Dell Data Guardian

Guide de l'administrateur de Windows, de Mac, d'un appareil mobile et du Web v2.0

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.

Marques déposées et marques commerciales utilisées dans Dell Encryption, Endpoint Security Suite Enterprise et dans la suite de documents 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®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, 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. Dropbox℠ est une marque de service de Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™ et Google™ Play sont des marques commerciales ou des marques déposées de Google Inc. aux États-Unis et dans d'autres pays. Apple®, App Store℠, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle® et iPod nano®, Macintosh® et Safari® sont des marques de service, des marques commerciales ou des marques déposées d'Apple, Inc. aux États-Unis et/ou dans d'autres pays. 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. 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. 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. Bing ® est une marque déposée de Microsoft Inc. Ask® est une marque déposée d'IAC Publishing, LLC. Les autres noms peuvent être des marques de leurs propriétaires respectifs.

Guide de l'administrateur de Windows, de Mac, d'un appareil mobile et du Web

2018 - 08

Rév. A01

Table des matières

1

Introduction

Toutes les informations relatives aux règles ainsi que leur description se trouvent dans AdminHelp.

Before You Begin

1 Installez le Serveur Dell avant de déployer les clients. Localisez le guide qui convient tel qu'illustré ci-dessous, suivez les instructions puis revenez à ce guide.

- *Security Management Server et de migration de Security Management Server*
- *Security Management Server Virtual Guide d'installation de Security Management Server Virtual)*
- Vérifiez que les stratégies sont définies comme vous le souhaitez. Naviguez dans AdminHelp, disponible à partir du « **?** » en haut à droite de l'écran. AdminHelp est une aide au niveau de la page, conçue pour vous aider à configurer et à modifier une règle et à comprendre les options disponibles avec votre Serveur Dell.

2 Lisez attentivement le chapitre Configuration requise de ce document.

3 Déployez les clients sur les utilisateurs.

Contacter Dell ProSupport

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

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

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

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

2

Configuration requise

Serveur Dell

Data Guardian pour Windows, Mac et appareils mobiles exige les serveurs Security Management Server ou Security Management Server Virtual v9.6 ou versions ultérieures. Le client Web Data Guardian exige les serveurs Security Management Server ou Security Management Server Virtual v9.8 ou versions ultérieures. Dans ce document, les deux serveurs sont appelés Serveur Dell, sauf lorsqu'il est nécessaire de désigner une version spécifique (par exemple, une procédure varie en cas d'utilisation de Security Management Server Virtual).

Data Guardian pour Windows

- Les meilleures pratiques informatiques doivent être suivies pendant le déploiement. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.
- Le compte utilisateur servant à l'installation/la mise à jour/la désinstallation doit correspondre à un administrateur local ou de domaine, qui peut être affecté temporairement par un outil de déploiement tel que Microsoft SMS ou Dell KACE. Les utilisateurs non-administrateurs et disposant de privilèges particuliers ne sont pas pris en charge.
- Sauvegardez toutes les données importantes avant de démarrer l'installation ou la désinstallation.
- Lors de l'installation, n'apportez aucune modification à l'ordinateur, notamment, n'insérez ou ne retirez pas de lecteurs externes (USB).
- Data Guardian est pris en charge avec certaines versions de Microsoft Office 2016 ainsi que Microsoft Office 365 Business et Business Premium. Il n'est pas pris en charge avec Office 365 Business Essentials.
- Pour le cryptage cloud, l'ordinateur doit disposer d'un lecteur de disque (valeur de lettre) attribuable disponible.
- Vérifiez que les périphériques cibles sont connectés à https://nomdevotreserveurdesécurité.domaine.com:8443/cloudweb/register et https://nomdevotreserveurdesécurité.domaine.com:8443/cloudweb.
- Avant de déployer Data Guardian, il est préférable de ne pas avoir créé de compte de stockage Cloud sur les périphériques cibles.

  Si les utilisateurs décident de conserver leurs comptes existants, ils doivent déplacer tout fichier devant rester *non crypté* en dehors du client de synchronisation avant d'installer Data Guardian.
- L'utilisateur doit être prêt à redémarrer son ordinateur Windows une fois l'installation du client terminée.
- Data Guardian ne perturbe pas le fonctionnement des clients de synchronisation. Les administrateurs et les utilisateurs doivent donc se familiariser avec le fonctionnement de ces applications avant de déployer Data Guardian. Pour plus d'informations, reportez-vous au support Box sur https://support.box.com/home, au support Dropbox sur https://www.dropbox.com/help, ou au support OneDrive sur http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Les documents Office protégés sont pris en charge avec Mozy, une solution complémentaire de Data Guardian, ainsi qu'avec les clouds, e-mails et produits de stockage NFS.
- Si Office 2010 est en cours d'exécution : si des règles ont été définies pour protéger les documents Office et les documents prenant en charge les macros, les utilisateurs doivent disposer d'Office 2010 Service Pack 1 ou version ultérieure (v14.0.6029 ou ultérieure). Voir https://support.microsoft.com/en-us/kb/2121559 pour déterminer si un Service Pack a été appliqué à une suite Microsoft Office 2010. Sans cette mise à jour, les documents protégés ne sont pas accessibles. Les nouveaux documents Office ne sont pas protégés quelle que soit la règle, à moins que la fonctionnalité d'analyse soit activée. La prochaine analyse convertit les documents Office en fichiers protégés, mais les utilisateurs ne peuvent y accéder sans une version d'Office prise en charge.
- Bien que Dell Encryption ne soit pas obligatoire, s'il est utilisé, la version du client Encryption doit être v8.12 ou une version ultérieure.
- Data Guardian ne prend pas en charge l'outil de restauration du système de Windows ou Windows Insider Preview.
- L'option Redirection de dossier de Microsoft n'est pas prise en charge avec Data Guardian.
- IPv6 n'est pas pris en charge avec le cryptage cloud.
- Consultez régulièrement le site www.dell.com/support pour obtenir la documentation la plus récente et des conseils techniques.

Pré-requis

Le programme d'installation installe le package redistribuable Microsoft Visual C++ 2015 (x86 et x64) s'il n'est pas déjà installé.

REMARQUE :

Pour Windows 7 et Windows 8.1, les dernières mises à jour Windows doivent être installées. Pour plus d'informations, voir https://support.microsoft.com/en-us/help/2919355 et https://support.microsoft.com/en-us/help/2999226.

Microsoft .Net 4.5.2 (ou version ultérieure) est requis pour Data Guardian. Tous les ordinateurs expédiés depuis l'usine Dell sont préinstallés avec .Net 4.5.2. Cependant, si vous n'effectuez pas l'installation sur du matériel Dell ou que vous procédez à une mise à niveau de Data Guardian sur du matériel Dell plus ancien, vous devez vérifier la version de .Net installée et la mettre à jour, si nécessaire, avant d'installer Data Guardian pour éviter tout échec d'installation/de mise à niveau. Pour vérifier la version de .Net installée, suivez ces instructions sur l'ordinateur ciblé pour l'installation : http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Pour installer Microsoft .Net Framework 4.5.2, accédez à https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Matériel

La configuration minimale requise doit répondre aux spécifications minimales du système d'exploitation. Le tableau suivant répertorie le matériel pris en charge pour le client Windows.

Matériel Windows
• 200 Mo d'espace disque disponible, selon le système d'exploitation
• Carte d'interface réseau 10/100/1000 ou Wi-Fi
• TCP/IP installé et activé

Si votre entreprise crypte les données pour un stockage dans le cloud, votre ordinateur doit disposer d'un caractère alphabétique libre pouvant être affecté à un lecteur de disque.

Systèmes d'exploitation

Le tableau suivant décrit les systèmes d'exploitation pris en charge.

Systèmes d'exploitation Windows (32 bits et 64 bits)
• Windows 7 SP1 : Entreprise, Professionnel, Ultimate
• Windows 8.1 Mise à jour 0-1 : Enterprise Edition, Pro Edition
• Windows 10 : Éducation, Entreprise, Pro Version 1607 (Mise à jour anniversaire/Redstone 1) jusqu'à la version 1803 (Mise à jour Spring Creators Update/Redstone 4)

REMARQUE :

Le client doit être sur l'un de ces systèmes d'exploitation. Dans le cas contraire, il sera bloqué. Si nécessaire, un paramètre d'une clé de Registre permet à l'administrateur de contourner le blocage.

Pour la prise en charge de Redstone 4, vous devez mettre l'agent à niveau avant d'effectuer la mise à niveau du système d'exploitation.

REMARQUE :

Data Guardian n'est pas compatible avec Windows Defender Exploit Guard (WDEG) de Microsoft dans Redstone 3 et versions ultérieures ou avec Enhanced Mitigation Experience Toolkit (EMET) dans Redstone 2 et versions antérieures.

Windows 7 n'est pas pris en charge avec la stratégie de géolocalisation pour les événements d'audit Data Guardian.

Data Guardian ne prend pas en charge plusieurs versions d'Office sur un ordinateur.

Fournisseurs de stockage cloud

Le tableau ci-dessous décrit les fournisseurs de stockage cloud qui fonctionnent avec Data Guardian pour Windows. Les mises à jour des fournisseurs de stockage cloud sont mises sur le marché fréquemment. Dell recommande de tester les nouvelles versions avec Data Guardian avant de les présenter à l'environnement de production.

Fournisseurs de stockage cloud

- Dropbox
- Dropbox for Business (Windows uniquement)

  REMARQUE :

  Selon la version de Serveur Dell utilisée par votre société, tous les fichiers et dossiers des comptes personnels Dropbox liés à des comptes professionnels peuvent être cryptés.

