# Dell Endpoint Security Suite Enterprise

## Advanced Threat Prevention Quick Start Guide v3.9

January 2024
Rev. A01

DELL Technologies

## Remarques, précautions et avertissements

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

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

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

# Contents

# 1

# Introduction

Before you perform tasks explained in this guide, the following components must be installed:

- Endpoint Security Suite Enterprise - refer to *Endpoint Security Suite Enterprise Advanced Installation Guide* or *Endpoint Security Suite Enterprise Basic Installation Guide*
- Security Management Server or Security Management Server Virtual Server - refer to *Security Management Server Installation and Migration Guide* or *Security Management Server Virtual Server Quick Start and Installation Guide*

This guide explains basic administration of Advanced Threat Prevention and should be used with *AdminHelp*, available in the Management Console.

## Contactez Dell ProSupport for Software

Appelez le 877-459-7304, poste 4310039, afin de recevoir 24x7 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 série 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 for Software.

# 2

# Démarrer

Ce chapitre indique les étapes recommandées pour commencer l'administration d'Advanced Threat Prevention.

Les étapes recommandées pour commencer l'administration d'Advanced Threat Prevention comprennent les phases suivantes :

- Configuration d'un locataire pour Advanced Threat Protection
  - Requise pour déployer Advanced Threat Prevention
  - Les licences Advanced Threat Prevention doivent être présentes sur Dell Server.
- Configuration de la mise à jour automatique de l'agent Advanced Threat Protection
  - Abonnement aux mises à jour automatiques pour Advanced Threat Prevention (facultatif)
  - Mises à jour disponibles tous les mois
- Attribution ou modification de rôles d'administrateur
  - Provisionnement ou récupération du service Advanced Threat Prevention
  - Sauvegarde et téléchargement des certificats existants d'Advanced Threat Prevention
  - Affichage, modification et validation des stratégies
- Configuration des notifications
  - Configuration des notifications par e-mail et sur le tableau de bord pour les alertes d'Advanced Threat Prevention (facultatif)
  - Personnalisation des notifications en fonction des besoins de votre entreprise

## Provision a Tenant

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

**Pré-requis**

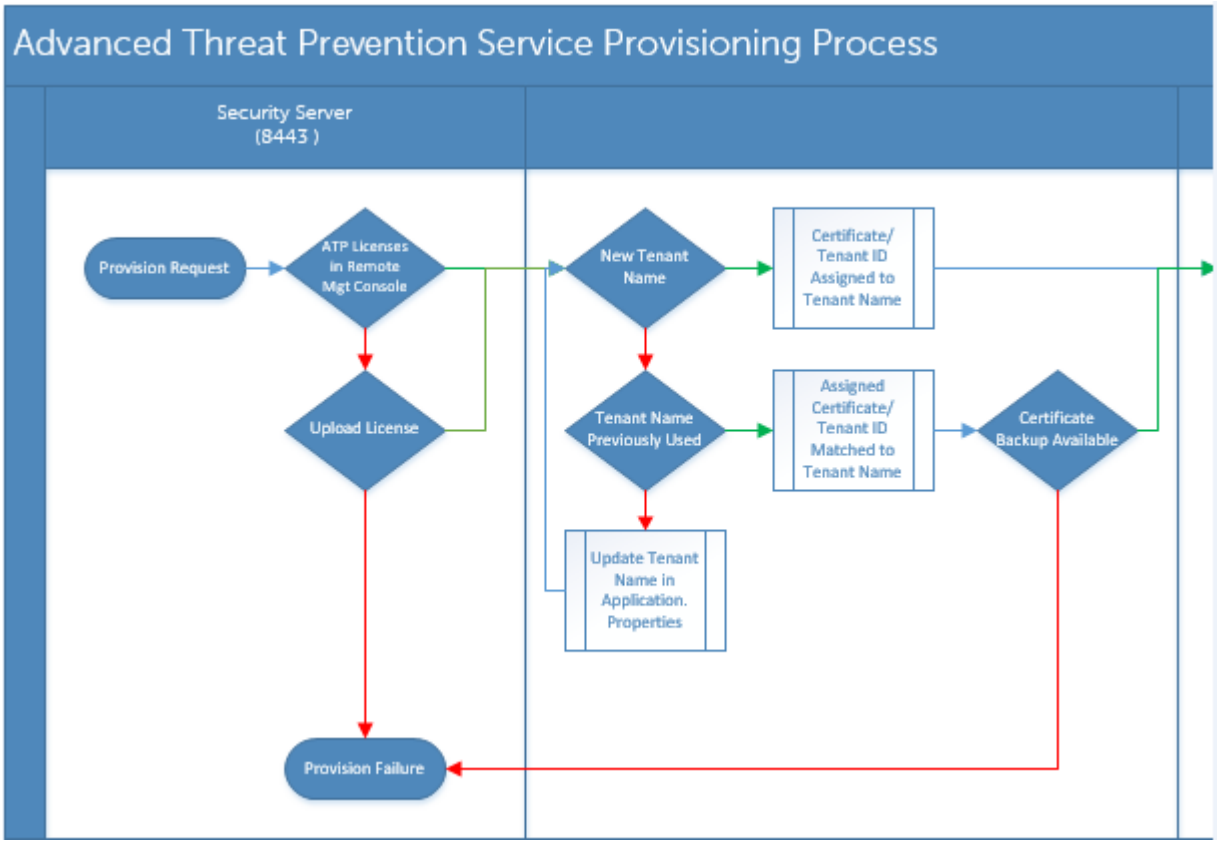
- Doit être effectué par un administrateur doté du rôle Administrateur système.
- Doit disposer d'une connexion à Internet pour provisionner sur Dell Server.
- Doit disposer d'une connexion à Internet sur le client pour afficher l'intégration de service en ligne Advanced Threat Prevention dans la console 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 Dell Server.

