Endpoint Security Suite Enterprise for Linux

Guide de l'administrateur v2.1

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.

2018 - 11

Rév. A01

Table des matières

1

Introduction

Endpoint Security Suite Enterprise for Linux Administrator Guide (Guide de l'administrateur d'Enterprise Edition Endpoint Security Suite Enterprise for Linux) fournit les informations nécessaires pour installer et déployer le logiciel client.

Présentation

Endpoint Security Suite Enterprise for Linux offre Advanced Threat Prevention au niveau du système d'exploitation et de la mémoire, le tout géré de manière centralisée depuis Serveur Dell. Grâce à la gestion centralisée, à la génération de rapports de conformité consolidés et aux alertes relatives aux menaces émises par la console, les organisations peuvent atteindre leurs objectifs de conformité et fournir les justifications associées pour tous les points de terminaison. Des fonctionnalités comme les modèles de rapports et de règles prédéfinis bénéficient d'une expertise intégrée, aidant ainsi les entreprises à réduire leurs coûts de gestion et à simplifier leurs opérations informatiques.

Security Management Server ou Security Management Server Virtual : fournit une administration centralisée des règles de sécurité, s'intègre avec les répertoires d'entreprise existants et crée des rapports. 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).

Advanced Threat Prevention for Linux a un fichier tar.gz, qui contient les trois RPM.

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

Ce chapitre présente la configuration matérielle et logicielle requise pour le client. Avant d'effectuer toute opération de déploiement, assurez-vous que l'environnement de déploiement respecte les exigences suivantes.

Matériel

Le tableau suivant indique la configuration matérielle minimale prise en charge.

Matériel

- Au moins 500 Mo espace disque libre
- 2 Go de RAM
- Carte d'interface réseau 10/100/1000 ou Wi-Fi

REMARQUE : IPv6 n'est pas pris en charge actuellement.

Logiciel

Le tableau suivant décrit les logiciels pris en charge.

Systèmes d'exploitation (noyaux de 64 bits)

- CentOS Linux v7.1 - v7.5
- Red Hat Enterprise Linux v7.1 - v7.5

Ports

- Le port 443 (https) est utilisé pour la communication et doit être ouvert sur le pare-feu pour que les agents puissent communiquer avec la Console de gestion. Si le port 443 est bloqué pour une raison quelconque, les mises à jour ne pourront pas être téléchargées et les ordinateurs ne pourront pas bénéficier de la protection la plus récente. Assurez-vous que les ordinateurs clients peuvent accéder aux éléments suivants :

Utilisation	Protocole d'application	Protocole de transport :	Numéro de port	Destination	Direction
Toutes les communications	HTTPS	TCP	443	Autoriser tout le trafic https vers *.cylance.com	Sortant
Communication avec Core Server	HTTPS	TCP	8888	Permet la communication Core Server	Entrant/sortant

- Pour plus d'informations, voir SLN303898.

Endpoint Security Suite Enterprise for Linux et dépendances

Endpoint Security Suite Enterprise for Linux utilise Mono et les dépendances pour s'installer et s'activer sur le SE Linux. Le programme d'installation télécharge et installe les dépendances requises. Après l'extraction du package, vous pouvez voir quelles dépendances sont en cours d'exploitation à l'aide de la commande suivante :

```
./showdeps.sh
```

Compatibilité

Le tableau suivant indique la compatibilité avec Windows, Mac et Linux.

n/a - Cette technologie ne s'applique pas à cette plate-forme.

Champ vide - Cette stratégie n'est pas prise en charge avec Endpoint Security Suite Enterprise.

Fonctionnalités	Stratégies	Windows	macOS	Linux
Actions de fichier				
	Quarantaine automatique (Dangereux)	x	x	x
	Quarantaine automatique (Anormal)	x	x	x
	Téléchargement auto	x	x	x
	Liste de confiance de la stratégie	x	x	x
Actions de mémoire				
	Protection de la mémoire	x	x	x
Exploitation				
	Zone dynamique d'empilement	x	x	x
	Protection de l'empilement	x	x	x
	Écraser le code	x	Sans objet	
	Collecte de données stockées en RAM	x	Sans objet	
	Charge malveillante	x		
Injection de processus				
	Attribution à distance de mémoire	x	x	Sans objet
	Adressage à distance de mémoire	x	x	Sans objet
	Écriture à distance dans la mémoire	x	x	Sans objet