- Box

  REMARQUE :

  Box Tools et Box Edit sont pas pris en charge par Data Guardian. L'utilisation de Box Tools peut entraîner la survenue d'un écran bleu.

- Google Drive

  REMARQUE :

  La sauvegarde et la synchronisation Google ne sont pas prises en charge.

- OneDrive
- OneDrive for Business
- Unified OneDrive

  REMARQUE :

  Unified OneDrive est un client de synchronisation unifié pour OneDrive et OneDrive for Business.

Microsoft Office

Data Guardian prend en charge les versions d'Office suivantes. Cependant, une seule version d'Office doit être installée.

Microsoft Office

- Office 2010 SP2
- Office 2013 SP1

Microsoft Office

- Office 2016
- Office 365 ProPlus : Différée 1705, Semi-annuelle 1708 et Tous les mois 1803

Data Guardian pour Mac

Le tableau suivant répertorie le matériel pris en charge pour le client Mac.

Matériel Mac

- Processeur Intel Core 2 Duo, Core i3, Core i5, Core i7, ou Xeon
- 2 Go de RAM
- 10 Go d'espace disque disponible

Systèmes d'exploitation

La liste suivante répertorie les systèmes d'exploitation pris en charge.

Systèmes d'exploitation Mac

- Mac OS X El Capitan 10.11.6
- macOS Sierra 10.12.6
- macOS High Sierra 10.13.5 - 10.13.6

Fournisseurs de stockage cloud

Selon les paramètres de règles, les éléments suivants peuvent s'afficher dans l'interface Mac de Data Guardian. L'utilisateur n'a pas besoin de télécharger ou d'installer le client de synchronisation Cloud.

Fournisseurs de stockage cloud

- Dropbox
- Box
- Google Drive
- OneDrive
- OneDrive for Business

Application Data Guardian pour appareils mobiles

La liste suivante répertorie les systèmes d'exploitation pris en charge avec l'application Data Guardian pour appareils mobiles.

Systèmes d'exploitation Android

- 4.4-4.4.4 KitKat
- 5.0-5.1.1 Lollipop
- 6.0 -6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo

Systèmes d'exploitation iOS

- iOS 9.x
- iOS 10.x-10.3
- iOS 11-11.3

Data Guardian pour le Web

Pour activer le client Web Data Guardian, l'administrateur met en place une machine virtuelle qui héberge le client Web et communique avec Serveur Dell v9.8 ou versions ultérieures.

Les environnements virtualisés suivants peuvent être utilisés pour déployer le client Web Data Guardian.

Environnements virtualisés

- 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

Environnements virtualisés

- 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

Navigateurs Web

Vous pouvez utiliser Data Guardian avec Internet Explorer, Mozilla Firefox, Google Chrome et Microsoft Edge.

Pour Mac, Safari est également pris en charge.

Langues prises en charge

Ces clients sont compatibles avec l'interface utilisateur multilingue (MUI – Multilingual User Interface) et prennent en charge les langues suivantes.

Langues prises en charge

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

3

Configurer et installer Data Guardian pour Windows

Paramètres de registre du client Data Guardian

Cette section décrit en détail tous les paramètres du registre approuvé Dell ProSupport des ordinateurs clients locaux, quel que soit le motif des paramètres de registre. Si un paramètre de registre chevauche deux produits, il est répertorié dans chaque catégorie.

Ces modifications de registre doivent être effectuées par les administrateurs uniquement et peuvent ne pas être appropriées ou fonctionner dans tous les cas de figure.

- Les niveaux de journalisation peuvent être augmentés pour aider au dépannage. Créez ou modifiez le paramètre de registre suivant :

  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  "LogVerbosity"=dword:0x1f (31)

  Par défaut, le niveau de journalisation est défini sur 0xf (15).

  Valeurs disponibles :

  Désactivé = 0x0 (0)

  Critique = 0x1 (1)

  Erreur = 0x3 (3)

  Avertissement = 0x7 (7)

  Information = 0xf (15)

  Débogage = 0x1f (31)

- Une fois Data Guardian installé, les utilisateurs internes sont automatiquement activés. Si nécessaire, vous pouvez modifier un paramètre de registre pour remplacer l'activation automatique.
  [HKLM\SOFTWARE\Dell\Dell Data Protection\Data Guardian]

  Valeur DWORD : DisableAutomaticActivation=1

  REMARQUE :
  Vous pouvez également confirmer les alias de votre domaine sur Serveur Dell. Voir Dépanner les problèmes d'activation automatique.

Configurer le serveur pour Data Guardian

En fonction des règles définies par un administrateur, Data Guardian protège les données, notamment :

- Les documents Office stockés localement, partagés avec d'autres utilisateurs de différentes façons ou stockés sur un média amovible. Les documents Office suivants peuvent être protégés : .docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf.

- Systèmes de partage de fichiers basés sur le cloud : les ordinateurs ou périphériques mobiles Windows capturent des données destinées au stockage cloud, cryptent ces données puis les chargent dans le cloud.

Informez les utilisateurs si votre entreprise utilise Data Guardian pour les documents Office uniquement, le stockage cloud uniquement, ou les deux.

Configuration de Dell Security Management Server Virtual pour Data Guardian

Pour configurer Dell Security Management Server Virtual de sorte qu'il prenne en charge Data Guardian, accédez à la Console de gestion à distance et réglez l'une ou les deux règles Data Guardian sur **Activé** :

- *Documents Office protégés* - Niveau Entreprise uniquement
- *Cryptage Cloud* - Niveau Entreprise, Groupes finaux, ou Points de terminaison

Configuration de Dell Security Management Server pour Data Guardian

Pour configurer Dell Security Management Server de sorte qu'il prenne en charge Data Guardian, accédez à la Console de gestion, et réglez l'une ou les deux règles Data Guardian sur **Activé** :

- *Documents Office protégés* - Niveau Entreprise uniquement
- *Cryptage Cloud* - Niveau Entreprise, Groupes finaux, ou Points de terminaison

Ensuite, configurez le Security Server pour autoriser les téléchargements du client Cloud.

Configuration de Security Management Server pour autoriser les téléchargements du client Data Guardian

Cette rubrique décrit la procédure à suivre pour permettre aux utilisateurs de télécharger le client Data Guardian pour Windows depuis Security Management Server.

1 Sur Security Management Server accédez au *<répertoire d'installation de Security Server>\webapps\root\cloudweb\brand\dell\resources* et ouvrez le fichier *messages.properties* dans un éditeur de texte.

2 Vérifiez que les entrées sont conformes aux informations suivantes :

```
download.deviceWin.mode=remote

download.deviceWin.local.filename.32=DataGuardian_32bit_setup.exe

download.deviceWin.local.filename.64=DataGuardian_64bit_setup.exe
```

3 Modifiez les entrées comme suit :

```
download.deviceWin.remote.link.32=https://<VOTRE URL HÔTE>:<PORT>/cloudweb/download/DataGuardian_32bit_setup.exe

download.deviceWin.remote.link.64=https://<VOTRE URL HÔTE>:<PORT>/cloudweb/download/DataGuardian_64bit_setup.exe
```

4 Enregistrez le fichier, puis fermez-le.

5 Rendez-vous sur <répertoire d'installation du serveur de sécurité> et créez un nouveau dossier dans cette catégorie en l'appelant Download (Serveur de sécurité\Download).

6 Dans le dossier Download, créez un autre dossier en l'appelant cloudweb (Security Server\Download\cloudweb).

7 Ajoutez les fichiers de configuration 64 bits et 32 bits de Data Guardian dans le dossier cloudweb et renommez-les, par exemple respectivement DataGuardian64.exe et DataGuardian32.exe.

Les noms de ces fichiers sont définis par l'utilisateur mais doivent correspondre aux noms de fichier figurant dans le fichier versions.xml.

8 Redémarrez Security Server pour appliquer les modifications.

Configuration du serveur Security Management Server pour le téléchargement automatique du client Data Guardian Windows (facultatif)

Pour les téléchargements automatiques, le fichier versions.xml et les fichiers binaires doivent se trouver au même emplacement. Le client doit pouvoir y accéder. Il peut donc s'agir d'IIS ou vous pouvez utiliser le dossier **Security Server\Download\cloudweb** que vous avez créé. Si vous utilisez le dossier cloudweb, suivez cet exemple de configuration.

1 Accédez au dossier **Security Server\Download\cloudweb**. (Voir l'étape 6 dans Configurer le Security Server pour autoriser les téléchargements du client Data Guardian.)

2 Créez un dossier nommé MiseàjourDataGuardian.

REMARQUE :
Nous avons utilisé MiseàjourDataGuardian dans cet exemple, mais vous pouvez choisir un autre nom.

3 Placez les fichiers exécutables mis à jour dans le dossier MiseàjourDataGuardian.

4 Créez un fichier *versions.xml* dans le dossier MiseàjourDataGuardian.

5 Ouvrez *versions.xml* dans un éditeur de texte et vérifiez que le chemin d'accès du nom de fichier est correct pour votre environnement.

Exemples :

```
<?xml version="1.0"?>
<VERSIONS>
<VERSION arch="x86" product="sl" version="0.x.x.xxxx" filename="/setup32.exe"/>
<VERSION arch="x64" product="sl" version="0.x.x.xxxx" filename="/setup64.exe"/>
</VERSIONS>
```

Version : version de fichier des éléments exécutables mis à jour

Nom du fichier setup.exe : le nom de configuration des fichiers exécutables est défini par l'utilisateur, mais il doit correspondre au nom de configuration figurant dans le fichier messages.properties. (Voir l'étape 3 dans Configurer le Security Server pour autoriser les téléchargements du client Data Guardian.)

