TREND MICRO™

11.0 OfficeScan™

Guide d'installation et de mise à niveau

Pour les grandes et moyennes entreprises

Endpoint Security

Protected Cloud

Web Security

N° de référence du document : OSEM116301_140127

Date de publication : avril 2014

Protégée par le brevet américain n° : 5,951,698

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

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du produit dans le centre d'aide en ligne et la Base de connaissances Trend Micro.

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 nous contacter à l'adresse docs@trendmicro.com.

Vous pouvez évaluer cette documentation sur le site Web suivant :

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

Table des matières

Préface

Chapitre 1: Planification de l'installation d'OfficeScan

Chapitre 2: Installation d'OfficeScan

Chapitre 3: Mise à niveau d'OfficeScan

Chapitre 4: Tâches après l'installation

Chapitre 5: Désinstallation et rétrogradation d'OfficeScan

Chapitre 6: Obtenir de l'aide

Annexe A: Exemple de déploiement

Index

Préface

Préface

Bienvenue dans Trend Micro™ OfficeScan™ *Guide d'installation et de mise à niveau* Ce document décrit les éléments requis et les procédures pour installer le serveur OfficeScan et mettre à jour le serveur et les agents.

Sujets abordés dans ce chapitre :

Remarque

Pour plus d'informations sur l'installation des agents, consultez le *Manuel de l'administrateur*.

Documentation OfficeScan

La documentation OfficeScan comprend les documents suivants :

TABLEAU 1. Documentation OfficeScan

DOCUMENTATION	DESCRIPTION
Guide d'installation et de mise à niveau	Document PDF contenant les exigences et les procédures d'installation du serveur OfficeScan
Manuel de l'administrateur	Document PDF contenant des informations relatives au démarrage, ainsi que les procédures d'installation des agents, et abordant l'administration des serveurs et des agents OfficeScan.
Aide	Fichiers HTML compilés au format WebHelp ou CHM contenant des descriptions de procédures, des conseils d'utilisation et des informations relatives aux champs. L'aide est accessible depuis les consoles du serveur OfficeScan, de l'agent et du serveur Policy Server, ainsi que depuis la configuration générale d'OfficeScan.
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 :

- Administrateur OfficeScan : responsables de l'administration d'OfficeScan, ce qui inclut l'installation et la gestion des serveurs et 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 sur les endpoints desquels est installé l'agent OfficeScan. 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.

NOMENCLATURE	DESCRIPTION
 **Remarque**	Remarques sur la configuration
 **Conseil**	Recommandations ou suggestions
 **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
Administrateur (ou administrateur OfficeScan)	Personne qui gère le serveur OfficeScan
Endpoint de l'agent	Endpoint sur lequel l'agent OfficeScan est installé

`Dossier d'installation de l'agent`	Dossier du 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
Utilisateur de l'agent (ou utilisateur)	Personne qui gère l'agent OfficeScan sur le endpoint de l'agent
Composants	Responsables du scan, de la détection et des actions contre les risques liés à la sécurité
Console	Interface utilisateur permettant de configurer et de gérer les paramètres des serveurs et des agents OfficeScan. La console employée pour le programme du serveur OfficeScan est appelée « console Web » et celle employée pour le programme de l'agent OfficeScan est appelée « console de l'agent ».
Agent de scan traditionnel	Agent OfficeScan ayant été configuré pour utiliser le scan traditionnel.
Double pile	Entités ayant à la fois une adresse IPv4 et une adresse IPv6. Par exemple : • Endpoints ayant à la fois une adresse IPv4 et une adresse IPv6. • Agents OfficeScan installés sur des endpoints à double pile. • Agents de mise à jour chargés de distribuer les mises à jour aux autres agents. • Serveur proxy à double pile, tel que DeleGate, pouvant effectuer la conversion entre adresses IPv4 et IPv6.
Service licence	Inclut les services antivirus, Damage Cleanup Services, les services de réputation de sites Web et anti-spyware, qui sont tous activés lors de l'installation du serveur OfficeScan
agent OfficeScan	Programme de l'agent OfficeScan
Service OfficeScan	Services hébergés via Microsoft Management Console (MMC). Par exemple, `ofcservice.exe`, le service principal d'OfficeScan.