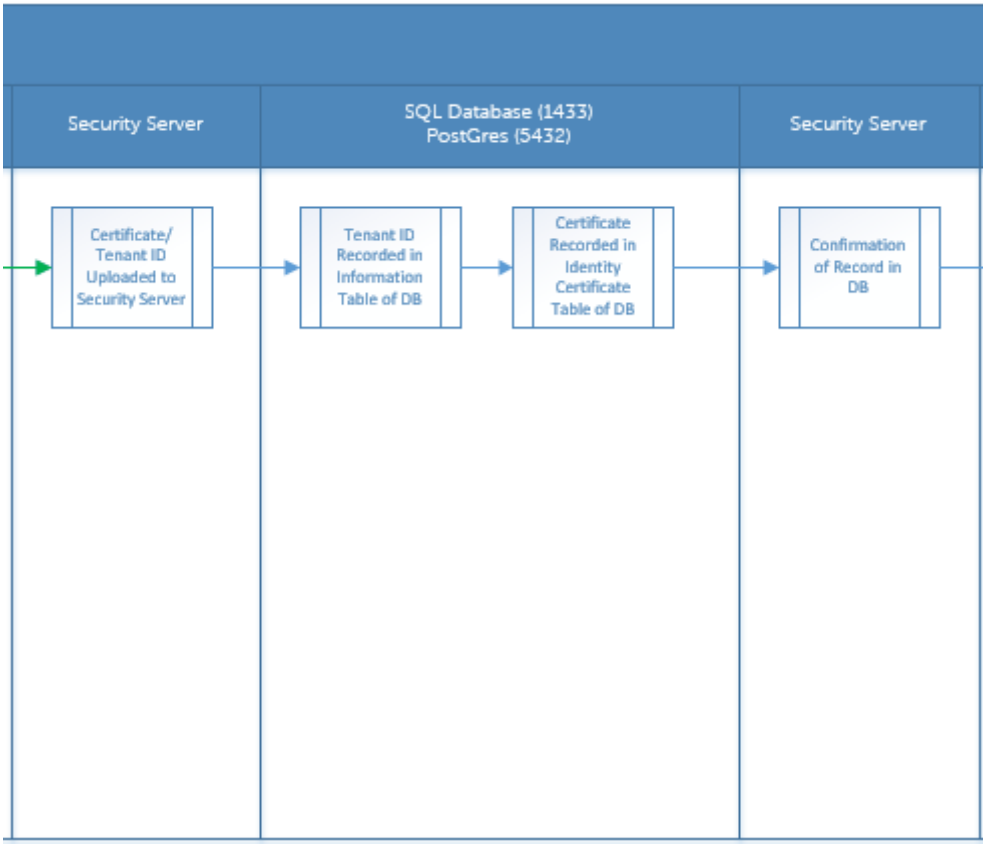
## Provisionner un service partagé

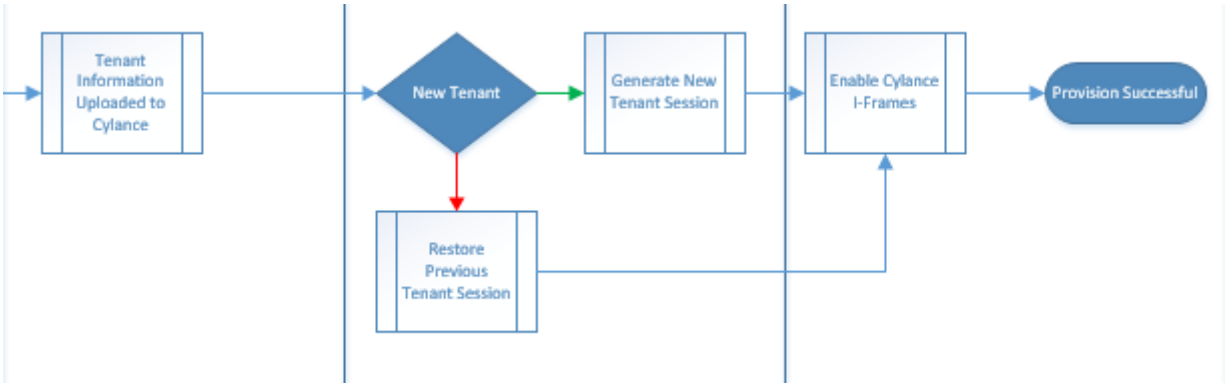
1. Connectez-vous à la console de gestion en tant qu'administrateur Dell.
2. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion > Services de gestion.**
3. Cliquez sur **Configurer le service Advanced Threat Protection**. Importez vos licences Advanced Threat Prevention en cas d'échec 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 Dell Server 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 Dell Server. 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**.

# Provisionnement et communication de l'agent

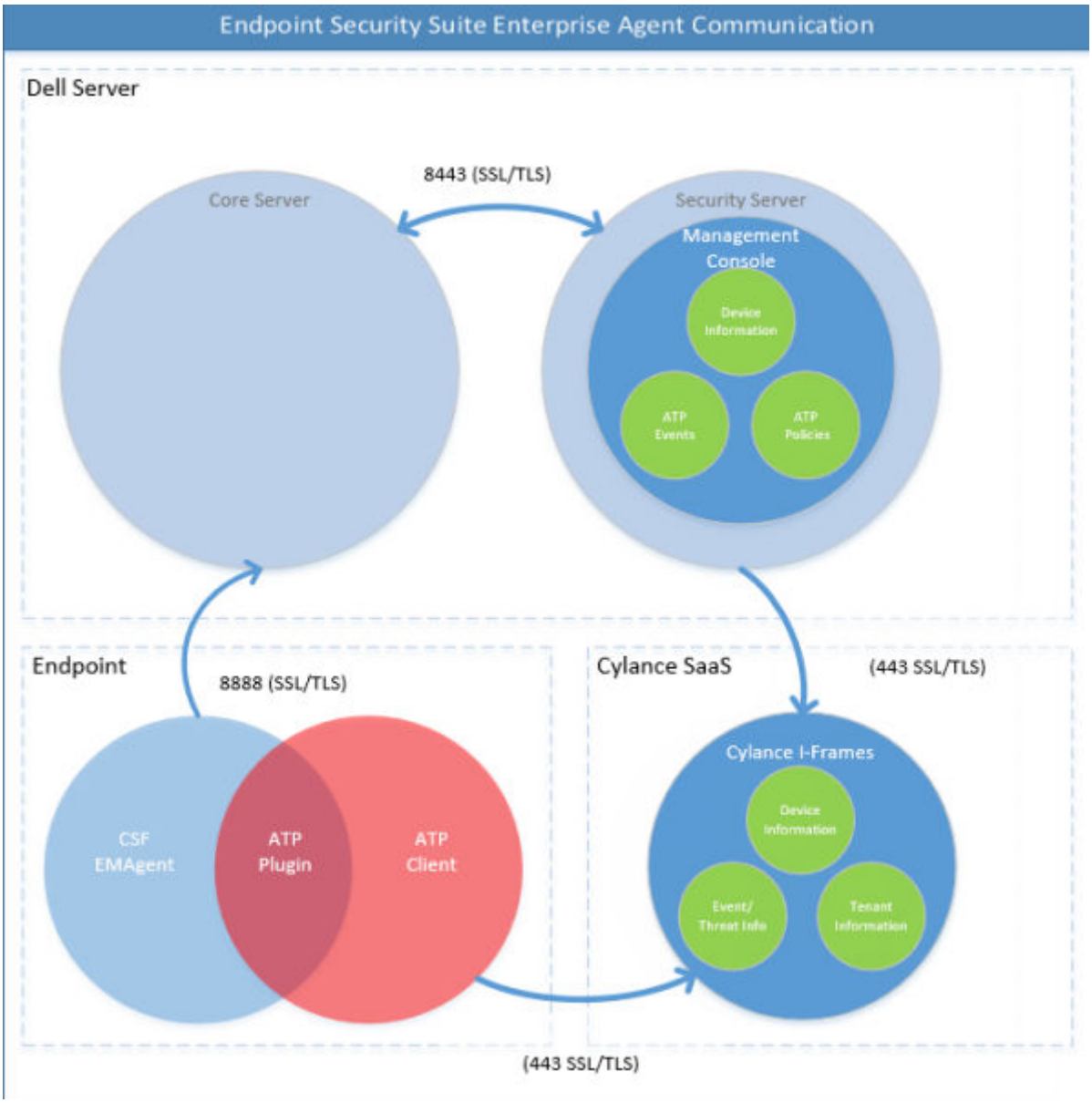
Les diagrammes suivants illustrent le processus de provisionnement du service Advanced Threat Prevention.



