OfficeScan™ *as a Service*

Manuel de l'administrateur

pour les grandes et moyennes entreprises

Document n° : OSEM07954/170822

Date de publication : Mars 2018

Protégé par le brevet américain n°: 5 951 698

Cette documentation présente les fonctionnalités principales du produit et/ou fournit les instructions d'installation pour un environnement de production. Lisez attentivement cette documentation avant d'installer ou d'utiliser le produit.

Pour plus d'informations concernant l'utilisation des fonctionnalités spécifiques de produit, consultez notre Trend Micro Centre d'aide en ligne et/ou notre Trend Micro base de connaissances.

Trend Micro cherche constamment à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez nous contacter à l'adresse docs@trendmicro.com.

Évaluez cette documentation sur le site Web suivant :

http://www.trendmicro.com/download/documentation/rating.asp

Table des matières

Chapitre 4: Paramètres du programme de l'agent OfficeScan

Partie III: Protection des Endpoints

Chapitre 5: Détection des programmes malveillants

Chapitre 6: Utilisation du pare-feu OfficeScan

Chapitre 12: Paramètres d’administration

Partie VI: Obtenir de l'aide

Chapitre 13: Assistance technique

Index

Préface

Ce document présente des informations de mise en route, les procédures d'installation des agents et la gestion des serveurs et des agents OfficeScan.

Les rubriques sont les suivantes :

Documentation OfficeScan

La documentation OfficeScan comprend les documents suivants :

TABLEAU 1. Documentation OfficeScan

DOCUMENTATION	DESCRIPTION
Manuel de l'administrateur	Document PDF contenant des informations de mise en route, les procédures d'installation de l'agent OfficeScan et des informations sur la gestion du serveur et des agents OfficeScan>
Aide	Fichiers ASPX Web ou HTML locaux qui fournissent des procédures, des conseils d'utilisation et des informations spécifiques du site. L'aide est accessible depuis le serveur OfficeScan et les consoles des agents.
Fichier Lisez-moi	contient une liste des problèmes connus et les étapes d'installation de base. Il peut aussi contenir des informations relatives au produit qui n'ont pas pu être intégrées à temps dans l'aide ou dans la documentation imprimée
Base de connaissances	Base de données en ligne contenant des informations sur la résolution des problèmes et le dépannage. Elle contient les dernières informations sur les problèmes connus identifiés pour les produits. Pour accéder à la base de connaissances, consultez le site Web suivant : http://esupport.trendmicro.com

Téléchargez les versions les plus récentes des documents PDF et du fichier Lisez-moi à l'adresse :

http://docs.trendmicro.com/fr-fr/enterprise/officescan.aspx

Public cible

La documentation OfficeScan est destinée aux catégories d'utilisateurs suivantes :

- Administrateurs OfficeScan : responsables de la gestion d'OfficeScan, y compris du serveur OfficeScan, et de l'installation et de la gestion des agents OfficeScan. Ces

utilisateurs sont supposés posséder des connaissances approfondies dans le domaine de la gestion des réseaux et des serveurs.

- Utilisateurs finaux : utilisateurs qui ont installé l'agent OfficeScan sur leurs endpoints. Leur niveau de compétence en informatique va du débutant à l'expert.

Conventions typographiques du document

La documentation utilise les conventions suivantes.

TABLEAU 2. Conventions typographiques du document

NOMENCLATURE	DESCRIPTION
MAJUSCULE	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets et options
Italique	Références à d'autres documents
`Police monospace`	Échantillons de lignes de commande, code du programme, URL Web, noms de fichiers et sortie d'un programme
Chemin > **de navigation**	Chemin de navigation permettant d'accéder à un écran particulier Par exemple, **Fichier** > **Enregistrer** signifie que vous devez cliquer sur **Fichier**, puis sur **Enregistrer** dans l'interface.
 **Remarque**	Remarques sur la configuration
 **Conseil**	Recommandations ou suggestions

NOMENCLATURE	DESCRIPTION
 **Important**	Informations sur les paramètres de configuration et les limites du produit obligatoires ou par défaut
 **AVERTISSEMENT!**	Actions critiques et options de configuration

Terminologie

Le tableau ci-dessous présente la terminologie officielle employée dans toute la documentation OfficeScan :

TABLEAU 3. Terminologie OfficeScan

TERMINOLOGIE	DESCRIPTION
agent OfficeScan	Programme de l'agent OfficeScan
OfficeScan	Solution de sécurité pour Endpoint de Trend Micro qui fournit l'architecture de base du serveur OfficeScan
Endpoint de l'agent	Endpoint sur lequel l'agent OfficeScan est installé
Utilisateur de l'agent (ou utilisateur)	Personne qui gère l'agent OfficeScan sur l'Endpoint de l'agent
Serveur	Programme serveur OfficeScan
Ordinateur serveur	Endpoint sur lequel est installé le serveur OfficeScan
Administrateur (ou administrateur OfficeScan)	Personne qui gère le serveur OfficeScan

TERMINOLOGIE	DESCRIPTION
Console	Interface utilisateur permettant de configurer et de gérer les paramètres du serveur OfficeScan La console employée pour le programme du serveur OfficeScan est appelée « console Web », et celle employée pour l'agent OfficeScan est appelée « console de l'agent ».
Risque liés à la sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Internet
Service licence	Inclut les services antivirus, Damage Cleanup Services, les services de Web Reputation et anti-spyware, qui sont tous activés lors de l'installation du serveur OfficeScan
Service OfficeScan	Services hébergés via Microsoft Management Console (MMC). Par exemple, `ofcservice.exe`, le OfficeScan Master Service.
Programme	Inclut l'agent OfficeScan
Composants	Responsables du scan, de la détection et des actions contre les risques liés à la sécurité

`Dossier d'installation de l'agent`	Dossier sur l'Endpoint qui contient les fichiers de l'agent OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	
	`C:\Program Files\Trend Micro\OfficeScan Client`
	
	`C:\Program Files (x86)\Trend Micro\OfficeScan Client`

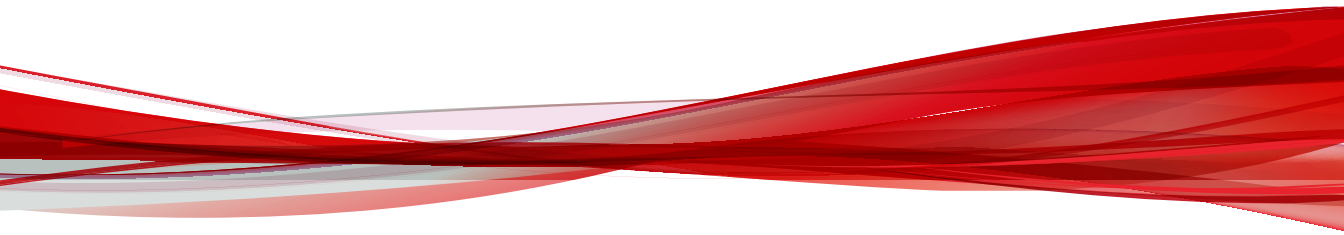
TERMINOLOGIE	DESCRIPTION

`Dossier d'installation du serveur`	Dossier sur l'Endpoint qui contient les fichiers du serveur OfficeScan. Si vous acceptez les paramètres par défaut pendant l'installation, vous trouverez le dossier d'installation à l'un des emplacements suivants :
	`C:\Program Files\Trend Micro\OfficeScan`
	`C:\Program Files (x86)\Trend Micro\OfficeScan`
	Par exemple, si un fichier particulier se trouve dans `\PCCSRV` du dossier d'installation du serveur, le chemin d'accès complet au fichier est le suivant :
	`C:\Program Files\Trend Micro\OfficeScan\PCCSRV\<nom_fichier>`.

Double pile	Entités ayant à la fois une adresse IPv4 et une adresse IPv6. Par exemple : • Endpoints utilisant des adresses IPv4 et IPv6 • agents OfficeScan installés sur des Endpoints à double pile • Agents de mise à jour chargés de distribuer les mises à jour aux agents • Serveur proxy à double pile, tel que DeleGate, pouvant effectuer la conversion entre adresses IPv4 et IPv6.
IPv4 pur	Une entité n'ayant qu'une adresse IPv4
IPv6 pur	Une entité n'ayant qu'une adresse IPv6

Partie I

Présentation d'OfficeScan Cloud Console



Chapitre 1

Présentation d'OfficeScan

Ce chapitre donne une présentation générale d'OfficeScan et présente certaines fonctions clés.

Les rubriques sont les suivantes :

Trend Micro™ OfficeScan™ Cloud Console

Trend Micro OfficeScan Cloud Console améliore la sécurité contre les menaces inconnues, jour zéro et basées sur le Web au-dessus et parallèlement à votre solution de protection d'Endpoint actuelle.

Solution intégrée, OfficeScan est composé du programme de l'agent OfficeScan qui réside sur l'Endpoint et d'un programme serveur qui gère tous les agents. L'agent OfficeScan protège l'Endpoint et communique son état de sécurité au serveur. Le serveur, via une console d'administration à interface Web, facilite l'application coordonnée de stratégies de sécurité et le déploiement de mises à jour vers chaque agent.

OfficeScan fonctionne sous Smart Protection Network™, une infrastructure de contenu client en ligne de nouvelle génération qui offre une sécurité plus intelligente que celle des méthodes classiques. Une technologie en ligne unique et l'allégement de l'agent réduisent le besoin de téléchargements conventionnels de fichiers de signatures et éliminent les retards couramment associés aux mises à jour des postes de travail. Les entreprises bénéficient d'une augmentation de la bande passante réseau, d'une réduction de la puissance de traitement et d'une diminution des coûts générés. Les utilisateurs accèdent immédiatement à la protection la plus récente où qu'ils se connectent, du réseau de l'entreprise, de leur domicile ou en déplacement.

Fonctions et avantages

Le tableau suivant décrit les fonctions et avantages clés fournis par OfficeScan.

FONCTION	AVANTAGE
Protection contre les ransomwares	Les fonctions de scan améliorées permettent d'identifier et de bloquer les programmes de Ransomware qui ciblent les documents s'exécutant sur des endpoints. Pour ce faire, elles identifient des comportements communs et bloquent des processus couramment associés à ces programmes.

Fonction	Avantage
Défense contre les menaces connectées	Configurez OfficeScan pour mettre en place un abonnement aux listes d'objets suspects du serveur Control Manager. À l'aide de la console de Control Manager, vous pouvez créer des actions personnalisées pour les objets détectés par les listes d'objets suspects afin de bénéficier d'une défense personnalisée contre les menaces identifiées par les endpoints protégés par des produits Trend Micro spécifiques à votre environnement. Vous pouvez configurer les agents OfficeScan pour envoyer des objets de fichiers susceptibles de contenir des menaces précédemment non identifiées à un analyseur Virtual Analyzer pour une analyse ultérieure. Après avoir évalué les objets, Virtual Analyzer ajoute tous les objets comportant des menaces inconnues à la liste des objets suspects de Virtual Analyzer et distribue les listes à d'autres agents OfficeScan dans tout le réseau.
Apprentissage automatique prédictif	Le moteur d'apprentissage automatique prédictif peut protéger votre réseau contre les nouvelles menaces, précédemment non identifiées ou inconnues grâce à la fonctionnalité d'analyse de fichier avancée et à la surveillance heuristique des processus. L'apprentissage automatique prédictif peut déterminer la probabilité de la présence d'une menace dans un fichier, ainsi que son type probable, vous protégeant ainsi des attaques « jour zéro ».
Protection contre les risques de sécurité	OfficeScan protège les ordinateurs contre les risques de sécurité en scannant les fichiers avant de mener une action spécifique selon chaque risque détecté. Un nombre élevé de risques de sécurité détectés en peu de temps témoigne d'une épidémie. Pour enrayer les épidémies, OfficeScan applique des stratégies de prévention des épidémies et isole les ordinateurs sur lesquels sont détectés les fichiers infectés jusqu'à ce qu'ils ne présentent plus aucun risque. OfficeScan utilise Smart Scan pour optimiser l'efficacité du processus de scan. Cette technologie consiste à transférer un grand nombre de signatures précédemment stockées sur le endpoint local vers des sources Smart Protection. Cette démarche réduit considérablement l'impact sur les systèmes et sur le réseau du volume sans cesse croissant de mises à jour de signatures vers les endpoints.

FONCTION	AVANTAGE
Damage Cleanup Services	Damage Cleanup Services™ débarrasse les ordinateurs des virus basés sur fichiers et des virus de réseau, ainsi que des résidus de virus et de vers (chevaux de Troie, entrées de Registre, fichiers viraux) et ce, à l'aide d'un processus totalement automatisé. Pour traiter les menaces et les nuisances générées par les chevaux de Troie, Damage Cleanup Services effectue les actions suivantes : • Détecte et supprime les chevaux de Troie actifs • Élimine les processus créés par les chevaux de Troie • Répare les fichiers système modifiés par les chevaux de Troie • Supprime les fichiers et les applications laissés par les chevaux de Troie Les services Damage Cleanup Services s'exécutent automatiquement en arrière-plan ; vous n'avez donc pas besoin de les configurer. Les utilisateurs ne remarquent même pas son activité. Toutefois, OfficeScan peut parfois demander à l'utilisateur de redémarrer son endpoint pour finaliser la suppression d'un cheval de Troie.
Web Reputation	La technologie de Web Reputation protège de manière proactive les Endpoints des agents au sein du réseau d'entreprise ou en-dehors de celui-ci contre les sites Web malveillants et potentiellement dangereux. Web Reputation rompt la chaîne d'infection et empêche le téléchargement de code malveillant. Vérifiez la crédibilité des sites et des pages Web en intégrant OfficeScan à Trend Micro Smart Protection Network.
Pare-feu OfficeScan	Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection » et à des scans antivirus réseau hautes performances. Créez des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquez-les à différents groupes d'utilisateurs.

FONCTION	AVANTAGE
Prévention contre la perte de données	La prévention contre la perte de données protège les actifs numériques d'une entreprise contre les fuites de données, délibérées ou accidentelles. La prévention contre la perte des données permet aux administrateurs ce qui suit : • L'identification de l'actif numérique à protéger • La création de stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes. • Le renforcement de la conformité à des normes de confidentialité établies
Contrôle des dispositifs	Le Contrôle des dispositifs régule l'accès aux périphériques de stockage externes et ressources réseau connectés aux ordinateurs. Le Contrôle des dispositifs prévient la perte et les fuites de données et, conjointement avec le scan de fichiers, contribue à la protection contre les risques de sécurité.
Surveillance des comportements	La surveillance des comportements contrôle en continu les agents, guettant des modifications inhabituelles apportées au système d'exploitation ou aux logiciels installés.
Indépendant des solutions de sécurité	Les agents s'exécutant en mode « Coexistence » sont compatibles sur n'importe quel Endpoint Windows pris en charge, exécutant n'importe quel logiciel de sécurité d'Endpoint.
Solution logiciel en tant que service	Comme le serveur OfficeScan est hébergé et géré dans le cloud, vous n'avez pas les charges de travail associées à la gestion d'un matériel local.

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Internet. Il repose sur des solutions à la fois sur site et Trend Micro hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage. Smart Protection Network utilise des agents légers pour accéder

à une combinaison unique de technologies en ligne de messagerie, de File Reputation et de sites Web, ainsi que de bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée alors qu'un nombre croissant de produits, de services et d'utilisateurs accèdent au réseau, créant un service de protection qui offre à ses utilisateurs une surveillance ciblée en temps réel.

Pour plus d'informations relatives au Smart Protection Network, veuillez vous reporter à :

http://www.trendmicro.fr/technologie-innovation/notre-technologie/smart-protection-network/

Services de Web Reputation

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de Web Reputation de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. Les services de Web Reputation continuent ensuite à scanner les sites et à empêcher les utilisateurs d'accéder à ceux qui sont infectés. Les fonctions de Web Reputation permettent de garantir que les pages consultées par les utilisateurs sont sans danger et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing, dont l'objectif est de duper les utilisateurs pour qu'ils divulguent des informations personnelles. Pour une plus grande précision et une réduction des faux positifs, la technologie de Web Reputation de Trend Micro affecte des scores de réputation à des pages et liens spécifiques de chaque site, plutôt que de classer comme suspects des sites entiers ou de les bloquer. En effet, il arrive souvent que seule une portion d'un site légitime ait été piratée et les réputations peuvent changer de manière dynamique au fil du temps

Les agents OfficeScan soumis aux stratégies de Web Reputation utilisent les services de Web Reputation. Les administrateurs OfficeScan peuvent soumettre tous les agents ou certains d'entre eux seulement à des stratégies de Web Reputation.

Liste de blocage de sites Web

Les sources Smart Protection téléchargent la liste de blocage de sites Web. Les agents OfficeScan qui sont soumis aux stratégies de Web Reputation ne téléchargent pas cette liste.

Remarque

Les administrateurs peuvent soumettre tous les agents ou seulement certains d'entre eux aux stratégies de Web Reputation.

Les agents soumis aux stratégies de Web Reputation vérifient la réputation d'un site par rapport à la liste de blocage de sites Web. Pour cela, ils envoient une requête de réputation de site Web à une source Smart Protection. L'agent compare les données de réputation qu'il reçoit de la source Smart Protection à la stratégie de Web Reputation en vigueur sur le endpoint. L'agent autorise ou bloque l'accès au site en fonction de la stratégie appliquée.

Smart Feedback

Trend Micro Smart Feedback assure la communication permanente entre les produits Trend Micro et les centres et technologies de recherche des menaces de la société, opérationnels 24h sur 24 et 7 jours sur 7. Chaque nouvelle menace identifiée par un contrôle de réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client.

Grâce à l'analyse constante des données de menaces collectées par son vaste réseau mondial de clients et de partenaires, Trend Micro assure une protection automatique et en temps réel contre les dernières menaces, offrant ainsi une sécurité « unifiée », très semblable à une surveillance de voisinage automatisée qui implique la communauté dans la protection de chacun. La confidentialité des informations personnelles ou professionnelles d'un client est toujours protégée car les données sur les menaces qui sont collectées reposent sur la réputation de la source de communication et non sur le contenu de la communication en question.

Exemples d'informations envoyées à Trend Micro :

- Sommes de contrôle de fichiers
- les sites Web visités
- Informations sur les fichiers, notamment la taille et le chemin
- Noms des fichiers exécutables

Vous pouvez interrompre à tout moment votre participation au programme depuis la console Web.

Conseil

Il n'est pas obligatoire de participer à Smart Feedback pour protéger ses endpoints. La participation de l'utilisateur est facultative et il peut y mettre fin à tout moment. Trend Micro recommande aux utilisateurs de participer à Smart Feedback afin d'assurer une meilleure protection globale à tous les clients Trend Micro.

Pour plus d'informations relatives au Smart Protection Network, veuillez vous reporter à :

http://www.trendmicro.fr/technologie-innovation/notre-technologie/smart-protection-network/

La console Web

La console Web est le point central permettant de surveiller OfficeScan sur l'ensemble du réseau de l'entreprise. La console présente des paramètres et des valeurs par défaut que vous pouvez configurer en fonction de vos spécifications et exigences de sécurité. La console Web utilise des technologies Internet standard telles que JavaScript, CGI, HTML et HTTPS.

Remarque

Configurez les paramètres de délai d'attente depuis la console Web.

Pour plus d'informations, voir *Configuration des paramètres de la console Web à la page 12-7*.

Utilisez la console Web pour effectuer les opérations suivantes :

- Gérer les agents installés sur les Endpoints en réseau
- Regrouper des agents par domaines logiques pour les configurer et les gérer tous ensemble
- Définir des configurations de scan sur un ou plusieurs Endpoints en réseau
- Configurer des notifications liées aux risques de sécurité affectant le réseau et afficher les journaux envoyés par les agents

Remarque

La console Web ne prend pas en charge Windows 8, 8.1, 10 ni Windows Server 2012 en mode Windows UI.

Bannière de la console Web

Dans la zone de la bannière de la console Web, vous disposez des options suivantes :

- **<nom du compte>** :cliquez sur le nom du compte (par exemple, racine) pour changer des informations du compte (par exemple, le mot de passe).
- **Déconnexion** :déconnecte l'utilisateur de la console Web

Obtenir de l'aide

Le menu **Aide** permet d'accéder aux informations de support suivantes :

- **Contents et index** : Ouvre l'aide en ligne
- **Assistance** : affiche la page Web d'assistance technique de Trend Micro, sur laquelle vous pouvez poser des questions et trouver des réponses aux questions les plus fréquentes concernant les produits Trend Micro.
- **Encyclopédie des menaces** : affiche le site Web de l'encyclopédie des menaces, qui renferme toutes les informations liées aux programmes malveillants dont Trend Micro dispose. Les experts en menaces de Trend Micro publient régulièrement leurs trouvailles en matière de détection de programmes malveillants, spam, URL malveillantes et vulnérabilités. L'encyclopédie des menaces explique également le

déroulement des attaques Web les plus courantes et fournit des informations connexes.

- **Contacter Trend Micro** : affiche la page **Nous contacter** du site Web de Trend Micro, qui contient les coordonnées de nos bureaux dans le monde entier.
- **À propos de** :fournit une vue d'ensemble du produit, des instructions pour vérifier les détails des versions de composants et un lien vers Assistance Intelligence System.

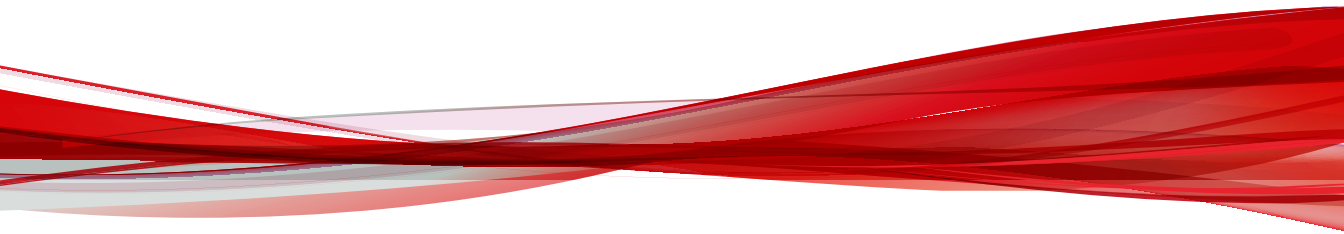
  Pour obtenir des informations détaillées, consultez la section *Assistance Intelligence System à la page 1-10*.

Assistance Intelligence System

Support Intelligence System est une page depuis laquelle vous pouvez facilement envoyer des fichiers à Trend Micro à des fins d'analyse. Ce système détecte le GUID du serveur OfficeScan et joint cette information au fichier que vous envoyez. En joignant ce GUID, vous permettez à Trend Micro de vous fournir un retour d'informations sur les fichiers envoyés pour évaluation.

Partie II

Gestion des agents OfficeScan



Chapitre 2

Installation de l'agent OfficeScan

Ce chapitre décrit la configuration système requise, les méthodes d'installation et les procédures de désinstallation du programme de l'agent OfficeScan.

Les rubriques sont les suivantes :

Configuration système requise pour l'agent OfficeScan

Nouvelles installations sur les plates-formes d'Endpoints Windows

Configuration requise pour Windows 7 (32/64 bits)

PHASE	CONFIGURATION REQUISE
Éditions (avec/sans SP1)	• Édition Familiale Basique • Édition Familiale Premium • Intégrale • Professional • Entreprise • Édition Professionnelle pour systèmes embarqués • Édition Intégrale pour systèmes embarqués • PC léger
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 1 Go (32 bits) ou 1,5 Go (64 bits) au minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Fonction Partage de fichiers simples désactivée • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

Configuration requise pour Windows 8/8.1 (32/64 bits)

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Professionnel • Entreprise
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 1 Go (32 bits) ou 1,5 Go (64 bits) au minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

Configuration requise pour Windows 10 (32/64 bits)

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Familiale • Professionnel • Éducation • Entreprise
Prise en charge des mises à jour	• Anniversary Update • Creators Update • Fall Creators Update
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64

PHASE	CONFIGURATION REQUISE
Mémoire RAM	• 1 Go (32 bits) ou 2 Go (64 bits) au minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 11.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

Nouvelles installations sur les plates-formes Windows Server

Plates-formes Windows Server 2008 (32 bits)

- *Windows Server 2008 à la page 2-6*
- *Windows Storage Server 2008 à la page 2-7*
- *Windows HPC Server 2008 à la page 2-7*
- *Clusters de basculement sous Windows Server 2008 (actif/passif) à la page 2-8*

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

TABLEAU 2-1. Windows Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 2)	• Standard • Entreprise • Datacenter • Web • Server Core
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-2. Windows Storage Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 2)	• Éléments de base
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-3. Windows HPC Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 2)	• Éléments de base
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64

PHASE	CONFIGURATION REQUISE
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-4. Clusters de basculement sous Windows Server 2008 (actif/passif)

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1 GHz (32 bits) ou 2 GHz (64 bits) au minimum ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

Plates-formes Windows Server 2008 (64 bits)

- *Windows Server 2008 à la page 2-10*
- *Windows Server 2008 R2 à la page 2-11*
- *Windows Storage Server 2008 à la page 2-12*
- *Windows Storage Server 2008 R2 à la page 2-12*
- *Windows HPC Server 2008 à la page 2-13*
- *Windows HPC Server 2008 R2 à la page 2-14*
- *Clusters de basculement sous Windows Server 2008 (actif/passif) à la page 2-15*

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

TABLEAU 2-5. Windows Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 2)	• Standard • Entreprise • Datacenter • Web • Server Core
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-6. Windows Server 2008 R2

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 1)	• Standard • Entreprise • Datacenter • Web • Server Core
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-7. Windows Storage Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 2)	• Éléments de base • Standard • Entreprise • Groupe de travail
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-8. Windows Storage Server 2008 R2

PHASE	CONFIGURATION REQUISE
Éditions (Service Pack 1)	• Éléments de base • Standard • Entreprise • Groupe de travail

PHASE	CONFIGURATION REQUISE
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-9. Windows HPC Server 2008

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan

PHASE	CONFIGURATION REQUISE
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-10. Windows HPC Server 2008 R2

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

TABLEAU 2-11. Clusters de basculement sous Windows Server 2008 (actif/passif)

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

Plate-forme Windows MultiPoint Server 2010 (64 bits)

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

Plate-forme Windows MultiPoint Server 2011 (64 bits)

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Premium
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Microsoft Internet Explorer 8.0 ou 9.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

Plates-formes Windows Server 2012 (64 bits)

- *Windows Server 2012 à la page 2-19*
- *Windows Server 2012 R2 à la page 2-19*
- *Windows Storage Server 2012 à la page 2-20*
- *Windows Storage Server 2012 R2 à la page 2-21*
- *Windows MultiPoint Server 2012 à la page 2-22*
- *Clusters de basculement sous Windows Server 2012 à la page 2-23*
- *Clusters de basculement sous Windows Server 2012 R2 à la page 2-24*

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

TABLEAU 2-12. Windows Server 2012

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Datacenter • Server Core
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-13. Windows Server 2012 R2

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Datacenter

PHASE	CONFIGURATION REQUISE
	• Server Core
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-14. Windows Storage Server 2012

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Groupe de travail
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64

PHASE	CONFIGURATION REQUISE
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-15. Windows Storage Server 2012 R2

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Groupe de travail
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-16. Windows MultiPoint Server 2012

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Premium
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre

PHASE	CONFIGURATION REQUISE
	• Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-17. Clusters de basculement sous Windows Server 2012

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut

PHASE	CONFIGURATION REQUISE
	Remarque Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-18. Clusters de basculement sous Windows Server 2012 R2

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 10.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

Plates-formes Windows Server 2016 (64 bits)

Remarque

Pour connaître les exigences relatives au processeur et à la mémoire vive pour une plate-forme spécifique, reportez-vous à la configuration système de Microsoft pour cette plate-forme.

TABLEAU 2-19. Windows Server 2016

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Datacenter • Server Core
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 11.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-20. Clusters de basculement sous Windows Server 2016

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• N/A
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 11.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

TABLEAU 2-21. Windows Storage Server 2016

PHASE	CONFIGURATION REQUISE
Éditions (aucun Service Pack requis)	• Standard • Groupe de travail
Processeur	• Processeur Intel Pentium 1,4GHz ou équivalent (2 GHz recommandé) • Processeur AMD™ 64 • Processeur Intel 64
Mémoire RAM	• 512 Mo minimum, avec au moins 100 Mo réservés exclusivement à OfficeScan • 2 Go recommandé
Espace disque disponible	• 800 Mo minimum • 1 Go recommandé

PHASE	CONFIGURATION REQUISE
Autres	• Écran avec résolution 1024 x 768 pixels, 256 couleurs minimum • Windows Internet Explorer 11.0 pour une installation Web • Activation de l'accès à distance au Registre • Autorisation du partage d'imprimantes/de fichiers au sein du pare-feu Windows (s'il est activé) • Activation de l'administrateur local par défaut **Remarque** Le mode Windows UI n'est pas pris en charge.

Outils de mise en package de l'agent

Utilisez l'**Outil de mise en package de l'agent** pour mettre à jour le package d'installation de l'agent OfficeScan que le serveur OfficeScan envoie aux Endpoints. Lorsque le serveur crée un nouveau package pour le programme d'installation de l'agent OfficeScan, OfficeScan applique tous les paramètres de domaine racine au nouveau package pour s'assurer que les nouvelles installations disposent des paramètres les plus actualisés.

Conseil

Trend Micro recommande de configurer les paramètres généraux de l'agent sur le domaine racine et de créer un nouveau package pour le programme de l'agent OfficeScan avant de commencer à installer des agents sur votre réseau.