6 Enregistrez le fichier, puis fermez-le.

7 Ajoutez les fichiers binaires à ce dossier.

8 Si vous utilisez IIS, redémarrez-le.

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

10 Dans le volet de gauche, cliquez sur **Populations** > **Entreprise**. L'onglet Règles de sécurité s'affiche.

11 Dans le groupe de technologie Data Guardian, cliquez sur **Cryptage Cloud > Afficher les paramètres avancés**.

12 Faites défiler jusqu'à la règle *URL du serveur de mise à jour de logiciels* et saisissez **https://<VOTRE URL D'HÔTE > / MiseàjourDataGuardian**.

REMARQUE :
MiseàjourDataGuardian est donné à titre de suggestion pour correspondre à l'exemple ci-dessus.

13 Cliquez sur **Enregistrer** pour placer la modification de la règle dans la file d'attente de validation.

14 Cliquez sur **Gestion** > **Valider**.

15 Saisissez un commentaire et cliquez sur **Valider les règles**.

Réinstallation d'une image d'un ordinateur doté de Data Guardian

Si une image de l'ordinateur a besoin d'être réinstallée et que l'ordinateur est doté de Data Guardian, demandez si l'utilisateur a travaillé hors ligne et s'il a créé des documents Office protégés pendant cette période. Si c'est le cas, des clés hors ligne ont été générées pour ces documents et celles-ci n'ont pas été mises en dépôt sur Serveur Dell.

1 Pour plus d'informations sur la récupération des clés Data Guardian créées hors ligne qui n'ont pas été mises en dépôt sur Serveur Dell, voir le *Guide de récupération*.

2 Vérifiez la présence d'un dossier de clés hors ligne avant de réinstaller l'image de l'ordinateur.

   Lorsque les premières clés mises en dépôt sont créées, un dossier Data Guardian est ajouté à C:\Program Files\Dell. Accédez au dossier Data Guardian > OfflineKeys. Si un tel dossier n'existe pas, vérifiez le dossier Mes documents de l'utilisateur.

Désactiver Microsoft Exploit Guard ou EMET dans les applications gérées

Sous Windows 10, vous pouvez activer ou intégrer les éléments suivants au système d'exploitation :

- Redstone 3 et versions ultérieures : Windows Defender Exploit Guard (WDEG)
- Redstone 2 et versions antérieures : Enhanced Mitigation Experience Toolkit (EMET)

Si ces fonctionnalités sont activées ou intégrées, vous devez configurer les paramètres pour désactiver ces applications gérées dans Data Guardian :

- winword.exe
- powerpnt.exe
- excel.exe
- acrord32.exe

Windows Defender Exploit Guard (WDEG)

Pour désactiver les applications gérées :

1 Accédez au **Centre de sécurité Windows Defender**.

2 Cliquez sur **Contrôle Applications et navigateur**.

3 Faites défiler jusqu'au bas de l'écran et cliquez sur **Paramètres de protection d'Exploit**.

4 Sélectionnez **Paramètres du programme**.

5 Cliquez sur **+** pour ajouter les applications gérées répertoriées ci-dessus.

6 Dans les propriétés de chaque application gérée, cochez la case *Remplacer* pour toute option définie sur *Activé* et basculez l'option sur **Désactivé**.

   REMARQUE :
   Si une application gérée est ouverte et qu'une boîte de dialogue vous demande de redémarrer le .exe, redémarrez-le une fois ces étapes terminées.

7 Cliquez sur **Appliquer**.

8 Cliquez sur **Oui**.

   Dans Paramètres du programme, l'application gérée répertorie les remplacements en fonction des options que vous avez modifiées.

Enhanced Mitigation Experience Toolkit (EMET)

Pour désactiver les applications gérées :

1 Accéder à **Configuration de l'application**.

2 Dans les options **Vérification de l'appelant ROP** et **Filtrage des adresses dans le tableau d'exportation des adresses (EAF)**, décochez les cases correspondantes aux applications gérées répertoriées ci-dessus.

Gérer les profils de fournisseur de protection du stockage Cloud

Data Guardian crypte les fichiers des utilisateurs et envoie les événements d'audit au Serveur Dell. Pour modifier le comportement de chaque fournisseur de stockage cloud, définissez chaque fournisseur sur l'une de ces valeurs :

Valeur	Description
Protéger	Autoriser le fournisseur/la connexion, crypter les fichiers et envoyer des événements d'audit sur l'activité des fichiers/dossiers.
Bloquer	Bloquer tous les accès au fournisseur/à la connexion.
Autoriser	Autoriser le fournisseur/la connexion à transiter sans cryptage, mais faire un audit de l'activité des fichiers/dossiers.
Éviter	Éviter la protection du fournisseur/de la connexion, sans cryptage ni audit. Lorsque cette valeur est définie, le dossier du fournisseur de stockage cloud ne s'affiche pas dans l'unité virtuelle Data Guardian sur l'ordinateur client.

Pour en savoir plus, voir l'*Aide administrateur*, disponible à partir de la Console de gestion à distance de Serveur Dell.

Autoriser/Refuser les utilisateurs de la liste d'accès total/liste noire

Vous pouvez déterminer quels utilisateurs externes peuvent s'enregistrer sur le Data Guardian afin d'utiliser Serveur Dell. Pour assurer une sécurité adéquate, configurez et gérez soigneusement ces listes.

- Un utilisateur interne se situe dans le domaine.
- Un utilisateur externe est un utilisateur hors domaine, c'est-à-dire soit une personne appartenant à une autre organisation avec laquelle un utilisateur interne souhaite partager des documents commercialement sensibles, soit un utilisateur interne désirant avoir accès à son ordinateur à partir d'un périphérique non membre du domaine.

Pour permettre à un utilisateur extérieur au domaine de l'organisation de s'inscrire pour utiliser Data Guardian :

1 Dans le volet de gauche de la console de gestion à distance, cliquez sur **Gestion > Gestion des utilisateurs externes**.

2 Cliquez sur **Ajouter**.

3 Sélectionnez le type d'accès à l'inscription :

Liste noire : bloque l'inscription d'un utilisateur ou d'un domaine. L'utilisateur ne peut pas ouvrir un document Office protégé ni un fichier .xen.

Liste d'accès total : autorise l'inscription et l'accès aux fichiers d'un utilisateur ou d'un domaine. Si un utilisateur ou un domaine sont également sur la liste noire, aucun accès n'est accordé.

4 Dans le champ Saisir un domaine/e-mail, saisissez le domaine de l'utilisateur pour autoriser l'accès à la totalité du domaine, ou une adresse e-mail pour autoriser l'accès uniquement à cet utilisateur.

REMARQUE : Pour les utilisateurs mobiles externes dans un environnement hébergé, l'e-mail doit être en minuscules.

5 Cliquez sur **Ajouter**.

Pour plus d'informations sur l'utilisation de la liste d'accès total/liste noire, voir l'*Aide administrateur*, accessible à partir de la Console de gestion.

Installez Data Guardian

Il existe deux méthodes d'installation de Data Guardian :

- Installer Data Guardian de manière interactive
- Installer Data Guardian par ligne de commande

Les utilisateurs Data Guardian doivent effectuer les tâches suivantes pour que les fichiers et dossiers de leurs clients de synchronisation Cloud soient protégés. Une fois le client Data Guardian installé, les utilisateurs doivent télécharger un fournisseur de stockage cloud :

- L'administrateur doit indiquer le fournisseur de synchronisation cloud à utiliser.

  ou

- Fournissez aux utilisateurs un lien de téléchargement et d'installation de Dropbox for Business ou OneDrive for Business/Unified OneDrive si votre entreprise utilise un de ces fournisseurs. Les utilisateurs de Dropbox for Business doivent se connecter à Dropbox for Business via Data Guardian.

Dossiers préexistants contenant des fichiers non cryptés

Lors du déploiement de Data Guardian, il est préférable de ne pas avoir créé de compte de fournisseur de stockage cloud sur les périphériques cibles.

Si un compte de fournisseur de stockage cloud est configuré pour les dossiers qui sont synchronisés sur l'ordinateur local avant l'installation de Data Guardian :

- Les dossiers et fichiers existants qui se synchronisent vers le cloud restent en clair
- Les fichiers que vous ajoutez à ces dossiers existants restent en clair
- Les fichiers qui se synchronisent depuis le cloud sont cryptés

  Si vous souhaitez que les fichiers déjà existants soient cryptés, accédez au Lecteur virtuel DDG vDisk (créé à l'installation de Data Guardian), créez un nouveau sous-dossier dans le client de synchronisation cloud et déplacez les fichiers déjà existants dans ce dossier.

  ou

  Pour les contenus volumineux, un administrateur ou un gestionnaire peut temporairement demander le menu Gérer les dossiers.

Menu Gérer les dossiers

Certains gestionnaires ou administrateurs peuvent avoir besoin de dépanner temporairement les dossiers partagés par plus d'un utilisateur. Vous pouvez demander l'autorisation de votre administrateur pour l'option Gérer les dossiers. En général, il s'agit d'une option temporaire.

Installation interactive de Data Guardian sous Windows

Vous devez disposer des droits d'administrateur pour installer Data Guardian. Si ce sont les utilisateurs qui installent le produit, informez-les de l'emplacement du kit d'installation.

Avant de commencer

Selon le serveur et le produit Data Guardian, procédez comme suit :

Dell Security Center hébergé	Local (pour Dell Management Server)	Cryptage Cloud
Pour les versions ultérieures.	Assurez-vous que vous connaissez le nom du Dell Security Management Server.	L'ordinateur doit disposer d'une lettre disponible, pouvant être attribuée à un lecteur de disque.