Fonctionnalités	Stratégies	Windows	macOS	Linux
	Écriture à distance de PE dans la mémoire	x	Sans objet	Sans objet
	Écraser le code à distance	x	Sans objet	
	Suppression de l'adressage de la mémoire à distance	x	Sans objet	
	Création de thread à distance	x	x	
	Planification APC à distance	x	Sans objet	Sans objet
	Injection de DYLD		x	x
Escalade				
	Lecture LSASS	x	Sans objet	Sans objet
	Attribution nulle	x	x	
Paramètres de protection				
	Contrôle de l'exécution	x	x	x
	Interdire l'arrêt du service depuis le périphérique	x	x	
	Arrêter les processus et sous-processus dangereux en cours d'exécution	x	x	x
	Détection de menace d'arrière plan	x	x	x
	recherche de nouveaux fichiers	x	x	x
	Taille de fichier d'archive maximale à analyser	x	x	x
	Exclure des dossiers spécifiques	x	x	x
	Copier les fichiers exemples	x		
Contrôle des applications				
	Fenêtre de modification	x		x
	Exclusion de dossiers	x		
Paramètres de l'agent				
	Activer le téléchargement automatique des fichiers journaux	x	x	x
	Activer les notifications sur le bureau	x		
Contrôle des scripts				

Fonctionnalités	Stratégies	Windows	macOS	Linux
	Script actif	x		
	Powershell	x		
	Macros Office	x		Sans objet
	Bloquer l'utilisation de la console Powershell	x		
	Approuver les scripts dans ces dossiers (et leurs sous-dossiers)	x		
	Niveau de journalisation	x		
	Niveau d'auto-protection	x		
	Mise à jour automatique	x		
	Exécuter une détection (à partir de l'interface utilisateur de l'agent)	x		
	Supprimer les éléments mis en quarantaine (interface utilisateur de l'agent et interface utilisateur de la console)	x		
	Mode Déconnecté	x		x
	Données de menace détaillées	x		
	Liste de confiance des certificats	x	x	Sans objet
	Copier les échantillons de programme malveillant	x	x	x
	Paramètres de proxy	x	x	x
	Vérification manuelle des stratégies (interface utilisateur de l'agent)	x	x	

3

Tâches

L'installation

Cette section présente Endpoint Security Suite Enterprise pour l'installation de Linux.

Pré-requis

Dell recommande de suivre les meilleures pratiques informatiques pendant le déploiement du logiciel client. Ceci inclut, sans s'y limiter, les environnements de test contrôlés pour les premiers tests et les déploiements échelonnés pour les utilisateurs.

Avant de démarrer ce processus, assurez-vous que les conditions préalables suivantes sont réunies :

- Assurez-vous que Serveur Dell et ses composants sont déjà installés.

  Si vous n'avez pas encore installé Serveur Dell, suivez les instructions figurant dans le guide approprié ci-dessous.

  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)
- Assurez-vous d'avoir le nom d'hôte du serveur et le port du Serveur Dell. Vous en aurez besoin pour l'installation du logiciel client.
- Vérifiez que l'ordinateur cible dispose d'une connectivité réseau à Serveur Dell.
- Si un certificat de serveur du client est manquant ou auto-signé, vous devez désactiver la confiance vis-à-vis du certificat SSL du côté du client uniquement.

Installation par ligne de commande

Pour installer le client Endpoint Security Suite Enterprise à l'aide de la ligne de commande, suivez les étapes ci-dessous.

La commande **sudo** doit être utilisée pour appeler les privilèges d'administration au cours de l'installation. Si vous y êtes invité, entrez vos informations d'identification.

L'approbation des empreintes digitales s'affiche uniquement au cours de la première installation.