Remarque

OfficeScan crée automatiquement un nouveau package pour le programme de l'agent OfficeScan quotidiennement. Vérifiez l'heure de la **Dernière génération de package** pour déterminer s'il convient de recréer un package pour l'agent OfficeScan.

Le serveur OfficeScan enregistre toutes les données dans le fuseau horaire UTC-06:00 (Amérique centrale), quel que soit l'emplacement de l'Endpoint. Pour déterminer l'heure à laquelle un événement s'est produit dans votre fuseau horaire, vous devez manuellement convertir la date/heure enregistrée.

Procédure

1. Accédez à **Agents** > **Outil de mise en package de l'agent**.
2. Cliquez sur **Génération immédiate d'un nouveau package**.
3. Après la génération du nouveau package, envoyez le programme d'installation de l'agent OfficeScan aux utilisateurs utilisant la console Control Manager.

Désinstallation de plugiciels

Les méthodes suivantes vous permettent de désinstaller l'agent OfficeScan des Endpoints.

Remarque

Trend Micro ne recommande pas d'effectuer une désinstallation manuelle, sauf si les processus de désinstallation automatisée ne fonctionnent pas.

- *Désinstallation de l'agent OfficeScan depuis la console Web à la page 2-30*
- *Exécution du programme de désinstallation de l'agent OfficeScan à la page 2-31*
- *Désinstallation manuelle de l'agent OfficeScan à la page 2-31*

Désinstallation de l'agent OfficeScan depuis la console Web

Désinstallez le programme de l'agent OfficeScan à partir de la console Web. N'effectuez la désinstallation que si vous rencontrez des problèmes avec le programme. Procédez immédiatement à la réinstallation afin d'assurer la continuité de la protection de l'Endpoint contre les risques pour la sécurité.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Tâches** > **Désinstallation de l'agent**.
4. Sur l'écran **Désinstallation de l'agent**, cliquez sur **Lancer la désinstallation**.

   Les agents OfficeScan reçoivent la commande après interrogation du serveur ou pendant la prochaine mise à jour programmée ou manuelle.

Programme de désinstallation de l'agent OfficeScan

Accordez aux utilisateurs le droit de désinstaller le programme de l'agent OfficeScan, puis demandez-leur d'exécuter le programme de désinstallation de l'agent depuis leur ordinateur.

Selon votre configuration, la désinstallation peut nécessiter un mot de passe. Si c'est le cas, veillez à partager le mot de passe uniquement avec les utilisateurs qui exécuteront le programme de désinstallation et à le modifier immédiatement s'il a été divulgué à d'autres utilisateurs.

Exécution du programme de désinstallation de l'agent OfficeScan

Procédure

1. Dans le menu **Démarrer** de Windows, cliquez sur **Programmes** > **Trend Micro OfficeScan Agent** > **Désinstaller l'agent OfficeScan**.

   Vous pouvez également effectuer cette procédure :

   a. Cliquez **Panneau de configuration** > **Ajout/Suppression de programmes**.

   b. Sélectionnez **Trend Micro OfficeScan Agent** et cliquez sur **Modifier**.

   c. Suivez les instructions à l'écran.

2. Si vous y êtes invité, entrez le mot de passe de désinstallation. OfficeScan informe l'utilisateur sur la progression de la désinstallation et l'avertit lorsque celle-ci est terminée. L'utilisateur n'a pas besoin de redémarrer le endpoint de l'agent pour terminer la désinstallation.

Désinstallation manuelle de l'agent OfficeScan

Procédez à la désinstallation manuelle uniquement si vous rencontrez des problèmes pour désinstaller l'agent OfficeScan à partir de la console Web ou après avoir exécuté le programme de désinstallation.

Procédure

1. Connectez-vous au endpoint de l'agent à l'aide d'un compte disposant de privilèges d'administrateur.

2. Cliquez avec le bouton droit de la souris sur l'icône de l'agent OfficeScan dans la barre d'état système et sélectionnez **Décharger OfficeScan**. Si vous êtes invité à saisir un mot de passe, indiquez le mot de passe de déchargement, puis cliquez sur **OK**.

Remarque

- Pour Windows 8, 8.1, 10, Windows Server 2012, et Windows Server 2016, passez en mode Poste de travail pour décharger l'agent OfficeScan.
- Désactivez le mot de passe sur les ordinateurs sur lesquels l'agent OfficeScan sera déchargé.

3. Si vous n'avez pas spécifié le mot de passe de déchargement, arrêtez les services suivants depuis Microsoft Management Console :
   - Service d'écoute d'OfficeScan NT
   - Service proxy d'OfficeScan NT (pour Windows Server 2008)
   - Service de scan en temps réel d'OfficeScanNT
   - Structure de la solution client commune Trend Micro
4. Supprimez le raccourci de l'agent OfficeScan dans le menu Démarrer.
   - Sous Windows 8, 8.1, 10, Windows Server 2012 et Windows Server 2016 :
     a. Passez en mode Bureau.
     b. Déplacez le curseur de la souris dans le coin inférieur droit de l'écran et cliquez sur **Démarrer** dans le menu qui s'affiche.

        L'écran **Page d'accueil** apparaît.
     c. Cliquez avec le bouton droit de la souris sur **Trend Micro OfficeScan**.
     d. Cliquez sur **Détacher de l'écran d'accueil**.
   - Sur toutes les autres plates-formes Windows :

     Cliquez sur **Démarrer** > **Programmes**, cliquez avec le bouton droit de la souris sur **Trend Micro OfficeScan Agent**, puis cliquez sur **Supprimer**.
5. Ouvrez l'éditeur de la base de registre (`regedit.exe`).

AVERTISSEMENT!

Cette procédure implique que vous supprimiez les clés de registre. Le fait d'apporter des modifications erronées à votre base de registre peut gravement affecter votre système. Effectuez toujours une copie sauvegarde avant de procéder à toute modification de la base de registre. Consultez l'aide de l'Éditeur du Registre pour obtenir des informations complémentaires.

6. Supprimez les clés de registre suivantes d'OfficeScan :

   - Si aucun autre produit Trend Micro n'est installé sur l'endpoint :
     - Pour les systèmes 32 bits :

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

     - Pour les systèmes 64 bits :

       `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`

   - Si d'autres produits Trend Micro sont installés sur l'endpoint, supprimez uniquement les clés suivantes :
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog`

       Pour les systèmes 64 bits :

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro \OfcWatchDog`

     - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

       Pour les systèmes 64 bits :

       `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro \PC-cillinNTCorp`

7. Supprimez les clés/valeurs de registre suivantes :

- Pour les systèmes 32 bits :
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\OfficeScanNT`
  - Moniteur OfficeScanNT (`REG_SZ`) sous `HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Run`
- Pour les systèmes 64 bits :
  - `HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft \Windows\CurrentVersion\Uninstall\OfficeScanNT`
  - Moniteur OfficeScanNT (`REG_SZ`) sous `HKEY_LOCAL_MACHINE \SOFTWARE\ Wow6432Node\Microsoft\Windows \CurrentVersion\Run`

8. Supprimez toutes les instances des clés de registre suivantes aux emplacements ci-après :

- Emplacements :
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services`
  - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services`
- Clés :
  - NTRtScan
  - tmccsf
  - TmFilter
  - TmListen
  - TmPreFilter
  - TmProxy

Remarque

TmProxy n'existe pas sur les plates-formes Windows 7/8/8.1/10 et Windows Server 2008 R2/2012/2012 R2/2016.

- tmtdi

Remarque

tmtdi n'existe pas sur les plates-formes Windows 7/8/8.1/10 et Windows Server 2008 R2/2012/2012 R2/2016.

- VSApiNt
- tmlwf (pour les ordinateurs fonctionnant sous Windows Server 2008/7/8/8.1/10/Server 2012/2016)
- tmwfp (pour les ordinateurs fonctionnant sous Windows Server 2008/7/8/8.1/10/Server 2012/2016)
- tmevtmgr
- tmeevw (pour les ordinateurs fonctionnant sous Windows 7/8/8.1/10/Server 2008 R2/Server 2012/2012 R2/2016)
- tmusa (pour les ordinateurs fonctionnant sous Windows 7/8/8.1/10/Server 2008 R2/Server 2012/2012 R2/2016)

9. Fermez l'Éditeur du Registre.

10. Supprimez manuellement les pilotes et les services Trend Micro à l'aide d'un éditeur de ligne de commande (Windows 8/8.1/10/Server 2012 uniquement) et des commandes suivantes :

    - `sc delete tmeevw`

      Pour Windows 7/8/8.1/10 et Windows Server 2008 R2/2012/2012 R2/2016

    - `sc delete tmusa`

      Pour Windows 7/8/8.1/10 et Windows Server 2008 R2/2012/2012 R2/2016

    - `sc delete tmccsf`

- `sc delete tmproxy`

  Pour Windows Server 2008

- `sc delete tmtdi`

  Pour Windows Server 2008

Remarque

Exécutez l'éditeur de ligne de commande avec les privilèges d'administrateur (par exemple, effectuez un clic droit sur `cmd.exe` et cliquez sur **Exécuter en tant qu'administrateur**) afin de vous assurer que la commande est exécutée correctement.

11. Redémarrez l'Endpoint de l'agent.

12. Si aucun autre produit Trend Micro n'est installé sur l'endpoint, supprimez le dossier d'installation `Trend Micro` (généralement, `C:\Program Files\Trend Micro`). Pour les ordinateurs 64 bits, le dossier d'installation figure sous `C:\Program Files (x86)\Trend Micro`.

13. Si d'autres produits Trend Micro sont installés, supprimez les dossiers suivants :

    - <dossier d'installation de l'agent>
    - Le dossier `BM` dans le dossier d'installation `Trend Micro` (généralement aux emplacements `C:\Program Files\Trend Micro\BM` pour les systèmes à 32 bits et `C:\Program Files (x86)\Trend Micro\BM` pour les systèmes à 64 bits)

Chapitre 3

Gestion de l'arborescence des agents

Ce chapitre décrit l'arborescence des agents, l'écran Gestion des agents et les options de domaine et de regroupement des agents OfficeScan.

Les rubriques sont les suivantes :

L'arborescence des agents OfficeScan

L'arborescence des agents OfficeScan affiche tous les agents actuellement géré par le serveur, groupés par domaine. Ce groupement permet de configurer et de gérer simultanément tous les membres du domaine et de leur appliquer la même configuration.

Écran Gestion des agents

Pour afficher cet écran, accédez à **Agents** > **Gestion des agents**.

Vous pouvez gérer les paramètres généraux des agents et afficher des informations relatives à l'état d'agents spécifiques (par exemple **Utilisateur de connexion**, **Adresse IP** et **État de la connexion**) dans l'écran **Gestion des agents**.

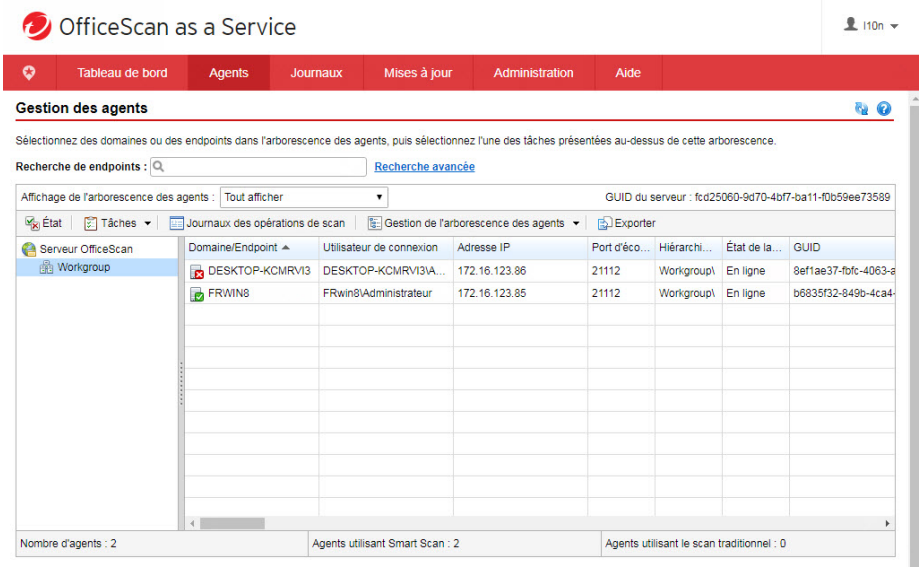


FIGURE 3-1. Écran Gestion des agents

Le tableau suivant répertorie les tâches que vous pouvez effectuer.

TABLEAU 3-1. Tâches de l'écran Gestion des agents

BOUTON DE MENU	TÂCHE
État	Afficher des informations détaillées sur les agents. Pour plus d'informations, voir *Affichage des informations sur les agents OfficeScan à la page 3-5*.
Tâches	Effectuez les opérations suivantes : • **Scan immédiat** Pour plus d'informations, voir *Configuration des paramètres de scan immédiat à la page 5-2*. • **Désinstallation de l'agent** Pour plus d'informations, voir *Désinstallation de l'agent OfficeScan depuis la console Web à la page 2-30*. • **Restauration depuis la mise en quarantaine centrale** Pour plus d'informations, voir *Restauration de fichiers mis en quarantaine à la page 5-22*.
Journaux des opérations de scan	Afficher les journaux des opérations de scan. Pour plus d'informations, voir *Affichage des journaux des opérations de scan à la page 9-2*.
Gestion de l'arborescence des agents	Gérer l'arborescence des agents. Pour plus d'informations, voir *Domaines OfficeScan à la page 3-6*.
Exporter	Exporter une liste des agents dans un fichier au format `.csv` (valeurs séparées par des virgules).

Recherche de l'arborescence des agents

Utilisez les fonctions de recherche et d'affichage au-dessus de l'arborescence de l'agent (**Agents** > **Gestion des agents**) pour localiser des Endpoints spécifiques gérés par OfficeScan.

Procédure

- Recherchez un agent à gérer en spécifiant son nom dans le champ **Recherche de endpoints**.

  Une liste de résultats s'affiche dans l'arborescence des agents. Pour disposer de plus d'options de recherche, cliquez sur **Recherche avancée**.

  Remarque

  Vous devez utiliser la fonction de recherche avancée pour rechercher des Endpoints en utilisant des adresses IPv4.

- Effectuez une recherche avancée en fonction des critères suivants :

SECTION	DESCRIPTION
Critères de base	Inclut des informations de base sur des Endpoints, telles que l'adresse IP, le système d'exploitation, le domaine, l'adresse MAC, la méthode de scan et l'état du service de Web Reputation • La recherche par segment IPv4 requiert une partie d'une adresse IP, commençant par le premier octet. La recherche renvoie tous les Endpoints dont l'adresse IP contient l'élément saisi. Par exemple, si vous tapez 10.5, vous trouverez tous les ordinateurs dont l'adresse IP est incluse dans une plage allant de 10.5.0.0 à 10.5.255.255. • La recherche par adresse MAC requiert une plage d'adresses MAC en notation hexadécimale, par exemple 000A1B123C12.
Version du composant	Cochez la case en regard du nom de composant, affinez le critère en sélectionnant **Antérieur à** ou **Antérieur ou égal à**, et saisissez un numéro de version. Le numéro de version actuel s'affiche par défaut.
État	Inclut des paramètres de l'agent

Cliquez sur **Rechercher** après avoir spécifié les critères de recherche. Une liste de noms d'Endpoints répondant aux critères s'affiche dans l'arborescence des agents.

Icônes de l'arborescence des agents

Les icônes de l'arborescence des agents OfficeScan fournissent des indications visuelles sur le type d'endpoint et l'état des agents OfficeScan gérés par OfficeScan.

TABLEAU 3-2. Icônes de l'arborescence des agents OfficeScan

ICÔNE	DESCRIPTION
	Domaine
	Racine
	Agent de mise à jour
	Agent de scan traditionnel
	Smart Scan est disponible pour l'agent OfficeScan
	Smart Scan n'est pas disponible pour l'agent OfficeScan
	Smart Scan est disponible pour l'agent de mise à jour
	Smart Scan n'est pas disponible pour l'agent de mise à jour

Affichage des informations sur les agents OfficeScan

L'écran Afficher l'état affiche des informations importantes sur les agents OfficeScan, notamment les privilèges, les informations détaillées sur le logiciel de l'agent et les événements système.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **État**.
4. Affichez les informations relatives à l'état en développant le nom du endpoint de l'agent. Si vous avez sélectionné plusieurs agents, cliquez sur **Développer tout** pour afficher les informations relatives à l'état de tous les agents sélectionnés.
5. (Facultatif) Utilisez le bouton **Réinitialiser** pour remettre à zéro le décompte de risques de sécurité.

Domaines OfficeScan

Un domaine dans OfficeScan est un groupe d'agents qui partagent la même configuration et exécutent les mêmes tâches. En regroupant les agents en domaines, vous pouvez configurer, gérer et appliquer la même configuration à tous les membres du domaine.

Vous pouvez effectuer les tâches suivantes lors du regroupement des agents dans des domaines :

- *Ajout d'un domaine à la page 3-7*
- *Suppression d'un domaine ou d'un agent à la page 3-7*
- *Attribution d'un nouveau nom à un domaine à la page 3-8*
- *Déplacement d'Agents OfficeScan vers un autre domaine ou vers un autre serveur OfficeScan à la page 3-9*

Ajout d'un domaine

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Cliquez sur **Gestion de l'arborescence des agents** > **Ajouter un domaine**.
3. Saisissez un nom pour le domaine que vous souhaitez ajouter.
4. Cliquez sur **Ajouter**.

   Le nouveau domaine apparaît dans l'arborescence des agents.
5. (Facultatif) Créez des sous-domaines.
   a. Sélectionnez le domaine parent.
   b. Cliquez sur **Gestion de l'arborescence des agents** > **Ajouter un domaine**.
   c. Saisissez le nom de sous-domaine.

Suppression d'un domaine ou d'un agent

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez :
   - Un ou plusieurs domaines
   - Un, plusieurs ou tous les agents appartenant à un domaine
3. Cliquez sur **Gestion de l'arborescence des agents** > **Supprimer un domaine/agent**.
4. Pour supprimer un domaine vide, cliquez sur **Supprimer un domaine/agent**. Si le domaine contient des agents et que vous cliquez sur **Supprimer un domaine/agent**, le serveur OfficeScan crée de nouveau le domaine et y regroupe tous les

agents lors de la connexion suivante de ces agents au serveur OfficeScan. Avant de supprimer le domaine, procédez comme suit :

a. Déplacez les agents vers d'autres domaines. Pour déplacer des agents vers d'autres domaines, faites-les glisser vers les domaines souhaités.

b. Supprimez tous les agents.

5. Pour supprimer un seul agent, cliquez sur **Supprimer un domaine/agent**.

Remarque

La suppression de l'agent de l'arborescence des agents ne le supprime pas du endpoint. L'agent OfficeScan peut toujours effectuer des tâches indépendantes du serveur, telles que la mise à jour des composants. Le serveur n'est cependant pas informé de l'existence de l'agent et ne peut donc pas lui envoyer de notifications, ni y déployer de configurations.

Attribution d'un nouveau nom à un domaine

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Sélectionnez un domaine dans l'arborescence des agents.
3. Cliquez sur **Gestion de l'arborescence des agents** > **Renommer un domaine**.
4. Entrez un nouveau nom pour le domaine.
5. Cliquez sur **Renommer**.

   Le nouveau nom du domaine apparaît dans l'arborescence des agents.

Déplacement d'Agents OfficeScan vers un autre domaine ou vers un autre serveur OfficeScan

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez un, plusieurs ou tous les agents.
3. Cliquez sur **Gestion de l'arborescence des agents** > **Déplacer un agent**.
4. Pour déplacer des agents vers un autre domaine :
   - Sélectionnez **Déplacer le ou les agents sélectionnés vers un autre domaine**.
   - Sélectionnez le domaine.
   - (Facultatif) Appliquez les paramètres du nouveau domaine aux agents.

   Conseil

   Vous pouvez également faire glisser les agents vers un autre domaine dans l'arborescence des agents.
5. Pour déplacer des agents vers un autre serveur OfficeScan :
   - Sélectionnez **Déplacer le ou les agents sélectionnés vers un autre serveur OfficeScan**.
   - Saisissez le nom ou l'adresse IPv4/IPv6 et le numéro de port HTTP ou SSL (443) du serveur.

   Remarque

   Si vous déplacez les agents OfficeScan vers une instance d'OfficeScan Cloud Console, vous pouvez obtenir des informations sur le serveur OfficeScan Cloud Console en accédant à la console Control Manager. Accédez à **Administration** > **Serveurs gérés** et, dans la liste déroulante **Type de serveur**, sélectionnez **OfficeScan**.

6. Cliquez sur **Déplacer**.

Chapitre 4

Paramètres du programme de l'agent OfficeScan

Ce chapitre décrit comment l'agent OfficeScan communique avec le serveur OfficeScan, comment démarrer et arrêter les services de l'agent OfficeScan et comment configurer les paramètres généraux de l'agent OfficeScan.

Les rubriques sont les suivantes :

Icônes de l'Agent OfficeScan

L'icône de l'agent OfficeScan dans la barre d'état système fournit des conseils visuels qui indiquent l'état actuel de l'agent OfficeScan et invitent les utilisateurs à effectuer certaines actions. À un moment donné, l'icône présentera une combinaison des conseils visuels suivants.

TABLEAU 4-1. État de l'agent OfficeScan indiqué par l'icône

ÉTAT DE L'AGENT	DESCRIPTION	CONSEIL VISUEL
Connexion de l'agent au serveur OfficeScan	Les agents en ligne sont connectés au serveur OfficeScan. Le serveur peut initier des tâches et déployer des paramètres vers ces agents.	L'icône contient un symbole représentant un battement de cœur.  La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel.
	Les agents hors ligne sont déconnectés du serveur OfficeScan. Le serveur ne peut pas gérer ces agents.	L'icône contient un symbole représentant l'arrêt d'un battement de cœur.  La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel.
	Les agents indépendants ne peuvent pas toujours communiquer avec le serveur OfficeScan.	L'icône contient les symboles de bureau et de signal.  La couleur de fond est une ombre de couleur bleue ou rouge, selon l'état du service de scan en temps réel.

ÉTAT DE L'AGENT	DESCRIPTION	CONSEIL VISUEL
Disponibilité des sources Smart Protection	Les sources Smart Protection incluent les serveurs Smart Protection Server et Trend Micro Smart Protection Network. Les agents de scan traditionnel se connectent aux sources Smart Protection pour les requêtes de Web Reputation. Les agents Smart Scan se connectent aux sources Smart Protection pour les requêtes de scan et de Web Reputation.	L'icône contient une coche si une source Smart Protection est disponible. 
		L'icône contient une barre de progression si aucune source Smart Protection n'est disponible et que l'agent tente d'établir la connexion avec les sources. 
		Pour les agents de scan traditionnel, aucune coche ni barre de progression ne s'affiche si Web Reputation a été désactivée.

ÉTAT DE L'AGENT	DESCRIPTION	CONSEIL VISUEL
État du service de scan en temps réel	OfficeScan utilise le service de scan en temps réel non seulement pour le scan en temps réel mais également pour les scans manuel et programmé. Le service doit être opérationnel, sinon l'agent devient vulnérable aux risques de sécurité.	Toute l'icône est ombrée en bleu si le service de scan en temps réel fonctionne. Deux nuances de bleu sont utilisés pour indiquer les de l'agent. • Pour le scan traditionnel :  • Pour Smart Scan : 
		Un ombrage rouge est appliqué à l'intégralité de l'icône si le service de scan en temps réel a été désactivé ou ne fonctionne pas. Deux nuances de rouge sont utilisées pour indiquer la méthode de scan de l'agent. • Pour le scan traditionnel :  • Pour Smart Scan : 
État du scan en temps réel	Le scan en temps réel fournit une protection proactive en scannant les fichiers au moment où ils sont créés, modifiés ou récupérés, afin de détecter tout risque de sécurité.	Il n'y a pas de conseils visuels si le scan en temps réel est activé.
		Toute l'icône est entourée d'un cercle rouge et contient une ligne diagonale rouge si le scan en temps réel est désactivé. 

État de l'agent	Description	Conseil visuel
État de mise à jour du fichier de signatures	Les agents doivent mettre à jour régulièrement le fichier de signatures pour protéger l'agent contre les nouvelles menaces.	Il n'y a aucun conseil visuel si le fichier de signatures est à jour ou légèrement obsolète.
		L'icône contient un point d'exclamation si le fichier de signatures est largement obsolète. Cela signifie que le fichier de signatures n'a pas été mis à jour depuis longtemps. 
État de la licence d'évaluation du serveur OfficeScan	Les agents en ligne sont connectés à un serveur OfficeScan qui utilise une licence d'évaluation qui a expiré.	Cette icône indique que la licence d'évaluation du serveur OfficeScan a expiré. 

Icônes Smart Scan

Les icônes suivantes peuvent s'afficher lorsque les agents OfficeScan utilisent Smart Scan.

Tableau 4-2. Icônes Smart Scan

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	En ligne	Disponible	Opérationnel	Activé
	En ligne	Disponible	Opérationnel	Désactivé

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Disponible	Opérationnel	Activé
	Hors ligne	Disponible	Opérationnel	Désactivé
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Indépendant	Disponible	Opérationnel	Activé

Icône	Connexion avec le serveur OfficeScan	Disponibilité des sources Smart Protection	Service de scan en temps réel	Scan en temps réel
	Indépendant	Disponible	Opérationnel	Désactivé
	Indépendant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Activé
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé
	Indépendant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel

Icônes de scan traditionnel

Les icônes suivantes peuvent s'afficher lorsque les agents OfficeScan utilisent le scan traditionnel.

Tableau 4-3. Icônes de scan traditionnel

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Activé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Disponible	Opérationnel	Désactivé	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Activé	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Disponible	Opérationnel	Désactivé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Indépendant	Disponible	Opérationnel	Activé	À jour ou légèrement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Activé	À jour ou légèrement obsolète
	Indépendant	Disponible	Opérationnel	Activé	Largement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Activé	Largement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Indépendant	Disponible	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Indépendant	Disponible	Opérationnel	Désactivé	Largement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Opérationnel	Désactivé	Largement obsolète
	Indépendant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Indépendant	Disponible	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Indépendant	Indisponible, reconnexion aux sources	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	En ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Hors ligne	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	À jour ou légèrement obsolète

Icône	Connexion avec le serveur OfficeScan	Services de Web Reputation fournis par les sources Smart Protection	Service de scan en temps réel	Scan en temps réel	Fichier de signatures de virus
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Activé	Largement obsolète
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	À jour ou légèrement obsolète
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Opérationnel	Désactivé	Largement obsolète
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	À jour ou légèrement obsolète
	Indépendant	Sans objet (fonctionnalité de Web Reputation désactivée sur l'agent)	Désactivé ou non opérationnel	Désactivé ou non opérationnel	Largement obsolète

Icônes de l’agent en mode Coexistence

L'icône de l'agent OfficeScan dans la barre d'état système fournit des indications visuelles qui montrent l'état actuel de l'agent OfficeScan et invitent les utilisateurs à effectuer certaines actions.

TABLEAU 4-4. Icônes de l’agent en mode Coexistence

ICÔNE	DESCRIPTION
	• L’agent OfficeScan est en ligne. • L’apprentissage automatique prédictif est activé et fonctionne correctement. • L'agent OfficeScan est connecté à Trend Micro Smart Protection Network.
	• L'agent OfficeScan tente de se reconnecter à Trend Micro Smart Protection Network. • L'agent OfficeScan est hors ligne. • L’apprentissage automatique prédictif est activé.
	• L’agent OfficeScan est en ligne. • L’apprentissage automatique prédictif est désactivé.
	• L'agent OfficeScan est hors ligne. • L’apprentissage automatique prédictif est désactivé. • L'agent OfficeScan ne peut pas se connecter à Trend Micro Smart Protection Network.
	• L’agent OfficeScan est en ligne. • L’apprentissage automatique prédictif n’est pas opérationnel ou un processus n’est pas disponible.
	• L'agent OfficeScan est hors ligne. • L’apprentissage automatique prédictif n’est pas opérationnel ou un processus n’est pas disponible. • L'agent OfficeScan ne peut pas se connecter à Trend Micro Smart Protection Network.

Paramètres généraux de l'agent

Les paramètres généraux de l'agent s'appliquent à tous les agents dépendant du serveur OfficeScan Cloud Console. OfficeScan Cloud Console classe par catégories les paramètres généraux de la manière suivante :

- *Paramètres de sécurité à la page 4-16*
- *Paramètres du réseau à la page 4-24*
- *Paramètres système à la page 4-22*
- *Paramètres de contrôle des agents à la page 4-25*

Paramètres de sécurité

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Paramètres de sécurité**.
3. Configurez les paramètres selon les besoins.