TERMINOLOGIE	DESCRIPTION
Solutions de plug-in	Fonctions natives d'OfficeScan et modules additionnels proposés via Plug-in Manager.
Programme	Inclut l'agent OfficeScan, Cisco Trust Agent et Plug-in Manager
IPv4 pur	Une entité n'ayant qu'une adresse IPv4
IPv6 pur	Une entité n'ayant qu'une adresse IPv6
Risques liés à la sécurité	Terme générique regroupant les virus/programmes malveillants, les spywares/graywares et les menaces Internet
Serveur	Programme serveur OfficeScan
Ordinateur serveur	Endpoint sur lequel le serveur OfficeScan est installé.

`Dossier d'installation du serveur`	Dossier du 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>`.

Agent Smart Scan	Agent OfficeScan ayant été configuré pour utiliser Smart Scan.

Chapitre 1

Planification de l'installation d'OfficeScan

Ce chapitre fournit des informations préalables et indique comment préparer l'installation de Trend Micro™ OfficeScan.

Sujets abordés dans ce chapitre :

Configuration requise pour une nouvelle installation et une mise à niveau

Effectuez une nouvelle installation du serveur et des agents OfficeScan Server sur des plates-formes serveur Windows prises en charge.

En outre, cette version d'OfficeScan prend en charge les mises à niveau depuis les versions suivantes :

- 10,6 Service Pack 3
- 10,6 Service Pack 2
- 10.6 Service Pack 1 Patch 1
- 10.6
- 10,5 Patch 5
- 10.0 Service Pack 1 Patch 5

Visitez le site Web suivant pour obtenir la liste complète des configurations requises pour une nouvelle installation :

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

Versions du produit

Installez une version complète ou une version d'évaluation d'OfficeScan. Les deux versions ont besoin d'un type de code d'activation différent. Pour obtenir un code d'activation, enregistrez le produit auprès de Trend Micro.

TABLEAU 1-1. Comparaison de versions

VERSION	DESCRIPTION
version complète	La version complète comprend toutes les fonctionnalités du produit et le service d'assistance technique, et offre une période de grâce (généralement 30 jours) après l'expiration de la licence. Lors que la période de grâce expire, l'assistance technique et les mises à jour des composants ne sont plus disponibles. Les moteurs de scan continuent à scanner les endpoints à l'aide des composants obsolètes. Ces composants obsolètes risquent de ne pas protéger totalement les endpoints contre les derniers risques de sécurité. Renouvelez la licence avant ou après son expiration en achetant un renouvellement de votre contrat de maintenance.
Version d'évaluation	La version d'évaluation comprend toutes les fonctionnalités du produit. Vous pouvez mettre à niveau une version d'évaluation vers la version complète à tout moment. S'il n'est pas mis à niveau à la fin de la période d'évaluation, OfficeScan désactive les mises à jour de composants, le scan et toutes les fonctionnalités des agents.

Clé d'enregistrement et codes d'activation

Pendant l'installation, indiquez les codes d'activation pour les services suivants :

- Antivirus
- Damage Cleanup Services™ (facultatif)
- Réputation de sites Web et anti-spyware (facultatif)

Utilisez la clé d'enregistrement fournie avec votre produit pour obtenir les codes d'activation (si ce n'est déjà fait). Le programme d'installation vous redirige automatiquement vers le site Web de Trend Micro, sur lequel vous pouvez enregistrer votre produit.

https://olr.trendmicro.com/

Une fois le produit enregistré, Trend Micro vous envoie les codes d'activation.

Contactez un revendeur local Trend Micro pour obtenir la clé d'enregistrement ou les codes d'activation, s'ils ne sont pas disponibles au moment de l'installation. Voir *Comment contacter Trend Micro à la page 6-11* pour obtenir des informations détaillées.

Remarque

Pour toute question sur l'enregistrement, consultez la page :

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

Éléments à prendre en compte pour une nouvelle installation

Lorsque vous effectuez une nouvelle installation du serveur OfficeScan, tenez compte des points suivants :

- *Prise en charge d'IPv6 à la page 1-4*
- *Emplacement du serveur OfficeScan à la page 1-5*
- *Installation à distance à la page 1-6*
- *Performances du serveur à la page 1-6*
- *Serveur dédié à la page 1-7*
- *Déploiement de la méthode de scan pendant l'installation à la page 1-7*
- *Trafic réseau à la page 1-9*
- *Logiciels de sécurité tiers à la page 1-10*
- *Active Directory à la page 1-11*
- *Serveur Web à la page 1-11*

