distance | HTTPS/8443 | Console de gestion et centre de commande pour le déploiement à toute l'entreprise. Un composant de 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 Rapporteur de conformité et la Console de gestion à distance. Collecte et stocke les données d'authentification. Contrôle l'accès basé sur des rôles. Un composant de 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 de DDP Enterprise Server - VE. | Tous |
| Security Server | HTTPS/8443 | Communique avec Proxy de stratégie, gère les extractions de clé de détection, les activations de client, les produits Data Guardian et les communications SED-PBA. Un composant de 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 de DDP Enterprise Server - VE. | Tous |
| Service Courtier de messages | TCP/61616 | Gère les communications entre les services de Dell Enterprise Server - VE. Organise les | Tous |



| Nom | Port par défaut | Description | Requis pour |
|-------------------------|--|--|--|
| | et STOMP/61613 (fermé ou, si configuré pour DMZ, port 61613 ouvert) | informations sur les stratégies créées par le Compatibility Server pour la mise en file d'attente de proxy des stratégies. Un composant de DDP Enterprise Server - VE. | |
| Serveur d'identité | HTTPS/8445 | Gère les demandes d'authentification de serveur, dont l'authentification du SED Manager. Exige un compte Active Directory. Un composant de 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 de DDP Enterprise Server - VE. | API Forensic |
| Serveur d'inventaire | 8887 | Traite la file d'attente de l'inventaire. Un composant de DDP Enterprise Server - VE. | Tous |
| 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 de DDP Enterprise Server - VE. | Édition Entreprise pour Mac Édition Entreprise pour Windows Mobile Edition |
| LDAP | 389/636, 3268/3269 RPC - 135, 49125+ | 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. 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. | Tous |
| Authentification client | HTTPS/8449 | Permet aux serveurs client de s'authentifier auprès de DDP Enterprise Server - VE. | Cryptage du serveur |
| Balise de rappel | HTTP/8446 | Permet d'insérer une balise de rappel dans chaque fichier Office protégé lors de l'exécution du mode protégé Office Data Guardian. | Data Guardian |

| Nom | Port par défaut | Description | Requis pour |
|--|-----------------|---|--|
| Advanced Threat Prevention | HTTPS/TCP/443 | Communication du client en cas d'utilisation d'Advanced Threat Prevention | Advanced Threat Prevention |
| Gestionnaire de périphériques EAS | N/A | Permet une fonctionnalité sans fil. Installé sur le Serveur d'accès au client Exchange. | Gestion d'appareils mobiles par Exchange ActiveSync. |
| Gestionnaire de boîtes aux lettres EAS | N/A | L'agent de boîtes aux lettres qui est installé sur le serveur de boîtes aux lettres Exchange. | Gestion d'appareils mobiles par Exchange ActiveSync. |

Synchronisation horaire NTP : TCP et UDP/123 (pour plus d'informations, reportez-vous à <https://help.ubuntu.com/lts/serverguide/NTP.html>.)