SECTION	SETTINGS

Paramètres de scan (général)	• **Exclure du scan en temps réel le dossier de la base de données du serveur OfficeScan** : empêche l'agent OfficeScan installé sur le serveur OfficeScan de scanner la base de données du serveur OfficeScan
	• **Exclure des dossiers et des fichiers Microsoft Exchange Server des scans** : empêche l'agent OfficeScan installé sur le serveur Microsoft Exchange de scanner les dossiers suivants du serveur Exchange :
	  • Les dossiers suivants de `\Exchsrvr\Mailroot\vsi 1` : `Queue`, `PickUp` et `BadMail`
	  • `.\Exchsrvr\mdbdata`, y compris ces fichiers : `priv1.stm`, `priv1.edb`, `pub1.stm` et `pub1.edb`

SECTION	SETTINGS
	• `.\Exchsrvr\Storage Group` Pour les dossiers de Microsoft Exchange 2007 ou version supérieure, vous devez ajouter manuellement les dossiers à la liste d'exclusion de scan. Pour plus d'informations sur les exclusions de scan, consultez le site Web suivant : http://technet.microsoft.com/en-us/library/bb332342.aspx • **Activer le scan différé pour les opérations de fichier** : permet aux utilisateurs de copier des fichiers, puis de les scanner une fois le processus de copie terminé, pour améliorer les performances des processus de copie et de scan **Important** Le scan différé nécessite la version 9.713 (ou une version ultérieure) du moteur de scan antivirus (VSAPI). • **Activer le démarrage anticipé de protection contre les programmes malveillants sur les Endpoints** : autorise l'agent OfficeScan de charger et de démarrer le scan avant d'autres pilotes logiciels tiers pendant le démarrage (uniquement pris en charge sous Windows 8, Windows Server 2012 ou versions ultérieures) **Remarque** Après avoir scanné tous les pilotes logiciels tiers, l'agent OfficeScan fournit des informations de classification de pilote au noyau du système. Les administrateurs peuvent définir des actions basées sur les classifications des pilotes dans la stratégie de groupe sous Windows et afficher les résultats des scans en utilisant l'Observateur d'événements sur des endpoints.
Paramètres de scan pour les fichiers	Dans les sections **Scan en temps réel** et **Scan manuel/Scan programmé/Scan immédiat**, configurez les paramètres suivants :

SECTION	SETTINGS
compressés volumineux	• **Ne pas scanner les fichiers si la taille du fichier compressé dépasse XX Mo** : permet à l'agent OfficeScan de vérifier la taille des fichiers individuels d'une archive compressée et ignore le scan des fichiers si la taille d'un fichier individuel dépasse le seuil configuré • **Dans un fichier compressé, scanner uniquement les XX premiers fichiers** : empêche l'agent OfficeScan de scanner tous les fichiers dans des archives qui contiennent un nombre de fichiers supérieur au seuil configuré
Paramètres de scan antivirus/ programme malveillant uniquement	**Nettoyer/supprimer les fichiers infectés dans les fichiers compressés** : l'agent OfficeScan tente d'effectuer l'action « Nettoyer » ou « Supprimer » sur des fichiers compressés de certains types d'archives contenant des programmes malveillants **Remarque** L'agent OfficeScan tente uniquement de « nettoyer » ou de « supprimer » les programmes malveillants dans des archives compressées si vous avez configuré l'action « Nettoyer » ou « Supprimer » pour le type de programme malveillant détecté.

Paramètres de scan anti-spyware/ grayware uniquement	• **Activer le mode d'évaluation** : l'agent OfficeScan consigne toutes les détections de spywares/graywares jusqu'à la date configurée et entreprend l'action suivante selon le type de scan :
	  • **Ignorer** : pendant un scan manuel, un scan immédiat et un scan programmé, l'agent OfficeScan consigne uniquement la détection
	  • **Refuser l'accès** : pendant un scan en temps réel, l'agent OfficeScan empêche l'exécution du spyware/grayware et consigne la détection

SECTION	SETTINGS
	Remarque Le mode d'évaluation a la priorité sur toute action de scan configurée par l'utilisateur. Par exemple, même si vous choisissez l'action « Nettoyer » lors du scan manuel, « Ignorer » reste l'action de scan lorsque l'agent OfficeScan est en mode d'évaluation. • **Recherche de cookies** : l'agent OfficeScan scanne tous les cookies pour détecter d'éventuels spywares/graywares • **Comptabiliser les cookies dans le journal de spywares** : l'agent OfficeScan crée des journaux pour les cookies détectés comme spywares/graywares
Paramètres de scan programmé	• **Rappeler le scan programmé aux utilisateurs XX minutes avant qu'il ne débute** : affiche un message de notification sur l'Endpoint avant le début du scan programmé **Remarque** Vous pouvez désactiver le message de notification dans l'onglet **Autres paramètres** de l'écran **Privilèges et autres paramètres**. • **Différer le scan programmé de XX heure(s) et XX minute(s) maximum** : définit la période maximale pendant laquelle les utilisateurs dotés du privilège **Différer le scan programmé** peuvent retarder ou suspendre un scan programmé **Remarque** Vous pouvez octroyer le privilège **Différer le scan programmé** dans l'onglet **Privilèges** de l'écran **Privilèges et autres paramètres**. • **Arrêter automatiquement le scan programmé lorsque le scan dure depuis plus de XX heure(s) et XX minute(s)** : arrête un long scan programmé après avoir atteint la durée configurée • **Ignorer le scan programmé lorsque l'autonomie de la batterie d'un Endpoint sans fil est inférieure à XX % et**

SECTION	SETTINGS
	que son adaptateur secteur est débranché : empêche l'agent OfficeScan de démarrer un scan programmé si l'autonomie de la batterie est faible **Reprendre un scan programmé** • **Reprendre un scan programmé interrompu** : reprend un scan programmé à l'heure spécifiée si l'utilisateur a interrompu le scan en mettant l'Endpoint hors tension • **Reprendre un scan programmé ignoré** : démarre un scan programmé à l'heure spécifiée si l'Endpoint n'était pas en cours d'exécution lorsque le scan programmé devait démarrer
Paramètres du pare-feu	• **Envoyer les journaux de pare-feu au serveur toutes/tous les** : définit la fréquence à laquelle les agents OfficeScan dotés du privilège **Autoriser les agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan** envoient des journaux de pare-feu au serveur **Remarque** Vous pouvez octroyer le privilège **Autoriser des agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan** dans l'onglet **Privilèges** de l'écran **Privilèges et autres paramètres**. • **Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système** : empêche l'agent OfficeScan de tenter de mettre à jour le pilote du pare-feu commun pendant les opérations normales • **Envoyer au serveur OfficeScan le nombre d'entrées du journal du pare-feu toutes les heures pour déterminer la possibilité d'une épidémie au niveau du pare-feu** : permet à l'agent OfficeScan d'envoyer des nombres de détections de pare-feu à OfficeScan toutes les heures
Paramètres de connexion suspecte	**Modifier la liste des adresses IP définie par l'utilisateur** : les administrateurs peuvent configurer l'agent OfficeScan pour autoriser, bloquer ou consigner toutes les connexions entre des agents et des adresses IP C&C définies par l'utilisateur

SECTION	SETTINGS
	Pour plus d'informations, voir *Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur à la page 4-21*.
Paramètres de surveillance des comportements	**Entreprendre automatiquement une action si l'utilisateur ne répond pas dans un délai de : XX seconde(s)** : définit la période maximale dont disposent les utilisateurs avant que la surveillance des comportements autorise l'exécution d'un programme **Remarque** Vous devez activer la surveillance des événements et définir l'action pour l'événement particulier sur **Demander si nécessaire** avant que l'agent OfficeScan n'affiche l'invite.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres des listes globales des adresses IP définies par l'utilisateur

Les administrateurs peuvent configurer OfficeScan de manière à autoriser, interdire ou consigner toutes les connexions entre les agents et des adresses IP C&C définies par l'utilisateur.

Remarque

Les listes d'adresses IP définies par l'utilisateur prennent uniquement en charge les adresses IPv4.

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Paramètres de sécurité**.

3. Accédez à la section **Paramètres de connexion suspecte**.
4. Cliquez sur **Modifier la liste des adresses IP définie par l'utilisateur**.
5. Dans l'onglet **Liste approuvée** ou **Liste bloquée**, ajoutez les adresses IP que vous souhaitez surveiller.
   a. Cliquez sur **Ajouter**.
   b. Sur l'écran qui s'affiche alors, saisissez l'adresse IP, la plage d'adresses IP ou l'adresse IPv4 et le masque de sous-réseau qu'OfficeScan doit surveiller.
   c. Cliquez sur **Enregistrer**.
6. Pour supprimer une adresse IP de la liste, cochez la case en regard de cette adresse, puis cliquez sur **Supprimer**.
7. Une fois les listes configurées, cliquez sur **Fermer** pour revenir à l'écran **Paramètres de l'agent général**.
8. Cliquez sur **Enregistrer** pour déployer la liste mise à jour sur les agents.

Paramètres système

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Système**.
3. Configurez les paramètres selon les besoins.

SECTION	SETTINGS
Paramètres de Certified Safe Software Service	**Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus** : interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par blocage des comportements de malwares, surveillance des événements, pare-feu ou antivirus pour réduire la probabilité de faux positifs
Redémarrage des services	**Redémarrer automatiquement un service de l'agent OfficeScan interrompu de façon inattendue** : redémarre les services de l'agent OfficeScan qui ont cessé de répondre de façon inattendue Configurez les éléments suivants : • **Redémarrer le service après ____ minutes** : Indiquez le temps (en minutes) devant s'écouler avant qu'OfficeScan ne redémarre un service. • **Si la première tentative de redémarrage du service échoue, réessayer __ fois** : Spécifiez le nombre maximum de nouvelles tentatives pour le redémarrage d'un service. Redémarrez manuellement un service s'il reste arrêté après le nombre maximum de nouvelles tentatives. • **Remettre à zéro le compteur d'échecs de redémarrage au bout de_ heure(s)** : Si un service reste arrêté une fois que le nombre maximal de nouvelles tentatives a été épuisé, OfficeScan attend un certain nombre d'heures avant de réinitialiser le compte d'échecs. Si un service reste arrêté une fois que le nombre d'heures s'est écoulé, OfficeScan le redémarre.

4. Cliquez sur **Enregistrer**.

Paramètres du réseau

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Réseau**.
3. Configurez les paramètres selon les besoins.

SECTION	SETTINGS
Paramètres de bande passante des journaux de virus/ programmes malveillants	**Permettre aux agents OfficeScan de créer une entrée unique dans le journal des virus/programmes malveillants pour les détections récurrentes d'un même virus/programme malveillant en l'espace d'une heure** : consolide les entrées de journaux de virus lors de la détection de plusieurs infections du même virus/programme malveillant sur une courte période L'agent OfficeScan peut détecter un même virus/programme malveillant à plusieurs reprises, ce qui sature rapidement le journal de virus/programmes malveillants et consomme de la bande passante réseau lors de l'envoi d'informations de journaux au serveur. L'activation de cette fonction permet de réduire le nombre d'entrées consignées dans le journal de virus/programmes malveillants et la bande passante du réseau consommée par les agents OfficeScan pour soumettre au serveur des informations du journal de programmes malveillants.
Intervalle d'interrogation du serveur	**Intervalle d'interrogation : XX minute(s)** : configure lesagents OfficeScan pour automatiquement tenter de se connecter à OfficeScan au même intervalle régulier afin de recevoir des paramètres ou des composants actualisés et de signaler l'état de l'agent OfficeScan **Remarque** Le serveur OfficeScan classifie tous les agents OfficeScan qui n'ont pas réussi à interroger le serveur à l'intervalle spécifié comme « non accessibles ».

4. Cliquez sur **Enregistrer**.

Paramètres de contrôle des agents

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Contrôle d'agent**.
3. Configurez les paramètres selon les besoins.

SECTION	SETTINGS
Paramètres généraux	**Ajouter le scan manuel au menu de raccourcis Windows sur les Endpoints** : affiche l'option de menu **Scan** dans le menu de raccourci des agents OfficeScan
Paramètres d'alerte	• **Afficher l'icône d'alerte dans la barre des tâches Windows si le fichier de signatures de virus n'a pas été mis à jour au bout de XX jour(s)** : affiche une icône d'alerte dans la barre des tâches de Windows pour rappeler aux utilisateurs de mettre à jour un fichier de signatures de virus obsolète après le nombre de jours spécifiés. • **Afficher un message de notification si l'Endpoint doit être redémarré pour charger un pilote en mode noyau** : affiche une notification sur l'Endpoint indiquant qu'un redémarrage est requis pour terminer l'installation d'un correctif ou d'un package de mise à niveau contenant un nouveau pilote en mode noyau

SECTION	SETTINGS
Configuration de la langue de l'agent	Vous pouvez configurer les agents OfficeScan de sorte qu'ils utilisent tous les paramètres de langue du serveur OfficeScan ou les paramètres de l'utilisateur connecté. • **Paramètres de langue locale sur l'endpoint** : l'agent OfficeScan s'affiche dans la langue configurée par l'utilisateur connecté.  **Remarque** Si l'agent OfficeScan ne prend pas en charge les paramètres de langue de l'utilisateur connecté, il utilise la langue du serveur OfficeScan. Si le endpoint ne prend pas en charge la langue du serveur OfficeScan, l'anglais est utilisé. • **Langue du serveur OfficeScan** : l'agent OfficeScan s'affiche dans la langue du serveur OfficeScan.  **Remarque** Si le endpoint ne prend pas en charge la langue du serveur OfficeScan, l'anglais est utilisé.

4. Cliquez sur **Enregistrer**.

Emplacement du endpoint

OfficeScan dispose d'une fonction de détection d'emplacement qui détermine si l'agent OfficeScan se trouve dans le réseau interne ou externe. La détection d'emplacement est utilisée par les fonctionnalités et services OfficeScan suivants :

- Web Reputation
- Prévention contre la perte de données
- Contrôle des dispositifs

L'emplacement de l'agent OfficeScan détermine si l'agent OfficeScan applique des paramètres de stratégie interne ou externe. Les administrateurs configurent généralement une stratégie plus stricte pour les agents OfficeScan externes.

Critères d'emplacement

Indiquez si l'emplacement est basé sur l'adresse IP de passerelle du endpoint de l'agent OfficeScan ou sur l'état de la connexion de l'agent OfficeScan au serveur OfficeScan ou à un serveur de référence.

- **État de la connexion de l'agent** : si l'agent OfficeScan peut se connecter au serveur OfficeScan ou à l'un des serveurs de référence attribués sur l'intranet, l'emplacement du endpoint est interne. De plus, si un endpoint situé hors du réseau de l'entreprise peut se connecter au serveur OfficeScan/serveur de référence, son emplacement est également considéré comme étant interne. Si aucune de ces conditions n'est vérifiée, l'emplacement du endpoint est externe.
- **Adresse IP de passerelle et adresse MAC** : si l'adresse IP de passerelle du endpoint de l'agent OfficeScan correspond à l'une des adresses IP de passerelle que vous avez spécifiées sur l'écran **Emplacement du endpoint**, l'emplacement du endpoint est considéré comme interne. Dans le cas contraire, l'emplacement du endpoint est externe.

Configuration des paramètres d'emplacement

Procédure

1. Accédez à **Agents** > **Emplacement du endpoint**.
2. Indiquez si l'emplacement dépend du paramètre **Serveurs de référence** ou **Adresses IP et MAC de passerelle**.
   - **Serveurs de référence** : les agents OfficeScan qui peuvent se connecter à un serveur de référence font partie du réseau interne

     Pour plus d'informations, voir *Serveurs de référence à la page 4-28*.
   - **Adresse IP de passerelle** : les agents OfficeScan qui peuvent se connecter à une passerelle font partie du réseau interne

a. Saisissez l'adresse IPv4/IPv6 de passerelle dans la zone de texte prévue à cet effet.

b. (Facultatif) Saisissez l'adresse MAC.

c. Cliquez sur **Ajouter**.

Remarque

Si vous ne saisissez pas d'adresse MAC, OfficeScan inclut toutes les adresses MAC appartenant à l'adresse IP spécifiée.

3. Cliquez sur **Enregistrer**.

Serveurs de référence

L'une des méthodes employées par l'agent OfficeScan pour déterminer la stratégie ou le profil à utiliser consiste à vérifier son état de connexion au serveur OfficeScan. Si un agent OfficeScan interne (ou un agent se trouvant au sein du réseau d'entreprise) ne peut pas se connecter au serveur, il passe à l'état hors ligne. L'agent applique ensuite une stratégie ou un profil destiné aux agents externes. Les serveurs de référence résolvent ce problème.

Un agent OfficeScan perdant sa connexion au serveur OfficeScan tentera de se connecter aux serveurs de référence. Si l'agent parvient à établir une connexion à un serveur de référence, il applique la stratégie ou le profil destiné aux agents internes.

Les stratégies et profils gérés par les serveurs de référence incluent :

- Profils de pare-feu
- Stratégies de Web Reputation
- Stratégies de protection des données
- Stratégies de contrôle des dispositifs

Prenez en compte les éléments suivants :

- Configurez les ordinateurs disposant de capacités de serveur, par exemple des serveurs Web, SQL ou FTP, comme serveurs de référence. Vous pouvez définir au maximum 320 serveurs de référence.
- Les agents OfficeScan se connectent au premier serveur de référence de la liste des serveurs de référence. Si la connexion ne peut pas être établie, l'agent tente de se connecter au serveur suivant de la liste.
- Les agents OfficeScan utilisent les serveurs de référence pour déterminer les paramètres appropriés pour l'antivirus (surveillance des comportements, contrôle des dispositifs, profils de pare-feu et stratégie de Web Reputation) ou la protection des données. Les serveurs de référence ne gèrent pas les agents et ne déploient pas les mises à jour et les paramètres des agents. C'est le serveur OfficeScan qui effectue ces tâches.
- Un agent OfficeScan ne peut pas envoyer de journaux à des serveurs de référence ni les utiliser en tant que sources de mise à jour.

Gestion de la liste de serveurs de référence

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils** ou **Agents** > **Emplacement du endpoint**.
2. En fonction de l'écran qui s'affiche, vous devez procéder de la façon suivante :
   - Si vous êtes sur l'écran **Profils de pare-feu pour les agents**, cliquez sur **Modifier la liste de serveurs de référence** .
   - Si vous êtes sur l'écran **Emplacement du endpoint**, cliquez sur **Liste des serveurs de référence**.
3. Sélectionnez **Activer la liste de serveurs de référence**.
4. Pour ajouter un endpoint à la liste, cliquez sur **Ajouter**.
   a. Spécifiez l'adresse IPv4/IPv6 du endpoint, son nom ou son nom de domaine complet (FQDN), par exemple :

- `computer.networkname`
- `12.10.10.10`
- `mycomputer.domain.com`

b. Saisissez le numéro de port au moyen duquel les agents communiquent avec ce endpoint. Spécifiez un port de contact ouvert quelconque (tels que les ports 20, 23 ou 80) sur le serveur de référence.

Remarque

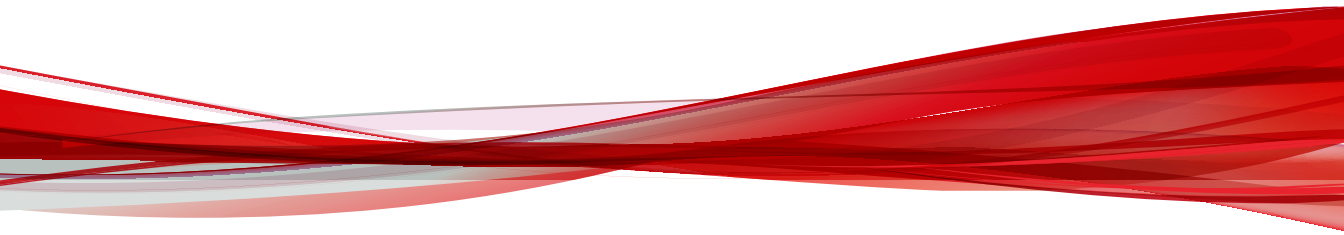
pour spécifier un autre numéro de port pour le même serveur de référence, répétez les étapes 2a et 2b. L'agent OfficeScan utilise le premier numéro de port de la liste et passe au suivant en cas d'échec de connexion.

c. Cliquez sur **Enregistrer**.

5. Pour modifier les paramètres d'un endpoint de la liste, cliquez sur son nom. Modifiez le nom ou le port du endpoint, puis cliquez sur **Enregistrer**.
6. Pour supprimer un endpoint de la liste, sélectionnez son nom, puis cliquez sur **Supprimer**.
7. Pour permettre aux endpoints de fonctionner en tant que serveurs de référence, cliquez sur **Affecter à des agents**.

Partie III

Protection des Endpoints



Chapitre 5

Détection des programmes malveillants

Cette section décrit comment configurer la détection des programmes malveillants sur les agents OfficeScan.

Les rubriques sont les suivantes :

Scan immédiat

Le scan immédiat est lancé à distance par des administrateurs via la console Web et peut être ciblé sur un ou plusieurs Endpoints de l'agent OfficeScan.

Configurez et appliquez des paramètres de scan immédiat à un ou plusieurs agents OfficeScan et domaines, ou à tous les agents OfficeScan gérés par le serveur.

Configuration des paramètres de scan immédiat

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Tâches** > **Scan immédiat**.

   L'écran **Scan immédiat** s'ouvre.
4. Pour modifier les paramètres de **scan immédiat** préconfigurés avant le lancement du scan, cliquez sur **Paramètres**.

   a. Sélectionnez les options suivantes :

   - **Activer le scan antivirus/programme malveillant**
   - **Activer le scan antispyware/grayware**

   Remarque

   Vous devez activer le scan de virus/programmes malveillants avant que vous puissiez activer le scan anti-spyware et anti-grayware.

   b. Configurez les paramètres **Cible**.

   Pour plus d'informations, voir *Scan immédiat : onglet cible à la page 5-3*.

   c. Configurez les paramètres **Action**.

Pour plus d'informations, voir *Scan immédiat : onglet Action à la page 5-5*.

d. Configurez les paramètres **Exclusion de scan**.

Pour plus d'informations, voir *Scan immédiat : onglet Exclusion du scan à la page 5-8*.

e. Cliquez sur **Précédent** pour revenir à l'écran **Scan immédiat**.

5. Dans l'arborescence des agents, sélectionnez les agents OfficeScan à scanner et cliquez sur **Lancer un scan immédiat**.

Le serveur envoie une notification aux agents OfficeScan sélectionnés.

6. Cliquez sur **Sélectionner les Endpoints n'ayant pas reçu de notification**, puis sur **Lancer un scan immédiat** pour renvoyer immédiatement la notification aux agents OfficeScan qui n'ont pas reçu la notification.

7. Cliquez sur **Arrêter la notification** pour annuler la notification aux agents OfficeScan.

Les agents OfficeScan ayant déjà démarré le scan continuent le scan en cours.

8. Pour les agents OfficeScan qui ont déjà commencé le scan, cliquez sur **Arrêter le scan immédiat** pour annuler le scan actif.

Scan immédiat : onglet cible

Procédure

1. Dans la section **Fichiers à scanner**, sélectionnez l'un des éléments suivants :

- **Tous les fichiers scannables** inclut tous les fichiers scannables. Les fichiers impossibles à analyser sont des fichiers protégés par un mot de passe, chiffrés ou dépassant les restrictions de scan définies par l'utilisateur

Remarque

Cette option offre le meilleur niveau de sécurité possible. Cependant, le scan de chaque fichier nécessite beaucoup de temps et de ressources et peut s'avérer redondant dans certaines situations. Par conséquent, il peut être utile de limiter le nombre de fichiers que l'agent doit inclure dans le scan.

- **Types de fichiers scannés par IntelliScan** scanne les fichiers d'après le véritable type de fichier.
- **Fichiers possédant les extensions suivantes (séparer les différentes entrées par une virgule) :** spécifie manuellement les fichiers à scanner en fonction de leur extension. Séparez les entrées par une virgule.

Remarque

Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

- **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

2. Dans la section **Paramètres de scan**, configurez les paramètres requis.

PARAMÈTRE	DESCRIPTION
Scanner les fichiers compressés	Scanne le nombre spécifié de couches de compression au sein d'un fichier archivé **Remarque** Le scan sur plusieurs couches peut détecter des programmes malveillants intentionnellement enfouis dans une archive compressée, cependant le scan peut affecter les performances du système.

PARAMÈTRE	DESCRIPTION
Scanner les objets OLE	Scanne le nombre spécifié de couches Object Linking and Embedding (OLE) dans un fichier **Détecter le code d'exploitation dans les fichiers OLE** : la détection d'exploitation OLE identifie les programmes malveillants de manière heuristique en vérifiant la présence de code d'exploitation dans les fichiers Microsoft Office. **Remarque** Le nombre de couches spécifié s'applique aux options **Scanner les objets OLE** et **Détecter le code d'exploitation dans les fichiers OLE**.
Scanner la zone d'amorçage	Scanne le secteur d'amorçage du disque dur de l'Endpoint à la recherche de virus/programmes malveillants

3. Dans la section **Utilisation du processeur**, sélectionnez l'un des éléments suivants :

   - **Élevé** : aucune interruption entre les scans
   - **Moyen** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 50% et pas d'interruption si elle est de 50% ou moins
   - **Faible** : interruption entre les scans de fichiers si la consommation de l'UC est supérieure à 20% et pas d'interruption si elle est de 20% ou moins

Scan immédiat : onglet Action

Procédure

1. Dans la section **Virus/programmes malveillants**, configurez les paramètres requis.

   a. Sélectionnez le type d'action que l'agent OfficeScan entreprend après la détection d'une menace pour la sécurité.

- **Utiliser ActiveAction** : cette fonction utilise un ensemble d'actions de scan pré-configurées destinées à lutter contre les virus et les programmes malveillants.

  Pour plus d'informations, voir *ActiveAction à la page 5-11*.

  - **Personnaliser l'action pour les virus/programmes malveillants probables** : sélectionnez et spécifiez l'action que l'agent OfficeScan entreprend en cas de programmes malveillants probables

- **Utiliser la même action pour tous les types de virus/programmes malveillants** : spécifiez l'action que l'agent OfficeScan entreprend sur toutes les menaces de programmes malveillants

- **Utiliser une action spécifique pour chaque type de virus/programme malveillant** : spécifiez l'action que l'agent OfficeScan entreprend en cas de menaces de sécurité spécifiques

  Pour plus d'informations, voir *Actions de scan personnalisées à la page 5-12*.

b. Sélectionnez **Sauvegarder les fichiers avant nettoyage** pour créer une copie chiffrée du fichier infecté sur l'Endpoint dans le dossier `<dossier d'installation de l'agent>\Backup`.

   La création d'une copie de sauvegarde du fichier vous permet de restaurer la version d'origine du fichier, si nécessaire.

c. Spécifiez l'emplacement du répertoire de quarantaine.

   - **Mettre en quarantaine sur le serveur gérant l'agent OfficeScan** : l'agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine au serveur de gestion OfficeScan

   - **Répertoire de quarantaine** : l'agent OfficeScan envoie une copie chiffrée de tous les fichiers mis en quarantaine à l'emplacement spécifié

   Pour plus d'informations, voir *Quarantine Directory à la page 5-14*.

d. Dans la section **Damage Cleanup Services**, configurez les éléments suivants :

   - **Type de nettoyage**

- **Nettoyage standard** : l'agent OfficeScan exécute l'une des actions suivantes au cours du nettoyage standard :
  - Détecte et supprime les chevaux de Troie actifs
  - Élimine les processus créés par les chevaux de Troie
  - Répare les fichiers système modifiés par les chevaux de Troie
  - Supprime les fichiers et les applications laissés par les chevaux de Troie
- **Nettoyage avancé** : outre les actions de nettoyage standard, l'agent OfficeScan interrompt les activités de logiciels de sécurité non autorisés, connus également sous le nom de « FakeAV », et certaines variantes de rootkits.

- **Exécuter la fonction Nettoyage dès qu'un virus/programme malveillant est détecté** : effectue le type de nettoyage configuré sur de probables menaces de programmes malveillants

Remarque

Vous pouvez sélectionner cette action uniquement si l'action appliquée aux virus/programmes malveillants potentiels n'est pas **Ignorer**, ni **Refuser l'accès**.

2. Dans la section **Spyware/Grayware**, sélectionnez l'action que l'agent OfficeScan entreprend après la détection de programmes espions/graywares.

- **Nettoyer** : termine tous les processus liés et supprime les valeurs de registre, fichiers, cookies et raccourcis associés

Remarque

Après avoir nettoyé des spywares/graywares, les agents OfficeScan sauvegardent les données concernant ces programmes. Vous pouvez restaurer ces données si vous estimez que l'accès à ces spywares/graywares est sans danger.

- **Ignorer** : consigne la détection mais permet l'exécution du programme

Scan immédiat : onglet Exclusion du scan

Procédure

1. Sélectionnez **Activer l'exclusion de scan**.
2. Dans la section **Liste des exclusions de scan (répertoires)**, configurez les paramètres requis.
   a. Sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** pour automatiquement exclure les répertoires associés à d'autres produits Trend Micro.

      Pour plus d'informations, voir *Exclusions du répertoire des produits Trend Micro à la page 5-21*.

   b. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

      - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
      - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   c. Saisissez un chemin d'accès à un répertoire à exclure des scans, puis cliquez sur le bouton **+**.

      L'agent OfficeScan ne scanne pas les fichiers situés dans le répertoire spécifié (et ses sous-répertoires).

Remarque

- Vous pouvez spécifier un maximum de 256 répertoires à exclure du scan.
- Les exclusions de répertoires prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 5-21*.

3. Dans la section **Liste des exclusions de scan (fichiers)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent
   - **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

   b. Saisissez un nom de fichier ou le nom de fichier avec un chemin d'accès à un répertoire complet à exclure des scans, puis cliquez sur le bouton **+**.

Remarque

- Vous pouvez spécifier un maximum de 256 fichiers à exclure du scan.
- Les exclusions de fichiers prennent en charge l'utilisation de caractères génériques.

  Pour plus d'informations, voir *Exceptions avec caractères génériques à la page 5-21*.

4. Dans la section **Liste des exclusions de scan (extensions de fichier)**, configurez les paramètres requis.

   a. Lorsque vous configurez une stratégie parent, indiquez comment les autres utilisateurs peuvent configurer des stratégies enfant.