1 Localisez et téléchargez le lot d'installation (DellESSE-1.x.x -xxx.tar.gz) à l'aide de votre compte FTP de Dell.

2 Extrayez le fichier tar.gz à l'aide de la commande suivante :

```
tar -xvf DellESSE*.tar.gz
```

```
[redacted] tmp]# tar -xvf DellESSE*.tar.gz
DellESSE-1.0.0-24-el7-x86_64.rpm
install.sh
uninstall.sh
showdeps.sh
versgate
DellEULA-en.txt
CylanceDellATPPlugin-2.0.1471.751-el7-x86_64.rpm
DellAdvancedThreatProtection-2.0.1471.751-el7-x86_64.rpm
```

3 La commande suivante exécute le script d'installation pour les RPM requis et les dépendances :

```
sudo ./install.sh
```

4 Dans *Dell Security Management Server Host?,* entrez le nom d'hôte entièrement qualifié du Serveur Dell pour gérer l'utilisateur de la cible. Par exemple, server.organization.com.

5 Dans *Dell Security Management Server Port?*, vérifiez que le port est défini sur 8888.

```
Dell Endpoint Security Suite Enterprise (ESSE) Installation
Dell Security Management Server Host?
Dell Security Management Server Port?
```

6 Entrez **y** lorsque vous êtes invité à installer le package DellESSE et ses dépendances.

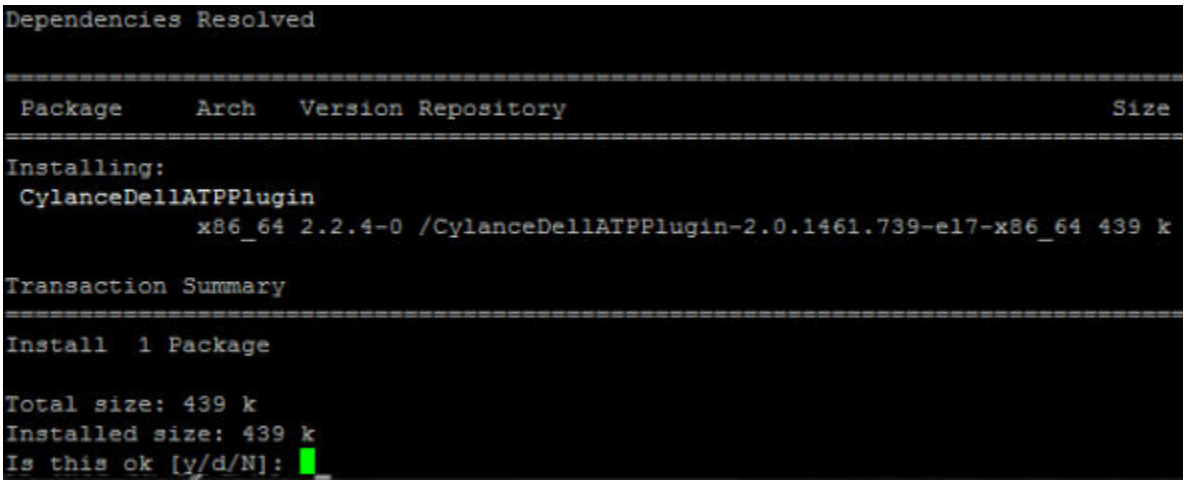
```
 libXfixes      x86_64 5.0.3-1.el7              base                      18 k
 libXrender     x86_64 0.9.10-1.el7             base                      26 k
 libXxf86vm     x86_64 1.1.4-1.el7              base                      18 k
 libexif        x86_64 0.6.21-6.el7             base                     347 k
 libjpeg-turbo x86_64 1.2.90-5.el7              base                     134 k
 libpng         x86_64 2:1.5.13-7.el7_2         base                     213 k
 libtiff        x86_64 4.0.3-27.el7_3           base                     170 k
 libxcb         x86_64 1.12-1.el7               base                     211 k
 libxshmfence   x86_64 1.2-1.el7                base                     7.2 k
 lyx-fonts      noarch 2.2.3-1.el7              epel                     159 k
 mesa-libEGL    x86_64 17.0.1-6.20170307.el7    base                      82 k
 mesa-libGL     x86_64 17.0.1-6.20170307.el7    base                     155 k
 mesa-libgbm    x86_64 17.0.1-6.20170307.el7    base                      32 k
 mesa-libglapi  x86_64 17.0.1-6.20170307.el7    base                      41 k
 pixman         x86_64 0.34.0-1.el7             base                     248 k

Transaction Summary
================================================================================
Install  1 Package (+27 Dependent packages)

Total size: 96 M
Total download size: 3.8 M
Installed size: 104 M
Is this ok [y/d/N]:
```