Installez Data Guardian

Soyez prêt à redémarrer l'ordinateur après l'installation de Data Guardian.

1 Pour télécharger le programme d'installation de Data Guardian, rendez-vous à l'emplacement spécifié par votre administrateur.

2 En fonction de votre système d'exploitation, sélectionnez le programme d'installation 32 bits ou 64 bits, généralement nommés **setup32.exe** et **setup64.exe**, et le copiez-le sur l'ordinateur local.

3 Double-cliquez sur le fichier pour lancer le programme d'installation.

4 Si vous recevez un avertissement de sécurité, cliquez sur **Exécuter**.

5 Sélectionnez une langue, puis cliquez sur **OK**.

6 Si vous êtes invité à installer Microsoft Visual C++ 2015 Redistributable Package ou Microsoft .NET Framework 4.5.2 Client Profile, cliquez sur **OK**.

7 Dans la page d'accueil, cliquez sur **Suivant**.

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

9 À l'écran Dossier de destination, cliquez sur **Suivant** pour installer à l'emplacement par défaut suivant **C:\Program Files\Dell\Data Guardian\.**

Sur **C:**, n'installez pas Data Guardian dans les dossiers Users ou Windows, ou à la racine d'un lecteur. Vous obtiendrez un message d'erreur.

10 Sélectionnez **Serveur Dell Management local** :

Dell Security Center hébergé	Serveur Dell Management local
Pour les versions ultérieures.	Dans le champ *Nom du serveur de gestion Dell :*, saisissez le nom du serveur avec lequel cet ordinateur communiquera, par exemple server.domain.com. Il n'est pas nécessaire d'inclure www ou http(s). Cette information est fournie par votre administrateur. Ne décochez pas la case *Activer la vérification de confiance SSL* sauf si votre administrateur vous le demande.

11 Cliquez sur **Suivant**.

12 Dans l'écran d'information Confirmer le serveur de gestion Dell, confirmez que l'adresse URL du serveur est correcte. Le programme d'installation ajoute www ou http(s) et le port. Cliquez sur **Suivant**.

13 Dans la fenêtre Type de gestion, sélectionnez cette option :

- Utilisation interne : utilisateur doté d'une adresse e-mail incluse dans le domaine de la société.

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

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

15 Lorsque l'écran Installation terminée s'affiche, cliquez sur **Terminer**.

16 Cliquez sur **Oui** pour redémarrer.

L'installation de Data Guardian est maintenant terminée.

17 Demandez aux utilisateurs finaux de confirmer l'activation. L'icône Data Guardian dans la barre d'état système affiche une coche verte  . En fonction de la manière dont Data Guardian est déployé au sein de l'entreprise, l'activation peut ne pas être immédiate. Si ce n'est pas le cas, l'utilisateur final doit l'activer manuellement. Dans un environnement hébergé, un utilisateur qui doit procède à l'activation manuelle doit relancer la réactivation à chaque fois qu'il redémarre son ordinateur ou le service Data Guardian. Voir le document *Data Guardian User Guide* (Guide d'utilisation de Data Guardian).

Installer Data Guardian par ligne de commande

- Les commutateurs et les paramètres de ligne de commande sont sensibles à la casse.
- Veillez à inclure une valeur contenant un ou plusieurs caractères spéciaux, tels qu'un espace dans la ligne de commande, entre des guillemets d'échappement.
- Le tableau suivant indique les commutateurs disponibles dans le cadre de l'installation.

Commutateur	Signification
/V	Transmission des variables au fichier .msi dans l'élément setup.exe. Le contenu doit toujours être entouré de guillemets en texte brut.
/S	Mode Silencieux

Option	Signification
/QB	Boîte de dialogue de progression dotée du bouton **Annuler** : vous invite à effectuer un redémarrage
/QB!	Boîte de dialogue de progression sans bouton **Annuler** : vous invite à effectuer un redémarrage
/QN	Pas d'interface utilisateur

- Le tableau suivant indique les paramètres disponibles dans le cadre de l'installation.

Paramètres
SERVER= <nom du serveur> (le nom de domaine complet (FQDN) du serveur Dell pour l'activation)
ENTERPRISE=1 (utilisateur interne)
ENABLESSLTRUST=0 (Désactiver la validation d'approbation SSL)
REBOOT=SUPPRESS (Null permet les redémarrages automatiques, SUPPRESS désactive le redémarrage)

Exemples de ligne de commande

- L'exemple suivant installe Data Guardian en mode silencieux, pour un utilisateur interne, sans validation d'approbation SSL, les journaux étant stockés dans C:\Library\Logs\Install.log.

```
setup.exe /S /V"/QB! REBOOT=SUPPRESS ENTERPRISE=1 SERVER=server.domain.com /L*V "c:\Library
\Logs\install.log" ENABLESSLTRUST=0"
```

Set GPO on Domain Controller to Enable Entitlements

- Si vos clients vont bénéficier de droits octroyés par Dell Digital Delivery, suivez les instructions ci-dessous pour définir le GPO sur le contrôleur de domaine, afin d'activer les droits en question (il peut s'agir d'un autre serveur que celui qui exécute Serveur Dell).
- Le poste de travail doit appartenir à l'unité organisationnelle dans laquelle l'objet GPO est appliqué.
- Assurez-vous que le port sortant 443 est disponible pour communiquer avec le Serveur Dell. Si le port 443 est bloqué (pour quelque raison que ce soit), la fonction de droits ne fonctionne pas.

1. Sur le contrôleur de domaine pour la gestion des clients, cliquez sur **Démarrer** > **Outils d'administration** > **Gestion des règles de groupe**.
2. Cliquez avec le bouton droit sur l'unité organisationnelle à laquelle la règle doit être appliquée, puis sélectionnez **Créer un objet GPO dans ce domaine** et **Le lier ici**.

3 Saisissez le nom du nouvel objet GPO, sélectionnez (aucun) dans le champ Objet GPO Starter source, puis cliquez sur **OK**.

4 Cliquez-droit sur l'objet GPO créé et sélectionnez **Modifier**.

5 L'Éditeur de gestion des règles de groupe se charge. Accédez à **Configuration de l'ordinateur** > **Préférences** > **Paramètres Windows** > **Registre**.

6 Cliquez avec le bouton droit sur le registre, puis sélectionnez **Nouveau** > **Élément de registre**. Renseignez les éléments suivants :

Action : Create

Ruche : HKEY_LOCAL_MACHINE

Chemin d'accès à la clé : SOFTWARE\Dell\Dell Data Protection

Nom de la valeur : Server

Type de valeur : REG_SZ

Données de valeur : <adresse IP du Serveur Dell>

7 Cliquez sur **OK**.

8 Déconnectez-vous, puis reconnectez-vous au poste de travail, ou exécutez **gpupdate /force** pour appliquer la règle de groupe.

Désinstaller Data Guardian

- Si un **utilisateur final** possède un compte administrateur local, il peut désinstaller Data Guardian. Pour en savoir plus, voir le *Guide d'utilisation de Data Guardian*. Cette section présente le processus d'administrateur permettant de désinstaller Data Guardian.

> **IMPORTANT: Fichiers non Office sur le Lecteur virtuel DDG vDisk**
> Avant de désinstaller Data Guardian, déplacez tous les fichiers importants à un emplacement hors de Lecteur virtuel DDG vDisk. Si vous désinstallez Data Guardian d'un ordinateur appartenant à des utilisateurs finaux, les dossiers et fichiers du Cloud sont cryptés et inaccessibles. Si cet utilisateur final quitte la société et qu'aucun autre utilisateur ne partage ce dossier ou fichier, les données sont illisibles mais sécurisées (pour afficher les fichiers, ré-installez Data Guardian).
>
> Les documents Office protégés restent cryptés si vous désinstallez Data Guardian. Pour décrypter, reportez-vous au *Guide de restauration* > *Restauration de Data Guardian*.

Désinstallation de ligne de commande

- Après son extraction du programme d'installation principal, le programme d'installation du client Data Guardian se trouve à **C:\Dell \DataGuardian_XXbit_setup.exe**.
- L'exemple suivant correspond à la désinstallation silencieuse du client Data Guardian.

```
setup.exe /x /s /v" /qn"
```

Lorsque vous y êtes invité, redémarrez l'ordinateur.

Utiliser Data Guardian avec Dropbox for Business

Data Guardian avec Dropbox for Business offre des fonctionnalités supplémentaires par rapport à Dropbox de base.

Vous pouvez définir des règles pour contrôler la façon dont les dossiers Dropbox professionnels et personnels sont protégés. Si votre entreprise autorise les comptes professionnels et personnels, les utilisateurs doivent comprendre le cryptage de chaque type de compte. Voir Règle pour les comptes professionnels et personnels.

Règle pour les comptes professionnels et personnels

Votre entreprise peut définir des lignes directrices sur l'utilisation de comptes professionnels et personnels par les membres de l'équipe. En outre, l'entreprise peut autoriser uniquement certains utilisateurs à avoir des comptes professionnels et personnels.

REMARQUE :
Si votre entreprise permet d'avoir des comptes professionnels et personnels, et qu'un utilisateur choisit d'utiliser les deux, celui-ci doit comprendre la gestion des dossiers pour les deux types de compte.

Le tableau suivant décrit le cryptage en fonction du paramètre de règle *Dropbox crypte les dossiers personnels*.