   - **Hériter du parent** : Les stratégies enfant doivent utiliser les paramètres configurés dans la stratégie parent

- **Étendre à partir du parent** : Les stratégies enfant peuvent ajouter des paramètres supplémentaires aux paramètres hérités de la stratégie parent

b. Sélectionnez ou saisissez une extension de fichier à exclure des scans, puis cliquez sur le bouton **Ajouter >**.

Remarque

- Vous pouvez spécifier au maximum 256 extensions de fichier à exclure du scan.
- Pour le scan manuel, le scan programmé et le scan immédiat, utilisez un point d'interrogation (?) pour remplacer un seul caractère ou un astérisque (*) pour remplacer plusieurs caractères comme caractères génériques. Par exemple, si vous ne souhaitez pas scanner tous les fichiers dont les extensions commencent par D, comme `DOC`, `DOT` ou `DAT`, saisissez `D*` ou `D??`.

Actions de scan

Vous pouvez configurer les agents OfficeScan pour utiliser un ensemble d'actions de scan prédéfinies ou des actions personnalisées basées sur le type de programme malveillant détecté.

Important

Certains fichiers ne sont pas nettoyables.

Pour plus d'informations, consultez :

- *ActiveAction à la page 5-11*
- *Actions de scan personnalisées à la page 5-12*
- *Fichiers non nettoyables à la page 5-15*

ActiveAction

À chaque type de virus/programme malveillant correspond une action de scan différente. Pour personnaliser les actions de scan, vous devez posséder les connaissances nécessaires sur les virus et programmes malveillants. Cette tâche peut être fastidieuse. L'agent OfficeScan utilise ActiveAction pour pallier à ces problèmes.

ActiveAction est un ensemble d'actions de scan pré-configurées, destinées à lutter contre les virus et les programmes malveillants. Si les actions de scan ne vous sont pas familières ou si vous ignorez quelle action est la mieux adaptée à tel ou tel type de virus ou programme malveillant, l'utilisation de l'outil ActiveAction est recommandée.

ActiveAction offre les avantages suivants :

- ActiveAction applique les actions de scan recommandées par Trend Micro. Vous ne perdez plus votre temps à configurer vous-même les actions de scan.
- Les créateurs de virus et de programmes malveillants modifient en permanence la manière dont leurs virus attaquent les Endpoints. Les paramètres d'ActiveAction sont mis à jour pour assurer une protection contre les menaces et les méthodes d'attaques les plus récentes des virus et programmes malveillants.

Le tableau suivant illustre comment ActiveAction traite chaque type de virus/programme malveillant.

TABLEAU 5-1. Actions de scan recommandées par Trend Micro contre les virus et les programmes malveillants

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Exploitation CVE	Ignorer	N/A	N/A	N/A
Canular	Quarantaine	N/A	Quarantaine	N/A
Chevaux de Troie	Quarantaine	N/A	Quarantaine	N/A
Virus	Nettoyer	Quarantaine	Nettoyer	Quarantaine

TYPE DE VIRUS/ PROGRAMMES MALVEILLANTS	SCAN EN TEMPS RÉEL		SCAN MANUEL/SCAN PROGRAMMÉ	
	PREMIÈRE ACTION	DEUXIÈME ACTION	PREMIÈRE ACTION	DEUXIÈME ACTION
Virus de test	Refuser l'accès	N/A	Ignorer	N/A
Utilitaire de compression	Quarantaine	N/A	Quarantaine	N/A
Autres	Nettoyer	Quarantaine	Nettoyer	Quarantaine
Virus/programmes malveillants probables	Refuser l'accès ou action configurée par l'utilisateur	N/A	Ignorer ou action configurée par l'utilisateur	N/A

Remarque

- Pour les virus et programmes malveillants probables, l'action par défaut est « Refuser l'accès » pendant le scan en temps réel et « Ignorer » pendant le scan manuel et le scan programmé. S'il ne s'agit pas des actions que vous souhaitez effectuer, vous pouvez les modifier par « Mettre en quarantaine », « Supprimer » ou « Renommer ».
- Certains fichiers ne sont pas nettoyables.
- ActiveAction n'est pas disponible pour le scan anti-spywares/graywares.

Actions de scan personnalisées

ACTION	DESCRIPTION
Supprimer	Supprime un fichier infecté.

ACTION	DESCRIPTION
Mise en quarantaine	Renomme, puis déplace le fichier infecté vers un répertoire de quarantaine temporaire sur l'Endpoint. L'agent OfficeScan envoie ensuite les fichiers en quarantaine vers le répertoire de quarantaine spécifié, qui se trouve par défaut sur le serveur de gestion. L'agent OfficeScan chiffre les fichiers en quarantaine envoyés à ce répertoire. Pour plus d'informations, voir *Quarantine Directory à la page 5-14*.
Nettoyer	Nettoie le fichier infecté avant d'autoriser l'accès complet au fichier. Si le fichier est impossible à nettoyer, l'agent OfficeScan effectue une deuxième action, pouvant être l'une des actions suivantes : « Mettre en quarantaine », « Supprimer », « Renommer » et « Ignorer ». Cette action peut être exécutée sur tous les types de menaces liées à la sécurité, à l'exception des virus/programmes malveillants probables. **Remarque** Certains fichiers ne sont pas nettoyables. Pour obtenir des informations détaillées, consultez la section *Fichiers non nettoyables à la page 5-15*.
Renommer	Remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier renommé. Ils peuvent l'ouvrir s'ils associent le fichier à une application déterminée. Le virus/programme malveillant peut s'exécuter lors de l'ouverture du fichier infecté renommé.
Ignorer	N'effectue aucune action sur les menaces détectées, mais consigne la détection dans les journaux.
Refuser l'accès	Lorsque l'agent OfficeScan détecte une tentative d'ouverture ou d'exécution d'un fichier infecté, il bloque immédiatement l'opération. Les utilisateurs peuvent supprimer manuellement le fichier infecté.

Quarantine Directory

Si l'action concernant un fichier infecté est « Mettre en quarantaine », agent OfficeScan chiffre le fichier et le déplace vers un dossier de quarantaine temporaire sous <Dossier d'installation de l'agent>\SUSPECT, puis l'envoie vers le répertoire de quarantaine désigné.

Remarque

Vous pouvez restaurer des fichiers encodés en quarantaine si vous devez y accéder par la suite.

Acceptez le répertoire de quarantaine par défaut, qui se trouve sur l'ordinateur du serveur OfficeScan. Le répertoire est au format URL. Il contient le nom d'hôte du serveur ainsi que l'adresse IP.

- Si le serveur gère simultanément des agents IPv4 et IPv6, utilisez le nom d'hôte de façon à ce que tous les agents OfficeScan puissent envoyer des fichiers mis en quarantaine au serveur.
- Si le serveur dispose uniquement d'une adresse IPv4 ou s'il est identifié par celle-ci, seuls les agents OfficeScan IPv4 purs et à double pile peuvent lui envoyer des fichiers mis en quarantaine.
- Si le serveur dispose uniquement d'une adresse IPv6 ou s'il est identifié par celle-ci, seuls les agents OfficeScan IPv6 purs et à double pile peuvent lui envoyer des fichiers mis en quarantaine.

Vous pouvez également définir un répertoire de quarantaine alternatif en saisissant son URL, chemin UNC ou chemin de fichier absolu. Les agents doivent être en mesure de se connecter à ce répertoire. Par exemple, le répertoire alternatif doit disposer d'une adresse IPv6 si des agents OfficeScan iPv6 purs ou à double pile sont censés lui envoyer des fichiers mis en quarantaine. Trend Micro vous recommande de désigner comme répertoire alternatif un répertoire à double pile, qui sera identifié par son nom d'hôte et dont vous saisirez le chemin UNC.

Reportez-vous au tableau suivant pour obtenir de l'aide sur l'utilisation d'une URL, d'un chemin UNC ou d'un chemin de fichier absolu :

TABLEAU 5-2. Répertoire de quarantaine

RÉPERTOIRE DE QUARANTAINE	FORMAT ACCEPTÉ	EXEMPLE	REMARQUES
Répertoire installé sur l'ordinateur serveur de gestion	URL	`http://<osceserver>`	Il s'agit du répertoire par défaut. Configurez les paramètres de ce répertoire, comme la taille du dossier de quarantaine.
	Chemin UNC	`\\<osceserver>\ofcscan\Virus`	
Répertoire sur un autre ordinateur serveur OfficeScan (si vous avez d'autres serveurs OfficeScan sur le réseau)	URL	`http://<osceserver2>`	Vérifiez que les agents OfficeScan peuvent se connecter à ce répertoire. Si vous spécifiez un répertoire non valide, l'agent OfficeScan conserve les fichiers en quarantaine dans le dossier SUSPECT jusqu'à ce que vous indiquiez un répertoire de quarantaine valide. Dans les journaux de virus/programmes malveillants du serveur, le résultat de scan est «Impossible d'envoyer le fichier en quarantaine vers le dossier de quarantaine spécifié». Si vous utilisez un chemin UNC, vérifiez que le répertoire de quarantaine est partagé avec le groupe «Tous» et que vous avez attribué des privilèges de lecture et d'écriture à ce groupe.
	Chemin UNC	`\\<osceserver2>\ofcscan\Virus`	
Autre Endpoint sur le réseau	Chemin UNC	`\\<nom_ordinateur>\temp`	
Autre répertoire se trouvant sur l'agent OfficeScan	Chemin de fichier absolu	`C:\temp`	

Fichiers non nettoyables

Le moteur de scan antivirus ne nettoie pas les fichiers suivants :

TABLEAU 5-3. Solutions aux fichiers non nettoyables

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés par des chevaux de Troie	Les chevaux de Troie sont des programmes qui exécutent des actions inattendues, non autorisées et généralement nuisibles, telles que l'affichage de messages, l'écrasement de fichiers ou le formatage de disques. Il est inutile de nettoyer les fichiers puisque les chevaux de Troie ne les infectent pas. Solution : le moteur Damage Cleanup et le modèle de nettoyage des dommages suppriment les chevaux de Troie.
Fichiers infectés par des vers	Un ver est un programme (ou ensemble de programmes) autonome qui peut répandre des copies fonctionnelles de lui-même ou de ses segments au sein d'autres systèmes de endpoint. La propagation se produit généralement par le biais de connexions réseau ou de pièces jointes d'e-mails. Les vers ne peuvent pas être nettoyés car le fichier constitue un programme autonome. Solution : Trend Micro recommande de supprimer les vers.
Fichiers infectés protégés en écriture	Solution : supprimez la protection en écriture pour permettre le nettoyage du fichier.
Fichiers protégés par mot de passe	Les fichiers protégés par mot de passe incluent les fichiers compressés protégés par mot de passe et les fichiers Microsoft Office protégés par mot de passe. Solution : supprimez la protection par mot de passe pour permettre le nettoyage du fichier.
Fichiers de sauvegarde	Les fichiers possédant une extension RB0~RB9 sont des copies de sauvegarde des fichiers infectés. Le processus de nettoyage crée une sauvegarde du fichier infecté au cas où le virus/programme malveillant l'endommagerait au cours du processus de nettoyage. Solution : si le nettoyage réussit, vous n'avez pas besoin de conserver la copie de sauvegarde du fichier infecté. Si le endpoint fonctionne correctement, vous pouvez supprimer le fichier de sauvegarde.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés dans la corbeille	Il peut arriver que le système n'autorise pas la suppression des fichiers infectés présents dans la corbeille, car le système est en cours d'exécution.

	Solution sous Windows XP ou Windows Server 2003 avec le système de fichiers NTFS :
	1. Connectez-vous au endpoint avec des privilèges d'administrateur.
	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Ouvrez l'invite de commande.
	4. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.
	5. Vérifiez si les fichiers ont été supprimés.

	Solution sous d'autres systèmes d'exploitation (ou ceux sans NTFS) :
	1. Redémarrez le endpoint en mode MS-DOS.
	2. Ouvrez l'invite de commande.
	3. Saisissez ce qui suit pour effacer les fichiers :
	`cd \`
	`cd recycled`
	`del *.* /S`
	La dernière commande supprime tous les fichiers de la corbeille.

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION
Fichiers infectés dans le dossier Temp de Windows ou dans un dossier temporaire d'Internet Explorer	Il peut arriver que le système n'autorise pas le nettoyage des fichiers infectés présents dans le dossier Temp de Windows ou dans le dossier temporaire d'Internet Explorer, car le endpoint les utilise. Les fichiers à nettoyer sont peut-être des fichiers temporaires nécessaires au fonctionnement de Windows.

	Solution sous Windows XP ou Windows Server 2003 avec le système de fichiers NTFS :
	1. Connectez-vous au endpoint avec des privilèges d'administrateur.
	2. Fermez toutes les applications en cours afin d'éviter que celles-ci ne verrouillent le fichier, empêchant ainsi Windows de le supprimer.
	3. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les endpoints Windows XP ou Windows Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd temp`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	4. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	a. Ouvrez l'invite de commande et accédez au dossier Temp d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary Internet Files` pour les endpoints Windows XP ou Server 2003).

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION

	b. Saisissez ce qui suit pour effacer les fichiers :
	
	`cd tempor~1`
	
	`attrib -h`
	
	`del *.* /S`
	
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.
	
	c. Vérifiez si les fichiers ont été supprimés.

	Solution sous d'autres systèmes d'exploitation (ou ceux sans NTFS) :
	
	1. Redémarrez le endpoint en mode MS-DOS.
	
	2. Si le fichier infecté se trouve dans le dossier Temp de Windows:
	
	a. Ouvrez l'invite de commande et accédez au dossier Temp de Windows (situé par défaut sous `C:\Windows\Temp` sur les endpoints Windows XP ou Windows Server 2003).
	
	b. Saisissez ce qui suit pour effacer les fichiers :
	
	`cd temp`
	
	`attrib -h`
	
	`del *.* /S`
	
	La dernière commande supprime tous les fichiers du dossier Temp de Windows.
	
	c. Redémarrez le endpoint en mode normal.
	
	3. Si le fichier infecté se trouve dans le dossier temporaire d'Internet Explorer:
	
	a. Ouvrez l'invite de commande et accédez au dossier Temp d'Internet Explorer (situé par défaut sous `C:\Documents and Settings\<Votre nom d'utilisateur>\Local Settings\Temporary`

FICHIER NON NETTOYABLE	EXPLICATION ET SOLUTION

	`Internet Files` pour les endpoints Windows XP ou Server 2003).
	b. Saisissez ce qui suit pour effacer les fichiers :
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	La dernière commande supprime tous les fichiers du dossier temporaire d'Internet Explorer.
	c. Redémarrez le endpoint en mode normal.

Fichiers compressés à l'aide d'un format de compression non pris en charge	Solution : décompressez les fichiers.
Fichiers verrouillés ou en cours d'exécution	Solution : déverrouillez les fichiers ou attendez qu'ils aient été exécutés.
Fichiers corrompus	Solution : supprimez les fichiers.

Support d'exclusion de scan

Lors de l'exclusion de répertoires et de noms de fichiers du scan anti-programmes malveillants, consultez les informations d'assistance technique suivantes :

- *Exclusions du répertoire des produits Trend Micro à la page 5-21*
- *Exceptions avec caractères génériques à la page 5-21*

Exclusions du répertoire des produits Trend Micro

Si vous sélectionnez **Exclure les répertoires dans lesquels sont installés des produits Trend Micro** dans la section **Liste des exclusions de scan (répertoires)**, l'agent OfficeScan exclut automatiquement les répertoires de produits suivants :

- <Dossier d'installation du serveur>
- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11 et 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

Exceptions avec caractères génériques

Les listes d'exclusion de scan pour les fichiers et les répertoires prennent en charge l'utilisation des caractères génériques. Utilisez le caractère « ? » pour remplacer un caractère et « * » pour en remplacer plusieurs.

Utilisez les caractères génériques avec précaution. L'utilisation d'un caractère erroné peut exclure des fichiers ou des répertoires incorrects. Par exemple, l'ajout de `C:\*` à la liste des exclusions de scan (fichiers) exclut l'intégralité du lecteur `C:\`.

TABLEAU 5-4. Exclusions de scan avec des caractères génériques

VALEUR	EXCLUS	NON EXCLUS

`c:\director*\fil\*.txt`	`c:\directory\fil\doc.txt`
	`c:\directories\fil\files\document.txt`
		`c:\directory\file\`
		`c:\directories\files\`
		`c:\directory\file\doc.txt`
		`c:\directories\files\document.txt`

`c:\director?\file\*.txt`	`c:\directory\file\doc.txt`	`c:\directories\file\document.txt`
`c:\director?\file\?.txt`	`c:\directory\file\1.txt`	`c:\directory\file\doc.txt` `c:\directories\file\document.txt`
`c:\*.txt`	Tous les fichiers `.txt` du répertoire `C:\`	Tous les autres types de fichiers du répertoire `C:\`
`[]`	Non pris en charge	Non pris en charge

Restauration de fichiers mis en quarantaine

Vous pouvez restaurer des fichiers mis en quarantaine par OfficeScan si vous estimez que la détection a fait une erreur. La fonctionnalité de restauration de fichiers depuis la mise en quarantaine centrale vous permet de rechercher des fichiers mis dans le répertoire de quarantaine et d'effectuer une vérification SHA1 afin de vous assurer que les fichiers que vous souhaitez restaurer n'ont subi aucune modification.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez un domaine ou un agent.
3. Cliquez sur **Tâches** > **Restauration depuis la mise en quarantaine centrale**.

L'écran **Critères de restauration depuis la mise en quarantaine centrale** s'affiche.

4. Saisissez le nom de l'élément que vous souhaitez restaurer dans le champ **Fichier/ Objet infecté**.

5. Vous avez également la possibilité d'indiquer une période, le nom d'une menace de sécurité et le chemin d'accès de l'élément.

6. Cliquez sur **Rechercher**.

   L'écran **Restauration depuis la mise en quarantaine centrale** s'affiche et indique les résultats de la recherche.

7. Sélectionnez **Ajouter le fichier restauré à la liste des exclusions au niveau du domaine** afin de vous assurer que tous les agents OfficeScan du ou des domaines dans lesquels est restauré le fichier ajoutent ce fichier à la liste des exclusions de scan.

   Cela empêchera OfficeScan de détecter à nouveau ce fichier en tant que menace lors des futurs scans.

8. Vous avez également la possibilité de saisir la valeur SHA-1 du fichier à des fins de vérification.

9. Sélectionnez le fichier à restaurer dans la liste et cliquez sur **Restaurer**.

Conseil

Pour afficher les agents OfficeScan sur lesquels le fichier est restauré, cliquez sur le lien qui se trouve dans la colonne **Endpoints**.

10. Cliquez sur **Fermer** dans la boîte de dialogue de confirmation.

    Pour vérifier qu'OfficeScan a bien restauré le fichier mis en quarantaine, voir *Affichage des journaux de restauration de la mise en quarantaine centralisée à la page 9-4*.

Chapitre 6

Utilisation du pare-feu OfficeScan

Ce chapitre décrit les fonctions et les configurations du pare-feu OfficeScan.

Les rubriques sont les suivantes :

Pare-feu OfficeScan

Le pare-feu OfficeScan protège les agents OfficeScan et les serveurs sur le réseau en utilisant une inspection avec état et un scan de virus réseau haute performance. Via la console d'administration centralisée, vous pouvez créer des règles pour filtrer les connexions par application, adresse IP, numéro de port ou protocole, puis appliquer les règles À différents groupes d'utilisateurs.

Remarque

Vous pouvez activer, configurer et utiliser le pare-feu OfficeScan sur des Endpoints Windows XP pour lesquels le pare-feu Windows est également activé. Cependant, vous devez gérer attentivement vos stratégies pour éviter de créer des stratégies de pare-feu conflictuelles et de produire des résultats inattendus. Consultez la documentation Microsoft pour obtenir des informations détaillées sur le pare-feu Windows.

Le tableau suivant décrit les fonctions fournies par le pare-feu OfficeScan.

FONCTION	DESCRIPTION
Filtrage du trafic	Le pare-feu OfficeScan filtre l'ensemble du trafic entrant et sortant, permettant ainsi de bloquer certains types de trafic sur la base des critères suivants : • Direction (entrant/sortant) • Protocole (TCP/UDP/ICMP/ICMPv6) • Ports de destination • Endpoints source et de destination
Filtrage d'applications	Le pare-feu OfficeScan filtre le trafic entrant et sortant d'applications spécifiées dans la liste d'exceptions du pare-feu, ce qui permet à ces applications d'accéder au réseau. La disponibilité de connexions réseau dépend des stratégies définies par l'administrateur.

FONCTION	DESCRIPTION
Liste Certified Safe Software	La liste locale Certified Safe Software contient une liste d'applications qui peuvent contourner les niveaux de sécurité de la stratégie de pare-feu. Le pare-feu OfficeScan autorise automatiquement les applications dans la liste Certified Safe Software à s'exécuter et à accéder au réseau. Vous pouvez également autoriser les agents OfficeScan à interroger une liste globale Certified Safe Software dynamiquement mise à jour hébergée sur des serveurs Trend Micro. **Important** L'interrogation de la liste globale Certified Safe Software impose l'activation du service de prévention des modifications non autorisées et du service Certified Safe Software.
Détection des virus réseau	Le pare-feu OfficeScan examine tous les paquets réseau pour détecter d'éventuels virus réseau.
Inspection avec état	Le pare-feu OfficeScan utilise l'inspection avec état pour surveiller et mémoriser toutes les connexions et les états de connexion à l'agent OfficeScan. Le pare-feu OfficeScan peut identifier les conditions spécifiques de toute connexion, prédire les actions qui doivent être effectuées et détecter toute coupure des connexions normales. L'utilisation efficace du pare-feu repose donc non seulement sur la création de profils et de stratégies, mais aussi sur l'analyse des connexions et le filtrage des paquets qui transitent par le pare-feu.
Système de détection d'intrusion	Le système de détection d'intrusion (SDI) contribue à identifier les fichiers de signatures contenus dans des paquets réseau pouvant indiquer une attaque de l'endpoint. Pour plus d'informations, voir *Système de détection d'intrusion à la page 6-8*.

Activation ou désactivation du pare-feu OfficeScan sur des Endpoints

Vous pouvez directement activer ou désactiver le pare-feu OfficeScan sur un Endpoint sélectionné.

Procédure

- Activez ou désactivez le pilote de pare-feu OfficeScan via Windows.
  a. Ouvrez les **propriétés de connexion au réseau Windows**.
  b. Cochez ou décochez la case **Pilote du pare-feu commun Trend Micro** pour la carte réseau.
- Activez ou désactivez le pilote de pare-feu OfficeScan à l'aide d'une invite de commande.
  a. Ouvrez une invite de commande et entrez `services.msc`.
  b. Démarrez ou arrêtez le **Pare-feu d'OfficeScan NT** dans Microsoft Management Console (MMC).

Stratégies de pare-feu

Les stratégies de pare-feu OfficeScan vous permettent de bloquer ou d'autoriser certains types de trafic réseau non spécifiés dans une exception de stratégie. Une stratégie définit également les fonctions de pare-feu qui sont activées ou désactivées. Attribuez une stratégie à un ou plusieurs profils de pare-feu.

Avec l'intégration d'Active Directory et de l'administration basée sur les rôles, chaque rôle d'utilisateur, selon les autorisations associées, peut créer, configurer ou supprimer des stratégies pour des domaines spécifiques.

Le tableau suivant décrit les tâches disponibles sur l'écran **Stratégies de pare-feu**.

TÂCHE	DESCRIPTION
Ajouter de nouvelles stratégies	Cliquez sur **Ajouter** pour créer une stratégie. Pour plus d'informations, voir *Ajout d'une stratégie de pare-feu à la page 6-6*.
Copier des paramètres de stratégies existantes	Sélectionnez une stratégie existante et cliquez sur **Copier** pour ouvrir l'écran **Copier stratégie**. Modifiez les paramètres de la stratégie si nécessaire.
Supprimer des stratégies existantes	Sélectionnez une stratégie existante, puis cliquez sur **Supprimer** pour supprimer la stratégie de la liste.
Modifier le modèle d'exception	Cliquez sur **Modifier le modèle d'exception** pour voir la liste **Modèle d'exception** actuelle. Pour plus d'informations, voir *Modification de la liste Modèle d'exception du pare-feu OfficeScan à la page 6-10*.
Modifier des stratégies existantes	Cliquez sur la **Description de la stratégie** d'une stratégie existante pour en modifier les paramètres.

Stratégies de pare-feu par défaut

OfficeScan est fourni avec un ensemble de stratégies par défaut, que vous pouvez modifier ou supprimer.

NOM DE LA STRATÉGIE	NIVEAU DE SÉCURITÉ	PARAMÈTRES DE L'AGENT	EXCEPTIONS	UTILISATION RECOMMANDÉE
Tous les accès	Faible	Activer le pare-feu	Aucun	À utiliser pour accorder aux agents un accès illimité au réseau

Nom de la stratégie	Niveau de sécurité	Paramètres de l'Agent	Exceptions	Utilisation recommandée
Ports de communication pour Trend Micro Control Manager	Faible	Activer le pare-feu	Autoriser tout le trafic TCP/UDP entrant/sortant via les ports 80 et 10319	À utiliser lorsque les agents disposent d'une installation d'agent MCP
Console ScanMail for Microsoft Exchange	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 16372	À utiliser lorsque les agents doivent accéder à la console ScanMail
Console InterScan Messaging Security Suite (IMSS)	Faible	Activer le pare-feu	Autoriser tout le trafic TCP entrant/ sortant via le port 80	À utiliser lorsque les agents doivent accéder à la console IMSS

Ajout d'une stratégie de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.
2. Sélectionnez cette option pour ajouter, copier ou modifier une stratégie.
   - Cliquez sur **Ajouter** pour créer une stratégie.
   - Sélectionnez une stratégie existante et cliquez sur **Copier** pour ouvrir l'écran **Copier stratégie**. Modifiez les paramètres de la stratégie si nécessaire.
   - Cliquez sur la **Description de la stratégie** d'une stratégie existante pour en modifier les paramètres.
3. Dans la section **Stratégie de pare-feu**, configurez les éléments suivants :
   - **Nom** : spécifiez un nom unique pour la stratégie de pare-feu d'OfficeScan.

- **Niveau de sécurité** : sélectionnez **Élevé**, **Moyen** ou **Bas** pour déterminer le type de trafic que le pare-feu OfficeScan autorise ou bloque.

Remarque

Le pare-feu OfficeScan autorise ou bloque automatiquement les connexions sur les ports spécifiés dans la liste **Modèle d'exception**.

Pour plus d'informations, voir *Modification de la liste Modèle d'exception du pare-feu OfficeScan à la page 6-10*.

4. Dans la section **Fonctions du pare-feu**, configurez les éléments suivants :

   - **Activer le pare-feu** : sélectionnez cette option pour activer le pare-feu OfficeScan pour cette stratégie.
   - **Activer le système de détection d'intrusion (SDI)** : sélectionnez cette option pour tenter d'identifier les signatures réseau pouvant indiquer une attaque.

     Pour plus d'informations, voir *Système de détection d'intrusion à la page 6-8*.
   - **Afficher une notification lorsqu'une violation du pare-feu est détectée** : sélectionnez cette option pour afficher une notification sur l'agent OfficeScan lorsque le pare-feu OfficeScan bloque un paquet sortant.

Important

Si vous attribuez à des utilisateurs l'autorisation de configurer les paramètres du pare-feu OfficeScan à l'aide de la console de l'agent OfficeScan, vous ne pouvez pas utiliser la console Web OfficeScan pour remplacer les paramètres configurés par l'utilisateur.

Les informations affichées sous **Paramètres**, sous l'onglet **Pare-feu** de la console de l'agent OfficeScan, reflètent toujours les paramètres configurés à partir de la console de l'agent OfficeScan et non de la console Web du serveur.

5. Dans la section **Liste Certified Safe Software**, configurez les éléments suivants :

   - **Activer la liste Certified Safe Software locale** : sélectionnez cette option pour autoriser le trafic réseau vers les applications que Trend Micro confirme être sûres, en utilisant la signature locale.

- **Activer la liste Certified Safe Software locale (accès à Internet requis)** : sélectionnez cette option pour autoriser le trafic réseau vers les applications que Trend Micro confirme être sûres, en utilisant la signature basée sur le cloud dynamiquement mise à jour.

Important

L'interrogation de la liste globale Certified Safe Software impose l'activation du service de prévention des modifications non autorisées et du service Certified Safe Software.

6. Dans la section **Exception**, gérez la liste Modèle d'exception qui s'applique uniquement à cette stratégie.

   Le pare-feu OfficeScan remplit automatiquement la liste des exceptions avec les entrées de la liste Modèle d'exception. Si vous ajoutez, modifiez ou supprimez une exception dans la liste des exceptions de stratégie, les modifications s'appliquent uniquement à la stratégie en cours et non à la liste Modèle d'exception.

   Pour plus d'informations sur l'ajout d'exceptions, reportez-vous à la rubrique *Ajout d'une exception de stratégie de pare-feu à la page 6-12* (suivez les instructions de l'étape 3).

7. Cliquez sur **Enregistrer**.

Système de détection d'intrusion

Le système de détection d'intrusion (SDI) contribue à identifier les fichiers de signatures contenus dans des paquets réseau pouvant indiquer une attaque de l'endpoint.

Le système de détection d'intrusion (SDI) contribue à empêcher les intrusions bien connues suivantes :

SYSTÈME	DESCRIPTION
Fragment trop important	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet TCP/UDP surdimensionné vers un Endpoint cible. Cela peut entraîner un dépassement de mémoire tampon, ce qui risque de geler ou de redémarrer l'Endpoint.