Prise en charge d'IPv6

Les exigences IPv6 pour une nouvelle installation du serveur OfficeScan sont les suivantes :

- Le serveur OfficeScan doit être installé sur Windows Server 2008 ou Windows Server 2012. Il ne peut pas être installé sur Windows Server 2003, car ce système d'exploitation ne prend que partiellement en charge l'adressage IPv6.
- Le serveur doit utiliser un serveur Web IIS. Le serveur Web Apache ne prend pas en charge l'adressage IPv6.
- Si le serveur peut gérer les agents IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et doit être identifié par son nom d'hôte. Si un serveur est identifié par ses adresses IPv4, les agents IPv6 ne peuvent pas s'y connecter. Le même problème se pose lorsque des agents IPv4 purs se connectent à un serveur identifié par son adresse IPv6.
- Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6. Lorsque le serveur est identifié par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.

  Remarque

  Le nom de domaine complet ne peut être spécifié que lors de l'installation locale du serveur. Il n'est pas pris en charge pour les installations à distance.

- Vérifiez que l'adresse IPv6 ou IPv4 de l'ordinateur hôte peut être récupérée en utilisant, par exemple, la commande « `ping` » ou « `nslookup` ».
- Si vous installez le serveur OfficeScan sur un endpoint IPv6 pur :
  - Configurez un serveur proxy à double pile, tel que DeleGate, qui peut assurer la conversion entre les adresses IPv4 et IPv6. Positionnez le serveur proxy entre le serveur OfficeScan et Internet, pour permettre au serveur de se connecter aux services hébergés de Trend Micro, tels que le serveur ActiveUpdate, le site Web d'enregistrement en ligne et Smart Protection Network.

Emplacement du serveur OfficeScan

OfficeScan peut s'adapter à tout un éventail d'environnements réseau. Par exemple, vous pouvez placer un pare-feu entre le serveur OfficeScan et ses agents, ou placer le serveur

et tous les agents derrière un seul pare-feu réseau. S'il existe un pare-feu entre le serveur et ses agents, configurez le pare-feu pour permettre le trafic entre les ports d'écoute des agents et du serveur.

Remarque

Pour plus d'informations sur la résolution des problèmes lors de la gestion des agents OfficeScan sur un réseau qui utilise le mode Network Address Translation (NAT), consultez le *Manuel de l'administrateur*.

Installation à distance

L'installation à distance permet de lancer l'installation sur un endpoint et d'installer OfficeScan sur un autre endpoint. Lorsque vous effectuez une installation à distance, le programme d'installation vérifie si le endpoint cible dispose de la configuration requise pour l'installation du serveur.

Pour garantir que l'installation puisse s'effectuer :

- Sur chaque endpoint cible, démarrez le service Accès à distance au Registre en utilisant un compte administrateur et non un compte système local. Le service Accès à distance au Registre est géré à partir de Microsoft Management Console (cliquez sur **Démarrer** > **Exécuter** et saisissez `services.msc`).
- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que le endpoint possède la configuration système requise pour le serveur OfficeScan. Voir *Configuration requise pour une nouvelle installation et une mise à niveau à la page 1-2* pour obtenir des informations complémentaires.

Performances du serveur

Les serveurs des réseaux de grandes entreprises exigent plus de puissance que ceux des PME.

Conseil

Trend Micro recommande de disposer au minimum de doubles processeurs à 2GHz et de plus de 2Go de mémoire vive pour le serveur OfficeScan.

Le nombre d'agents de endpoint en réseau qu'un seul serveur OfficeScan peut gérer dépend de différents facteurs, tels que les ressources serveur disponibles et la topologie du réseau. Contactez votre revendeur Trend Micro afin qu'il vous aide à déterminer le nombre d'agents que le serveur peut gérer.

Serveur dédié

Lorsque vous sélectionnez le endpoint devant héberger le serveur OfficeScan, tenez compte des points suivants :

- La charge processeur que le endpoint doit gérer
- Si le endpoint assure d'autres fonctions

Si le endpoint cible assure d'autres fonctions, choisissez un endpoint qui n'exécute pas d'applications stratégiques ou consommant beaucoup de ressources.

Déploiement de la méthode de scan pendant l'installation

Dans cette version d'OfficeScan, vous pouvez configurer les agents pour qu'ils utilisent le mode Smart Scan ou le scan traditionnel.