Cryptage	Paramètre de règle	Considérations relatives au déploiement
Crypter tous les fichiers et dossiers professionnels et personnels.	Règle > Dropbox crypte les dossiers personnels > configurée sur **Sélectionné** (par défaut)	Avant de déployer Data Guardian, les utilisateurs doivent sauvegarder les fichiers professionnels préexistants qui se trouvent dans les dossiers de synchronisation de stockage cloud en dehors des dossiers de synchronisation. Les utilisateurs dotés de fichiers personnels qui doivent rester non cryptés doivent les déplacer hors des dossiers de synchronisation professionnels ou dissocier les comptes personnels des clients de synchronisation professionnels. Une fois Data Guardian déployé, les fichiers et dossiers cloud ne peuvent être affichés que sur les ordinateurs ou périphériques exécutant Data Guardian. Si un dossier personnel est crypté de manière non intentionnelle, voir la section « Décrypter des dossiers dans un compte personnel » du Guide d'utilisation de Dell Data Guardian.
Crypter tous les fichiers et dossiers de comptes professionnels. Autoriser que les fichiers et dossiers de comptes personnels restent non cryptés.	Règle > Dropbox crypte les dossiers personnels > configurée sur **Non sélectionné**	Vous pouvez utiliser la règle facultative Message Dropbox crypte les dossiers personnels pour afficher un message personnalisé pour rappeler aux utilisateurs de **ne pas** stocker de fichiers professionnels dans les comptes personnels, puisque ces fichiers ne seront pas protégés. Le message s'affiche dans les cas suivants : • À chaque fois que l'utilisateur se connecte • Lorsque l'utilisateur crée ou ajoute un nouveau fichier ou dossier à un compte Dropbox personnel Si vous configurez la règle Dropbox crypte les dossiers personnels sur **Faux** pour un point final ou un groupe de points finaux, les comptes personnels de tous les utilisateurs sur ces points finaux resteront non cryptés.

Dossiers professionnels et personnels

Si votre organisation est dotée de Dropbox for Business et que vous permettez aux utilisateurs d'avoir des dossiers professionnels et personnels, vous pouvez exécuter des rapports pour s'assurer que tous les fichiers professionnels sont dotés de l'extension de fichier .xen, au cas où un utilisateur copierait un fichier non protégé sensible dans un dossier professionnel. Voir Dépannage de Data Guardian.

Afficher les rapports

Les informations relatives à votre environnement Data Guardian sont disponibles dans la Console de gestion. Sélectionnez **Génération de rapports > Événements d'audit** pour les événements d'audit liés aux dossiers des clients de synchronisation sur le cloud et aux documents Office protégés.

À des fins de conformité et de surveillance des détails des périphériques, des détails de bouclier ou des événements d'audit, consultez la section **Rapports > Gérer les rapports**.

Pour en savoir plus, voir l'*Aide administrateur*, disponible à partir de la Console de gestion.

Dépannage de Data Guardian

Utiliser l'écran Détails

Vous pouvez utiliser l'écran *Détails* pour les problèmes de dépannage ou de support. Par exemple :

- si un utilisateur crée un dossier, mais qu'il ne se crypte pas, sélectionnez **Détails** > **Fichiers** > **État du dossier** pour en vérifier l'état.
- Si un utilisateur final demande une assistance, vous pouvez lui indiquer de configurer l'écran Détails optimisés et de sélectionner l'onglet **Détails** > **Règle**. Cet onglet répertorie les règles en vigueur.
- Afficher les journaux pour le dépannage.

Utiliser l'écran Détails optimisés

- Tout en appuyant sur **<Ctrl><Maj>**, cliquez sur l'icône de Data Guardian, dans la barre d'état système, puis sélectionnez **Détails**.
- Outre les fichiers et dossiers, les éléments suivants s'affichent :

  Sécurité : affiche la clé, le type de clé, et l'état. Ce volet répertorie temporairement certains fichiers Office protégés jusqu'à ce qu'ils soient envoyés à Serveur Dell. La durée d'affichage dépend de l'intervalle d'interrogation.

  Audit : affiche les modules, l'ID utilisateur et le type d'événement. Les informations sont mises en file d'attente dans ce journal d'audit, puis envoyées au Serveur Dell aux intervalles spécifiés. L'administrateur peut consulter les **Événements d'audit** dans le volet de gauche de la Console de gestion pour effectuer un audit.

  Règle : affiche les noms et valeurs de règle.

Affichage des fichiers journaux

- Cliquer sur **Afficher le journal** dans le coin inférieur gauche de l'écran Détails.

  Vous trouverez également les fichiers journaux sur **C:\ProgramData\Dell\Data Guardian**.

  Les fichiers journaux des documents Office protégés se trouvent dans le dossier Custom.xml.

Dépanner les problèmes d'activation automatique

Si Data Guardian ne s'active pas automatiquement pour plusieurs utilisateurs, vous pouvez modifier les paramètres de registre du client Data Guardian. Il est également conseillé de vérifier les alias sur Serveur Dell :

1 Dans la console de gestion, accédez à **Populations > Domaines**, puis sélectionnez un domaine et tous les sous-domaines désirés.
2 Sur la page Détails du domaine, cliquez sur l'onglet **Paramètres**.
3 Dans le champ *Alias*, vérifiez que tous les alias sont corrects.

Fournir des droits temporaires de gestion de dossiers

Vous pouvez octroyer des droits temporaires de gestion des dossiers à un administrateur ou un utilisateur. Par exemple, si les utilisateurs ont chargé des fichiers dans le cloud avant l'installation de Data Guardian, vous pouvez fournir des droits temporaires de gestion de dossiers à certains utilisateurs afin qu'ils puissent gérer le cryptage de chaque dossier au sein des dossiers des clients de synchronisation.

Pour octroyer les droits de gestion des dossiers :

1 Dans la console de gestion, cliquez sur **Populations** > **Points de terminaison**.
2 Recherchez ou cliquez sur un point de terminaison, puis cliquez sur l'onglet **Règles de sécurité**.
3 Sélectionnez **Cryptage Cloud**, puis cliquez sur **Afficher les paramètres avancés**.
4 Cliquez sur la case à cocher en regard de *Gestion de dossiers activée* pour sélectionner la règle.
5 Cliquez sur **Enregistrer**.
6 Dans le volet de gauche, cliquez sur **Gestion** > **Valider**.
7 Saisissez un commentaire et cliquez sur **Valider les règles**.

REMARQUE :
Dell recommande de décocher la case à cocher *Gestion de dossiers activée* une fois les dossiers cryptés ou que le dépannage est terminé, pour désactiver la règle pour ce point de terminaison.

Pour gérer les dossiers sur le point de terminaison :

1 Créez un dossier dans le dossier du client de synchronisation et ajoutez-y des fichiers, de sorte qu'ils soient cryptés dans le cloud.
2 Cliquez sur l'icône de Data Guardian dans la barre d'état système et sélectionnez **Gérer les dossiers**.

   Pour chaque client de synchronisation, une vue hiérarchique des dossiers synchronisés sur le cloud s'affiche. Tous les dossiers sont sélectionnés par défaut. Désélectionnez les dossiers que vous ne souhaitez pas crypter. Si vous désélectionnez un dossier dans Gérer les dossiers, une analyse de décryptage déchiffre les fichiers existants dans ce dossier. Les nouveaux fichiers de ce dossier ne sont pas cryptés sur le disque local ou dans le cloud.

   REMARQUE :
   Si vous faites glisser un fichier crypté dans un dossier qui est désélectionné dans Gérer les dossiers dans le cloud ou sur l'unité virtuelle Data Guardian, le fichier reste crypté et vous ne pouvez pas en afficher le contenu. En outre, si vous partagez le dossier avec un autre utilisateur Data Guardian pour qui la règle Gérer les dossiers n'est pas activée, celui-ci ne pourra pas afficher le contenu des fichiers car ils resteront cryptés.

3 Pour crypter un dossier déjà existant, activez manuellement le cryptage pour ce dossier. Les fichiers sont cryptés lorsque les fichiers se synchronisent sur le Cloud.

Questions fréquemment posées

FAQ sur la gestion des dossiers

Question

J'ai un dossier contenant des fichiers que j'ai partagé avec un autre utilisateur. Dans la barre d'état système, j'ai utilisé l'utilitaire Data Guardian **> Gérer les dossiers** pour décrypter le contenu de ce dossier. Récemment, mes fichiers sont redevenus cryptés dans le Cloud. Ce dossier ne s'affiche plus dans l'utilitaire Gestion des dossiers ; je ne peux donc plus décrypter ces fichiers dans le cloud.

Réponse

Un ID de clé de cryptage est associé à un dossier en fonction du premier utilisateur qui ajoute un fichier à ce dossier. Si un utilisateur crée un dossier et n'ajoute pas de fichiers, sa clé n'est pas associée à ce dossier. L'utilisateur dont l'ID de clé de cryptage a été placée sur le dossier est le seul qui peut voir le dossier dans l'utilitaire Gestion des dossiers. Si l'utilisateur dont l'ID de clé de cryptage est défini sur le dossier désélectionne le dossier dans l'utilitaire Gérer les dossiers et le partage avec un autre utilisateur de Data Guardian, le Data Guardian du deuxième utilisateur crypte à nouveau le contenu.

Solution

1 Créer un nouveau dossier.

2 Déplacez tous les fichiers devant être cryptés dans le nouveau dossier.

3 Dans la barre d'état système, utilisez à nouveau l'utilitaire **Dell Data Guardian** > **Gérer les dossiers** pour décrypter ces fichiers.

REMARQUE :

Si vous décryptez le contenu d'un dossier partagé avec d'autres utilisateurs Data Guardian, le client Data Guardian des autres utilisateurs appliquera la règle de cryptage de celui-ci. La meilleure pratique consiste à utiliser l'utilitaire Gérer les dossiers pour décrypter uniquement les fichiers qui ne sont pas partagés avec d'autres utilisateurs Data Guardian.