SYSTÈME	DESCRIPTION
Ping of Death	Attaque de refus de service dans le cadre de laquelle un pirate dirige un paquet ICMP/ICMPv6 surdimensionné vers un Endpoint cible. Cela peut entraîner un dépassement de mémoire tampon, ce qui risque de geler ou redémarrer l'Endpoint.
ARP conflictuel	Type d'attaque où un pirate envoie à un Endpoint cible une requête ARP (Address Resolution Protocol) avec des adresses IP source et de destination identiques. L'Endpoint cible s'envoie continuellement une réponse ARP (son adresse MAC), ce qui entraîne son gel ou son blocage.
Flux SYN	Attaque de refus de service dans le cadre de laquelle un programme envoie plusieurs paquets de synchronisation TCP (SYN) à un Endpoint. L'Endpoint envoie alors continuellement en réponse des accusés de réception de synchronisation (SYN/ACK). Cela peut épuiser la mémoire de l'Endpoint et finalement bloquer l'Endpoint.
Fragment de chevauchement	Similaire à une attaque Teardrop, cette attaque de refus de service envoie des fragments TCP de chevauchement à l'Endpoint. Par conséquent, les informations de l'en-tête sont écrasées dans le premier fragment TCP qui risque alors de passer à travers le pare-feu. Le pare-feu peut ensuite autoriser les fragments suivants contenant du code malveillant à atteindre l'Endpoint cible.
Teardrop	Similaire à une attaque de fragment de chevauchement, cette attaque de refus de service a trait à des fragments IP. Une valeur de décalage prêtant à confusion dans le deuxième fragment IP ou dans un fragment ultérieur peut provoquer le blocage du système d'exploitation de l'Endpoint récepteur lorsque celui-ci tente de réassembler les fragments.
attaque par fragment minuscule	Avec ce type d'attaque, un fragment TCP de petite taille force la première en-tête de paquet TCP dans le fragment suivant. Cela peut amener les routeurs filtrant le trafic à ignorer les fragments suivants qui peuvent contenir des données malveillantes.
IGMP fragmenté	Attaque de refus de service qui envoie des paquets IGMP fragmentés à un Endpoint cible, lequel ne peut pas les traiter correctement. Cela peut geler ou ralentir l'Endpoint.

SYSTÈME	DESCRIPTION
attaque LAND	Type d'attaque qui envoie à l'Endpoint des paquets de synchronisation IP (SYN) dont les adresses source et cible sont identiques. L'Endpoint s'envoie alors en réponse un accusé de réception de synchronisation (SYN/ACK). Cela peut geler ou ralentir l'Endpoint.

Modification de la liste Modèle d'exception du pare-feu OfficeScan

Vous pouvez utiliser l'écran **Modifier le modèle d'exception** pour gérer le trafic réseau afin d'autoriser ou de bloquer les agents OfficeScan. Le pare-feu OfficeScan fournit des exceptions par défaut que vous pouvez modifier ou supprimer.

Pour plus d'informations, voir *Exceptions de stratégie de pare-feu par défaut à la page 6-11*.

Le tableau suivant décrit les tâches disponibles sur l'écran **Modifier le modèle d'exception**.

TÂCHE	DESCRIPTION
Ajouter de nouvelles exceptions	Cliquez sur **Ajouter** pour créer une exception. Pour plus d'informations, voir *Ajout d'une exception de stratégie de pare-feu à la page 6-12*. **Important** Après l'ajout d'une nouvelle exception, vous devez enregistrer la liste **Modèle d'exception** pour appliquer la nouvelle exception. Si vous sortez de l'écran **Modifier le modèle d'exception** sans enregistrer les modifications, le pare-feu OfficeScan n'enregistre pas la nouvelle exception.
Supprimer des exceptions existantes	Sélectionnez une exception existante, puis cliquez sur **Supprimer** pour supprimer l'exception de la liste **Modèle d'exception**.

Tâche	Description
Modifier les exceptions existantes	Cliquez sur le **Nom** d'un modèle existant pour modifier les paramètres d'exception.
Réorganiser la priorité des exceptions	Cliquez sur les flèches vers le haut ou le bas en regard d'une exception pour modifier la priorité selon laquelle le pare-feu OfficeScan effectue une action sur le trafic réseau.
Enregistrer les modifications apportées à la liste d'exceptions	Cliquez sur l'un des boutons suivants pour enregistrer les modifications apportées à la liste **Modèle d'exception** : • **Enregistrer les modifications du modèle** : enregistre les paramètres du modèle d'exception actuel mais n'applique pas les paramètres aux stratégies existantes • **Enregistrer et appliquer aux stratégies existantes** : enregistre les paramètres du modèle d'exception actuel et applique immédiatement les paramètres à toutes les stratégies existantes

Exceptions de stratégie de pare-feu par défaut

Nom de l'exception	Action	Protocole	Port	Direction
DNS	Autoriser	TCP/UDP	53	Entrant et sortant
NetBIOS	Autoriser	TCP/UDP	137, 138, 139, 445	Entrant et sortant
HTTPS	Autoriser	TCP	443	Entrant et sortant
HTTP	Autoriser	TCP	80	Entrant et sortant
Telnet	Autoriser	TCP	23	Entrant et sortant
SMTP	Autoriser	TCP	25	Entrant et sortant

Nom de l'exception	Action	Protocole	Port	Direction
FTP	Autoriser	TCP	21	Entrant et sortant
POP3	Autoriser	TCP	110	Entrant et sortant
LDAP	Autoriser	TCP/UDP	389	Entrant et sortant

Remarque

Les exceptions par défaut s'appliquent à tous les agents. Si vous souhaitez qu'une exception par défaut s'applique uniquement à certains agents, modifiez-la et indiquez les adresses IP de ces agents.

L'exception LDAP n'est pas disponible si vous effectuez une mise à niveau à partir d'une version précédente d'OfficeScan. Ajoutez cette exception manuellement si vous ne la voyez pas dans la liste d'exceptions.

Ajout d'une exception de stratégie de pare-feu

Lors de l'ajout de nouvelles exceptions, assurez-vous de ne pas bloquer les ports utilisés pour la communication entre le serveur OfficeScan et l'agents OfficeScan.

Vous pouvez localiser les ports d'écoute utilisés par le serveur OfficeScan et les agents OfficeScan de la manière suivante :

- Port d'écoute du serveur : accédez à **Administration** > **Paramètres** > **Connexion de l'agent**. Le numéro de port se trouve sous **Paramètres de connexion de l'agent**.
- Port d'écoute de agent OfficeScan : accédez à **Agents** > **Gestion des agents** > **État**. Le numéro de port se trouve sous **Informations de base**.

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Stratégies**.

2. Cliquez sur **Modifier le modèle d'exception**.
3. Cliquez sur **Ajouter**.
4. Entrez un nom pour l'exception de stratégie.
5. Sélectionnez le type d'application. Vous pouvez sélectionner toutes les applications ou spécifier un chemin d'application ou des clés de registre.

Remarque

Vérifiez le nom et les chemins complets saisis. L'exception d'application ne prend pas en charge les caractères génériques.

6. Sélectionnez l'action qu'OfficeScan effectue sur le trafic réseau (bloquer ou autoriser le trafic qui répond aux critères d'exception) et la direction du trafic (trafic réseau entrant ou sortant sur l'Endpoint agent OfficeScan).
7. Sélectionnez le type de protocole réseau : TCP, UDP, ICMP ou ICMPv6.
8. Spécifiez les ports de l'Endpoint agent OfficeScan sur lesquels effectuer l'action.
9. Sélectionnez les adresses IP d'Endpoints agent OfficeScan à inclure dans l'exception.

   Par exemple, si vous choisissez de refuser tout le trafic réseau (entrant et sortant) et que vous saisissez l'adresse IP d'un seul Endpoint sur le réseau, tout agent OfficeScan dont la stratégie contient cette exception ne peut pas envoyer de données vers cette adresse IP ni en recevoir de celle-ci.

   - **Toutes les adresses IP** : inclut toutes les adresses IP.
   - **Adresse IP unique** : saisissez une adresse IPv4 ou IPv6, ou un nom d'hôte.
   - **Plage (pour IPv4 ou IPv6)** : saisissez une plage d'adresses IPv4 ou IPv6.
   - **Plage (pour IPv6)** : saisissez un préfixe et une longueur d'adresse IPv6.
   - **Masque de sous-réseau** : saisissez une adresse IPv4 et son masque de sous-réseau.
10. Cliquez sur **Enregistrer**.

L'écran **Modifier le modèle d'exception** s'ouvre avec la nouvelle exception ajoutée.

11. Cliquez sur l'un des boutons suivants pour appliquer la nouvelle exception à la liste :

    - **Enregistrer les modifications du modèle** : enregistre les paramètres du modèle d'exception actuel mais n'applique pas les paramètres aux stratégies existantes
    - **Enregistrer et appliquer aux stratégies existantes** : enregistre les paramètres du modèle d'exception actuel et applique immédiatement les paramètres à toutes les stratégies existantes

Profils de pare-feu

Les profils de pare-feu OfficeScan définissent quels agents OfficeScan appliquent une stratégie de pare-feu OfficeScan particulière. Créez des rôles utilisateur qui peuvent créer, configurer ou supprimer des profils pour des domaines spécifiques.

Le tableau suivant présente les tâches disponibles sur l'écran **Profils de pare-feu**.

TÂCHE	DESCRIPTION
Remplacez les paramètres de pare-feu de l'agent OfficeScan	Sélectionnez **Écraser le niveau de sécurité/la liste des exceptions de l'agent** pour remplacer les paramètres de profils de l'agent OfficeScan par les paramètres du serveur. **Important** Seuls les utilisateurs connectés à l'aide du compte administrateur intégré ou les utilisateurs disposant d'autorisations de gestion complètes peuvent activer l'option **Écraser le niveau de sécurité/la liste des exceptions de l'agent**.

TÂCHE	DESCRIPTION
Ajouter de nouveaux profils	Cliquez sur **Ajouter** pour créer un profil. Pour plus d'informations, voir *Ajout d'un profil de pare-feu à la page 6-16*.
Supprimer des profils existants	Sélectionnez un profil existant et cliquez sur **Supprimer** pour supprimer le profil de la liste.
Modifier la liste des serveurs de référence	Cliquez sur **Modifier la liste des serveurs de référence** pour définir les paramètres d'emplacement d'Endpoint. Le pare-feu OfficeScan utilise la liste de serveurs de référence pour déterminer si un Endpoint se trouve dans un réseau interne ou externe. **Important** Seuls les utilisateurs connectés à l'aide du compte administrateur intégré ou ceux disposant d'autorisations de gestion complètes peuvent voir et configurer la liste des serveurs de référence. Pour plus d'informations, voir *Serveurs de référence à la page 4-28*.
Modifier des profils existants	Cliquez sur le **Nom** d'un profil existant pour en modifier les paramètres.
Réorganiser la priorité des profils	Cliquez sur les flèches vers le haut ou le bas en regard d'un profil pour modifier la priorité selon laquelle le pare-feu OfficeScan effectue une action sur les agents OfficeScan. **Important** Les Endpoints des agents OfficeScan qui correspondent à plusieurs définitions de profil appliquent uniquement les paramètres du profil ayant la plus haute priorité.
Envoyer les paramètres de profil aux agents OfficeScan	Cliquez sur **Appliquer les profils aux agents** pour déployer les paramètres de profils de pare-feu OfficeScan sur les agents OfficeScan.

Ajout d'un profil de pare-feu

Procédure

1. Accédez à **Agents** > **Pare-feu** > **Profils**.
2. Sélectionnez cette option pour ajouter ou modifier un profil.
   - Cliquez sur **Ajouter** pour créer un profil.
   - Cliquez sur le **Nom** d'un profil existant pour en modifier les paramètres.
3. Sélectionnez **Activer ce profil** pour autoriser OfficeScan à déployer le profil sur les agents OfficeScan.
4. Dans la section **Paramètres des profils**, configurez les options suivantes :
   - **Nom** : saisissez un nom unique pour le profil.
   - **Description** : (facultatif) saisissez une description pour le profil.
   - **Stratégie** : sélectionnez une stratégie de pare-feu OfficeScan existante à appliquer au profil.

     Pour plus d'informations, voir *Stratégies de pare-feu à la page 6-4*.
   - Sélectionnez les critères que le pare-feu OfficeScan utilise pour définir les agents OfficeScan auxquels le profil s'applique.

CRITÈRES	DESCRIPTION
Endpoint	Sélectionnez cette option pour appliquer le profil aux agents OfficeScan sélectionnés depuis l'arborescence des agents. Cliquez sur **Sélectionner des Endpoints dans l'arborescence des agents** pour ouvrir l'écran **Paramètres de profil de pare-feu**. Sélectionnez les agents OfficeScan requis et cliquez sur **Sélectionner**.

CRITÈRES	DESCRIPTION
Plate-forme	Sélectionnez cette option pour appliquer le profil à des types de système d'exploitation spécifiques. • **Plates-formes Windows Server prises en charge** • **Plates-formes de postes de travail Windows prises en charge** Pour obtenir une liste de systèmes d'exploitation pris en charge, consultez le document *Configuration système requise d'OfficeScan*.
Nom de connexion	Sélectionnez cette option pour appliquer le profil à certains utilisateurs spécifiques connectés à des Endpoints. Spécifiez le nom de connexion d'utilisateurs particuliers. Le pare-feu OfficeScan applique le profil sur les agents OfficeScan sur lesquels les utilisateurs spécifiés sont connectés.
Description de la carte d'interface réseau	Sélectionnez cette option pour appliquer le profil aux Endpoints qui utilisent des cartes d'interface réseau (NIC) spécifiques. Saisissez une description de carte d'interface réseau complète ou partielle. **Conseil** Trend Micro recommande de saisir le fabricant de la carte d'interface réseau (NIC), car les descriptions NIC commencent en général par le nom du fabricant. Par exemple, si vous saisissez « Intel », toutes les cartes d'interface réseau fabriquées par Intel remplissent les critères. Si vous saisissez un modèle de carte d'interface réseau particulier, par exemple « Intel(R) Pro/100 », seules les descriptions NIC commençant par « Intel(R) Pro/100 » remplissent les critères.

CRITÈRES	DESCRIPTION
Emplacement de l'agent	Sélectionnez cette option pour appliquer le profil en fonction de l'état de connexion de l'agent OfficeScan. • **Internes : les agents OfficeScan peuvent se connecter à un serveur de référence configuré** **Remarque** Cliquez sur **Modifier la liste de serveurs de référence** pour configurer les paramètres d'emplacement. Pour plus d'informations, voir *Serveurs de référence à la page 4-28*. • **Externes : les agents OfficeScan ne peuvent pas se connecter à un serveur de référence configuré**

5. Dans la section **Privilèges d'utilisateur**, configurez les options suivantes :

   - **Autoriser l'utilisateur à modifier le niveau de sécurité** : sélectionnez cette option pour permettre aux utilisateurs de définir le niveau de sécurité du pare-feu OfficeScan à l'aide de la console de l'agent OfficeScan
   - **Autoriser l'utilisateur à modifier les exceptions de stratégie** : sélectionnez cette option pour permettre aux utilisateurs de définir des exceptions de stratégie de pare-feu OfficeScan personnalisées à l'aide de la console de l'agent OfficeScan

   Important

   Seuls les agents OfficeScan disposant du privilège **Afficher les paramètres du pare-feu sur la console de l'agent OfficeScan** affichent les paramètres du pare-feu sur la console agent OfficeScan.

6. Cliquez sur **Enregistrer**.

   Le profil s'affiche dans la liste Profils de pare-feu.

7. Cliquez sur **Appliquer les profils aux agents** pour envoyer les profils mis à jour aux agents OfficeScan.

Configuration des paramètres généraux de pare-feu

Procédure

1. Accédez à **Agents** > **Paramètres généraux de l'agent**.
2. Cliquez sur l'onglet **Paramètres de sécurité**.
   a. Rendez-vous à la section **Paramètres du pare-feu**.
   b. Configurez les paramètres selon les besoins.
      - **Envoyer les journaux de pare-feu au serveur toutes/tous les** : définit la fréquence à laquelle les agents OfficeScan dotés du privilège **Autoriser les agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan** envoient des journaux de pare-feu au serveur

        Remarque

        Vous pouvez octroyer le privilège **Autoriser des agents OfficeScan à envoyer les journaux du pare-feu au serveur OfficeScan** dans l'onglet **Privilèges** de l'écran **Privilèges et autres paramètres**.

      - **Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système** : empêche l'agent OfficeScan de tenter de mettre à jour le pilote du pare-feu commun pendant les opérations normales
      - **Envoyer au serveur OfficeScan le nombre d'entrées du journal du pare-feu toutes les heures pour déterminer la possibilité d'une épidémie au niveau du pare-feu** : permet à l'agent OfficeScan d'envoyer des nombres de détections de pare-feu à OfficeScan toutes les heures

3. Cliquez sur l'onglet **Système**.

   a. Accédez à la section **Paramètres de Certified Safe Software Service**.

   b. Configurez les paramètres selon les besoins.

      - **Activer Certified Safe Software Service pour la surveillance des comportements, le pare-feu et les scans antivirus** : interroge les centres de données Trend Micro pour vérifier la sécurité d'un programme détecté par blocage des comportements de malwares, surveillance des événements, pare-feu ou antivirus pour réduire la probabilité de faux positifs

4. Cliquez sur **Enregistrer**.

Configuration des notifications de pare-feu pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après que le pare-feu OfficeScan a bloqué un trafic sortant enfreignant la stratégie du pare-feu.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations du pare-feu**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Test du pare-feu OfficeScan

Pour garantir le bon fonctionnement du pare-feu OfficeScan, effectuez un test sur un agent OfficeScan ou un groupe d'agents OfficeScan.

AVERTISSEMENT!

Testez les paramètres du programme de l'agent OfficeScan dans un environnement contrôlé uniquement. N'effectuez aucun test sur des endpoints connectés au réseau ou à Internet. Vous risqueriez d'exposer les endpoints des agents OfficeScan aux virus, aux attaques pirates et à d'autres risques.

Procédure

1. Créez et enregistrez une stratégie de test. Configurez les paramètres pour bloquer les types de trafic que vous souhaitez tester. Par exemple, pour empêcher l'agent OfficeScan d'accéder à Internet, procédez comme suit :

   a. Configurez le niveau de sécurité sur **Faible** (Autoriser tout le trafic entrant/sortant).

   b. Sélectionnez **Activer le pare-feu et Avertir les utilisateurs en cas de violation du pare-feu**.

   c. Créez une exception bloquant le trafic HTTP (ou HTTPS).

2. Créez et enregistrez un profil de test en sélectionnant les agents sur lesquels vous souhaitez tester les fonctions du pare-feu. Associez la stratégie de test au profil de test.

3. Cliquez sur **Affecter un profil aux agents**.

4. Vérifiez le déploiement.

   a. Cliquez sur **Agents** > **Gestion des agents**.

   b. Sélectionnez le domaine auquel l'agent appartient.

   c. Sélectionnez **Affichage Pare-feu** dans l'affichage de l'arborescence des agents.

   d. Vérifiez la présence d'une coche verte dans la colonne **Pare-feu** de l'arborescence des agents. Si vous avez activé le système de détection d'intrusion pour cet agent, vérifiez qu'une coche verte est également présente sous la colonne **SDI**.

e. Vérifiez que l'agent applique la bonne stratégie de pare-feu. La stratégie apparaît dans la colonne **Stratégie de pare-feu** dans l'arborescence des agents.

5. Testez le pare-feu sur le endpoint de l'agent en essayant d'envoyer ou de recevoir le type de trafic que vous avez configuré dans la stratégie.

6. Pour tester une stratégie configurée pour empêcher l'agent d'accéder à Internet, ouvrez un navigateur Web sur le endpoint de l'agent. Si vous avez configuré OfficeScan pour qu'il affiche un message de notification pour les violations de pare-feu, le message s'affiche sur le endpoint de l'agent lorsqu'une violation de trafic sortant se produit.

Chapitre 7

Utilisation de la prévention des épidémies

Cette section décrit les épidémies de risques pour la sécurité qui se déclarent lorsque les détections de virus/programmes malveillants, spywares/graywares et sessions de partage de dossiers dépassent le seuil défini sur une certaine période.

Les rubriques sont les suivantes :

Stratégies de prévention des épidémies

Lorsqu'une épidémie se produit, appliquez l'une des stratégies suivantes :

Limitation/interdiction de l'accès aux dossiers partagés

Pendant les épidémies, vous pouvez limiter ou interdire l'accès aux dossiers partagés sur le réseau pour empêcher la propagation des risques de sécurité à travers les dossiers partagés.

Lorsque cette stratégie entre en vigueur, les utilisateurs peuvent continuer de partager des dossiers mais elle ne s'applique pas aux dossiers qui viennent d'être partagés. Vous devez donc informer les utilisateurs pour qu'ils ne partagent pas les dossiers au cours d'une épidémie ou déployer de nouveau la stratégie pour l'appliquer aux dossiers qui viennent d'être partagés.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Limitation/interdiction de l'accès aux dossiers partagés**.
5. Sélectionnez l'une des options suivantes :

- **Autoriser l'accès en lecture seule** : limite l'accès aux dossiers partagés
- **Refuser l'accès**

Remarque

le paramètre d'accès en lecture seule ne s'applique pas aux dossiers partagés déjà configurés pour interdire tout accès.

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Blocage des ports vulnérables

Pendant les épidémies, bloquez les ports vulnérables que les virus/programmes malveillants pourraient exploiter pour accéder aux endpoints agent OfficeScan.

AVERTISSEMENT!

Configurez alors les paramètres de prévention des épidémies avec soin. Le blocage des ports utilisés rendra indisponibles les services réseau qui dépendent de ces ports. Par exemple, si vous bloquez le port sécurisé, OfficeScan ne peut plus communiquer avec l'agent pendant l'épidémie.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.

4. Cliquez sur **Blocage des ports**.
5. Sélectionnez **Bloquer un port sécurisé**.
6. Sélectionnez les ports à bloquer dans la colonne **Ports bloqués**.
   a. Si aucun port ne figure dans le tableau, cliquez sur **Ajouter**. Dans l'écran qui s'affiche, sélectionnez les ports à bloquer puis cliquez sur **Enregistrer**.
      - **Tous les ports (y compris ICMP)** :bloque tous les ports sauf le port sécurisé. Pour bloquer également le port sécurisé, cochez la case Bloquer le port sécurisé dans l'écran précédent.
      - **Ports spécifiés**
        - **Ports fréquemment utilisés** :sélectionnez au moins un numéro de port pour permettre à OfficeScan d'enregistrer les paramètres de blocage des ports.
        - **Ports fréquemment utilisés par les chevaux de Troie** :bloque les ports habituellement utilisés par les programmes de type Cheval de Troie.
        - **Tout numéro de port compris entre 1 et 65535 ou une plage de ports** :vous pouvez indiquer de façon facultative la direction du trafic à bloquer et certains commentaires, comme la raison pour laquelle vous bloquez les ports spécifiés.
        - **Protocole ping (Rejeter ICMP)** :cliquez sur cette option pour bloquer uniquement les paquets ICMP, tels que les requêtes ping.

   b. Pour modifier les paramètres du ou des ports bloqués, cliquez sur le numéro du port.
   c. Dans l'écran qui s'affiche, modifiez les paramètres puis cliquez sur **Enregistrer**.
   d. Pour supprimer un port de la liste, sélectionnez la case à cocher en regard du numéro de port puis cliquez sur **Supprimer**.
7. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

8. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Interdiction de l'accès en écriture aux fichiers et dossiers

Les virus/programmes malveillants peuvent modifier ou supprimer les fichiers et les dossiers des endpoints hôtes. En cas d'épidémie, configurez OfficeScan de telle sorte que les virus/programmes malveillants ne puissent pas modifier ou supprimer des fichiers et dossiers sur les endpoints des agents OfficeScan. .

AVERTISSEMENT!

OfficeScan ne prend pas en charge l'interdiction du droit en écriture sur des lecteurs réseau mappés.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Interdire l'accès en écriture aux fichiers et dossiers**.
5. Entrez le chemin du répertoire. Lorsque vous aurez saisi le chemin d'accès au répertoire que vous souhaitez protéger, cliquez sur **Ajouter**.

   Remarque

   Saisissez le chemin d'accès absolu au répertoire, et non le chemin d'accès virtuel.

6. Spécifiez les fichiers à protéger dans les répertoires protégés. Sélectionnez tous les fichiers ou uniquement les fichiers avec une extension déterminée. Pour les extensions de fichiers, spécifiez une extension qui ne figure pas dans la liste proposée en la saisissant dans la zone de texte, puis en cliquant sur **Ajouter**.

7. Pour protéger des fichiers spécifiques, sous **Fichiers à protéger**, entrez le nom de fichier complet et cliquez sur **Ajouter**.

8. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

9. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Refus de l'accès aux fichiers compressés exécutables

Lorsqu'une épidémie se déclare, il est préférable de refuser l'accès aux fichiers compressés exécutables afin d'éviter la propagation sur l'ensemble du réseau du risque de sécurité que ces fichiers peuvent potentiellement représenter. Vous pouvez décider d'autoriser l'accès aux fichiers sécurisés créés par les programmes de compression de fichiers exécutables pris en charge.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Démarrer la prévention des épidémies**.

4. Cliquez sur **Refuser l'accès aux fichiers compressés exécutables**.

5. Faites votre choix dans la liste des programmes de compression de fichiers exécutables pris en charge, puis cliquez sur **Ajouter** pour autoriser l'accès aux fichiers compressés exécutables créés par ces programmes.

   Remarque

   Vous pouvez uniquement approuver l'utilisation des fichiers compressés créés par les programmes de compression qui se trouvent dans la liste. La prévention des épidémies refuse l'accès à tout autre format de fichier compressé exécutable.

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants

Vous pouvez configurer la prévention des épidémies afin d'assurer la protection contre les menaces de sécurité qui utilisent des processus mutex en écrasant les ressources requises par la menace pour parvenir à infecter le système et s'y propager. La prévention des épidémies crée des règles d'exclusion mutuelle pour les fichiers et processus associés à des programmes malveillants connus, empêchant ainsi ces programmes malveillants d'accéder à ces ressources.

Conseil

Trend Micro recommande la conservation de ces exclusions jusqu'à la mise en œuvre d'une solution durable contre ces menaces liées à des programmes malveillants. Contactez l'assistance pour obtenir le nom des mutex permettant d'assurer une protection lors d'épidémies.

Remarque

La gestion des exclusions mutuelles requiert le service de prévention des modifications non autorisées et prend uniquement en charge les plates-formes 32 bits.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.

2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Démarrer la prévention des épidémies**.
4. Cliquez sur **Créer une règle de traitement par exclusion mutuelle (mutex) pour les fichiers/processus de programmes malveillants**.
5. Saisissez le nom du mutex contre lequel assurer une protection dans la zone de texte prévue à cet effet.

   Ajoutez ou supprimez des noms de mutex dans la liste à l'aide des boutons **+** et **-**.

   Remarque

   La prévention des épidémies prend en charge la gestion des exclusions mutuelles sur un maximum de six menaces mutex.

6. Cliquez sur **Enregistrer**.

   L'écran **Paramètres de prévention des épidémies** s'affiche de nouveau.

7. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

Configuration de la prévention des épidémies de risques liés à la sécurité

Lorsqu'une épidémie se produit, appliquez les mesures de prévention des épidémies pour répondre à l'épidémie et la contenir. Configurez soigneusement les paramètres de prévention car une mauvaise configuration peut entraîner des problèmes de réseau imprévus.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.

3. Cliquez sur **Démarrer la prévention des épidémies**.

4. Cliquez sur l'une des stratégies suivantes de prévention des épidémies, puis configurez les paramètres qui s'y appliquent :

   - *Limitation/interdiction de l'accès aux dossiers partagés à la page 7-2*
   - *Blocage des ports vulnérables à la page 7-3*
   - *Interdiction de l'accès en écriture aux fichiers et dossiers à la page 7-5*
   - *Refus de l'accès aux fichiers compressés exécutables à la page 7-6*
   - *Création d'une règle de traitement par exclusion mutuelle pour les fichiers/processus de programmes malveillants à la page 7-7*

5. Sélectionnez les stratégies à appliquer.

6. Sélectionnez le nombre d'heures pendant lesquelles la prévention des épidémies sera active. La valeur par défaut est fixée à 48 heures. Vous pouvez restaurer manuellement les paramètres du réseau avant l'expiration de la période de prévention des épidémies.

   AVERTISSEMENT!

   N'autorisez pas l'activation permanente de la prévention des épidémies. Pour bloquer ou refuser l'accès à certains fichiers, dossiers ou ports jusqu'à nouvel ordre, modifiez directement les paramètres du endpoint et du réseau au lieu d'utiliser OfficeScan.

7. Acceptez ou modifiez le message de notification de l'agent par défaut.

   Remarque

   Pour configurer OfficeScan afin de recevoir une notification lors d'une épidémie, accédez à **Administration** > **Notifications** > **Épidémie**.

8. Cliquez sur **Démarrer la prévention des épidémies**.

   Les mesures de prévention des épidémies que vous avez sélectionnées s'affichent dans une nouvelle fenêtre.

9. De retour dans l'arborescence des agents, observez la colonne **Prévention des épidémies**.

Une coche apparaît sur les endpoints qui appliquent des mesures de prévention des épidémies.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux agentss des notifications leur demandant d'activer cette fonctionnalité)
- Événement lié aux agents OfficeScan (qui activent la prévention des épidémies)

Désactivation de la prévention des épidémies

Si vous êtes absolument certain que l'épidémie détectée a été contenue et qu'OfficeScan a déjà nettoyé ou mis en quarantaine tous les fichiers infectés, rétablissez les valeurs normales de vos paramètres réseau en désactivant la fonction de prévention des épidémies.