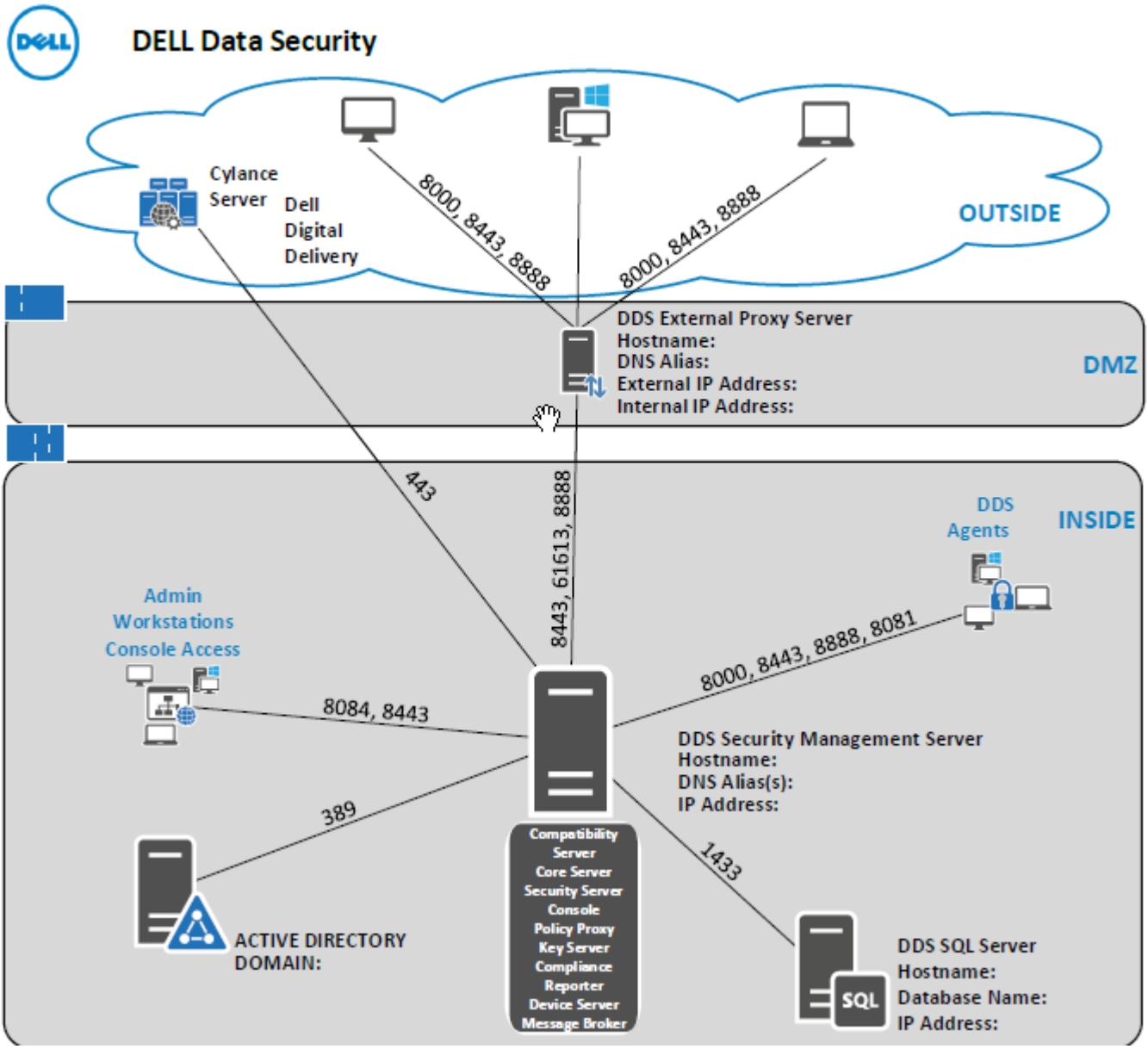






Le diagramme suivant illustre le processus de communication agent d'Advanced Threat Prevention.




Le schéma suivant illustre l'architecture et la communication de Dell Server.



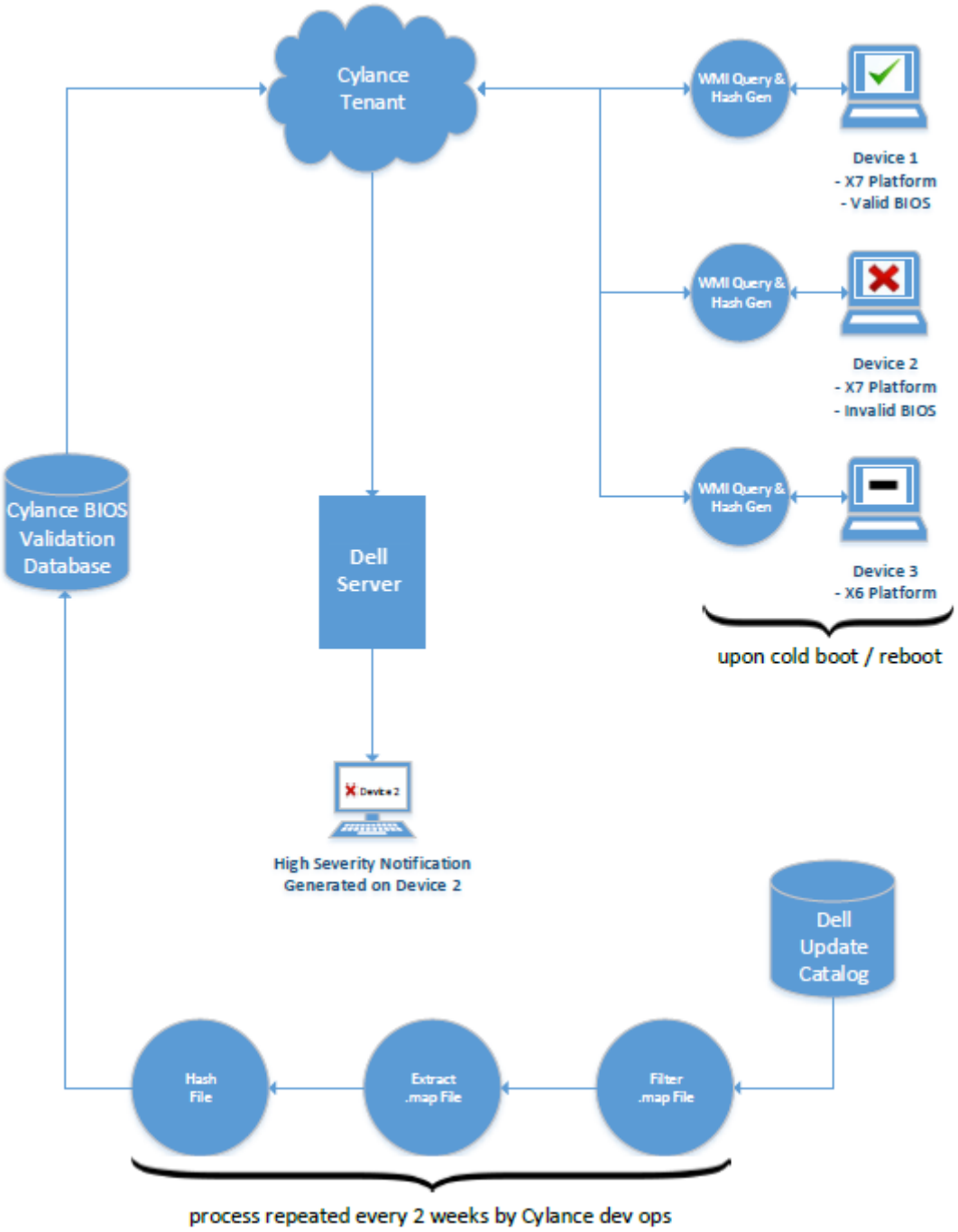

# Activation de la vérification de l'intégrité de l'image BIOS

La règle de vérification de l'intégrité de l'image du BIOS est activée par défaut lorsque le commutateur principal d'Advanced Threat Prevention est activé.

Pour obtenir un aperçu du processus de vérification de l'intégrité de l'image BIOS, voir la section Processus de vérification de l'intégrité de l'image BIOS.