7 Entrez **y** si vous y êtes invité à effectuer une approbation des *empreintes*.

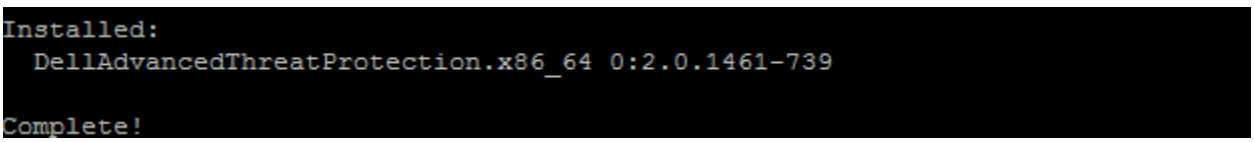
```
Total                                                   452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78 a7c2 7bbl 24c6 a8a7 f4a0 0eb5
 Package        : centos-release-7-3.1611.el7.centos.x86_64 (@anaconda)
 From           : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

8 Entrez **y** lorsque vous êtes invité à installer le package *DellAdvancedThreatProtection*.

9 Entrez **y** lorsque vous êtes invité à installer le package *CylanceDellATPPlugin*.



10 L'installation est terminée.



11 Voir Vérifier Endpoint Security Suite Enterprise pour l'installation de Linux.

Désinstallation avec ligne de commande

Pour désinstaller Endpoint Security Suite Enterprise for Linux à l'aide de la ligne de commande, suivez les étapes ci-dessous.

1 Accédez à une fenêtre de terminal.

2 Désinstallez le package à l'aide de la commande suivante :

```
sudo ./uninstall.sh
```

3 Appuyez sur **Entrée**.

Endpoint Security Suite Enterprise for Linux est désormais désinstallé. Vous pouvez utiliser l'ordinateur normalement.

Afficher les détails

Une fois Endpoint Security Suite Enterprise for Linux installé, il est reconnu par le Serveur Dell en tant que point de terminaison.

atp -t

La commande **atp - t** affiche toutes les menaces détectées sur le périphérique, ainsi que l'action appliquée. Les menaces sont une catégorie d'événements récemment détectés comme fichiers ou programmes potentiellement dangereux qui nécessitent une action corrective guidée.

```
Quarantined 17E76B830F9F30A39F078F5A69AD87B3838DB73A28EC893BD06EAF95D6E464E2 /tmp/threats/LINUXTarGz
Archive
Quarantined 20FBC1FDFCDC96A7E21FB1C700A6517A61711732A0D31FC25A60609710ECBE09 /tmp/threats/LINUXAutoB
lockNoService
Quarantined 2D49A3F81AF3362FE806E417DF2807C960314FF4F271B5B1360964163CB49886 /tmp/threats/LINUXGBL2
Quarantined 52D74BD1555D7C82746112C44F4D9A916B9DA286DD5B14D7665D4167BB1EB5D8 /tmp/threats/LINUXRunni
ngAutoQ
Quarantined 70F193F3C2023A7542338142CA89F1076A238AB7BAAD4202B2DCEDA7286E43D9 /tmp/threats/LINUXTest1
Quarantined 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F0158E0D519CEC1D868E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC28640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED085ED042423A172B4BED7702E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F178A6413A8A7E84437098777711FB1CA6E31F /tmp/threats/LINUXAutoB
lockExecution
```

Ces entrées détaillent les mesures prises, l'ID de hachage et l'emplacement de la menace.

- **Dangereux** : fichier suspect qui risque d'être un programme malveillant
- **Anormal** : fichier suspect qui pourrait être un programme malveillant
- **En quarantaine** : fichier déplacé de son emplacement d'origine, stocké dans le dossier de quarantaine et dont l'exécution sur le périphérique est bloquée.
- **Exonéré** : fichier dont l'exécution est autorisée sur le périphérique.
- **Effacé** : fichier effacé de l'organisation. Les fichiers autorisés comprennent des fichiers exonérés, ajoutés à la liste sécurisée et supprimés du dossier Quarantaine sur le périphérique.

Pour plus d'informations sur la classification des menaces d'Advanced Threat Prevention, voir la rubrique *AdminHelp*, disponible sur la console de gestion à distance du Serveur Dell.

Vérifier l'installation

Si vous le souhaitez, vous pouvez vérifier que l'installation a réussi.

- Sur le client, accédez à une fenêtre de terminal.
- Avant la réception d'une séquence de stratégie, le client s'enregistre sur le Dell Server.
- Le fichier */var/log/Dell/ESSE/DellAgent.00.log* détaille la communication avec le Dell Server et l'interaction plug-in/service.
  Le texte ci-joint confirme que le client a reçu les stratégies depuis le Serveur Dell :