Question

Je synchronise un dossier décrypté que j'ai désélectionné à l'aide de l'utilitaire Gérer les dossiers. Pourtant, lorsque je tente de le charger dans mon navigateur web, je peux seulement charger des fichiers cryptés.

Réponse

Data Guardian n'est pas conçu pour rechercher activement des dossiers dans le cloud. Avec les dossiers non cryptés, Data Guardian peut synchroniser via le client de synchronisation, car il ne contrôle pas cet environnement. Les fichiers chargés dans un navigateur web doivent être cryptés.

Solution

Ajoutez les fichiers au dossier de synchronisation.

Question

J'ai récemment désinstallé mon système de partage de fichiers Cloud de mon ordinateur. Pourtant, quand j'ouvre l'utilitaire Gérer les dossiers, l'un des clients de synchronisation était toujours répertorié comme option.

Réponse

Data Guardian ne contrôle pas l'installation ou la désinstallation des logiciels tiers. Ils ne disparaissent pas de la liste d'options car ils ne sont pas conçus pour supprimer vos fichiers existants au moment de leur désinstallation. Ces fichiers sont toujours protégés par Data Guardian, même si le client de synchronisation n'est plus installé.

Solution

Pour supprimer l'option du client de synchronisation désinstallé de l'utilitaire Gérer les dossiers, déplacez les fichiers ou dossiers que vous souhaitez conserver hors du dossier de synchronisation, puis supprimez le dossier. Après sa suppression, le dossier n'est plus répertorié dans l'utilitaire Gérer les dossiers.

Forum aux questions - Divers

Question

Un utilisateur utilisant Data Guardian en mode Documents Office protégés ne peut ni copier ni coller.

Réponse

Certaines fonctionnalités de Data Guardian sont gérées via la barre d'état système. Vérifiez si l'utilisateur l'a modifiée.

Solution

Les paramètres par défaut de la barre d'état système doivent être utilisés. L'utilisateur doit conserver ces paramètres.

Question

J'ai modifié la règle **Obscurcissement des noms de fichiers** en remplaçant GUID par Extension uniquement. Toutefois, les fichiers qui se trouvent dans des dossiers que j'avais synchronisés précédemment sont encore cryptés dans l'autre format, avec des noms de fichiers GUID. Pourquoi ?

Réponse

Lorsque vous modifiez une règle sur Security Management Server/Security Management Server Virtual, Security Management Server maintient la règle précédente pour ce dossier. Si vous créez de nouveaux dossiers, la nouvelle règle leur sera appliquée, et les fichiers de ces dossiers seront cryptés au format **Extension uniquement**.

Solution

Pour appliquer de nouveau le format **Extension uniquement** aux anciens fichiers, transférez-les par couper-coller dans un nouveau dossier auquel la nouvelle règle est appliquée.

4

Configurer et installer Data Guardian sur Mac

Data Guardian pour Mac est conçu pour partager des fichiers entre les fournisseurs de chiffrement Cloud. Toutefois, si les règles « Documents Office protégés » sont activées pour les Mac, tous les audits de fichiers et la traçabilité sont perdus si le fichier est enregistré par l'utilisateur sur le Mac local. Si une traçabilité et un audit de fichiers très stricts sont requis par votre entreprise, choisissez l'option *Non sélectionné* pour la règle **Autoriser l'activation Data Guardian Mac** afin d'éviter que Data Guardian ne s'active sur des Mac.

Tâches de serveur

Pré-requis

Avant d'effectuer ces tâches, confirmez ce qui suit :

- Installation de Serveur Dell et de ses composants. Voir l'une des sections suivantes :
  - *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)*
  - *Security Management Server Virtual Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Security Management Server Virtual)*
- Dans la console de gestion, attribuez un Rôle d'administrateur Dell approprié.

Stratégies

Par défaut, Data Guardian chiffre les fichiers des utilisateurs et envoie les événements d'audit à Security Management Server Virtual. Dans ce document, les deux serveurs sont appelés « Dell Server », sauf lorsqu'il est nécessaire de désigner une version spécifique (par exemple, une procédure varie en cas d'utilisation de Security Management Server Virtual).

Pour que les événements d'audit incluent des données de géolocalisation, vous devez activer le WiFi. Pour plus d'informations sur la géolocalisation et les événements d'audit, voir l'*Aide de l'administrateur*.

Pour modifier le comportement par défaut pour chaque fournisseur de stockage Cloud pris en charge, définissez la règle des *Fournisseurs de protection de stockage Cloud*. Si votre entreprise préfère un fournisseur de stockage Cloud spécifique, configurez cette règle sur **Bloquer** pour les autres fournisseurs. Pour en savoir plus sur les règles, voir l'*Aide de l'administrateur*, disponible à partir de la Console de gestion.

REMARQUE :
L'option Contournement de cette règle est pour Windows. Si vous sélectionnez Contournement pour Mac, elle affiche Autoriser à l'utilisateur final.

Configurer Security Server pour autoriser les téléchargements du client Cloud

Avant d'effectuer ces tâches, confirmez ce qui suit :

- Installation de Serveur Dell et de ses composants. Voir l'une des sections suivantes :
  - *Security Management Server Installation and Migration Guide (Guide d'installation et de migration de Security Management Server)*
  - *Security Management Server Virtual Quick Start Guide and Installation Guide (Guide de démarrage rapide et Guide d'installation de Security Management Server Virtual)*
- Dans la console de gestion, attribuez un Rôle d'administrateur Dell approprié.

Security Management Server

1 Sur Security Management Server, rendez-vous sur <rép. d'install. de Security Server>\webapps\cloudweb\brand\dell\resources\
2 Ouvrez le fichier **messages.properties** dans un éditeur de texte.
3 Vérifiez que les entrées sont conformes aux informations suivantes :
Pour une installation **locale** :

download.deviceWin.mode=local

download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg

Pour une installation **à distance** :

```
download.deviceWin.mode=remote
```

```
download.deviceMac.remote.link=https://[NomMachine:adresseIP]:[port]/yourpath/filename.dmg
```

4 Enregistrez les fichiers, puis fermez-les.
5 Rendez-vous sur <rép. d'install. de Security Server> et créez un nouveau dossier nommé Download (Security Server\Download).
6 Dans le dossier Download (Téléchargement), créez un dossier CloudWeb (Security Server\Download\CloudWeb).
7 Ajoutez les programmes d'installation de Dell Data Guardian dans ce dossier.

Virtual Edition : installez manuellement une version différente du client Cloud

Aucune action n'est nécessaire pour permettre aux utilisateurs de télécharger le dernier programme d'installation de Dell Data Guardian. La dernière version du programme d'installation est préinstallée sur le serveur de sécurité de Security Management Server Virtual.

Pour procéder à l'installation manuelle d'une autre version du programme d'installation de Data Guardian sur le serveur de sécurité de Security Management Server Virtual, mettez à jour le fichier message.properties.

1 Accédez à :
/opt/dell/server/security-server/webapps/root/cloudweb/brand/dell/resources/
2 Ouvrez le fichier **messages.properties** dans un éditeur de texte.
Pour une installation **locale** :

```
download.deviceWin.mode=local
```

```
download.deviceMac.local.filename=Dell-Data-Guardian-0.x.x.xxxx.dmg
```

Pour une installation **à distance** :

download.deviceWin.mode=remote

```
download.deviceMac.remote.link=https://[NomMachine:adresseIP]:[port]/yourpath/filename.dmg
```

3 Enregistrez les fichiers, puis fermez-les.
4 Copiez les fichiers dans /opt/dell/server/security-server/download/cloudweb.
5 Ajoutez les programmes d'installation de Data Guardian à ce dossier.

Autoriser/refuser des utilisateurs sur la liste l'accès total/liste noire

Les entrées de la liste d'accès total et la liste noire déterminent les utilisateurs pouvant s'inscrire sur Serveur Dell pour utiliser Data Guardian.

Liste d'accès total

La liste d'accès total permet à des utilisateurs ou groupes d'utilisateurs particuliers de s'inscrire sur Serveur Dell afin d'utiliser Data Guardian.

Les utilisateurs externes doivent être placés sur la liste d'accès total pour pouvoir effectuer un enregistrement. Regardez les exemples suivants pour permettre aux utilisateurs de s'inscrire :

Type d'utilisateur	Entrée
Toutes les adresses e-mail organisation.com	`organization.com`
Un utilisateur spécifique	`jdoe@organization.com`
Tous les utilisateurs Gmail	`gmail.com`

Liste noire

La liste noire empêche des utilisateurs ou groupes d'utilisateurs donnés de s'inscrire sur Serveur Dell et d'utiliser Data Guardian. Les utilisateurs dont les adresses e-mail sont placées sur la liste noire reçoivent un message indiquant qu'il leur est impossible de s'inscrire auprès de Data Guardian.

REMARQUE :
Si un utilisateur est déjà enregistré, cette liste ne peut **pas** l'empêcher d'utiliser Data Guardian.

Vous pouvez utiliser la liste noire pour exclure des utilisateurs spécifiques appartenant à des groupes approuvés sur la liste d'accès total. En outre, vous pouvez placer l'ensemble d'un domaine sur la liste noire, ce qui empêchera toute personne possédant une adresse e-mail incluse dans ce domaine de s'inscrire. Regardez les exemples suivants pour empêcher un utilisateur ou un groupe de s'inscrire sur Serveur Dell :

Type d'utilisateur	Entrée
Toutes les adresses e-mail organisation.com	`organization.com`
Un utilisateur spécifique et cette adresse e-mail	`jdoe@organization.com`
Tous les utilisateurs Gmail	`gmail.com`

Pour modifier la liste d'accès total ou la liste noire, suivez les instructions ci-dessous :

1 Dans le volet de gauche de la console de gestion à distance, cliquez sur **Gestion > Gestion des utilisateurs externes**.
2 Cliquez sur **Ajouter**.
3 Sélectionnez le type d'accès à l'inscription :

Liste noire : bloque l'inscription d'un utilisateur ou d'un domaine. L'utilisateur ne peut pas ouvrir un document Office protégé ni un fichier .xen.