Scan traditionnel

Le scan traditionnel est la méthode utilisée dans toutes les anciennes versions d'OfficeScan. Un agent de scan traditionnel stocke tous les composants OfficeScan sur le endpoint de l'agent et scanne tous les fichiers localement.

Smart Scan

Smart Scan exploite les signatures de menaces stockées en ligne. En mode Smart Scan, l'agent OfficeScan effectue d'abord un scan local pour rechercher les risques de sécurité.

Si l'agent ne parvient pas à déterminer le risque que présente le fichier durant le scan, il se connecte à un serveur Smart Protection Server.

Smart Scan présente les avantages et fonctionnalités suivants :

- Offre des fonctions de surveillance de l'état de sécurité rapides et en temps réel sur le web
- Réduit le temps global nécessaire pour assurer la protection contre les menaces émergentes
- Réduit l'utilisation de la bande passante réseau durant les mises à jour des fichiers de signatures. Au lieu d'être diffusée sur de nombreux agents, la masse des mises à jour des définitions de signatures est simplement mise en ligne.
- Réduit le coût et le temps de gestion associés aux déploiements de fichiers de signatures dans l'entreprise
- Diminue la mémoire utilisée par le noyau sur les endpoints. Augmentation minimale de la consommation au fil du temps

Déploiement de la méthode de scan

Pendant les nouvelles installations, la méthode de scan par défaut des agents est la méthode Smart Scan. OfficeScan vous permet également de personnaliser la méthode de scan pour chaque domaine après l'installation du serveur. Tenez compte de ce qui suit :

- Si vous n'avez pas changé de méthode de scan après l'installation du serveur, tous les agents que vous installez utiliseront Smart Scan.
- Pour utiliser le scan traditionnel sur tous les agents, changez la méthode de scan de niveau racine en scan traditionnel après l'installation du serveur.
- Si vous voulez utiliser à la fois le scan traditionnel et Smart Scan, Trend Micro vous recommande de conserver Smart Scan comme méthode de scan de niveau racine, puis de modifier la méthode de scan sur les domaines devant appliquer le scan traditionnel.

Trafic réseau

Lorsque vous planifiez un déploiement, tenez compte du trafic réseau généré par OfficeScan. Le serveur génère du trafic :

- lorsqu'il se connecte au Trend Micro ActiveUpdate Server pour vérifier et télécharger les composants mis à jour,
- lorsqu'il prévient les agents de télécharger des composants mis à jour,
- lorsqu'il notifie les agents des changements de configuration.

L'agent OfficeScan génère du trafic :

- lorsqu'il démarre,
- lorsqu'il met à jour les composants,
- lorsqu'il met à jour les paramètres et installe un correctif de type hotfix,
- lorsqu'il recherche des risques de sécurité,
- lorsqu'il bascule entre le mode « itinérance » et le mode « normal »,
- lorsqu'il bascule entre le scan traditionnel et le mode Smart Scan.

Trafic réseau pendant les mises à jour de composants

Lorsqu'il met à jour un composant, OfficeScan génère un trafic réseau important. Pour réduire le trafic réseau généré au cours des mises à jour des composants, OfficeScan réalise une duplication des composants. Au lieu de télécharger l'intégralité d'un fichier de signatures mis à jour, OfficeScan télécharge seulement les signatures « incrémentielles » (des versions plus petites du fichier de signatures complet) et les fusionne avec l'ancien fichier de signatures après le téléchargement.

Les agents OfficeScan mis régulièrement à jour ne téléchargent que le fichier de signatures incrémentiel. Sinon, ils téléchargent le fichier de signatures complet.

Trend Micro publie régulièrement de nouveaux fichiers de signatures. Trend Micro publie également un nouveau fichier de signatures dès la découverte d'un virus/programme malveillant destructeur circulant activement.

Agents de mise à jour et trafic réseau

Si le réseau reliant les agents et le serveur OfficeScan présente des sections à faible bande passante ou à fort trafic, désignez certains agents OfficeScan comme agents de mise à jour, ou sources de mise à jour pour les autres agents. Cela aide à répartir la charge de travail en ce qui concerne le déploiement des composants vers tous les agents.

Par exemple, si vous disposez d'un bureau distant comportant au moins 20 endpoints, désignez un agent de mise à jour afin qu'il réplique les mises à jour du serveur OfficeScan et fonctionne comme point de distribution pour les autres endpoints d'agent du réseau local. Consultez le *Manuel de l'administrateur* pour plus d'informations sur les agents de mise à jour.