```
2017.12.12 14:26:02.794 [02390] (00009) I Comm    : Received Id=ba150b8e-b1d3-44
5a-81e9-426e77fbb043
2017.12.12 14:26:02.795 [02390] (00009) I Comm    : ReceivedEdition enterprisesc
rver
2017.12.12 14:26:02.847 [02390] (00009) I Comm    : Successfully added memory ex
clusions to policy
2017.12.12 14:26:03.322 [02390] (00009) I Comm    : new policy seq# 9 received
2017.12.12 14:26:03.385 [02390] (00009) I Comm    : registered Centos7-3-64-MH w
ith server
2017.12.12 14:26:03.392 [02390] (00009) I Comm    : closing connection to https:
--More--(39%)
```

  Le texte ci-joint confirme que le service Dell a été arrêté pour charger le plug-in Advanced Threat Prevention :

```
//cedmz.credce.com:8888/agent
2017.12.12 14:27:05.883 [02390] (00009) I Comm    : next contact with server sch
eduled for 12/12/2017 8:27:05 PM
2017.12.12 14:27:10.442 [02390] (00005) I Agent   : Dell Data Protection stopped
---date--- ----time---- --pid-- -thrid-   -subsys-  ----------------------------
--message-------------------------------
2017.12.12 14:27:12.968 [02551] (00005) I Agent   : service name is "DellMgmtAge
nt"
2017.12.12 14:27:12.970 [02551] (00005) I Agent   : product name is "Dell Data P
```

Le texte ci-joint confirme les trois Endpoint Security Suite Enterprise pour les plug-ins Linux chargés :

```
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : machine name is "centosvm2.ddsdemos.com"
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : process is 64-bit
2018.02.18 10:51:36.952 [01077] (00005) I Agent   : domain is "(none)"
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Server Communication Manager" 1.
 Id={CAA1A89F-AF21-4C1E-9407-1E185FFEEB5C} in 69 ms
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Auditing and Reporting Service"
.0 Id={0E969074-3164-467F-BF3D-D9E695F48240} in <1 ms
2018.02.18 10:51:37.069 [01077] (00005) I AdvATP  : Advanced Threat Prevention Cylance component lo
ging initialized
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded plugin "Advanced Threat Prevention" 1.0
d={96BBD97F-9BF0-4D61-94F8-A9884F8DC287} in 8 ms
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded 3 plugins
2018.02.18 10:51:37.090 [01077] (00010) I Comm    : AgentID 00397403-c05f-4cbf-b6b4-e15dd577186a
2018.02.18 10:51:37.102 [01077] (00011) I AdvATP  : AdvancedAtpManager Starting
2018.02.18 10:51:37.125 [01077] (00011) I AdvATP  : management is active
2018.02.18 10:51:37.129 [01077] (00011) I AdvATP  : processing new policies - Policy list count=1
```

`atp -s` - Affiche les éléments suivants :

- État de l'enregistrement
- Numéro de série : à utiliser pour contacter le support. Il s'agit de l'identificateur unique de l'installation.
- Stratégie

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp -s
Registration Status: Registered
Serial Number: 0088ab40-ce18-43fa-a959-85f44e5ff251
Policy:  (Online)
```

La commande suivante détaille les variables de ligne de commande pour Endpoint Security Suite Enterprise pour Linux :