## Processus de vérification

Le diagramme suivant illustre le processus de vérification de l'intégrité de l'image BIOS.




Si la règle *Activer l'assurance du BIOS* est sélectionnée dans la console de gestion, le locataire Cylance vérifie une valeur de hachage BIOS sur les ordinateurs de points de terminaison afin de garantir que le BIOS n'a pas été modifié par rapport à la version d'usine Dell, ce qui est un vecteur d'attaque possible. Si une menace est détectée, une notification est transmise à Dell Server et l'administrateur informatique est averti dans la console de gestion à distance. Pour consulter la présentation de ce processus, voir la section « Processus de vérification de l'intégrité de l'image BIOS ».

**REMARQUE :** Une image usine personnalisée ne peut pas être utilisée avec cette fonction, car le BIOS a été modifié.

| **Modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image BIOS** | |
|---|---|
| • Latitude 3470<br>• Latitude 3570<br>• Latitude 7275<br>• Latitude 7370 | • OptiPlex 5040<br>• OptiPlex 7040<br>• OptiPlex 7440<br>• Precision Mobile Workstation 3510 |

| Modèles d'ordinateur Dell pris en charge avec la vérification de l'intégrité de l'image BIOS | | |
|---|---|---|
| • Latitude E5270<br>• Latitude E5470<br>• Latitude E5570<br>• Latitude E7270<br>• Latitude E7470<br>• Latitude Rugged 5414<br>• Latitude Rugged 7214 Extrême<br>• Latitude Rugged 7414<br>• OptiPlex 3040<br>• OptiPlex 3240 | • Precision Mobile Workstation 5510<br>• Precision Workstation 3620<br>• Precision Workstation 7510<br>• Precision Workstation 7710<br>• Precision Workstation T3420<br>• Venue 10 Pro 5056<br>• Venue Pro 5855<br>• Venue XPS 12 9250<br>• XPS 13 9350<br>• XPS 9550 | |

# Configuration de la mise à jour automatique de l'agent Advanced Threat Prevention

Pour recevoir les mises à jour automatiques de l'agent Advanced Threat Prevention, vous pouvez vous inscrire dans la console de gestion. Le fait de s'inscrire pour recevoir les mises à jour automatiques de l'agent permet aux clients de télécharger et d'appliquer les mises à jour depuis le service Advanced Threat Prevention. Mises à jour et publications mensuelles.

**REMARQUE :**

Les mises à jour automatiques de l'agent sont prises en charge par la version 9.4.1 ou les versions ultérieures du Dell Server.

**Mises à jour automatique de l'agent de réception**

Pour vous inscrire et recevoir les mises à jour automatique de l'agent :

1. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion** > **Services de gestion**.
2. Sur l'onglet *Menaces avancées*, sous *Mise à jour automatique de l'agent*, cliquez sur le bouton **Activé**, puis cliquez sur **Enregistrer les préférences**.

   Le renseignement des informations et l'affichage des mises à jour automatiques peuvent prendre quelques instants.

**Arrêter la réception de mises à jour automatiques de l'agent**

Pour ne plus recevoir les mises à jour automatiques de l'agent :

1. Dans le volet de gauche de la console de gestion, cliquez sur **Gestion** > **Services de gestion**.
2. Sur l'onglet *Menaces avancées*, sous *Mise à jour automatique de l'agent*, cliquez sur le bouton **Désactivé**, puis cliquez sur **Enregistrer les préférences**.

# Attribution ou modification de rôles d'administrateur

Afficher ou modifier des privilèges de l'administrateur existants à partir de la page Administrateurs de la console de gestion.

**Rôles d'administrateur**

La fonction de connexion de l'administrateur est intégrée à Active Directory pour simplifier le processus de gestion des administrateurs et pour vous permettre d'exploiter votre infrastructure existante d'authentification des utilisateurs. Les rôles attribués aux administrateurs définissent le niveau d'accès autorisé pour chaque administrateur. Par exemple, il est possible que certains administrateurs soient uniquement autorisés à mettre en œuvre une récupération avec l'aide du support technique, tandis que d'autres disposent d'un accès total pour modifier les règles de sécurité. Vous pouvez attribuer des rôles d'administrateur à des groupes Active Directory. De cette façon, pour modifier le niveau d'accès administrateur dont disposent les utilisateurs, il suffit d'une simple modification de leur appartenance à un groupe AD. Compliance Reporter permet d'accorder aux utilisateurs hors domaine un accès aux rapports uniquement.

Le rôle d'administrateur système est nécessaire pour effectuer les tâches suivantes :

- Provisionnement ou récupération du service Advanced Threat Prevention
- Abonnement aux mises à jour automatiques pour Advanced Threat Prevention
- Configuration des notifications par e-mail et sur le tableau de bord pour les alertes d'Advanced Threat Prevention

- Sauvegarde et téléchargement des certificats existants d'Advanced Threat Prevention

**REMARQUE :** Le rôle d'administrateur de la sécurité est nécessaire pour afficher, modifier ou valider les règles.

Pour afficher ou modifier les privilèges de l'administrateur existants, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Administrateurs**.
2. Recherchez ou sélectionnez la ligne qui affiche le nom d'utilisateur de l'administrateur approprié pour afficher les détails de l'utilisateur.
3. Affichez ou modifiez les rôles d'administrateur dans le volet droit.
4. Cliquez sur **Enregistrer**.

**REMARQUE :** Dell recommande d'attribuer les rôles d'administrateur au niveau de groupe plutôt qu'au niveau de l'utilisateur.

Pour afficher, attribuer, ou modifier les rôles d'administrateur au niveau de groupe, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Groupes d'utilisateurs**.
2. Recherchez ou sélectionnez un nom de groupe, puis l'onglet **Administrateur**. La page Détail des groupes d'utilisateurs s'affiche.
3. Sélectionnez ou désélectionnez les rôles d'administrateur attribués au groupe.
4. Cliquez sur **Enregistrer**.

Si vous supprimez un groupe qui possède des droits d'administrateur, puis rajoutez plus tard le groupe, il reste un groupe d'administrateurs.

Pour afficher, attribuer, ou modifier les rôles d'administrateur au niveau de l'utilisateur, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Utilisateurs**.
2. Recherchez ou sélectionnez un nom d'utilisateur, puis cliquez sur l'onglet Administrateur.
3. Sélectionnez ou désélectionnez les rôles d'administrateur attribués à l'utilisateur.
4. Cliquez sur **Enregistrer**.

Rôles d'administrateur - Attribuez ou modifiez les rôles de l'utilisateur, puis cliquez sur **Enregistrer**.

Rôles de groupe hérités - Liste en lecture seule des rôles que l'utilisateur a hérités d'un groupe. Pour modifier les rôles, cliquez sur l'onglet **Groupes d'utilisateurs** de cet utilisateur, puis sélectionnez le nom du groupe.

Rôles délégués - Déléguez des droits de l'administrateur à un utilisateur.

# Configuration des notifications

Dans la console de gestion à distance, vous pouvez vous abonner pour recevoir les notifications. La liste des notifications fournit un récapitulatif configurable des actualités, des alertes et des événements à afficher dans le tableau de bord ou à envoyer sous forme de notifications par e-mail.

**Types de notification**

Vous pouvez sélectionner les types de notification à inclure dans la liste. Les notifications concernant les types restants sont cachées. Les notifications de **Threat Protection** et **d'événements de menaces avancées** s'appliquent à Advanced Threat Prevention.