Procédure

1. Accédez à **Agents** > **Prévention des épidémies**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine () pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Rétablir les paramètres**.
4. Pour faire savoir aux utilisateurs que l'épidémie est terminée, sélectionnez **Avertir les utilisateurs une fois les paramètres d'origine restaurés**.
5. Acceptez ou modifiez le message de notification de l'agent par défaut.
6. Cliquez sur **Rétablir les paramètres**.

Remarque

Si vous ne restaurez pas les paramètres réseau manuellement, OfficeScan les restaure automatiquement après expiration du nombre d'heures spécifié dans **Restaurer automatiquement les paramètres initiaux du réseau après __ heures** dans l'écran **Paramètres de prévention des épidémies**. La valeur par défaut est fixée à 48 heures.

OfficeScan consigne les événements suivants dans les journaux d'événements du système :

- Événements liés aux serveurs (qui lancent le processus de prévention des épidémies et envoient aux agents OfficeScans des notifications leur demandant d'activer cette fonctionnalité)
- Événement lié aux agents OfficeScan (qui activent la prévention des épidémies)

7. Après avoir désactivé la prévention des épidémies, recherchez les risques de sécurité sur les endpoints en réseau pour vous assurer que l'épidémie a été contenue.

Partie IV

Surveillance d'OfficeScan

Chapitre 8

Tableau de bord

Ce chapitre présente le tableau de bord OfficeScan et les widgets disponibles. Le tableau de bord fournit un aperçu de l'état de sécurité de votre réseau.

Les rubriques sont les suivantes :

Onglets et widgets

Les widgets constituent les composants centraux du tableau de bord. Les widgets fournissent des informations spécifiques sur les différents événements liés à la sécurité. Certains widgets vous permettent d'exécuter certaines tâches, telles que la mise à jour de vieux composants.

Les informations fournies par les widgets proviennent des sources suivantes :

- Serveur et agents OfficeScan
- solutions plugicielles et leurs agents
- Trend Micro Smart Protection Network

Remarque

Activez Smart Feedback afin d'afficher les données de Smart Protection Network. Pour plus d'informations sur Smart Feedback, voir *Smart Feedback à la page 12-2*.

Les onglets fournissent un endroit pour accueillir les widgets. Le **Tableau de bord** peut contenir un maximum de 30 onglets.

Utilisation des onglets

Gérez les onglets en ajoutant, renommant, modifiant la disposition, supprimant et basculant automatiquement entre les vues des onglets.

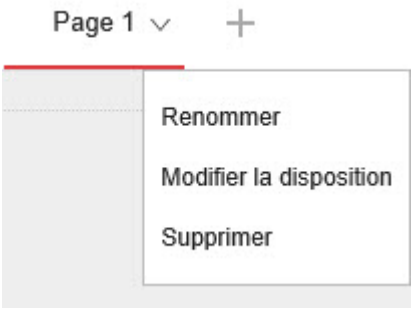
Procédure

1. Accédez à **Tableau de bord**.
2. Pour ajouter un onglet :
   a. Cliquez sur l'icône Ajouter.

b. Entrez un nom pour le nouvel onglet.

3. Pour renommer un onglet :

a. Passez le curseur au-dessus du nom de l'onglet et cliquez sur la flèche vers le bas.



b. Cliquez sur **Renommer** et tapez le nouveau nom de l'onglet.

4. Pour modifier la disposition des widgets d'un onglet :

a. Passez le curseur au-dessus du nom de l'onglet et cliquez sur la flèche vers le bas.

b. Cliquez sur **Modifier la disposition**.

c. Sélectionnez la nouvelle disposition dans l'écran qui s'affiche.

d. Cliquez sur **Enregistrer**.

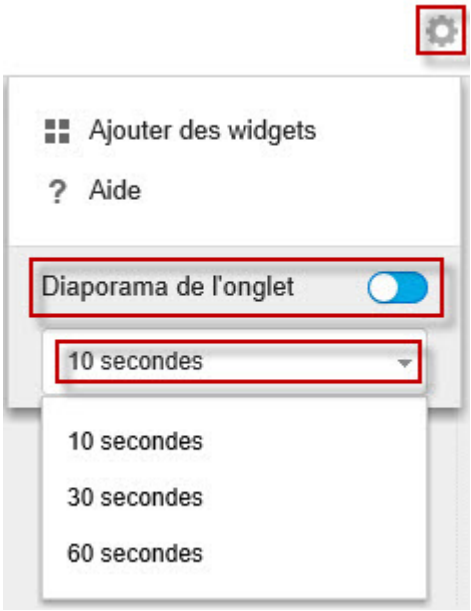
5. Pour supprimer un onglet :

a. Passez le curseur au-dessus du nom de l'onglet et cliquez sur la flèche vers le bas.

b. Cliquez sur **Supprimer** et confirmez.

6. Pour lire un diaporama de l'onglet :

a. Cliquez sur le bouton **Paramètres** à droite de l'onglet.



b. Activez le contrôle **Diaporama de l'onglet**.

c. Sélectionnez la durée d'affichage de chaque onglet avant le passage à l'onglet suivant.

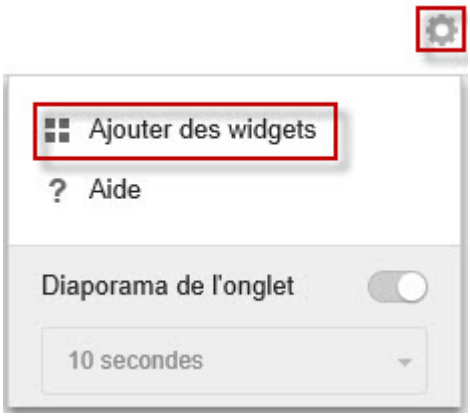
Utilisation des widgets

Gérer les widgets par ajout, déplacement, redimensionnement, changement de nom et suppression des éléments.

Procédure

1. Accédez à **Tableau de bord**.
2. Cliquez sur un onglet.
3. Pour ajouter un widget :

a. Cliquez sur le bouton **Paramètres** à droite de l'onglet.



b. Cliquez sur **Ajouter des widgets**.

c. Sélectionnez les widgets à ajouter.

- Dans la liste déroulante au-dessus des widgets, sélectionnez une catégorie pour mieux cibler les sélections.
- Utilisez la zone de recherche de texte située en haut de l'écran afin de rechercher un widget spécifique.

d. Cliquez sur **Ajouter**.

4. Pour déplacer un widget vers un nouvel emplacement dans le même onglet, faites glisser un widget vers un nouvel emplacement.

5. Redimensionnez un widget dans un onglet à plusieurs colonnes en pointant le curseur sur la bordure droite du widget, puis en déplaçant le curseur vers la gauche ou la droite.

6. Pour renommer un widget :

a. Cliquez sur l'icône des paramètres (>).

b. Saisissez le nouveau titre.

Remarque

Pour certains widgets, par exemple **Mashup d'OfficeScan et des plug-ins**, des éléments liés aux widgets peuvent être modifiés.

c. Cliquez sur **Enregistrer**.

7. Pour supprimer un widget, cliquez sur l'icône Supprimer (>).

Widgets de l'onglet Récapitulatif

L'onglet **Résumé** fournit une vue d'ensemble de l'état de sécurité de tous les agents OfficeScan de votre réseau.

Important

Le serveur OfficeScan enregistre toutes les données dans le fuseau horaire UTC-06:00 (Amérique centrale), quel que soit l'emplacement de l'Endpoint. Pour déterminer l'heure à laquelle un événement s'est produit dans votre fuseau horaire, vous devez manuellement convertir la date/heure enregistrée.

Remarque

Vous ne pouvez pas ajouter, supprimer ou modifier les widgets qui s'affichent dans l'onglet **Résumé**.

Widgets disponibles :

- *Détections de menaces globales et widget Violations de stratégie à la page 8-7*
- *Widget d'état d'endpoint à la page 8-8*
- *Widget Récapitulatif des ransomwares à la page 8-9*
- *Widget Principales détections de ransomware à la page 8-13*
- *Widget Détection des risques de sécurité dans le temps à la page 8-14*

Détections de menaces globales et widget Violations de stratégie

Ce widget fournit une vue d'ensemble de toutes les détections de menaces et les violations de stratégie sur le réseau au cours des dernières 24 heures.

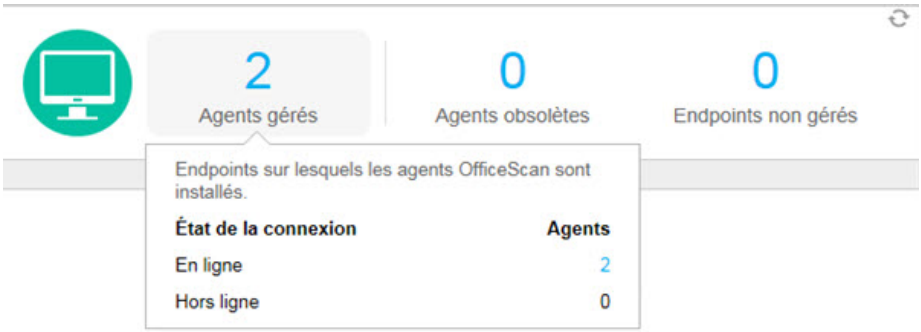
Survolez avec la souris le nombre de menaces ou de violations pour afficher le détail des types spécifiques de détections qui se sont produites pour chaque groupe. Pour afficher les journaux pour une fonctionnalité spécifique, cliquez sur le nombre à droite.

TABLEAU 8-1. Catégories de détection

CATÉGORIE	DESCRIPTION
Menaces connues	Affiche toutes les fonctionnalités qui détectent des menaces de sécurité confirmées par Trend Micro • Virus/programmes malveillants • Spyware/Grayware • Web Reputation

CATÉGORIE	DESCRIPTION
Menaces inconnues	Affiche toutes les fonctionnalités qui détectent les menaces potentielles à l'aide de techniques heuristiques avancées, d'analyses ou de modélisation de fonctionnalités • Apprentissage automatique prédictif • Surveillance des comportements • Connexions suspectes • Objets de fichiers suspects
Violations de stratégie	Affiche toutes les fonctionnalités qui contiennent des violations de stratégie spécifiques à vos normes de sécurité d'entreprise • Pare-feu • Contrôle des dispositifs • Prévention contre la perte de données

Widget d'état d'endpoint



Ce widget fournit une vue d'ensemble de la connexion et de l'état de mise à jour des agents OfficeScan sur votre réseau.

Passez la souris sur un nombre pour afficher le détail des différents états. Pour afficher les journaux d'un état spécifique, cliquez sur le nombre à droite.

TABLEAU 8-2. Groupes d'agents/endpoints

GROUPE	DESCRIPTION
Agents gérés	Affiche le dernier état de connexion signalé des agents OfficeScan sur votre réseau • En ligne • Hors ligne
Agents obsolètes	Affiche une liste de catégories de composants et le nombre d'agents OfficeScan comportant un composant obsolète dans chaque catégorie.

Widget Récapitulatif des ransomwares

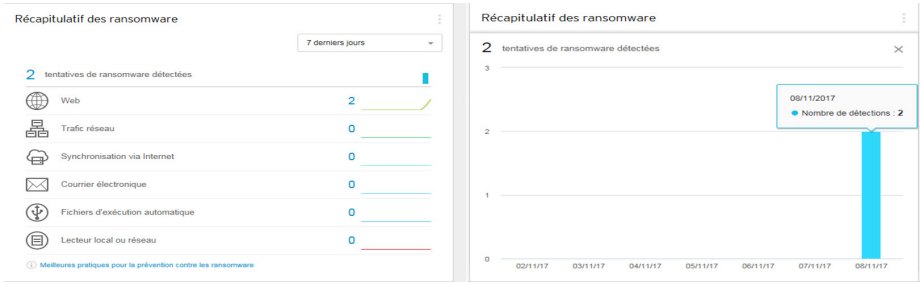


FIGURE 8-1. Affichage par défaut présentant toutes les données des ransomwares et une vue agrandie du graphique à barres « Tentatives d'exécution de ransomwares détectées »

Ce widget fournit une vue d'ensemble de toutes les attaques de ransomwares survenues sur la période spécifiée.

La vue par défaut affiche un résumé de toutes les détections de ransomwares et classe par catégorie les tentatives sur la base du canal de l'infection.

- Cliquez sur le nombre de détections de ransomwares dans la vue par défaut pour ouvrir l'écran **Risques de sécurité - ransomwares** répertoriant les détails de la détection des ransomwares.

Cliquez sur un des graphiques sur le côté droit du widget pour afficher une vue agrandie des données du graphique.

- Passez le curseur de la souris au-dessus du ou des nœuds d'un jour particulier pour afficher le nombre total de détections correspondant à la catégorie de détection affichée. Cliquez sur un nœud pour revenir à l'écran **Risques de sécurité - ransomwares** répertoriant les détails de la détection des ransomwares pour ce jour particulier.

TABLEAU 8-3. Canaux de détection de ransomwares

CANAL	DESCRIPTION	DÉTECTÉ PAR
Web	Fichiers téléchargés à l'aide d'un client Web (par exemple, un navigateur ou un client FTP)	• Web Reputation • Scan en temps réel • Surveillance des comportements
Trafic réseau	Ransomwares détectés par la fonctionnalité Connexions suspectes	• Connexions suspectes
Synchronisation via Internet	Fichiers synchronisés avec le dossier de synchronisation local par les services Cloud Storage Service pris en charge suivants : • Microsoft™ OneDrive™ • Box	• Scan en temps réel • Surveillance des comportements • Apprentissage automatique prédictif

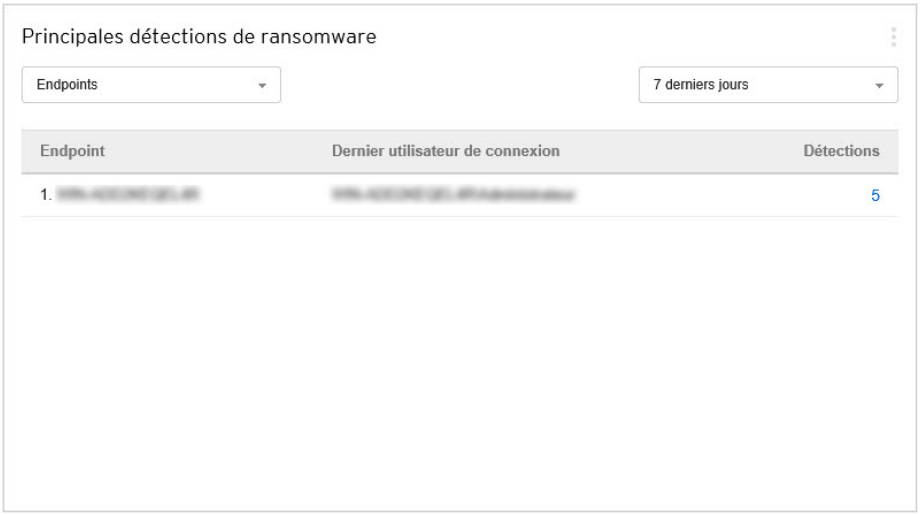
CANAL	DESCRIPTION	DÉTECTÉ PAR
Courrier électronique	Pièces jointes d'e-mail ouvertes à l'aide de Microsoft Outlook **Remarque** OfficeScan classe toutes les pièces jointes ouvertes à l'aide d'autres applications clientes de messagerie dans le canal **Lecteur local ou réseau**.	• Scan en temps réel • Surveillance des comportements
Fichiers d'exécution automatique	Programmes situés sur des lecteurs de stockage amovibles et exécutés par un fichier d'exécution automatique **Remarque** OfficeScan classe tous les autres fichiers/programmes non exécutés par le programme d'exécution automatique sur les périphériques de stockage amovibles dans le canal **Lecteur local ou réseau**.	• Scan en temps réel • Surveillance des comportements
Lecteur local ou réseau	Ransomwares détectés sur des lecteurs locaux ou réseau, notamment : • Pièces jointes d'e-mail ouvertes à l'aide de clients de messagerie autres que Microsoft Outlook • Fichiers sur des périphériques de stockage amovibles non exécutés par le programme d'exécution automatique	• Scan en temps réel • Scan manuel • Scan programmé • Scan immédiat • Surveillance des comportements

Journaux Menaces de sécurité - Ransomware

Les journaux Menaces de sécurité - Ransomware présentent toutes les menaces de ransomware détectées sur votre réseau, quel que soit le type de scan qui a détecté la menace.

PHASE	DESCRIPTION
Date/heure	Moment de la détection
Menace de sécurité	Nom de la menace pour la sécurité
Catégorie	Type de scan qui a détecté la menace
Chemin d'accès au fichier/URL/Afficher la source	Emplacement dans lequel la détection de menace s'est produite ou liste utilisée pour détecter le site Web malveillant
Action	Action entreprise sur la menace
Canal d'infection	Canal d'où provient la menace
Endpoint	Endpoint sur lequel la détection a eu lieu

Widget Principales détections de ransomware



Ce widget fournit une vue d'ensemble des principales détections de ransomware sur la période spécifiée.

Utilisez la liste déroulante pour sélectionner le type de données de ransomwares à afficher.

AFFICHER	DESCRIPTION
Endpoints	Affiche les endpoints présentant le plus grand nombre de détections de ransomwares sur votre réseau Cliquez sur le nombre de détections de ransomwares pour ouvrir l'écran **Risques de sécurité - ransomwares** qui affiche des informations détaillées sur la détection de ransomwares.
Types de ransomwares	Affiche les types de ransomwares présentant le plus grand nombre de détections sur votre réseau Cliquez sur le lien **Nom de la menace** pour ouvrir l'encyclopédie des menaces de Trend Micro pour obtenir des informations plus précises sur le type de menace spécifique.

AFFICHER	DESCRIPTION
Domaines	Affiche les domaines des ransomwares présentant le plus grand nombre de détections sur votre réseau Cliquez sur le lien **Nom de la menace** pour ouvrir l'encyclopédie des menaces de Trend Micro pour obtenir des informations plus précises concernant le domaine spécifique.

Widget Détection des risques de sécurité dans le temps

Ce widget fournit une vue d'ensemble des endpoints de votre réseau pour lesquels des menaces ont été détectées et des types de menaces affectant votre réseau sur une période définie.

Cliquez sur le bouton **Endpoints affectés** ou **Types de menaces** pour passer d'une vue à l'autre.

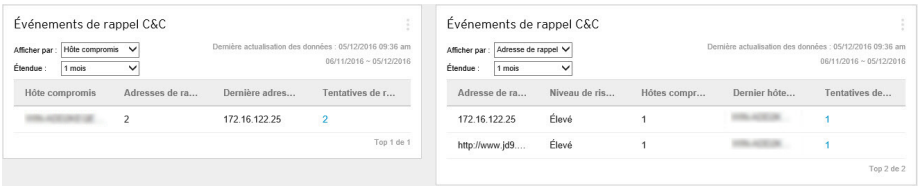
AFFICHER	DESCRIPTION
Endpoints affectés	Affiche le nombre d'endpoints présentant des détections de menaces ou des violations de stratégie pour la période spécifiée Cliquez sur le nœud d'un jour particulier pour passer à l'écran **Gestion des agents**, qui affiche tous les endpoints concernés pour ce jour dans l'arborescence des agents.
Types de menaces	Affiche un graphique qui met en évidence le nombre de menaces et les violations de stratégie enregistrées pour la période spécifiée • Cliquez sur les noms des types de menaces en bas du graphique pour afficher/masquer les informations de détection sur le graphique. • Passez le curseur sur le ou les nœuds d'un jour particulier pour afficher le nombre total de détections pour les types de menaces affichés. Cliquez sur un nœud pour passer à l'écran de journaux pour le type de menace mis en surbrillance dans la liste.

Widgets OfficeScan

Les widgets OfficeScan fournissent une référence rapide pour les états de sécurité et détection d'agent OfficeScan, les informations des plug-ins et les incidents d'épidémie.

Widgets disponibles :

Widget Événements de rappel C&C



Ce widget affiche toutes les informations relatives aux événements de rappel C&C, y compris la cible de l'attaque et l'adresse source de rappel.

Vous pouvez choisir de visualiser les informations de rappel C&C à partir d'une liste de serveurs C&C spécifiques. Pour choisir la source de la liste (Intelligence globale, Virtual Analyzer), cliquez sur l'icône Modifier (>) et faites votre sélection dans la liste déroulante **Source de la liste C&C**.

Utilisez la liste déroulante **Affichage par** pour sélectionner le type de données de rappel C&C qui s'affiche :

- **Hôte compromis** : Affiche les informations C&C les plus récentes par endpoint ciblé

TABLEAU 8-4. Informations sur l'hôte compromis

COLONNE	DESCRIPTION
Hôte compromis	Nom du endpoint ciblé par l'attaque C&C
Adresses de rappel	Le nombre d'adresses de rappel que le endpoint a tenté de contacter
Dernière adresse de rappel	La dernière adresse de rappel que le endpoint a tenté de contacter
Tentatives de rappel	Le nombre de fois que le endpoint ciblé a tenté de contacter avec l'adresse de rappel **Remarque** Cliquez sur le lien hypertexte pour ouvrir l'écran **Journaux de rappel C&C** et afficher des informations plus détaillées.

- **Adresse de rappel** : affiche les informations C&C les plus récentes par adresse de rappel C&C

TABLEAU 8-5. Informations d'adresse C&C

COLONNE	DESCRIPTION
Adresse de rappel	Adresse des rappels C&C provenant du réseau
Niveau de risque C&C	Le niveau de risque de l'adresse de rappel déterminé soit par la liste Informations globales, soit par la liste Virtual Analyzer
Hôtes compromis	Le nombre de endpoints que l'adresse de rappel a ciblé
Dernier hôte compromis	Nom du dernier endpoint qui a tenté de contacter l'adresse de rappel C&C

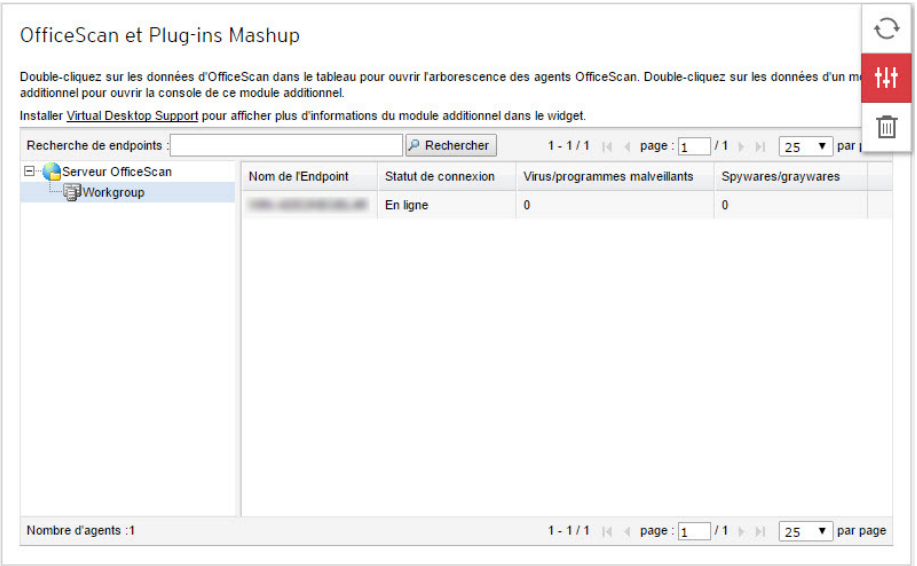
COLONNE	DESCRIPTION
Tentatives de rappel	Le nombre de tentatives de rappels réalisé sur l'adresse du réseau **Remarque** Cliquez sur le lien hypertexte pour ouvrir l'écran **Journaux de rappel C&C** et afficher des informations plus détaillées.

Widget Détection des risques liés à la sécurité

Ce widget affiche le nombre de risques de sécurité détectés et le nombre d'endpoints concernés.

Cliquez sur le nombre d'endpoints pour ouvrir l'écran **Gestion des agents** qui répertorie les agents OfficeScan concernés dans l'arborescence des agents.

Widget OfficeScan et Plug-ins Mashup



Ce widget combine les données des agents OfficeScan et des programmes de plug-in installés et les présente dans l'arborescence des agents. Ce widget vous aide à évaluer rapidement le niveau de protection des agents et réduit le temps nécessaire à la gestion de chaque plugiciel.

Ce widget affiche les données pour les programmes de plug-in suivants :

- Trend Micro Virtual Desktop Support

Important

Vous devez activer un programme de plug-in pris en charge pour que le widget de mashup puisse afficher les données correspondantes. Mettez les programmes de plug-in à niveau si des versions plus récentes sont disponibles.

Pour sélectionner les colonnes qui s'affichent dans l'arborescence des agents, cliquez sur le bouton **Autres options** dans le coin supérieur droit du widget, puis cliquez sur le bouton **Paramètres**.

Cliquez sur les données sous une colonne pour ouvrir la console du programme de plug-in correspondant ou l'écran OfficeScan **Gestion des agents**. L'écran qui s'affiche dépend du type de données sur lequel vous avez cliqué.

Widget Connectivité de l'agent antivirus

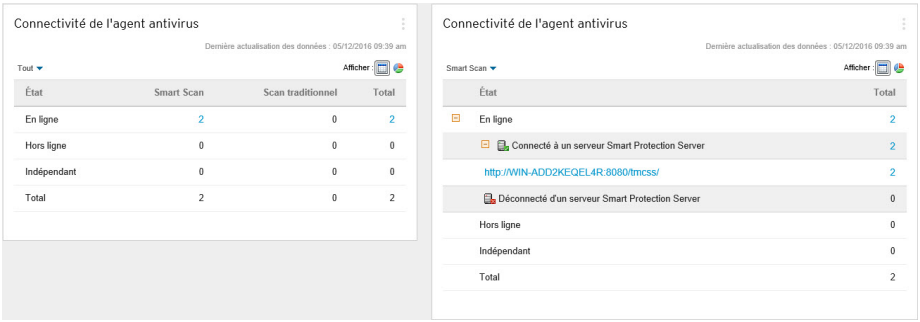


FIGURE 8-2. Vue par défaut affichant tous les agents Smart Scan et de scan traditionnel et vue de l'agent Smart Scan étendue avec les serveurs Smart Protection Server

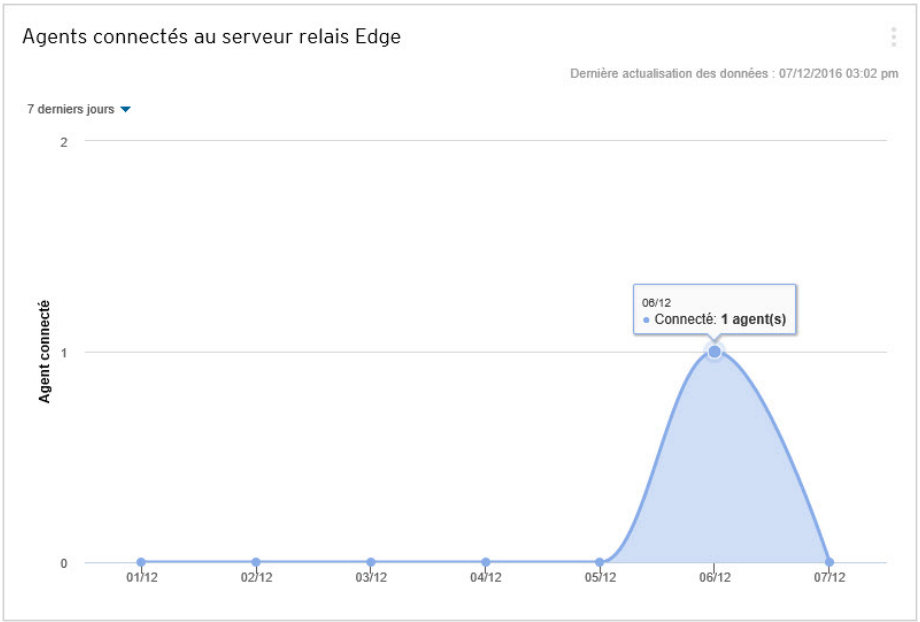
Ce widget affiche l'état de connexion des agents OfficeScan au serveur OfficeScan en relation à la méthode de scan configurée (Smart Scan et scan traditionnel).

Vous pouvez choisir d'afficher les données dans un tableau ou dans un graphique circulaire en cliquant sur les icônes d'affichage ( ).

Utilisez la liste déroulante au-dessus du tableau/graphique pour modifier le type de données qui s'affiche. Cliquez sur le nombre de n'importe quel état pour ouvrir l'écran **Gestion des agents** qui répertorie les agents OfficeScan associés dans l'arborescence des agents.

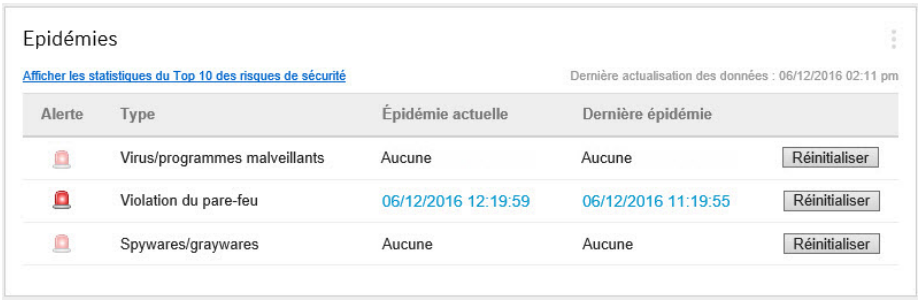
AFFICHER	DESCRIPTION
Tout	Affiche l'état de connexion de tous les agents OfficeScan pour les deux méthodes de scan
Scan traditionnel	Affiche l'état de connexion de tous les agents OfficeScan qui utilisent la méthode de scan traditionnel
Smart Scan	Affiche l'état de connexion de tous les agents OfficeScan qui utilisent la méthode Smart Scan Lorsque vous affichez l'état de connexion de l'agent dans un tableau : • Développez les informations sur les agents « En ligne » pour voir l'état de connexion des agents disposant d'un serveur Smart Protection Server. • Cliquez sur l'URL pour ouvrir la console d'administration de Smart Protection Server. **Remarque** Seuls les agents en ligne (sous le serveur OfficeScan) peuvent signaler leur état de connexion aux serveurs Smart Protection Server.