`/opt/cylance/desktop/atp --help`

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp --help
usage: atp <options>
options:
    -r, --register=token    : register with Dell Data Security servers with the
provided token
    -s, --status            : get status of Advanced Threat Prevention
    -u, --checkupdates      : check for updates
    -b, --start-bg-scan     : start background scan
    -B, --stop-bg-scan      : stop background scan
    -d, --scan-dir=dir      : scan directory
    -l, --getloglevel       : get current log level
    -L, --setloglevel=level : set log level
    -P, --getpolicytime     : get the policy update time
    -p, --checkpolicy       : check for policy updates
    -t, --threats           : list threats
    -q, --quarantine=id     : quarantine a file by id (hash)
    -w, --waive=id          : waive a file by id (hash)
    -v, --version           : print this tools version
    -h, --help              : atp help
```

La commande *atp* Advanced Threat Prevention est ajoutée au répertoire */usr/sbin*, qui est normalement inclus dans une variable PATH du Shell, de sorte qu'il puisse être utilisé dans la plupart des cas sans un chemin précis.

Dépannage

Désactiver le certificat SSL de confiance

Si un certificat de serveur de l'ordinateur est manquant ou auto-signé, vous devez désactiver la confiance vis-à-vis du certificat SSL du côté du client uniquement.

Si vous utilisez un certificat inhabituel, importez le certificat racine vers le magasin de certificats Linux, puis redémarrez Endpoint Security Suite pour les services Linux avec la commande suivante : `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Accédez à une fenêtre de terminal.

2 Entrez le chemin d'accès à CsfConfig app :
`/usr/lib/dell/esse/CsfConfig`

3 Exécutez CsfConfig.app :
`sudo ./CsfConfig`

Les paramètres par défaut sont indiqués ci-après :

Paramètres actuels :

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = Faux

DumpXmlInventory = Faux

DumpPolicies = Faux

4 Saisissez **-help** pour répertorier les options.

5 Pour désactiver le certificat SSL de confiance sur l'ordinateur cible, entrez la commande suivante :

```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

Ajout de modifications de règles et d'inventaire XML au dossier Journaux

Pour ajouter le fichier inventory.xml ou policies.xml au dossier Journaux :

1 Exécutez *CsfConfig app*, comme indiqué ci-dessus.

2 Pour modifier *DumpXmlInventory* sur *Vrai*, entrez la commande suivante :

```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 Pour modifier *DumpPolicies* sur *Vrai*, entrez la commande suivante :

```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

Les fichiers de règles sont vidés uniquement en cas de modification de règle.

4 Pour afficher les journaux inventory.xml et policies.xml, accédez à */var/log/Dell/Dell Data Protection*.

REMARQUE : Les modifications apportées à CsfConfig peuvent ne pas s'appliquer immédiatement.

Collecte de fichiers journaux

Les journaux de Endpoint Security Suite Enterprise for Linux se trouvent à l'emplacement suivant : */var/log/Dell/ESSE*. Pour générer des journaux, utilisez la commande suivante : **. /getlogs.sh**

Pour plus d'informations sur la collecte des journaux, voir SLN303924.

Provision a Tenant

Un locataire doit être provisionné dans Serveur Dell pour que l'application des stratégies Advanced Threat Prevention devienne active.

Pré-requis

- Doit être effectué par un administrateur doté du rôle Administrateur système.
- Doit disposer d'une connexion à Internet pour provisionner sur Serveur Dell.
- Doit disposer d'une connexion à Internet sur le client pour afficher l'intégration de service en ligne Advanced Threat Prevention dans la console de gestion.
- Le provisionnement est basé sur un jeton qui est généré à partir d'un certificat pendant le provisionnement.
- Les licences Advanced Threat Prevention doivent être présentes sur Serveur Dell.