Les types incluent :

- **Mise à jour** : informations sur les mises à jour du produit à venir. Pour afficher et recevoir des mises à jour sur les produits, vous devez vous inscrire pour les recevoir. Sélectionnez **Gestion des services > Notifications des produits**, cliquez sur **Activé**, puis cliquez sur **Enregistrer les préférences**.
- **Config** : informations sur les changements de configuration.
- **Base de connaissances** : des récapitulatifs et des liens vers des articles de la base de connaissances comportant des informations techniques approfondies telles que des solutions de contournement et des méthodes de configuration.
- **Annonce** : actualités des prochaines versions et des nouveaux produits.
- **Licence** : vous alerte lorsque votre volume de licences disponibles est faible ou lorsque vous avez dépassé le nombre de licences d'accès client.
- **Threat Protection** : une alerte de menace émise par Advanced Threat Prevention.
- **Événement de menace avancée** : événement détecté par Advanced Threat Prevention. Le résumé contient la liste des événements de types Critique, Majeur, Mineur, Avertissement et Information, avec des liens vers des informations plus détaillées.
- **Événement de menace** : événement détecté par Threat Protection.
- **Certificat** : notification d'expiration du certificat.

- **Exceptions de Dell Server** : un problème de communication du serveur Dell Server empêche l'envoi des notifications suivantes : Threat Protection, Mise à jour, Configuration, Base de connaissances et Annonce.

Après avoir sélectionné un ou plusieurs types, cliquez sur l'espace neutre au-dessus de la liste pour appliquer les sélections.

Sélectionnez **Effacer les éléments sélectionnés** pour réinitialiser les sélections dans cette liste.

**Niveaux de priorité**

**REMARQUE :** Les niveaux de priorité des notifications ne sont pas liés aux niveaux de priorité affichés sur le tableau de bord autres que ceux de la zone des notifications.

Les priorités sont Critique, Élevée, Moyenne et Basse. Ces niveaux de priorité sont mutuellement relatifs dans un type de notification.

Vous pouvez sélectionner les niveaux de priorité des notifications à inclure dans les listes de la zone des notifications sur le tableau de bord ou de notifications par e-mail. Les notifications concernant les autres niveaux de priorité ne sont pas incluses dans les listes des notifications sur le tableau de bord ou par e-mail.

Sélectionnez **Effacer les éléments sélectionnés** pour réinitialiser les sélections dans cette liste. Toutes les notifications s'affichent (si elles ne sont pas filtrées ailleurs).

# 3

# Stratégies

Ce chapitre présente la gestion des règles d'Advanced Threat Prevention.

- Activation d'Advanced Threat Prevention
- Paramètres de règle recommandés
- Validation des modifications des règles

Pour consulter la liste complète des règles d'Advanced Threat Prevention et leur description, voir *AdminHelp*, disponible dans la console de gestion.

## Activation d'Advanced Threat Prevention

La règle Advanced Threat Prevention est **désactivée** par défaut et doit être **activée** pour pouvoir activer les règles d'Advanced Threat Prevention. Les règles d'Advanced Threat Prevention sont disponibles aux niveaux Entreprise, Groupe de points de terminaison et Point de terminaison.

Pour activer la règle Advanced Threat Prevention au niveau Entreprise, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Cliquez sur **Threat Prevention**.
3. Faites basculer le commutateur principal Advanced Threat Prevention de **Désactivé** à **Activé**.

Pour activer la règle Advanced Threat Prevention au niveau Groupe de points de terminaison, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Groupe de points de terminaison**.
2. Cliquez sur **Threat Prevention**.
3. Faites basculer le commutateur principal Advanced Threat Prevention de **Désactivé** à **Activé**.

Pour activer la règle Advanced Threat Prevention au niveau Point de terminaison, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Points de terminaison**.
2. Cliquez sur **Threat Prevention**.
3. Faites basculer le commutateur principal Advanced Threat Prevention de **Désactivé** à **Activé**.

## Paramètres de règle recommandés

- Pour obtenir la dernière liste des paramètres de règle recommandés, voir l'article de la Base de connaissances SLN301562.

## Validation des modifications des règles

Pour valider les règles qui ont été modifiées et enregistrées :

1. Dans le volet gauche de la console de gestion, cliquez sur **Gestion > Valider**.
2. Dans le champ Commentaire, entrez une description de la modification.
3. Cliquez sur **Valider les règles**.

Une validation/publication des règles se produit lorsqu'un administrateur clique sur **Valider les règles**. Les informations suivantes sont affichées :

- Modifications de règles en attente : nombre de modifications de règles prêtes à être validées.
- Date de validation : date et heure de validation des règles.
- Modifié par : nom de l'utilisateur de l'administrateur qui a effectué la validation des règles.
- Commentaire : commentaires ajoutés lors de la validation des règles.
- Version : nombre d'enregistrements de règles depuis la dernière validation de règles plus la version précédente.

# 4

# Menaces

Ce chapitre explique comment identifier et gérer les menaces d'un environnement d'entreprise suite à l'installation d'Advanced Threat Prevention.

- Identification d'une menace
  - Affichage des événements de menace
  - Score Cylance et mises à jour des modèles de menace
  - Affichage des données de menace détaillées
- Gestion d'une menace
  - Exportation des données de menace vers un fichier CSV
  - Gestion de la liste de quarantaine globale

## Identification d'une menace

**Notifications par e-mail et sur le tableau de bord**

Si vous avez défini des notifications par e-mail pour Threat Protection et les événements de menaces avancées, un administrateur est averti par e-mail des événements et menaces d'Advanced Threat Prevention.

Le résumé des notifications sur le tableau de bord dans la console de gestion affiche les événements et menaces d'Advanced Threat Prevention en tant que types de notifications de Threat Protection et d'événements de menaces avancées.

- Type Threat Protection : alerte de menace émise par Advanced Threat Prevention.
- Type Événement de menace avancée : événement détecté par Advanced Threat Prevention. Un événement n'est pas nécessairement une menace.

Le tableau suivant fournit des informations détaillées sur les étiquettes et la gravité des menaces ainsi que sur les menaces proprement dites.

| Étiquette | Gravité | Détail |
|---|---|---|
| ThreatFound | Critique | Indique qu'un exécutable portable (PE) a été identifié sur un appareil, mais qu'il n'a pas été bloqué ni mis en quarantaine sur le terminal, ce qui signifie qu'une menace est active sur le système. |
| ThreatBlocked | Avertissement | Indique qu'un exécutable portable a été identifié sur l'appareil, mais que son exécution a été bloquée. Cette menace n'a pas été spécifiquement mise en quarantaine et résulte probablement du fait que la stratégie de mise en quarantaine automatique n'a pas été activée ou que le fichier se trouve à un emplacement qui nous empêche d'y écrire avec le compte du système local (partage réseau, périphérique USB qui a été retiré, etc.). |
| ThreatTerminated | Avertissement | Indique qu'un exécutable portable a été identifié sur l'appareil et que son processus a été interrompu, car son exécution était active. Cela n'indique pas que le fichier a été mis en quarantaine, car l'exécutable portable peut avoir été exécuté à partir d'un autre emplacement. Il est recommandé de rechercher un autre événement en corrélation avec ce terminal et cet exécutable pour confirmer que la menace a été correctement contenue. |
| MemoryViolationBlocked | Avertissement | Indique qu'un exécutable ou un script a tenté de s'exécuter, mais qu'il était en violation de la stratégie Protection de la mémoire ou Contrôle des scripts. L'exécution de l'exécutable ou du script a été bloquée par la suite. En général, cela indique que la stratégie décrite |