Agents connectés au widget du serveur relais Edge



Ce widget affiche le nombre d'agents OfficeScan connectés au serveur relais Edge OfficeScan pour une période définie.

Widget Épidémies

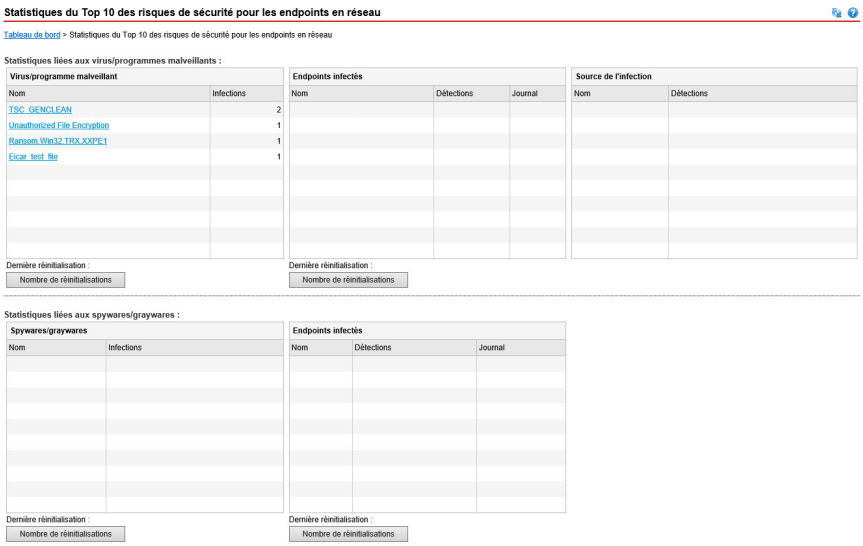


Le widget **Épidémies** affiche l'état de toute épidémie de risque de sécurité actuelle, ainsi que la dernière alerte d'épidémie.

- Cliquez sur le lien de date/heure de l'alerte pour afficher plus de détails sur l'épidémie.
- **Réinitialisez** l'état des informations d'alerte d'épidémie et appliquez immédiatement les mesures de prévention d'épidémie lorsque OfficeScan détecte une épidémie.

  Pour plus d'informations sur l'application des mesures de prévention des épidémies, voir *Stratégies de prévention des épidémies à la page 7-2*.

- Cliquez sur **Afficher les statistiques du Top 10 des risques de sécurité** afin d'afficher les risques liés à la sécurité les plus courants, les endpoints comptant le plus grand nombre de risques et les sources d'infections principales.

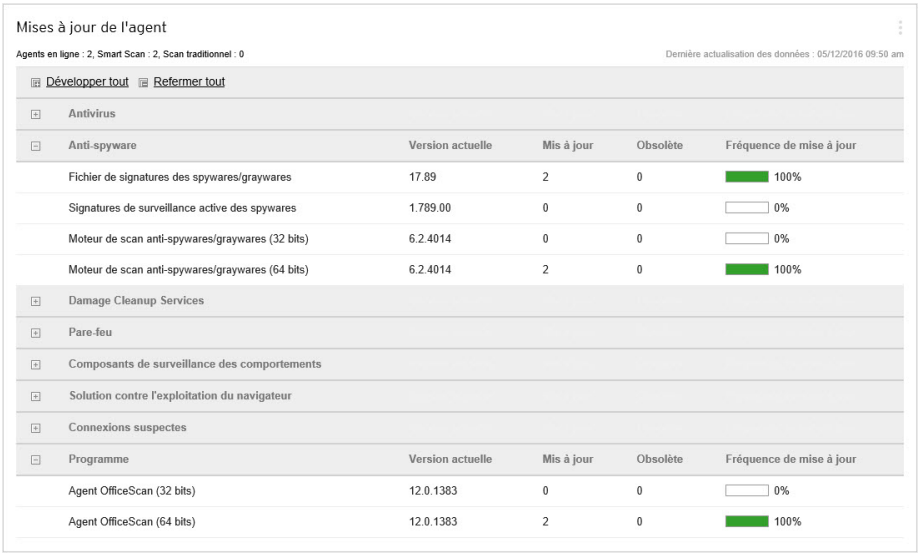


Sur l'écran des **Statistiques du Top 10 des risques de sécurité**, vous pouvez :

- Consulter des informations détaillées sur un risque de sécurité en cliquant sur le nom de ce risque.

- Consulter l'état général d'un endpoint particulier en cliquant sur son nom.
- Consulter les journaux de risques de sécurité relatifs à ce endpoint en cliquant sur le bouton **Afficher** correspondant au nom de ce endpoint.
- Réinitialiser les statistiques dans chaque tableau en cliquant sur **Réinitialiser nombre**.

Widget Mises à jour de l'agent



Ce widget affiche les composants et les programmes qui protègent les agents OfficeScan contre les risques de sécurité.

Cliquez sur le nombre « Obsolète » pour ouvrir l'écran **Gestion des agents** qui répertorie les agents OfficeScan qui nécessitent des mises à jour dans l'arborescence des agents.

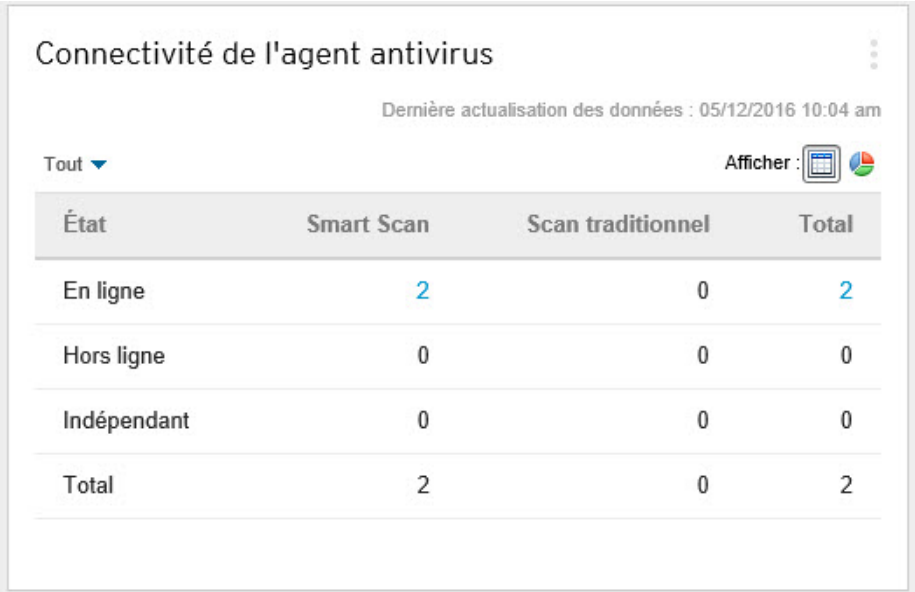
Widget de gestion

Le widget de gestion affiche l'état de connexion des agents OfficeScan avec le serveur OfficeScan.

Widgets disponibles :

- *Widget Connectivité agent-serveur à la page 8-24*

Widget Connectivité agent-serveur



Ce widget indique l'état de la connexion de tous les agents au serveur OfficeScan.

Vous pouvez basculer entre le tableau et le graphique circulaire en cliquant sur les icônes d'affichage ( ).

Cliquez sur le nombre de n'importe quel état pour ouvrir l'écran **Gestion des agents** qui répertorie les agents OfficeScan associés dans l'arborescence des agents.

Chapitre 9

Logs

Ce chapitre décrit comment accéder à des événements système et des journaux de détection de sécurité à l'aide de la console Web.

Les rubriques sont les suivantes :

Affichage des journaux des opérations de scan

Lorsque le scan manuel, le scan programmé ou le scan immédiat s'exécute, l'agent OfficeScan crée un journal de scan contenant des informations sur le scan. Vous pouvez consulter le journal de scan à partir du serveur OfficeScan ou des consoles des agents OfficeScan.

Important

Le serveur OfficeScan enregistre toutes les données dans le fuseau horaire UTC-06:00 (Amérique centrale), quel que soit l'emplacement de l'Endpoint. Pour déterminer l'heure à laquelle un événement s'est produit dans votre fuseau horaire, vous devez manuellement convertir la date/heure enregistrée.

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, cliquez sur l'icône du domaine racine ( ) pour inclure tous les agents ou sélectionnez des domaines ou des agents spécifiques.
3. Cliquez sur **Journaux des opérations de scan**.

   L'écran **Critères des journaux des opérations de scan** s'ouvre.
4. Spécifiez les critères de journaux, puis cliquez sur **Afficher les journaux**.
5. Affichez les journaux. Les journaux contiennent les informations suivantes :

ÉLÉMENT	DESCRIPTION
Heure de début	Heure de début du scan
Heure de fin	Heure à laquelle le scan s'est arrêté
Endpoint	Endpoint sur lequel le scan a été effectué

Élément	Description
Status	État de l'achèvement du scan • **Terminé** :le scan s'est déroulé normalement. • **Interrompu** :l'utilisateur a interrompu le scan avant qu'il ne soit terminé. • **Arrêté de manière inattendue** :Le scan a été interrompu par l'utilisateur, le système, ou par un événement inattendu. Par exemple, il se peut que le service de scan en temps réel d'OfficeScan se soit terminé de façon inattendue ou que l'utilisateur ait forcé l'Endpoint à redémarrer.
Type de scan	Type de scan effectué (scan manuel, scan immédiat, scan programmé)
Scanné	Nombre d'objets scannés
Virus/programmes malveillants	Nombre de détections de virus/programmes malveillants
Programmes espions/ graywares	Nombre de détections de spywares/graywares
Signatures Smart Scan	Version de Signature Smart Scan Agent
Fichier de signatures de virus	Version du fichier de signatures de virus
Fichier de signatures de programmes espions/ graywares	Version du fichier de signatures des spywares/ graywares

6. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Affichage des journaux de restauration de la mise en quarantaine centralisée

Après un nettoyage destiné à éliminer les programmes malveillants, les agents OfficeScan sauvegardent les données concernant ces programmes. Demandez à un agent en ligne de restaurer les données sauvegardées si vous considérez qu'elles ne présentent pas de danger. Les informations relatives aux données de sauvegarde des programmes malveillants restaurées, au Endpoint concerné et au résultat de la restauration sont disponibles dans les journaux.

Important

Le serveur OfficeScan enregistre toutes les données dans le fuseau horaire UTC-06:00 (Amérique centrale), quel que soit l'emplacement de l'Endpoint. Pour déterminer l'heure à laquelle un événement s'est produit dans votre fuseau horaire, vous devez manuellement convertir la date/heure enregistrée.

Procédure

1. Accédez à **Journaux** > **Agents** > **Restauration depuis la mise en quarantaine centrale**.
2. Consultez les colonnes **Réussi**, **Échoué** et **En attente** pour savoir si OfficeScan est parvenu à restaurer les données mises en quarantaine.
3. Cliquez sur les liens numérotés de chaque colonne pour afficher des informations détaillées sur chaque Endpoint concerné.

   Remarque

   Pour les restaurations ayant **Échoué**, vous pouvez lancer une nouvelle tentative de restauration du fichier sur l'écran **Détails de la restauration depuis la mise en quarantaine centralisée**, en cliquant sur **Tout restaurer**.

4. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Affichage des journaux d'évènements du système

OfficeScan enregistre les événements liés au programme serveur, tels que les arrêts et les démarrages. Ces journaux permettent de vérifier si le serveur et les services OfficeScan fonctionnent correctement.

Important

Le serveur OfficeScan enregistre toutes les données dans le fuseau horaire UTC-06:00 (Amérique centrale), quel que soit l'emplacement de l'Endpoint. Pour déterminer l'heure à laquelle un événement s'est produit dans votre fuseau horaire, vous devez manuellement convertir la date/heure enregistrée.

Procédure

1. Accédez à **Journaux** > **Événements système**.
2. Sous **Événement**, vérifiez les journaux pour lesquels une action supplémentaire est requise. OfficeScan consigne les événements suivants :

TABLEAU 9-1. Journaux des événements du système

TYPE DE JOURNAL	ÉVÉNEMENTS
OfficeScan Master Service et serveur de base de données	• Service principal démarré • Service principal fermé correctement • Échec de fermeture du service principal
Accès à la console Web basé sur les rôles	• Connexion à la console • Déconnexion de la console • Expiration de la session (l'utilisateur est automatiquement déconnecté)

TYPE DE JOURNAL	ÉVÉNEMENTS
Authentification serveur	• L'agent OfficeScan a reçu des commandes non valides de la part du serveur • Certificat d'authentification non valide ou ayant expiré

3. Pour sauvegarder les journaux dans un fichier CSV (valeurs séparées par des virgules), cliquez sur **Exporter vers fichier CSV**. Ouvrez le fichier ou enregistrez-le à un emplacement donné.

Chapitre 10

Notifications

Ce chapitre décrit comment configurer OfficeScan pour notifier les utilisateurs finaux après la détection d'un risque lié à la sécurité.

Les rubriques sont les suivantes :

Notifications de l'agent OfficeScan

OfficeScan peut afficher des messages de notification sur des Endpoints d'agent OfficeScan :

- Immédiatement après la détection d'un risque pour la sécurité. Activez le message de notification et modifiez éventuellement son contenu.
- Immédiatement après la détection d'une menace Web. Activez le message de notification et modifiez éventuellement son contenu.

Configuration des notifications de virus/programme malveillant pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux du résultat d'une tentative de nettoyage de mise en quarantaine de virus ou de programme malveillant.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Virus/Programmes malveillants**.
3. Configurez les paramètres de détection.
   a. Choisissez d'afficher une notification pour tous les événements liés aux virus/programmes malveillants ou séparez les notifications en fonction des niveaux de gravité suivants :
      - **Élevé** : l'agent OfficeScan n'a pas pu traiter un programme malveillant critique
      - **Moyen** : l'agent OfficeScan n'a pas pu traiter un programme malveillant
      - **Faible** : l'agent OfficeScan est parvenu à résoudre toutes les menaces
   b. Acceptez ou modifiez les messages par défaut.

4. Cliquez sur **Enregistrer**.

Configuration des notifications de spyware/grayware pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux du résultat d'une tentative de nettoyage ou de mise en quarantaine d'un spyware/grayware.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Spywares/Graywares**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications de pare-feu pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après que le pare-feu OfficeScan a bloqué un trafic sortant enfreignant la stratégie du pare-feu.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations du pare-feu**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications de Web Reputation pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après la détection d'une tentative d'accès à un site Web malveillant.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations de la Web Reputation**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications de contrôle des dispositifs pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après le blocage de l'accès à un appareil non autorisé.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations du contrôle des dispositifs**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications de surveillance des comportements pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après le blocage d'un accès à une application ou un processus, ou après la détection d'un programme récemment trouvé.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations de la stratégie de surveillance des comportements**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications de rappels C&C pour les agents OfficeScan

Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux lorsque l'Endpoint tente de contacter un serveur C&C inconnu.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Rappels C&C**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Configuration des notifications d’apprentissage automatique prédictif pour les agents OfficeScan

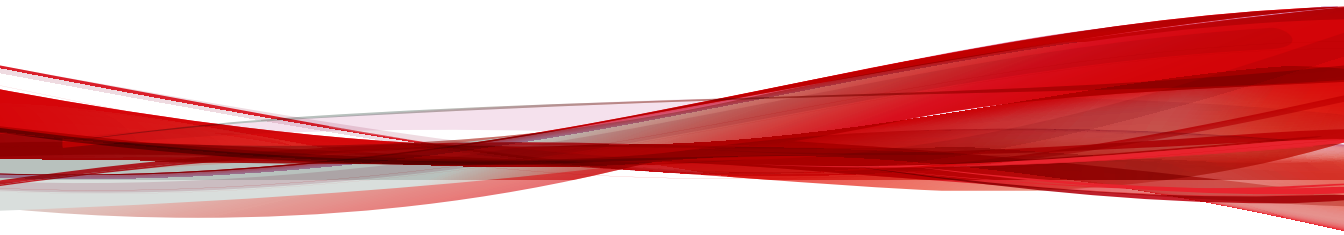
Vous pouvez configurer l'agent OfficeScan pour notifier les utilisateurs finaux après la détection d’une menace inconnue.

Procédure

1. Accédez À **Administration** > **Notifications** > **Agent**.
2. Dans la liste déroulante **Type**, sélectionnez **Violations de l’apprentissage automatique prédictif**.
3. Acceptez ou modifiez les messages par défaut.
4. Cliquez sur **Enregistrer**.

Partie V

Mises à jour et administration



Chapitre 11

Mises à jour

Ce chapitre décrit comment configurer des mises à jour d'agent OfficeScan et décrit les composants mis à jour sur les agents.

Les rubriques sont les suivantes :

Configuration des mises à jour programmées pour les agents OfficeScan

Configurez OfficeScan pour automatiquement mettre à jour tous les agents OfficeScan selon un programme défini. L'actualisation permanente des composants garantit que vous bénéficiez de la meilleure protection contre les toutes dernières menaces.

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique**.
2. Configurez la programmation pour la fonction **Mise à jour programmée**.
   - **Minute(s)** ou **Heure(s)**

     L'option **Mettre à jour les configurations des agents une seule fois par jour** est disponible lors de la programmation d'une mise à jour à intervalles d'une heure ou d'un certain nombre de minutes. Le fichier de configuration contient tous les paramètres des agents OfficeScan configurés à l'aide de la console Web.

     Conseil

     Trend Micro met fréquemment à jour les composants ; cependant, les paramètres de configuration d'OfficeScan sont probablement modifiés moins fréquemment. La mise à jour des fichiers de configuration avec les composants nécessite plus de bande passante et augmente le temps nécessaire à OfficeScan pour terminer la mise à jour. C'est la raison pour laquelle Trend Micro recommande de mettre à jour les configurations des agents OfficeScan une seule fois par jour.

   - **Quotidienne** ou **Hebdomadaire**

     Indiquez l'heure de la mise à jour et la durée pendant laquelle le serveur OfficeScan demande aux agents de mettre à jour les composants.

Conseil

Ce paramètre permet d'éviter que tous les agents en ligne se connectent simultanément au serveur à l'heure spécifiée, réduisant de manière significative le trafic sur le serveur. Par exemple, si l'heure de début a été définie sur 12h00 et que la durée est de 2 heures, OfficeScan demande de façon aléatoire à tous les agents en ligne de mettre à jour les composants entre 12h00 et 14h00.

3. Cliquez sur **Enregistrer**.

Sources de mise à jour des agents OfficeScan

Les agents peuvent obtenir des mises à jour depuis la source de mise à jour standard (serveur OfficeScan) ou des composants spécifiques depuis des sources de mise à jour personnalisées, telles que le serveur Trend Micro ActiveUpdate. Pour obtenir des informations détaillées, voir *Source de mise à jour standard pour les Agents OfficeScan à la page 11-4* et *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 11-6*.

Prises en charge d'IPv6 pour les mises à jour des agents OfficeScan

Un agent IPv6 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv4 pures, telles que :

- un serveur OfficeScan IPv4 pur
- un agent de mise à jour IPv4 pur
- Toute source de mise à jour personnalisée IPv4 pure
- Trend Micro ActiveUpdate Server

De même, un agent IPv4 pur ne peut pas effectuer de mises à jour à partir de sources de mise à jour IPv6 pures, telles qu'un serveur OfficeScan ou un agent de mise à jour IPv6 pur.

Un serveur proxy à double pile pouvant convertir les adresses IP, tel que DeleGate, est nécessaire pour permettre aux agents de se connecter aux sources de mise à jour.

Source de mise à jour standard pour les Agents OfficeScan

Le serveur OfficeScan est la source de mise à jour standard pour les agents.

Si le serveur OfficeScan est inaccessible, les agents ne disposeront pas de source de sauvegarde et seront par conséquent obsolètes. Pour mettre à jour les agents qui ne peuvent pas se connecter au serveur OfficeScan, Trend Micro recommande d'utiliser Agent Packager. Utilisez cet outil pour créer un package contenant les composants les plus récents disponibles sur le serveur, puis exécutez ce package sur les agents.

Remarque

L'adresse IP de l'agent (IPv4 ou IPv6) détermine si la connexion au serveur OfficeScan peut être établie. Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour des agents, consultez *Prises en charge d'IPv6 pour les mises à jour des agents OfficeScan à la page 11-3*.

Configuration de la source de mise à jour standard des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Sélectionnez **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)**.
3. Cliquez sur **Notifier tous les agents**.

Processus de mise à jour de l'agent OfficeScan

Remarque

Cette rubrique explique le processus de mise à jour des agents OfficeScan. Le processus de mise à jour des agents de mise à jour est traité dans la section *Sources de mises à jour personnalisées pour les agents de mises à jour à la page 11-9*.

Après avoir défini et enregistré la liste des sources de mise à jour personnalisées, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent OfficeScan est mis à jour à partir de la première source de la liste.
2. Si la mise à jour est impossible à partir de la première source, l'agent OfficeScan effectue une tentative avec la seconde source, etc.
3. Si la mise à jour n'est possible à partir d'aucune des sources, l'agent OfficeScan vérifie les paramètres suivants sur l'écran **Source de mise à jour** :

TABLEAU 11-1. Paramètres supplémentaires de sources de mise à jour personnalisées

PARAMÈTRE	DESCRIPTION
Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan	Si ce paramètre est actif, les agents de mise à jour s'exécutent directement à partir du serveur OfficeScan et ignorent l'option Liste des sources de mise à jour personnalisées. Si ce paramètre est désactivé, les agents de mise à jour appliquent les paramètres de source de mise à jour personnalisée configurés pour des agents normaux.
Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables:	

PARAMÈTRE	DESCRIPTION
Composants	Si ce paramètre est activé, l'agent procède à la mise à jour des composants à partir du serveur OfficeScan. S'il est désactivé, l'agent essaie ensuite de se connecter directement au serveur Trend Micro ActiveUpdate si l'une des conditions suivantes est vérifiée : • Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées.
Paramètres de domaine	Si ce paramètre est activé, l'agent met à jour les paramètres au niveau du domaine à partir du serveur OfficeScan.
Programmes et correctifs de type hot fix des agents OfficeScan	Si ce paramètre est activé, l'agent met à jour les programmes et les correctifs de type hot fix à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources disponibles, l'agent abandonne le processus de mise à jour.

Sources de mise à jour personnalisées pour les agents OfficeScan

Les agents OfficeScan peuvent être mis à jour à partir du serveur OfficeScan, mais également à partir de sources de mise à jour personnalisées. Les sources de mise à jour personnalisées contribuent à la réduction du trafic de mise à jour des agents OfficeScan dirigé vers le serveur OfficeScan et permettent aux agents OfficeScan ne pouvant pas se connecter au serveur OfficeScan d'être mis à jour rapidement. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour.

Conseil

Trend Micro recommande de définir certains agents OfficeScan en tant qu'agents de mise à jour et de les ajouter à la liste.

Configuration de sources de mise à jour personnalisées pour les agents OfficeScan

Important

OfficeScan XG Service Pack 1 (ou version ultérieure) prend en charge l'utilisation du protocole de communication HTTPS entre les agents de mise à jour et les agents OfficeScan configurés pour recevoir des mises à jour des agents de mise à jour. Vous devez mettre à niveau les agents de mise à jour et tous les agents OfficeScan qui dépendent des agents de mise à jour vers OfficeScan XG Service Pack 1 avant de remplacer le protocole de communication par HTTPS.

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.
2. Sélectionnez **Source de mise à jour personnalisée**.
3. Sélectionnez la façon dont les agents de mise à jour et les agents OfficeScan reçoivent les mises à jour.
   - **Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan**
   - Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables:
     - **Composants**
     - **Paramètres de domaine**
     - **Programmes et correctifs de type hot fix des agents OfficeScan**

   Pour plus d'informations, voir *Processus de mise à jour de l'agent OfficeScan à la page 11-5*.
4. Si vous avez indiqué au moins un agent de mise à jour en tant que source de mise à jour, cliquez sur **Rapport d'analyse de l'agent de mise à jour** pour générer un rapport mettant en évidence l'état de la mise à jour des Endpoints.

Pour plus de détails sur ce rapport, voir *Rapport d'analyse de l'agent de mise à jour à la page 11-12*.

5. Ajoutez ou modifiez la **Liste des sources de mise à jour personnalisées**.

   - Cliquez sur **Ajouter** pour spécifier une nouvelle source de mise à jour.
   - Cliquez sur une valeur dans la colonne **Plage IP** pour modifier une source de mise à jour existante.

   Remarque

   Modifiez une source de mise à jour existante pour définir le protocole de communication d'un agent de mise à jour XG SP1 (ou version ultérieure) existant sur HTTPS.

   L'écran **Ajouter/Modifier plage d'adresses IP et source de mise à jour** s'affiche.

6. Configurez les adresses IP des Endpoints qui reçoivent des mises à jour de la source de mise à jour.

   - **IPv4** : spécifiez la plage d'adresses IPv4 des Endpoints qui utilisent la source de mise à jour.
   - **IPv6** : spécifiez le préfixe et la longueur de l'adresse IPv6 des Endpoints qui utilisent la source de mise à jour.

   Remarque

   Assurez-vous que les agents OfficeScan peuvent se connecter à la source de mise à jour en utilisant leurs adresses IP. Par exemple, si vous avez indiqué une plage d'adresses IPv4, la source de mise à jour doit avoir une adresse IPv4. Si vous avez indiqué un préfixe IPv6 et une longueur, la source de mise à jour doit avoir une adresse IPv6.

   Pour plus d'informations sur la prise en charge d'IPv6 pour les mises à jour des Endpoints, consultez *Sources de mise à jour des agents OfficeScan à la page 11-3*.

7. Spécifiez la source de mise à jour. Vous pouvez sélectionner un agent de mise à jour si un tel agent a été affecté ou saisir l'URL d'une source spécifique.

- **URL** : spécifiez l'URL de la source de mise à jour.

  Remarque

  Pour remplacer le protocole d'agent de mise à jour HTTP existant par HTTPS, modifiez la valeur du champ **URL**.

- **Agent de mise à jour** : sélectionnez un agent de mise à jour préconfiguré dans la liste déroulante et sélectionnez la manière dont les agents OfficeScan se connectent à l'agent de mise à jour.

  - **Utiliser l'adresse IP de l'agent de mise à jour pour la connexion**
  - **Utiliser le nom d'hôte de l'agent de mise à jour pour la connexion**

  Remarque

  L'OfficeScan configure automatiquement l'URL de la **source externe** sur le protocole HTTPS si l'agent de mise à jour a été mis à jour vers OfficeScan XG SP1 ou une version ultérieure.

8. Cliquez sur **Enregistrer**.
9. Gérez la **Liste des sources de mise à jour personnalisées**.
   a. Supprimez une source de mise à jour depuis la liste en cochant la case correspondante et en cliquant sur **Supprimer**.
   b. Pour déplacer une source de mise à jour, cliquez sur la flèche haut ou bas. Vous ne pouvez déplacer qu'une source à la fois.
10. Cliquez sur **Notifier tous les agents**.

Sources de mises à jour personnalisées pour les agents de mises à jour

En plus du serveur OfficeScan, les agents de mise à jour peuvent effectuer la mise à jour depuis des sources de mise à jour personnalisées. Les sources de mise à jour personnalisées contribuent à la réduction du trafic de mise à jour des agents dirigé vers le

serveur OfficeScan. Spécifiez les sources de mise à jour personnalisées dans la Liste de sources de mise à jour personnalisées, qui peut accueillir jusqu'à 1024 sources de mise à jour. Voir *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 11-6* pour connaître les étapes de configuration de la liste.

Remarque

Assurez-vous que l'option **Les agents de mise à jour effectuent la mise à jour des composants, des paramètres du domaine, des programmes des agents et des correctifs de type hot fix, uniquement à partir du serveur OfficeScan** est désactivée sur l'écran **Source de mise à jour pour les agents** (**Mises à jour** > **Agents** > **Source de mise à jour**) pour que les agents de mise à jour puissent se connecter aux sources de mise à jour personnalisées.

Après avoir défini et enregistré la liste, le processus de mise à jour s'effectue de la façon suivante :

1. L'agent de mise à jour effectue la mise à jour à partir de la première entrée de la liste.
2. S'il ne peut pas effectuer la mise à jour à partir de la première entrée, il essaie avec la seconde entrée, et ainsi de suite.
3. Si l'agent ne parvient à effectuer la mise à jour à partir d'aucune des entrées, il vérifie les options suivantes sous l'en-tête **Les agents OfficeScan mettent à jour les éléments suivants à partir du serveur OfficeScan si toutes les sources personnalisées sont indisponibles ou introuvables** :

   - **Composants** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

     Si l'option est désactivée, l'agent essaie ensuite de se connecter directement au serveur Trend Micro ActiveUpdate si l'une des conditions suivantes est remplie :

     Remarque

     Vous ne pouvez mettre à jour des composants qu'à partir du serveur Active Update. Les paramètres de domaine, les programmes et les correctifs de type hot fix ne peuvent être téléchargés qu'à partir du serveur ou des agents de mise à jour.