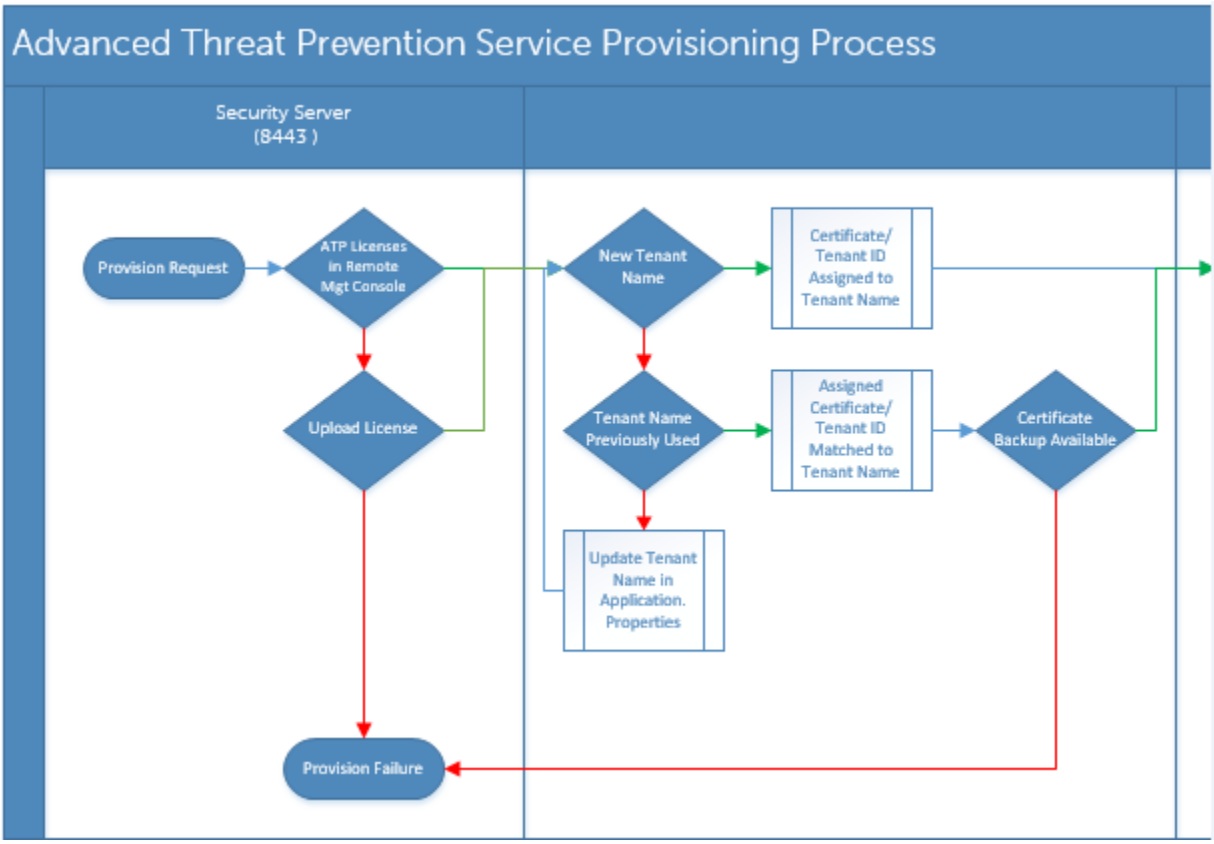
Provisionner un service partagé

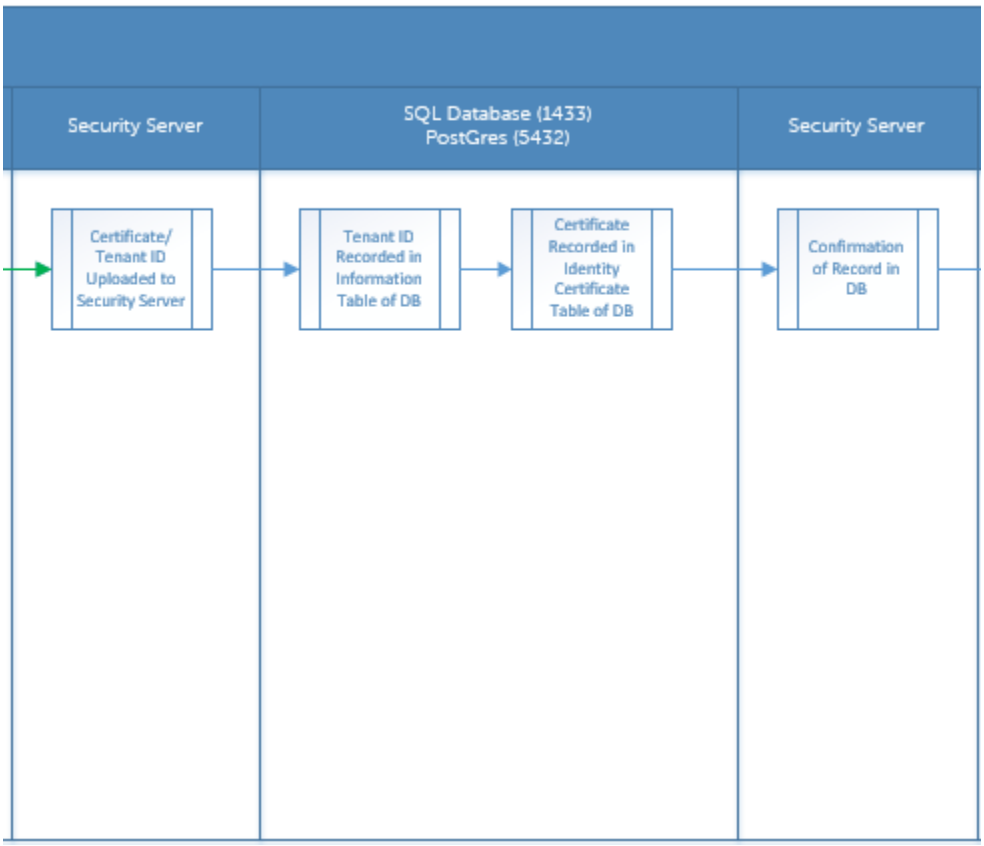
1. Connectez-vous à la console de gestion à distance en tant qu'administrateur Dell.
2. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion > Services de gestion.**
3. Cliquez sur **Configurer le service Advanced Threat Protection**. Importez vos licences Advanced Threat Prevention en cas d'échec à ce stade.
4. La configuration guidée commence une fois que les licences sont importées. Cliquez sur **Suivant** pour commencer.
5. Lisez et acceptez les termes du CLUF et cliquez sur **Suivant**.
6. Fournissez les identifiants à Serveur Dell pour le provisionnement du service partagé. Cliquez sur **Suivant**. *Le provisionnement d'un service partagé existant de marque Cylance n'est pas pris en charge.*