| Étiquette | Gravité | Détail |
|---|---|---|
| | | Protection de la mémoire ou Contrôle des scripts en corrélation a été définie sur Bloquer. |
| MemoryViolationTerminated | Avertissement | Indique qu'un exécutable ou un script s'exécute activement et est en violation de la stratégie Protection de la mémoire ou Contrôle des scripts. L'exécutable ou le script a été arrêté par la suite. En général, cela indique que la stratégie décrite Protection de la mémoire ou Contrôle des scripts en corrélation a été définie sur Arrêter. |
| MemoryViolation | Avertissement | Indique qu'un exécutable ou un script est en violation de la stratégie Protection de la mémoire ou Contrôle des scripts. Aucune action n'a été effectuée dans l'exécutable ou le script, probablement parce que la stratégie est définie sur Autoriser. |
| ThreatRemoved | Informations | Indique qu'un exécutable portable précédemment marqué, qui était considéré comme une menace, a été supprimé du terminal. Cela peut indiquer que l'exécutable portable a été retiré de la quarantaine ou supprimé de l'emplacement initial. Cette opération est courante avec les exécutables portables initialement détectés sur un support amovible (USB, CD-ROM, etc.). |
| ThreatQuarantined | Informations | Indique qu'un exécutable portable a été identifié comme une menace potentielle et qu'il a été mis en quarantaine par la suite avec succès. Cela indique que la stratégie de mise en quarantaine automatique des menaces en fonction de la classification de contenu Anormal (score Cylance de 0 à 60) ou Dangereux (score Cylance de 60 à 100) est activée. |
| ThreatWaived | Informations | Indique qu'un exécutable portable identifié comme une menace potentielle a été exonéré en fonction de la liste blanche globale ou par une quarantaine locale. Cela peut également indiquer que le hachage SHA256 a été ajouté aux stratégies « Exonération » ou « Liste blanche globale » dans Dell Security Management Server. |
| ThreatChanged | Informations | Indique si le score Cylance d'un exécutable portable a changé. Cela se produit généralement en cas de notation en deux étapes effectuée par Cylance. L'analyse du moteur de notation locale de la menace ne correspond peut-être pas à l'analyse du moteur Cloud Cylance. Dans ce cas, en raison des données supplémentaires dont dispose le moteur Cloud Cylance, c'est le score obtenu par ce moteur qui est utilisé. Cela peut également indiquer qu'une mise à jour de Cylance a initialisé une nouvelle analyse des fichiers qui étaient auparavant considérés comme des menaces, et qu'un nouveau score calculé a résolu cet exécutable portable, qui n'est plus considéré comme une menace. |
| ProtectionStatusChanged | Informations | Indique si l'état de protection d'un terminal a été modifié. Cela se déclenche lorsque l'agent Dell Encryption Management Agent se reconnecte aux services Cylance par le biais des plug-ins Cylance. Cette opération est généralement déclenchée lorsqu'un terminal a redémarré, car il existe une courte période pendant laquelle CSF peut ne pas s'être connecté aux plug-ins Cylance pendant le démarrage. |

Cliquez sur une notification pour obtenir plus de détails. Le résumé comprend des liens vers des informations supplémentaires sur la menace ou l'événement.

**Onglet Menaces avancées**

L'onglet Menaces avancées offre un affichage dynamique des informations d'événements détaillées pour l'ensemble de l'entreprise, y compris la liste des périphériques où se sont produits les événements et les actions liées à ces derniers exécutées sur ces périphériques.

Pour accéder à l'onglet Menaces d'entreprise avancées, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Sélectionnez l'onglet **Menaces avancées**.

Les informations concernant les événements, les périphériques et les actions sont organisées selon les onglets suivants :

- **Protection** : répertorie les fichiers et scripts potentiellement dangereux ainsi que des détails les concernant, notamment les périphériques sur lesquels ces fichiers et scripts ont été détectés.
- **Agents** : fournit des informations sur les périphériques exécutant le client Advanced Threat Prevention ainsi que l'option d'exportation des informations ou de suppression des périphériques de la liste.
- **Liste globale** : répertorie des fichiers dans la liste de Mise en quarantaine globale et la Liste de sécurité et fournit l'option de déplacement des fichiers vers ces listes.
- **Options** : fournit un moyen d'intégration avec Security Information Event Management (SIEM).
- **Certificat** : permet le chargement de certificats. Après le chargement, les certificats s'affichent dans l'onglet de la liste globale et peuvent être placés sur liste blanche.

Les tableaux figurant dans les onglets peuvent être organisés comme suit :

- Ajouter ou supprimer des colonnes dans le tableau : cliquez sur la flèche en regard de n'importe quel en-tête de colonne, sélectionnez **Colonnes**, puis sélectionnez les colonnes à afficher. Décochez la case des colonnes à masquer.
- Trier les données : cliquez sur un en-tête de colonne.
- Regrouper par colonne : faites glisser l'en-tête de colonne vers le haut jusqu'à ce qu'il devienne vert.

**Onglet des événements de menaces avancées**

L'onglet Événements de menaces avancées affiche des informations sur les événements destinées à toute l'entreprise en fonction des informations disponibles dans le serveur Dell Server.

L'onglet indique si le service Advanced Threat Prevention est configuré et si des licences sont disponibles.

Pour exporter des données depuis l'onglet Événements de menaces avancées, cliquez sur le bouton **Exporter**, puis sélectionnez le format de fichier **Excel** ou **CSV**.

**REMARQUE :** Les fichiers Excel sont limités à 65 000 lignes. Les fichiers CSV n'ont aucune limite de taille.

**Score Cylance et mises à jour des modèles de menace**

Un score Cylance est attribué à chaque fichier considéré comme anormal ou dangereux. Le score indique le degré de probabilité qu'il s'agisse d'un fichier de programme malveillant. Plus le chiffre est élevé, plus le degré de probabilité est élevé.

Le modèle de menace prédictif utilisé pour protéger les périphériques reçoit des mises à jour périodiques pour améliorer les taux de détection.

Sur la page Protection de la console de gestion, deux colonnes montrent dans quelle mesure un nouveau modèle de menace affecte votre organisation. Affichez et comparez les colonnes État de production et Nouvel état pour voir quels fichiers des périphériques pourraient être concernés par un changement de modèle.

Pour afficher les colonnes État de production et Nouvel état :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Sélectionnez l'onglet **Menaces avancées**.
3. Cliquez sur l'onglet **Protection**.
4. Cliquez sur la flèche vers le bas dans un en-tête de colonne du tableau.
5. Placez le pointeur de la souris sur **Colonnes**.
6. Sélectionnez les colonnes **État de production** et **Nouvel état**.

**État de production** : état du modèle actuel (Sûr, Anormal ou Dangereux) du fichier.

**Nouvel état** : état du modèle du fichier dans le nouveau modèle.

Par exemple, un fichier considéré comme Sûr dans le modèle actuel peut devenir Dangereux dans le nouveau modèle. Si votre organisation a besoin de ce fichier, vous pouvez l'ajouter à la liste blanche. Un fichier qui n'a jamais été examiné ou noté par le modèle actuel peut être considéré comme Dangereux par le nouveau modèle. Si votre organisation a besoin de ce fichier, vous pouvez l'ajouter à la liste blanche.

***Seuls les fichiers détectés sur le périphérique de votre organisation dont le score Cylance a changé s'affichent.***
Certains fichiers peuvent changer de score sans pour autant changer d'état. Par exemple, si le score Cylance d'un fichier passe de 10 à 20, l'état du fichier peut rester Anormal. Le fichier s'affiche ensuite dans la liste des modèles mise à jour (si ce fichier existe sur les périphériques de votre organisation).