Liste d'accès total : autorise l'inscription et l'accès aux fichiers d'un utilisateur ou d'un domaine. Si un utilisateur ou un domaine sont également sur la liste noire, aucun accès n'est accordé.

4 Dans le champ Saisir un domaine/e-mail, saisissez le domaine de l'utilisateur pour autoriser l'accès à la totalité du domaine, ou une adresse e-mail pour autoriser l'accès uniquement à cet utilisateur.

5 Cliquez sur **Ajouter**.

Pour plus d'informations sur l'utilisation de la liste d'accès total/liste noire, voir l'*Aide administrateur*, accessible à partir de la Console de gestion à distance de Serveur Dell.

Un utilisateur externe peut demander l'accès à un utilisateur interne pour obtenir la clé d'un fichier protégé. Si l'utilisateur interne n'est pas disponible, vous pouvez utiliser la console de gestion à distance pour accepter ou refuser l'accès.

1 Sélectionnez **Gestion > Gestion des demandes de clés**.

2 Pour plus d'informations, sélectionnez **?** (Aide).

Tâches client

Prérequis

- Vérifiez que les périphériques cibles sont connectés à :
  - https://yoursecurityservername.domain.com:8443/cloudweb/register
  - https://yoursecurityservername.domain.com:8443/cloudweb
- Veillez à ce que l'utilisateur effectuant l'installation dispose d'un compte d'administrateur local pour l'installation.
- Si l'installation est effectuée à l'aide de la ligne de commande, assurez-vous de disposer du nom de domaine complet de Security Server sur lesquels les utilisateurs vont s'activer.

Meilleures pratiques

Pendant le déploiement, assurez-vous de suivre les meilleures pratiques informatiques. Ceci inclut (liste non exhaustive) :

- Des environnements de test contrôlés pour effectuer les tests initiaux
- Des déploiements échelonnés pour les utilisateurs

Installer le client

À ce stade, les utilisateurs qui ont été ajoutés à la liste blanche peuvent s'inscrire sur : https://nomdevotresecurityserver.domaine.com:8443/cloudweb/register.

Après l'inscription, l'utilisateur reçoit un e-mail le dirigeant vers https://nomdevotresecurityserver.domaine.com:8443/cloudweb pour se connecter et télécharger le client approprié.

L'installation du client Mac est facultative pour les administrateurs, car les utilisateurs finaux installent généralement le client Mac eux-mêmes (après l'enregistrement) à partir du site https://yoursecurityservername.domain.com:8443/cloudweb.

Toutefois, vous pouvez installer le client Mac si votre organisation vous oblige à le faire. Installez le client Data Guardian à l'aide de l'interface utilisateur ou de la ligne de commande, par le biais de toute technologie Push disponible dans votre organisation. L'inscription et l'activation par l'utilisateur final restent obligatoires.

Mise à niveau à partir de versions antérieures de Cloud Edition

Si une entreprise dispose d'une version antérieure de Cloud Edition et effectue une mise à niveau de Data Guardian, la précédente version de Cloud Edition est supprimée.

REMARQUE :
Si une entreprise effectue une mise à niveau de Cloud Edition vers Data Guardian, les utilisateurs doivent s'authentifier et lier à nouveau Data Guardian avec leur fournisseur de stockage Cloud. Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

Options d'installation

Pour installer/mettre à niveau le client, sélectionnez l'une des options suivantes :

- Installation interactive : il s'agit de la méthode la plus simple pour installer Data Guardian pour Mac. Cependant, n'utilisez cette méthode que si vous prévoyez d'installer le client sur un ordinateur à la fois.

  ou

- Installation avec ligne de commande : pour cette méthode d'installation avancée, les administrateurs doivent connaître la syntaxe de la ligne de commande. Cette méthode peut être utilisée pour une installation ou une mise à niveau par installation scriptée, à l'aide de fichiers séquentiels ou de toute autre technologie Push disponible dans votre entreprise.

Installation interactive

1. Pour le client Data Guardian, localisez le programme d'installation de **Dell-Data-Guardian--0.x.x.xxxx.dmg.**
2. Utilisez le fichier **.pkg** situé dans DDPSL-Explorer-0.x.x.xxxx.dmg pour effectuer une installation ou une mise à niveau. Vous pouvez utiliser une installation à partir d'un script, des fichiers de commandes ou toute technologie Push disponible dans votre organisation.
3. Double-cliquez sur le package **Dell-Data-Guardian-x.x.x**.
4. Cliquez sur **Continuer**.
5. Dans la fenêtre Introduction, cliquez sur **Continuer**.
6. Dans la fenêtre Contrat de licence de logiciel, cliquez sur **Continuer**.
7. Cliquez sur **Accepter** pour continuer.
8. Dans la fenêtre Type de configuration, sélectionnez **Serveur Dell Management local**.

   REMARQUE :
   L'option *Dell Security Center hébergé* concerne une version ultérieure.

9. Dans la fenêtre Type d'installation, effectuez l'une des actions suivantes :
   - Cliquez sur **Installer**, puis passez à l'étape 9.
   - Cliquez sur **Modifier l'emplacement d'installation**.
     1. Dans la fenêtre Sélection de la destination, sélectionnez tous les utilisateurs ou un utilisateur unique.
     2. Cliquez sur **Continuer**.
     3. Cliquez sur **Installer**, puis passez à l'étape 9
10. Dans la boîte de dialogue, saisissez votre nom et votre mot de passe et cliquez sur **Installer le logiciel**.
11. Dans la page Résumé, cliquez sur **Fermer**.
12. Reportez-vous à Activation de l'utilisateur final.

    REMARQUE :
    Si une entreprise effectue une mise à niveau de Cloud Edition vers Data Guardian, les utilisateurs doivent s'authentifier et lier à nouveau Data Guardian avec leur fournisseur de stockage Cloud. Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

13. Fermez la fenêtre .dmg afin d'ouvrir le Finder.

Installation par ligne de commande

1. Montez le fichier .dmg.

2 Effectuez une installation par ligne de commande du package à l'aide de la commande d'installation :

```
sudo installer -pkg/Volumes/Dell\ Data\ Guardian"Dell-Data-Guardian\ 0.x.x.xxxx.pkg" -target /
```

3 Demandez aux utilisateurs d'activer Data Guardian. Reportez-vous à Activation de l'utilisateur final.

Activation de l'utilisateur final

Lorsque vous ouvrez Dell Data Guardian sur un Mac pour la première fois, suivez ces étapes :

1 Dans Finder, sélectionnez **Applications** et double-cliquez sur **Dell Data Guardian**.
2 Lorsque la fenêtre Serveur Dell s'affiche, saisissez l'adresse de Serveur Dell et cliquez sur **Enregistrer**.

La fenêtre des informations d'identification s'ouvre.

3 Saisissez l'adresse e-mail de votre domaine et le mot de passe du domaine.
4 Cliquez sur **Connexion** pour activer Dell Data Guardian.

Une fois l'application Dell Data Guardian ouverte et l'activation réussie, le nom du fournisseur de stockage cloud s'affiche en gris dans le volet de gauche.

Si une entreprise souhaite que tous ses utilisateurs collaborent en utilisant le même fournisseur de Cloud, l'administrateur peut définir une règle pour autoriser uniquement ce fournisseur et bloquer l'affichage d'autres fournisseurs.

Si l'authentification de l'application Dell Data Guardian est révoquée ou expire, le nom du fournisseur de stockage Cloud est également grisé.

5 Dans le volet de gauche, sélectionnez le fournisseur de stockage Cloud.

Une fenêtre vous demandant d'entrer vos identifiants s'affiche. Une fois authentifié, le nom du fournisseur de stockage cloud est activé.

6 Pour plus d'informations sur l'authentification, voir l'Aide en ligne de Dell Data Guardian.

Désinstaller Data Guardian

Cette section présente le processus d'administrateur permettant de désinstaller Data Guardian. Pour effectuer la désinstallation, vous devez posséder un compte administrateur local. Si un utilisateur final possède un compte administrateur local, il peut désinstaller lui-même Data Guardian pour Mac.

Procédez de l'une des manières suivantes pour supprimer Data Guardian :

Finder

1 Tout en appuyant sur la touche <option>, sélectionnez **Accéder** dans la barre de menus.
2 Ouvrez le dossier **~/Library/Application Support/Dell**.
3 Effectuez un clic droit sur le dossier **Dell DataGuardian**, puis sélectionnez **Déplacer vers la corbeille**.
4 À partir de l'option **Accéder** dans la barre de menus, ouvrez le dossier Applications et déplacez l'application **Dell Data Guardian** vers la corbeille.
5 Cliquez sur **OK**.
6 Si vous y êtes invité, saisissez le mot de passe d'administrateur.

Terminal

Data Guardian peut se trouver dans les emplacements suivants.

1 Utilisez ces commandes :
   - rm -R ~/Applications/Data\ Guardian.app
   - rm -R ~/Library/Application Support/Dell/DataGuardian

2 Supprimez le dossier **Dell DataGuardian**.

5

Configurer et installer Data Guardian pour le client Web

Ce client Web permet aux utilisateurs d'afficher un document Office protégé ou un fichier .xen sans installer le client Data Guardian. En règle générale, Dell recommande d'utiliser Security Management Server ou Security Management Server Virtual en premier.