7. Téléchargez le certificat. Celui-ci est nécessaire à la récupération en cas de sinistre affectant Serveur Dell. Ce certificat n'est pas automatiquement sauvegardé. Sauvegardez le certificat à un emplacement sûr sur un autre ordinateur. Cochez la case pour confirmer que vous avez sauvegardé le certificat et cliquez sur **Suivant**.
8. La configuration est terminée. Cliquez sur **OK**.

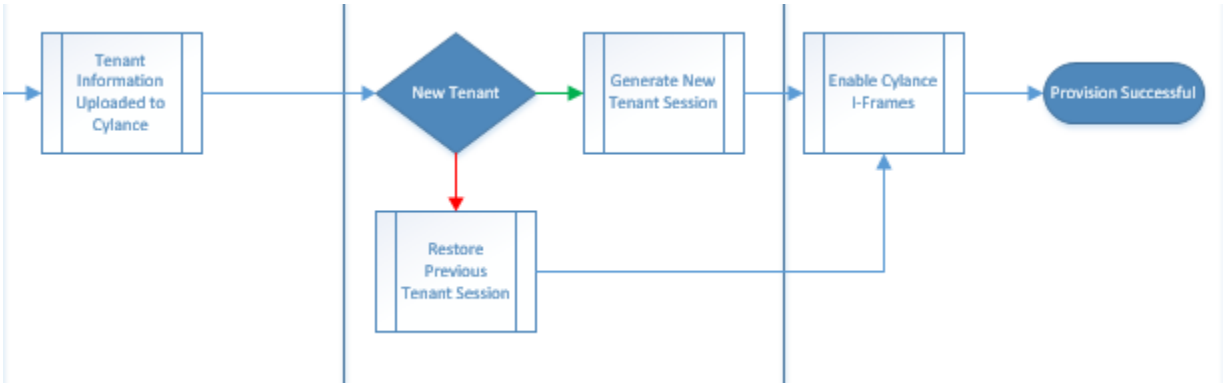
Dépannage de provisionnement

Provisionnement et communication de l'agent

Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Prevention


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
Provision Failure
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB



Le diagramme suivant illustre le processus de communication agent d'Advanced Threat Prevention.