**Comparaison entre le nouveau modèle et le modèle actuel**

Vous pouvez maintenant examiner les différences entre le modèle actuel et le nouveau modèle.

Les deux scénarios possibles à prendre en compte sont les suivants :

État de production = Sûr, Nouvel état = Anormal ou Dangereux

- Votre entreprise considère le fichier comme sûr
- Votre entreprise est configurée de manière à mettre les éléments anormaux et dangereux en quarantaine automatique

Dans les scénarios ci-dessus, nous vous recommandons de placer sur liste fiable les fichiers que vous voulez autoriser dans votre organisation.

**Identifier les classifications**

Pour identifier les classifications qui peuvent avoir un impact sur votre organisation, Dell recommande l'approche suivante :

1. Appliquez un filtre à la colonne Nouvel état pour afficher tous les fichiers non sûrs, anormaux et mis en quarantaine.
2. Appliquez un filtre à la colonne État de production pour afficher tous les fichiers sûrs.
3. Appliquez un filtre à la colonne Classification pour montrer uniquement les menaces fiables et locales.

Fiable : les fichiers locaux ont été analysés par Cylance et sont considérés comme sûrs. Placez ces éléments sur liste blanche après examen. Si la liste filtrée contient une grande quantité de fichiers, vous devrez peut-être définir la priorité à l'aide d'attributs supplémentaires. Par exemple, ajoutez un filtre à la colonne Détecté par pour examiner les menaces détectées par le contrôle d'exécution. Celles-ci ont été identifiées lorsqu'un utilisateur a tenté d'exécuter une application et nécessitent une plus grande attention que des fichiers dormants identifiés par la détection des menaces en arrière-plan ou File Watcher.

Les informations destinées à la comparaison entre les modèles proviennent de la base de données, non de vos périphériques. Ainsi, aucune nouvelle analyse n'est exécutée pour la comparaison des modèles. Toutefois, lorsqu'un nouveau modèle est disponible et que l'Agent adéquat est installé, une nouvelle analyse est effectuée sur votre organisation et tous les changements de modèle sont appliqués.

Reportez-vous à *AdminHelp* pour plus d'informations.

**Affichage des événements Web Protection et Firewall**

Les menaces sont réparties en catégories : logiciels malveillants ou de type Exploit, Filtre Web, Pare-feu ou Événements hors catégorie. Vous pouvez trier la liste des événements de menace en cliquant sur le titre d'une colonne. Vous pouvez afficher les événements de menace pour l'ensemble de l'entreprise ou pour un seul point final. Pour afficher les événements de menace d'un point de terminaison spécifique, ouvrez l'onglet Événements de menace d'entreprise, puis sélectionnez le périphérique dans la colonne ID de périphérique.

Pour afficher les événements de menace de toute l'entreprise, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Cliquez sur l'onglet **Événements de menace**.
3. Sélectionnez le niveau de gravité voulu et la période pour laquelle afficher les événements.

Pour afficher les menaces d'un point de terminaison spécifique, procédez comme suit :

1. Dans le volet gauche, cliquez sur **Populations > Points de terminaison**.
2. Recherchez ou sélectionnez un nom d'hôte, puis cliquez sur l'onglet **Événements de menaces**.

# Gestion d'une menace

Vous pouvez mettre les menaces en quarantaine, les répertorier dans une liste de sécurité, les ignorer et les exporter.

Procédez comme suit au niveau Entreprise :

- Exportez une menace ou un script qui a déclenché une alerte
- Mettez en quarantaine une menace
- Répertoriez une menace dans la liste de sécurité
- Modifiez manuellement la liste globale

Pour gérer une menace identifiée au niveau Entreprise :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Sélectionnez l'onglet **Menaces avancées**.
3. Sélectionnez Protection.

Dans le tableau Contrôle des scripts, vous pouvez exporter un script qui est répertorié dans le tableau comme menace potentielle.

**Gérer les menaces d'entreprise avancées**

L'onglet Protection contient des informations relatives aux fichiers et aux scripts potentiellement dangereux.

**Tableau des menaces**

Dans le tableau Menaces, vous pouvez exporter une menace, la mettre en quarantaine ou la répertorier dans la liste de sécurité. Vous pouvez aussi ajouter manuellement une menace dans la liste de quarantaine globale.

Le tableau répertorie tous les événements trouvés dans l'entreprise. Un événement peut être également une menace éventuelle.

Affichez des informations supplémentaires sur une menace spécifique en cliquant sur le lien de son nom (les détails s'affichent dans une nouvelle page) ou en cliquant n'importe où dans la ligne de la menace (les détails s'affichent au bas de la page).

Pour afficher des informations sur les menaces dans le tableau, cliquez sur la flèche de la liste déroulante d'un en-tête de colonne pour sélectionner et ajouter des colonnes. Les colonnes affichent les métadonnées concernant le fichier telles que Classifications, Score Cylance (niveau de confiance), Sévérité AV Industry (renvoie vers VirusTotal.com pour comparaison avec d'autres fournisseurs), Date de première détection, SHA256, MD5, Informations sur le fichier (auteur, description, version) et Détails de la signature.

**Commandes**

- **Exporter** : exportez les données de menace vers un fichier .CSV. Sélectionnez les lignes à exporter, puis cliquez sur **Exporter**.
- **Quarantaine globale :** ajoutez un fichier à la liste de quarantaine globale. La menace est mise définitivement en quarantaine depuis tous les périphériques.
- **Sûr** : ajoutez un fichier à la liste fiable. Le fichier est définitivement considéré comme inoffensif sur tous les périphériques.

  **REMARQUE :** à l'occasion, un « bon » fichier peut être mis en quarantaine ou signalé comme dangereux (cela peut se produire si les caractéristiques de ce fichier ressemblent fortement à celles des fichiers malveillants). Lever le fichier ou le mettre sur la liste fiable peut être utile dans ce cas.

- **Modifier la liste globale** : ajoutez ou supprimez des fichiers de la liste de quarantaine globale.
- **Ignorer** : ajoutez un fichier dans la liste Ignoré sur un ordinateur. Ce fichier sera autorisé à s'exécuter sur l'ordinateur.

**Gestion des menaces avancées de point de terminaison**

Pour gérer une menace identifiée sur un ordinateur :

1. Dans le volet gauche, cliquez sur **Populations > Entreprise**.
2. Sélectionnez l'onglet **Menaces avancées**.
3. Sélectionnez Agents.
4. Sélectionnez un nom d'agent, puis sélectionnez la commande appropriée : **Exporter**, **Mettre en quarantaine**, ou **Ignorer** une menace.

# 5

# Mode Déconnecté

Le mode Déconnecté permet à un serveur Dell Server de gérer les points de terminaison d'Advanced Threat Prevention sans connexion client à Internet ou à un réseau externe. Il permet également au serveur Dell Server de gérer les clients sans connexion à Internet, ni service Advanced Threat Prevention configuré ou hébergé. Le serveur Dell Server capture toutes les données de menace et d'événements en mode Déconnecté.

Pour déterminer si un serveur Dell Server s'exécute en mode Déconnecté, cliquez sur l'icône en forme d'engrenage en haut à droite de la console de gestion à distance et sélectionnez À propos. L'écran À propos indique si un serveur Dell Server est en mode Déconnecté juste en-dessous de la version du serveur.Dell Server

Les points suivants distinguent le mode Déconnecté d'une installation connectée standard du serveur Dell Server.