- L'option **Les agents téléchargent des mises à jour depuis le serveur Trend Micro ActiveUpdate** est activée dans **Agents** > **Gestion des agents**, sous **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**.
- Le serveur ActiveUpdate n'est pas inclus dans la liste de sources de mise à jour personnalisées.

- **Paramètres de domaine** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.
- **Programmes et correctifs de type hot fix des agents OfficeScan** : Si l'option est activée, l'agent effectue la mise à jour à partir du serveur OfficeScan.

4. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Le processus de mise à jour est différent si l'option **Source de mise à jour standard (mise à jour depuis le serveur OfficeScan)** est activée et si le serveur OfficeScan informe l'agent de la nécessité de mettre à jour les composants. Le processus est le suivant :

1. L'agent effectue la mise à jour directement à partir du serveur OfficeScan et ignore la liste des sources de mise à jour.
2. S'il ne peut pas être mis à jour à partir du serveur, l'agent tente de se connecter directement au serveur Trend Micro ActiveUpdate si l'une des conditions suivantes est remplie :
   - Dans **Agents** > **Gestion des agents**, cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres** > **Paramètres de mise à jour**. L'option **Les agents OfficeScan téléchargent des mises à jour depuis le serveur Trend Micro ActiveUpdate** est activée.
   - Le serveur ActiveUpdate est la première entrée de la liste de sources de mise à jour personnalisées.

Conseil

Ne placez le serveur ActiveUpdate en haut de la liste que si vous rencontrez des problèmes de mise à jour à partir du serveur OfficeScan. Lorsque des agents OfficeScan effectuent la mise à jour directement depuis le serveur ActiveUpdate, ils consomment une grande quantité de bande passante réseau et Internet.

3. S'il ne peut pas obtenir les mises à jour à partir des sources possibles, l'agent de mise à jour abandonne le processus de mise à jour.

Rapport d'analyse de l'agent de mise à jour

Générez le rapport d'analyse de l'agent de mise à jour pour analyser l'infrastructure de mise à jour et déterminer quels agents téléchargent des mises à jour partielles à partir des agents de mise à jour et d'autres sources de mise à jour.

Remarque

Ce rapport inclut tous les agents OfficeScan configurés pour recevoir des mises à jour partielles des agents de mise à jour. Si vous avez délégué la tâche de gestion d'un ou de plusieurs domaines à d'autres administrateurs, ceux-ci visualisent également tous les agents OfficeScan configurés pour recevoir des mises à jour partielles d'agents de mise à jour appartenant aux domaines qu'ils ne gèrent pas.

OfficeScan exporte le Rapport d'analyse de l'agent de mise à jour dans un fichier de valeurs séparées par des virgules (`.CSV`).

Ce rapport contient les informations suivantes :

- agent OfficeScan endpoint
- adresse IP
- Chemin d'accès de l'arborescence des agents
- Source de mise à jour
- Si les agents téléchargent les éléments suivants à partir des agents de mise à jour :
  - Composants

- Paramètres de domaine
- Programmes et correctifs de type hot fix des agents OfficeScan

Important

Le rapport d'analyse de l'agent de mise à jour répertorie uniquement les agents OfficeScan configurés pour recevoir des mises à jour partielles d'un agent de mise à jour. Les agents OfficeScan configurés pour recevoir des mises à jour complètes (y compris les composants, paramètres de domaine, programmes de l'agent OfficeScan et correctifs de type hot fix) ne figurent pas dans le rapport.

Pour plus de détails sur la génération du rapport, reportez-vous à *Sources de mise à jour personnalisées pour les agents OfficeScan à la page 11-6*.

Chapitre 12

Paramètres d'administration

Ce chapitre décrit les paramètres d'administration disponibles pour le serveur et les agents OfficeScan.

Les rubriques sont les suivantes :

Smart Feedback

Trend Micro Smart Feedback partage les informations sur les menaces anonymes avec Smart Protection Network, ce qui permet à Trend Micro d'identifier rapidement les nouvelles menaces et d'y répondre. Vous pouvez désactiver Smart Feedback à tout moment via cette console.

Participation au programme Smart Feedback

Procédure

1. Accédez à **Administration** > **Smart Protection** > **Smart Feedback**.
2. Cliquez sur **Activer Trend Micro Smart Feedback**.
3. Pour aider Trend Micro à mieux connaître votre entreprise, sélectionnez son **secteur d'activité**.
4. Pour envoyer des informations sur des menaces de sécurité potentielles dans les fichiers de vos agents OfficeScan, cochez la case **Activer les commentaires sur les fichiers programme suspects**.

   Remarque

   Les fichiers envoyés à Smart Feedback ne contiennent pas de données utilisateur et ne sont utilisés que pour l'analyse des menaces.

5. Pour configurer les critères d'envoi de vos commentaires, sélectionnez le nombre de détections pour un laps de temps donné qui déclencheront cet envoi.
6. Pour réduire les risques d'interruption du réseau, indiquez la bande passante maximale qu'OfficeScan peut utiliser pour l'envoi des commentaires.
7. Cliquez sur **Enregistrer**.

Paramètres de notification

OfficeScan vous permet de configurer les notifications d'agents pour informer les utilisateurs finaux de détections sur des Endpoints spécifiques.

Pour obtenir des informations sur les différents types de paramètres de notification d'agent OfficeScan, consultez le chapitre suivant : *Notifications à la page 10-1*.

Paramètres généraux d'administration

Configuration des paramètres de proxy pour les connexions d'agent

Les agents utilisent les paramètres de serveur proxy configurés dans les options Internet de Windows lors de la connexion au serveur OfficeScan et à Trend Micro Smart Protection Network.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Proxy**.
2. Si le serveur proxy requiert une authentification, saisissez le nom d'utilisateur et le mot de passe, puis confirmez le mot de passe.

3. Cliquez sur **Enregistrer**.

Configuration des paramètres de suppression des agents inactifs

Vous pouvez configurer à quel moment OfficeScan change l'état des agents OfficeScan à « inactif ». OfficeScan définit un agent comme étant « inactif » après l'absence de réponse de l'agent OfficeScan au serveur pour l'une des raisons suivantes :

- Le programme de l'agent OfficeScan a été supprimé de l'Endpoint manuellement
- Un utilisateur a désactivé ou déchargé le programme de l'agent OfficeScan pour une période prolongée

Vous pouvez configurer OfficeScan pour automatiquement supprimer les agents OfficeScan inactifs de l'arborescence des agents.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Agents inactifs**.
2. Sélectionnez **Activer la suppression automatique des agents inactifs**.
3. Précisez ensuite combien de jours doivent s'écouler avant qu'OfficeScan considère l'agent OfficeScan comme étant inactif.
4. Cliquez sur **Enregistrer**.

Configuration des paramètres de l'enregistrement de Control Manager

Par défaut, l'enregistrement dans Control Manager est automatiquement configuré pendant le processus de provisionnement d'OfficeScan. Vous pouvez effectuer l'enregistrement sur un autre serveur Control Manager local si nécessaire (par exemple, vous souhaitez vous abonner à des listes d'objets suspects à partir d'un serveur Control Manager local).

Important

- OfficeScan prend uniquement en charge le réenregistrement sur des serveurs Control Manager 7.0 (ou version ultérieure) locaux.
- Si vous procédez à un enregistrement sur un serveur Control Manager 7.0 (ou version ultérieure) local, vous devez d'abord exécuter l'outil de connexion à distance OfficeScan en tant que Service sur un endpoint dans la zone démilitarisée pour permettre la communication entre la console OfficeScan cloud et le serveur Control Manager local.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Control Manager**.
2. Cliquez sur **Enregistrer auprès d'un autre serveur Control Manager**.
3. Spécifiez le **nom de domaine complet ou l'adresse IP** du nouveau serveur Control Manager.

   Important

   - Vous devez spécifier un serveur Control Manager local différent de celui qu'OfficeScan a actuellement enregistré.
   - Si vous avez défini un endpoint pour établir une connexion à distance à un serveur Control Manager local, spécifiez le **Nom de domaine complet ou l'adresse IP du serveur** de l'endpoint proxy inverse.

4. Spécifiez le **Port (HTTPS)** du serveur Control Manager.

   Important

   Si vous avez défini un endpoint pour établir une connexion à distance à un serveur Control Manager local, spécifiez le **Port (HTTPS)** de l'endpoint proxy inverse.

5. En regard de **Certificat de Control Manager**, cliquez sur **Parcourir...**, puis sélectionnez le fichier de certificat téléchargé à partir du serveur Control Manager cible.

Pour obtenir le fichier de certificat Control Manager, accédez au serveur Control Manager local et copiez le fichier de certificat sur le serveur OfficeScan à partir de l'emplacement suivant :

```
<Dossier d'installation de Control Manager>\Certificate\CA
\TMCM_CA_Cert.pem
```

Important

Si votre société utilise un certificat personnalisé sur le serveur Control Manager, vous devez télécharger le certificat d'autorité de certification racine pendant l'enregistrement de Control Manager.

Pour plus d'informations, voir *Autorisation de certificat de Control Manager à la page 12-6*.

6. Si le serveur Web IIS du serveur Control Manager local requiert une authentification, saisissez le nom d'utilisateur et le mot de passe.

7. Spécifiez le **Nom d'affichage de l'entité** qui identifie le serveur OfficeScan sur la console Control Manager.

   Par défaut, le nom d'affichage de l'entité inclut le nom d'hôte de l'ordinateur serveur et le nom de ce produit (par exemple, Server01_OSCE).

8. Cliquez sur **Connecter**.

Autorisation de certificat de Control Manager

Avant d'enregistrer OfficeScan sur le serveur Control Manager, vous devez d'abord obtenir le fichier de certificat de Control Manager à partir du serveur Control Manager à l'emplacement suivant :

```
<Dossier d'installation de Control Manager>\Certificate\CA
\TMCM_CA_Cert.pem
```

OfficeScan et Control Manager utilisent le chiffrement du certificat et de la clé publique pour garantir que seule une communication autorisée d'enregistrement et de gestion des stratégies est établie entre les serveurs. Si l'un des serveurs détecte une communication non autorisée, il rejette l'enregistrement ou les paramètres de stratégie reçus.

Important

Si votre société utilise un certificat personnalisé sur le serveur Control Manager, vous devez télécharger le certificat d'autorité de certification racine pendant l'enregistrement de Control Manager.

Configuration des paramètres de la console Web

Configurez les paramètres de la console Web OfficeScan pour déterminer comment les utilisateurs accèdent à la console Web et quelle est la fréquence de rafraîchissement de l'écran.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Console Web**.
2. Configurez les paramètres requis.

SECTION	SETTINGS
Paramètres d'actualisation automatique	Sélectionnez **Actualiser automatiquement la console Web** pour permettre au serveur OfficeScan d'actualiser les données à l'écran à l'intervalle spécifié • **Intervalle d'actualisation** : sélectionnez la fréquence (en secondes) à laquelle la console Web actualise les données affichées
Paramètres d'expiration de délai	Sélectionnez **Déconnecter automatiquement les utilisateurs inactifs** pour permettre au serveur OfficeScan de déconnecter les utilisateurs à l'intervalle spécifié • **Intervalle d'inactivité** : sélectionnez la période d'inactivité (en minutes) au terme de laquelle la console Web déconnecte automatiquement les utilisateurs

3. Cliquez sur **Enregistrer**.

Configuration des paramètres de la liste d'objets suspects

Pendant l'enregistrement de OfficeScan sur une instance locale de Control Manager, celle-ci déploie une clé API vers OfficeScan pour démarrer le processus d'abonnement. Pour activer ce processus d'abonnement automatique, vérifiez avec l'administrateur de Control Manager que Control Manager est connecté à Deep Discovery et que les paramètres requis sont configurés.

Important

La synchronisation de la liste des objets suspects est disponible uniquement si vous enregistrez OfficeScan sur un serveur local Control Manager 7.0 ou version ultérieure.

Pour plus d'informations sur l'enregistrement auprès d'un serveur Control Manager, consultez *Configuration des paramètres de l'enregistrement de Control Manager à la page 12-4*.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Liste d'objets suspects**.
2. Sélectionnez la liste à activer sur les agents.
   - Liste d'URL suspectes
   - Liste d'adresses IP suspectes (disponible uniquement lors de l'abonnement au serveur Control Manager enregistré)
   - Liste de fichiers suspects (disponible uniquement lors de l'abonnement au serveur Control Manager enregistré)
   - Liste de domaines suspects (disponible uniquement lors de l'abonnement au serveur Control Manager enregistré)

   Les administrateurs peuvent synchroniser manuellement les listes d'objets suspects à tout moment en cliquant sur le bouton **Synchroniser maintenant**.
3. Sous **Mettre à jour les listes d'objets suspects sur les agents OfficeScan**, indiquez quand les agents doivent mettre à jour les listes d'objets suspects.

- **En fonction de la programmation de mise à jour des composants de l'agent OfficeScan** :les agents OfficeScan mettent à jour les listes d'objets suspects en fonction du programme de mise à jour actuel.
- **Automatiquement après la mise à jour des listes d'objets suspects sur le serveur** :les agents OfficeScan mettent automatiquement les listes des objets suspects à jour lorsque le serveur OfficeScan a reçu des listes mises à jour.

Remarque

Les agents OfficeScan non configurés pour recevoir des mises à jour des agents de mise à jour effectuent des mises à jour incrémentielles des listes d'objets suspects abonnées pendant la synchronisation.

4. Cliquez sur **Enregistrer**.

Migration depuis un serveur OfficeScan local vers un serveur SaaS

OfficeScan prend en charge la migration des paramètres de serveur et d'agent OfficeScan d'un serveur OfficeScan local exécutant la version XG SP1 (ou une version ultérieure). Assurez-vous de mettre à niveau tous les agents OfficeScan que vous souhaitez migrer vers le serveur OfficeScan avant de tenter le processus de migration.

Le processus de migration impose l'exécution des tâches suivantes :

1. Utilisez l'outil de migration de serveur pour importer les paramètres de serveur OfficeScan source vers la console OfficeScan.

   Pour plus d'informations, voir *Utilisation de l'outil d'exportation des paramètres d'OfficeScan à la page 12-10*.

2. Migrez les paramètres de stratégie de serveur OfficeScan source vers la console OfficeScan as a Service (avec Control Manager).

   Pour plus d'informations, voir *Migration des paramètres de stratégie OfficeScan locale vers la console OfficeScan as a Service (avec Control Manager) à la page 12-15*.

3. Déplacez les agents OfficeScan du serveur source vers OfficeScan

Important

Avant de déplacer les agents OfficeScan vers le serveur OfficeScan, assurez-vous de modifier les paramètres de proxy pour les agents OfficeScan sur la console du serveur local sur **Utiliser les paramètres proxy de Windows** afin de permettre aux agents OfficeScan de se connecter à une instance d'OfficeScan Cloud Console.

Pour plus d'informations, consultez la rubrique *Configuration des paramètres proxy d'agent interne* du *Manuel de l'administrateur OfficeScan*.

Pour plus d'informations, voir *Déplacement d'Agents OfficeScan vers un autre domaine ou vers un autre serveur OfficeScan à la page 3-9*.

Utilisation de l'outil d'exportation des paramètres d'OfficeScan

Important

Cette version d'OfficeScan prend uniquement en charge les migrations à partir de la version XG SP1 d'OfficeScan et versions ultérieures. Assurez-vous de mettre à niveau le serveur OfficeScan source et tous les agents OfficeScan migrés vers la version XG SP1 avant de tenter de migrer des paramètres.

Pour obtenir la liste complète des éléments migrés par l'outil d'exportation des paramètres d'OfficeScan, reportez-vous à *Outil d'exportation des paramètres d'OfficeScan à la page 12-12*.

Procédure

1. Recherchez le package de l'outil de migration de serveur.
   - Dans la console Web OfficeScan, accédez à **Administration** > **Paramètres** > **Migration de serveur** et cliquez sur le lien **Télécharger l'outil d'exportation des paramètres d'OfficeScan**.
2. Copiez l'outil d'exportation des paramètres d'OfficeScan sur l'ordinateur du serveur OfficeScan source.

Important

Vous devez utiliser l'outil d'exportation des paramètres d'OfficeScan d'OfficeScan XG Service Pack 1 sur la version du serveur OfficeScan source pour vous assurer que toutes les données sont correctement mises en forme pour le nouveau serveur cible. OfficeScan XG Service Pack 1 n'est pas compatible avec les versions antérieures de l'outil de migration de serveur.

3. Double-cliquez sur `OfficeScanSettingsExportTool.exe` pour démarrer l'outil d'exportation des paramètres d'OfficeScan.

   L'outil d'exportation des paramètres d'OfficeScan s'exécute.

Remarque

Les noms par défaut des packages d'exportation sont les suivants :

- `OfficeScan_Agent_DLP_Policies.zip` (utilisé pour l'importation des paramètres de stratégie dans Control Manager)
- `OfficeScan_Agent_Policies.zip` (utilisé pour l'importation des autres paramètres de stratégie de l'agent OfficeScan dans Control Manager)
- `OfficeScan_Server_Migration.zip` (utilisé pour l'importation de tous les paramètres de stratégie de l'agent OfficeScan et des paramètres du serveur OfficeScan vers un autre serveur OfficeScan Cloud Console ou local)

4. Copiez le ou les packs d'exportation vers un emplacement accessible par le serveur OfficeScan ou Control Manager de destination.

5. Pour importer les paramètres vers le serveur OfficeScan de destination :

   a. Dans la console Web OfficeScan, accédez à **Administration** > **Paramètres** > **Migration du serveur** et cliquez sur le bouton **Importer des paramètres...**.

   b. Recherchez le pack `OfficeScan_Server_Migration.zip` et cliquez sur **Ouvrir**.

   c. Vérifiez que le serveur contient tous les paramètres de la version OfficeScan précédente.

6. Pour importer les paramètres de stratégie de l'agent OfficeScan sur la console Control Manager de destination :

a. Dans la console Web de Control Manager, accédez à **Stratégies** > **Gestion des stratégies**.

b. Dans la liste déroulante **Produit**, sélectionnez **Agent OfficeScan**.

c. Cliquez sur **Importer des paramètres**.

d. Recherchez le pack `OfficeScan_Agent_Policies.zip` et cliquez sur **Ouvrir**.

7. Pour importer les paramètres de stratégie DLP de l'agent OfficeScan sur la console Control Manager de destination :

a. Dans la console Web de Control Manager, accédez à **Stratégies** > **Gestion des stratégies**.

b. Dans la liste déroulante **Produit**, sélectionnez **Prévention contre la perte de données d'OfficeScan**.

c. Cliquez sur **Importer des paramètres**.

d. Recherchez le pack `OfficeScan_Agent_DLP_Policies.zip` et cliquez sur **Ouvrir**.

8. Déplacez les anciens agents OfficeScan vers le nouveau serveur OfficeScan.

Outil d'exportation des paramètres d'OfficeScan

OfficeScan fournit l'outil d'exportation des paramètres d'OfficeScan, qui permet aux administrateurs de copier les paramètres OfficeScan d'anciennes versions d'OfficeScan vers la version actuelle. L'outil d'exportation des paramètres d'OfficeScan effectue la migration des paramètres suivants :

<table>
<tr><th>FONCTION</th><th>PARAMÈTRES MIGRÉS</th></tr>
<tr><td>Gestion des agents

Remarque
L'outil d'exportation des paramètres d'OfficeScan effectue la migration des paramètres de gestion des agents appropriés vers les packs <code>OfficeScan_Agent_DLP_Policies.zip</code> et <code>OfficeScan_Agent_Policies.zip</code> qui seront utilisés lors de l'importation vers un serveur Control Manager.</td><td>• Scan manuel
• Scan programmé
• Scan en temps réel
• Scan immédiat
• Méthode de scan
• Web Reputation
• Surveillance des comportements
• Contrôle des dispositifs
• Prévention contre la perte de données
• Privilèges et autres paramètres
• Paramètres des services complémentaires
• Liste des spywares/ graywares approuvés
• Apprentissage automatique prédictif
• Connexion suspecte
• Liste des programmes approuvés

Remarque
• L'outil de migration de serveur ne migre pas les répertoires de sauvegarde pour les paramètres Scan manuel, Scan programmé, Scan en temps réel et Scanner.
• Les paramètres conservent les configurations au niveau de la racine et du domaine.</td></tr>
<tr><td>Regroupement des agents</td><td>Tous les paramètres

Remarque
Les structures de domaine Active Directory s'affichent après la première synchronisation avec Active Directory.</td></tr>
</table>

Fonction	Paramètres migrés
Paramètres généraux de l'agent	Tous les paramètres
Emplacement du endpoint	• Paramètres de détection d'emplacement • Listes des adresses IP et MAC de passerelle
Prévention contre la perte de données	• Identificateurs de données • Modèles
Pare-feu	• Stratégies • Profils
Maintenance des journaux	Tous les paramètres
Source de mise à jour des agents	• Source de mise à jour des agents • Liste des sources de mise à jour personnalisées
Sources Smart Protection	Liste des sources Smart Protection personnalisées
Notifications	• Paramètres généraux de notification • Paramètres de notification aux administrateurs • Paramètres de notification d'épidémies • Paramètres de notification aux agents
Proxy	Tous les paramètres
Agents inactifs	Tous les paramètres
Gestionnaire de quarantaine	Tous les paramètres
Console Web	Tous les paramètres
Paramètres d'`ofcscan.ini`	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION] : tous les paramètres

FONCTION	PARAMÈTRES MIGRÉS
Paramètres d'`ofcserver.ini`	[INI_SERVER_DISK_THRESHOLD] : tous les paramètres

Remarque

- L'outil ne sauvegarde pas les listes d'agents OfficeScan du serveur OfficeScan ; seules les structures de domaine sont sauvegardées.
- L'agent OfficeScan effectue uniquement la migration des fonctions disponibles sur l'ancienne version de son serveur. Pour les fonctions qui n'étaient pas disponibles sur l'ancien serveur, l'agent OfficeScan applique les paramètres par défaut.

Migration des paramètres de stratégie OfficeScan locale vers la console OfficeScan as a Service (avec Control Manager)

OfficeScan XG SP1 (ou version ultérieure) fournit un outil d'exportation des stratégies que vous pouvez utiliser pour migrer les stratégies d'un serveur OfficeScan local vers la console OfficeScan as a Service (avec Control Manager) pour vous assurer de maintenir votre niveau de sécurité actuel sans devoir reconfigurer tous vos paramètres de stratégie actuels.

Remarque

L'outil d'exportation des stratégies peut uniquement exporter des paramètres de stratégie de niveau domaine. Si vous avez configuré des agents OfficeScan individuels avec des paramètres personnalisés, vous devez recréer manuellement les stratégies individuelles.

Procédure

1. Accédez à l'ordinateur serveur OfficeScan XG SP1 source.
2. Utilisez un éditeur de ligne de commande et accédez au répertoire suivant :

   ```
   <répertoire d'installation du serveur>\PCCSRV\Admin\Utility
   \PolicyExportTool
   ```

3. Exécutez la commande suivante :

   `PolicyExportTool.exe -cmconsole`

   L'outil d'exportation des stratégies enregistre les paramètres de stratégie à l'emplacement suivant :

   `<répertoire d'installation du serveur>\PCCSRV\Admin\Utility\PolicyExportTool\PolicyClient_CMConsole.zip`

4. Connectez-vous à la console OfficeScan as a Service (avec Control Manager) et accédez à **Stratégies** > **Gestion des stratégies**.

5. Dans la liste déroulante **Produit**, sélectionnez **Agent OfficeScan**.

6. Cliquez sur **Importer des paramètres**.

7. Sélectionnez le fichier `<répertoire d'installation du serveur>\PCCSRV\Admin\Utility\PolicyExportTool\PolicyClient_CMConsole.zip` et importez.

   Les paramètres de stratégie migrés s'affichent dans la liste de gestion de stratégies de l'agent OfficeScan. OfficeScan as a Service (avec Control Manager) ajoute le nom de domaine d'origine d'OfficeScan à la fin de chaque nom de stratégie.

Partie VI

Obtenir de l'aide

Chapitre 13

Assistance technique

Découvrez les rubriques suivantes :

Ressources de dépannage

Avant de contacter le service d'assistance technique, consultez les ressources d'aide en ligne suivantes fournies par Trend Micro.

Utilisation du portail d'assistance

Le portail d'assistance de Trend Micro est une ressource en ligne disponible 24 h/24 et 7 j/7 qui contient les informations les plus récentes à la fois sur les problèmes courants et exceptionnels.

Procédure

1. Accédez à http://esupport.trendmicro.com.
2. Sélectionnez un des produits disponibles ou cliquez sur le bouton approprié pour chercher des solutions.
3. Utilisez la zone **Recherche de support** pour rechercher les solutions disponibles.
4. Si aucune solution n'est trouvée, cliquez sur **Contactez l'Assistance** et sélectionnez le type d'assistance dont vous avez besoin.

   Conseil

   Pour envoyer une demande d'assistance en ligne, visitez l'adresse suivante :

   http://esupport.trendmicro.com/srf/srfmain.aspx

   Un ingénieur d'assistance Trend Micro étudie le cas et répond en 24 heures maximum.

Encyclopédie des menaces

De nos jours, la plupart des programmes malveillants sont des menaces combinées : deux technologies ou plus qui sont combinées afin de contourner les protocoles de

sécurité des ordinateurs. Trend Micro lutte contre ces programmes malveillants complexes grâce à des produits qui créent une stratégie de défense personnalisée. L'Encyclopédie des menaces fournit une liste complète des noms et des symptômes de plusieurs menaces combinées, y compris les programmes malveillants, spams, URL malveillantes et failles connues.

Accédez à http://about-threats.trendmicro.com/fr/threatencyclopedia#malware pour en savoir plus sur :

- Les programmes malveillants et les codes mobiles malicieux actuellement actifs ou « en circulation »
- Les pages contenant des informations relatives aux menaces rassemblées pour former un historique complet des attaques Web
- Les informations sur les menaces Internet concernant les attaques ciblées et les menaces de sécurité
- Les informations sur les attaques Web et sur les tendances sur Internet
- Rapports hebdomadaires sur les programmes malveillants.

Comment contacter Trend Micro

Les revendeurs Trend Micro peuvent être contactés par téléphone ou courrier électronique :

Adresse	Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	+33 (0) 1 76 68 65 00
Site Web	http://www.trendmicro.fr
Adresse électronique	sales@trendmicro.fr

- Sites d'assistance à travers le monde :

  http://www.trendmicro.com/us/about-us/contact/index.html

- Comment contacter Trend Micro :

  http://www.trendmicro.fr/apropos/contact/index.html

- Documentation sur les produits Trend Micro :

  http://docs.trendmicro.com/fr-fr/home.aspx

Optimisation de la demande d'assistance

Pour améliorer la résolution de vos problèmes, préparez les informations suivantes :

- Étapes permettant de reproduire le problème
- Informations concernant l'appareil ou le réseau
- Marque de l'ordinateur, modèle et tout matériel complémentaire ou périphériques connectés
- Quantité de mémoire et d'espace disque disponible
- Version du système d'exploitation et du Service Pack
- Version de l'agent installé
- Numéro de série ou code d'activation
- Description détaillée de l'environnement d'installation
- Texte exact du message d'erreur affiché

Envoi de contenu suspect à Trend Micro

Plusieurs façons d'envoyer du contenu suspect à Trend Micro pour une analyse plus poussée sont à votre disposition.

services de réputation de messagerie (Email Reputation Services)

Lancez une interrogation de la réputation d'une adresse IP spécifique et indiquez un agent de transfert de messages à inclure dans la liste globale des éléments approuvés :

https://ers.trendmicro.com/

Reportez-vous à l'entrée suivante de la Base de connaissances pour envoyer des échantillons de messages à Trend Micro :

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Services de File Reputation

Collectez des informations système et envoyez le contenu de fichiers suspects à Trend Micro :

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Notez le numéro de dossier à des fins de suivi.

Services de Web Reputation

Lancez une interrogation de l'évaluation de sécurité et du type de contenu d'une URL que vous pensez correspondre à un site de phishing ou un autre « vecteur de menaces » (source de menaces Internet intentionnelles telles que les spywares et programmes malveillants) :

http://global.sitesafety.trendmicro.com/

Si l'évaluation attribuée est incorrecte, envoyez une demande de reclassification à Trend Micro.

Autres ressources

Outre les solutions et l'assistance disponibles en ligne, d'autres ressources, dont le but est de maintenir à jour vos systèmes, de vous informer des innovations les plus récentes et

de vous faire connaître les dernières tendances en matière de sécurité, sont également consultables.

Centre de téléchargement

Trend Micro est susceptible de publier, de temps à autre, un patch corrigeant un problème connu ou une mise à niveau s'appliquant à un produit ou service particulier. Pour savoir si des patches sont disponibles, rendez-vous sur le site :

http://downloadcenter.trendmicro.com/index.php?regs=fr

Si l'un des patches disponibles n'a pas été appliqué (les patches sont datés), ouvrez le fichier Lisez-moi afin de déterminer s'il convient à votre environnement. Le fichier Lisez-moi contient également des instructions d'installation.

Commentaires relatifs à la documentation

Trend Micro cherche toujours à améliorer sa documentation. Si vous avez des questions, des commentaires ou des suggestions à propos de ce document ou de tout autre document Trend Micro, veuillez consulter le site suivant°:

http://www.trendmicro.com/download/documentation/rating.asp

Index

TREND MICRO INCORPORATED

Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France

Tél. : +33 (0) 1 76 68 65 00 sales@trendmicro.fr

www.trendmicro.com

Item Code: OSFM08045/170922