Télécharger le fichier OVA

Au cours de l'installation initiale, Data-Guardian -Web 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.

Pour télécharger le fichier OVA :

1 Naviguez jusqu'à la page de support du produit 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**.
4 Sous « Afficher par : », sélectionnez **Tout afficher**.
5 Sous Dell Data Security, sélectionnez **Télécharger**.

Installer Data Guardian pour le Web

Installer et configurer Data-Guardian-Web

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

1 Localisez les fichiers Data Guardian dans le média d'installation et double-cliquez sur **Data-Guardian -Web-1.x.x .ova** pour procéder à l'importation dans VMware.
2 Mise sous tension de Data-Guardian -Web.
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 À l'invite de modification du mot de passe par défaut, sélectionnez **Oui**.
7 Sur l'écran *Définir le mot de passe ddguser*, saisissez le mot de passe actuel (par défaut), **ddguser**, 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
8 Répétez l'étape précédente pour les comptes *ddgconsole* et *ddgsupport*.

REMARQUE :
Pour conserver le mot de passe par défaut, qui est le même que le nom, cliquez sur **Annuler**. Pour modifier le mot de passe, saisissez **ddgconsole** ou **ddgsupport** dans le champ Mot de passe actuel.

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 FQDN, puis sélectionnez **OK**.

10 Si vous disposez de plusieurs nœuds et d'un équilibreur de charge, entrez un Nom d'hôte d'équilibreur de charge.

11 Dans la boîte de dialogue *Configurer les paramètres de réseau*, choisissez l'une des deux options ci-après, puis sélectionnez **OK**.

- (Par défaut) Utiliser DHCP
- (Recommandé) dans le champ Utiliser DHCP, appuyez sur la barre d'espacement 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, server DNS 3

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

12 Lorsque l'écran scp s'affiche, ne cliquez pas sur OK. Vous devez d'abord ajouter les fichiers .cer et .key à l'application ou l'extraire du fichier .pfx ou .p7b de l'autorité de certification (CA). Reportez-vous à Utiliser l'outil WinSCP.

REMARQUE :
Si vous cliquez sur OK dans l'écran scp avant de les extraire, vous devez redémarrer Data-Guardian-Web et naviguer jusqu'à la fenêtre de dialogue *Configurer les paramètres de réseau*.

Utiliser l'outil WinSCP

Dans Windows, utilisez votre compte ddgconsole pour copier de manière sécurisée (SCP) le fichier de certificat SSL et le fichier de clé SSL.

1 Dans Windows, ouvrez l'outil WinSCP.

2 Sur la page WinSCP, saisissez le nom d'hôte.

3 Saisissez le nom d'utilisateur par défaut de ddgconsole et le mot de passe par défaut (ou vos nom d'utilisateur et mot de passe modifiés).

4 Cliquez sur **Connexion**.

5 Faites glisser le certificat, la clé, le fichier .pfx ou .p7b de votre lecteur local vers le répertoire **opt/dell/files**.

6 Si vous avez ajouté un fichier .pfx ou .p7b, saisissez un mot de passe lorsque vous y êtes invité. Le certificat et la clé sont extraits par l'autorité de certification et ajoutés à **apache2/ssl/folder**.

Si vous le souhaitez, au lieu de faire glisser le fichier .pfx ou .p7b, vous pouvez extraire manuellement le certificat. Voici un exemple de code :

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
```

Voici un exemple de code pour extraire la clé privée du fichier .pfx :

```
openssl pkcs12 -in domain.pfx -nocerts -nodes -out domain.key
```

7 Retournez à l'écran scp de la console d'administration.

Console Administration

Sur l'écran scp de la console d'administration :

1 Cliquez sur **OK**. L'écran *Installation du certificat de proxy inverse Apache2* s'affiche et répertorie les certificats.

2 Sélectionnez un certificat et cliquez sur **Entrée**.

3 Effectuez l'une des opérations suivantes :

- Si vous avez ajouté une clé à l'outil WinSCP, sélectionnez la clé sur l'écran suivant et appuyez sur **Entrée**.

- Si vous avez saisi un mot de passe pour l'outil WinSCP pour un fichier .pfx ou .p7b, saisissez-le lorsque vous y êtes invité et cliquez sur **OK**.

4 À l'écran Configurer Dell Server, saisissez le nom d'hôte de votre serveur, puis cliquez sur **OK**. Une boîte de dialogue indique l'adresse URL à utiliser lors du provisionnement. L'URL est au format suivant : **https://node.domain.com/edap-admin-ui/provision_node**.

> **REMARQUE :**
> **node.domain.com** est le nom que vous avez entré dans *Configurer le nom d'hôte*. L'URL pointe sur ce nœud.

5 Ouvrez un navigateur et saisissez cette URL.

6 Lorsque la page de provisionnement de nœuds Dell Data Guardian s'ouvre, cliquez sur **Démarrer le provisionnement de nœuds**.

7 Sur la page de connexion, entrez votre adresse e-mail de domaine et votre mot de passe, puis cliquez sur **Se connecter**. La boîte de dialogue Dell Data Guardian indique que le provisionnement a réussi.

8 Retournez à l'écran Console d'administration qui a répertorié votre URL et cliquez sur **OK**. Le serveur d'applications redémarre et la Console Administration > Menu principal s'ouvre.

Tâches supplémentaires :

- Fournissez l'URL aux utilisateurs internes afin de leur permettre d'accéder au client Web de Data Guardian.
  - Pour un seul nœud, l'URL est au format suivant : **https://nodename/** où le nom de nœud reflète le nom d'hôte entré dans l'écran *Configurer le nom d'hôte*.
  - Dans le cas de plusieurs nœuds, l'URL est au format suivant : **https://loadBalancerName/** où le nom de nœud reflète le nom d'hôte de l'équilibreur de charge entré dans l'écran *Configurer le nom d'hôte*.
- Pour accéder au serveur, à l'avenir, pour des mises à jour de cette machine virtuelle ou pour vérifier les journaux, vous devez activer SSH pour cette machine virtuelle. Sélectionnez **Configuration de base > Paramètres SSH** pour activer SSH pour un utilisateur ddgsupport.
- Dans la console de gestion, si vous modifiez une quelconque stratégie de portail Web basée sur les nœuds, vous devez redémarrer l'appliance. Voir Redémarrer l'appliance. Après le redémarrage, vous devez vous connecter avec vos informations d'identification ddguser.

Ouverture de la Console de gestion

Ouvrez la console de gestion à l'adresse https://server.domain.com:8443/webui/

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

Les navigateurs Web suivants sont pris en charge avec la Console de gestion :

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

Tâches de configuration de base du terminal Data Guardian

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

Modification du nom d'hôte

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser .

1 Dans le menu *Configuration de base*, sélectionnez **Nom d'hôte**.

2 Utilisez la touche Retour arrière pour supprimer le nom d'hôte Data-Guardian-Web 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. Il n'est pas nécessaire de commencer à utiliser .

1 Dans le menu *Configuration de base*, sélectionnez **Réseau**.
2 À l'écran *Configurer les paramètres de réseau*, choisissez l'une des deux options ci-après, puis sélectionnez **OK**.
   - (Par défaut) Utiliser DHCP (IPv4)
   - (Recommandée) Dans le champ Utiliser DHCP, appuyez sur la barre d'espacement pour supprimer le X et saisir manuellement ces adresses, le cas échéant :

     Static IP (Adresse IP statique)

     Masque de réseau

     Passerelle par défaut

     Serveur DNS 1

     Serveur DNS 2

     Serveur DNS 3

     Il est possible de sélectionner IPv6 ou IPv4 pour une configuration statique.

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

Modifier les mots de passe utilisateur

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser .

Vous pouvez modifier les mots de passe pour ces utilisateurs :

- ddguser (administrateur du terminal) : cet utilisateur a accès au terminal Data Guardian et à ses menus.
- ddgconsole (accès au shell) : cet utilisateur dispose d'un accès au shell de Data Guardian. L'accès au shell permet à un administrateur réseau de vérifier et dépanner la connectivité réseau.
- ddgsupport (administrateur Dell ProSupport) : cet utilisateur ne peut être utilisé que pour Dell ProSupport. Pour des raisons de sécurité, vous contrôlez le mot de passe de ce compte.

1 Dans le menu *Configuration de base*, sélectionnez **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 une lettre majuscule
   - Au moins 1 chiffre
   - Au moins un caractère spécial

REMARQUE : Si vous souhaitez sélectionner plusieurs comptes d'utilisateur, utilisez la touche Espace du clavier pour afficher la liste de sélection.

Enable SSH (Activer SSH)

Cette tâche peut être réalisée à tout moment. Il n'est pas nécessaire de commencer à utiliser .

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

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

Démarrer ou arrêter les services

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

1 Pour démarrer ou arrêter simultanément tous les services, dans le menu *Configuration de base*, sélectionnez **Démarrer l'application** ou **Arrêter l'application**.
2 Dans l'invite de commande, cliquez sur **Oui**.

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

Redémarrer l'appliance

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

1 Dans le menu *Configuration de base*, sélectionnez **Redémarrer l'appliance**.
2 Dans l'invite de commande, cliquez sur **Oui**.
3 Après le redémarrage, connectez-vous au serveur Data Guardian.

Arrêter l'appliance

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 Dans l'invite de commande, cliquez sur **Oui**.
3 Après le redémarrage, connectez-vous au serveur Data Guardian.

Tâches administratives

Définir ou modifier la langue du terminal

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 la langue voulue.

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 **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**.