**Activation du client**

Un jeton d'installation est généré lorsque l'administrateur télécharge une licence Advanced Threat Prevention, ce qui permet l'activation du client Advanced Threat Prevention.

**Console de gestion**

Les éléments suivants ne sont **pas disponibles** dans la console de gestion lorsque le serveur Dell Server s'exécute en mode Déconnecté :

- Zones spécifiques à Advanced Threat Prevention : menaces avancées par priorité, (menaces avancées) événements par classification, Top 10 des menaces avancées et événements Advanced Threat Prevention.
- L'onglet **Entreprise > Menaces avancées** fournit un affichage dynamique des informations d'événements détaillées pour l'ensemble de l'entreprise, y compris la liste des périphériques où se sont produits les événements et les actions liées à ces derniers exécutées sur ces périphériques.
- (Volet de navigation gauche) Gestion des services qui permet l'activation du service Advanced Threat Prevention et l'inscription aux notifications du produit.

Les éléments suivants **sont disponibles** dans la console de gestion pour prendre en charge le mode Déconnecté :

- L'onglet **Entreprise > Événements de menaces avancées** répertorie les informations d'événements pour l'ensemble de l'entreprise en fonction des informations disponibles sur le serveur Dell Server, même en mode Déconnecté.

**Fonctionnalités**

La fonctionnalité suivante n'est pas disponible dans la console de gestion lorsque le serveur Dell Server s'exécute en mode Déconnecté :

- Mise à niveau, mise à jour et migration du serveur Security Management Server
- Mise à jour automatique du serveur Security Management Server Virtual - La mise à jour doit être exécutée manuellement
- Mise à jour des profils Cloud
- Mise à jour automatique d'Advanced Threat Prevention
- Chargement de fichiers exécutables anormaux ou dangereux pour l'analyse Advanced Threat Prevention
- Chargement de fichier Advanced Threat Prevention et de fichier journal

La fonctionnalité suivante diffère :

- Le serveur Dell Server envoie la liste de sécurité globale, la liste de quarantaine et la liste de sécurité aux ordinateurs clients.
- La liste de sécurité globale est importée vers le serveur Dell Server au moyen de la règle Autorisation globale.
- La liste de quarantaine est importée vers le serveur Dell Server au moyen de la règle Liste de quarantaine.
- La liste de sécurité est importée vers le serveur Dell Server au moyen de la règle Liste de sécurité.

Ces règles sont uniquement disponibles en mode Déconnecté. Pour plus d'informations sur ces règles, voir la rubrique *AdminHelp*, disponible dans la console de gestion à distance.

Pour plus d'informations sur le mode Déconnecté, voir la rubrique « Mode Déconnecté » dans *AdminHelp*, disponible dans la console de gestion.

# Identification et gestion des menaces en mode Déconnecté

Pour gérer les menaces en mode Déconnecté, vous devez d'abord définir les règles Advanced Threat Prevention suivantes en fonction des besoins de votre entreprise :

- Autorisation globale
- Liste de quarantaine
- Liste de sécurité

Ces règles sont envoyées au client Advanced Threat Prevention uniquement si Dell Server détecte un jeton d'installation en mode Déconnecté, qui comporte le préfixe "DELLAG".

Reportez-vous à *AdminHelp* pour obtenir des exemples de ces règles.

Pour voir les fichiers identifiés comme menaces potentielles par Advanced Threat Prevention, accédez à l'onglet **Enterprise > Événements de menaces avancées.** Cet onglet contient une liste des informations des événements pour l'ensemble de l'entreprise et des actions effectuées, comme Bloqué ou Arrêté.

# 6

# Dépannage

## Récupération d'Advanced Threat Prevention

**Récupération du service**

Vous aurez besoin de votre certificat sauvegardé pour récupérer le service Advanced Threat Prevention.

1. Dans le volet gauche de la console de gestion, cliquez sur **Gestion > Gestion des services**.
2. Cliquez sur **Récupérer le service Advanced Threat Prevention**.
3. Suivez la procédure de récupération du service guidée et téléchargez le certificat d'Advanced Threat Prevention lorsque vous y êtes invité.

## Trouver le code de produit avec Windows PowerShell

- Vous pouvez facilement identifier le code de produit, si le code de produit change à l'avenir, à l'aide de cette méthode.

  ```
  Get-WmiObject  Win32_Product | Where-Object {$_.Name -like '*Cylance*'} | FT IdentifyingNumber, Name, LocalPackage
  ```

  La sortie produira le chemin complet et le nom du fichier .msi (le nom du fichier converti en valeur hexadécimale).

## Advanced Threat Prevention

- Pour que le plug-in Advanced Threat Prevention surveille HKLM\SOFTWARE\Dell\Dell Data Protection pour détecter les modifications de la valeur LogVerbosity et mette à jour le niveau de journalisation client en conséquence, définissez la valeur suivante.

  [HKLM\Software\Dell\Dell Data Protection]

  "LogVerbosity"=DWORD:<see below>

  Dump: 0

  Fatal: 1

  Erreur 3

  Warning 5

  Info 10

  Verbose 12

  Trace 14

  Debug 15

  La valeur de registre est vérifiée lorsque le service Advanced Threat Prevention démarre ou à chaque fois que la valeur change. Si la valeur de registre n'existe pas, il n'y a pas de modification du niveau de journalisation.

  Utilisez ce paramètre de registre uniquement pour les tests/le débogage, car ce paramètre de registre contrôle la verbosité du log pour les autres composants, y compris Encryption et Encryption Management Agent.

- Le mode de compatibilité permet aux applications de s'exécuter sur l'ordinateur client alors que les règles « Protection de la mémoire » ou « Protection de la mémoire et contrôle des scripts » sont activées. L'activation du mode de compatibilité nécessite l'ajout d'une valeur de registre sur l'ordinateur client.

  Pour activer le mode de compatibilité, procédez comme suit :

  1. Dans la console de gestion, désactivez la règle *Protection de la mémoire activée*. Si la règle *Contrôle des scripts* est activée, désactivez-la.

2. Ajoutez la valeur de registre CompatibilityMode.
   a. Dans l'Éditeur de registre de l'ordinateur client, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop`.
   b. Effectuez un clic droit sur **Desktop**, cliquez sur **Permissions**, puis désignez-vous comme propriétaire et attribuez-vous le droit Contrôle total.
   c. Cliquer avec le bouton droit sur **Bureau**, puis choisissez **NouvelleValeur binaire**.
   d. Pour le nom, saisissez `CompatibilityMode`.
   e. Ouvrez le paramètre de registre et changez la valeur en `01`.
   f. Cliquez sur **OK**, puis fermez l'Éditeur de registre.

   Pour ajouter la valeur de registre à l'aide d'une commande, vous pouvez exécuter l'une des options de ligne de commande suivantes sur l'ordinateur client :

   - (Pour un seul ordinateur) Psexec :

     ```
     psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop /v
     CompatibilityMode /t REG_BINARY /d 01
     ```

   - (Pour plusieurs ordinateurs) Commande Invoke-Command :

     ```
     $servers = "testComp1","testComp2","textComp3"

     $credential = Get-Credential -Credential {UserName}\administrator

     Invoke-Command -ComputerName $servers -Credential $credential -ScriptBlock {New-Item
     -Path HKCU:\Software\Cylance\Desktop -Name CompatibilityMode -Type REG_BINARY -Value
     01}
     ```

3. Dans la console de gestion, réactivez la règle *Protection de la mémoire activée*. Si la règle *Contrôle des scripts* était précédemment activée, réactivez-la.