Trend Micro Control Manager et trafic réseau

Trend Micro Control Manager™ gère les produits et les services Trend Micro au niveau de la passerelle, du serveur de messagerie, du serveur de fichiers et des postes de travail de l'entreprise. La console de gestion de type Web de Control Manager permet de surveiller les produits et les services de l'ensemble du réseau à partir d'un point unique.

Utilisez Control Manager pour gérer plusieurs serveurs OfficeScan de manière centralisée. Un serveur Control Manager bénéficiant d'une connexion Internet rapide et fiable peut télécharger les composants depuis le Trend Micro ActiveUpdate Server. Control Manager déploie ensuite les composants sur un ou plusieurs serveurs OfficeScan ne possédant pas de connexion Internet, ou disposant d'une connexion peu fiable.

Pour plus de détails, consultez la documentation de Control Manager.

Logiciels de sécurité tiers

Supprimez les logiciels de sécurité de endpoints du endpoint sur lequel vous installez le serveur OfficeScan. Ces applications peuvent empêcher l'installation du serveur OfficeScan ou affecter ses performances. Installez le serveur et l'agent OfficeScan immédiatement après avoir supprimé le logiciel tiers pour protéger le endpoint contre les risques de sécurité.

Remarque

OfficeScan ne peut pas désinstaller automatiquement le composant serveur d'un produit antivirus tiers, mais peut désinstaller le composant agent. Consultez le *Manuel de l'administrateur d'OfficeScan* pour obtenir des informations détaillées.

Active Directory

Vérifiez que tous les serveurs OfficeScan font partie d'un domaine Active Directory pour tirer profit des fonctionnalités de Role-based Administration et de conformité de la sécurité.

Serveur Web

Les fonctions du serveur Web OfficeScan sont les suivantes :

- il permet aux utilisateurs d'accéder à la console Web,
- il accepte les commandes des agents,
- il permet aux agents de répondre aux notifications du serveur.

Vous pouvez utiliser un serveur Web IIS ou Apache. Si vous utilisez un serveur Web IIS, assurez-vous que l'ordinateur serveur n'exécute pas d'applications verrouillant IIS. Le programme d'installation arrête et redémarre le service IIS pendant l'installation.

Si vous utilisez un serveur Web Apache, le compte administrateur est le seul compte créé sur ce dernier. Créez un autre compte à partir duquel vous exécuterez le serveur Web pour éviter que le serveur OfficeScan ne soit compromis si un pirate parvient à prendre le contrôle du serveur Web Apache.

Consultez le site *http://www.apache.org* pour accéder aux dernières informations sur les mises à niveau, les patchs et les problèmes de sécurité du serveur Web Apache.

Éléments à prendre en compte pour la mise à niveau

Tenez compte des points suivants lors de la mise à niveau du serveur et des agents OfficeScan :

Prise en charge d'IPv6

Les exigences IPv6 pour la mise à niveau du serveur et de l'agent OfficeScan sont les suivantes :

- Le serveur OfficeScan à mettre à niveau doit être installé sur Windows Server 2008 ou 2012. Les serveurs OfficeScan sur Windows Server 2003 ne peuvent pas être mis à niveau, car ce système d'exploitation ne prend que partiellement en charge l'adressage IPv6.
- Le serveur OfficeScan à mettre à niveau doit être la version 10.x.
- Le serveur doit utiliser déjà un serveur Web IIS. Le serveur Web Apache ne prend pas en charge l'adressage IPv6.
- Affectez une adresse IPv6 au serveur. De plus, le serveur doit être identifié par son nom d'hôte, de préférence son nom de domaine complet (FQDN ou (Fully Qualified Domain Name). Si le serveur est identifié par son adresse IPv6, tous les agents actuellement gérés par le serveur perdent la connexion à celui-ci. Si le serveur est identifié par son adresse IPv4, il ne peut pas déployer l'agent sur des endpoints IPv6 purs.
- Vérifiez que l'adresse IPv6 ou IPv4 de l'ordinateur hôte peut être récupérée en utilisant, par exemple, la commande **`ping`** ou **`nslookup`**.

Systèmes d'exploitation non pris en charge

OfficeScan ne prend plus en charge les systèmes d'exploitation Windows 95, 98, Me, NT, 2000 et la plate-forme d'architecture Itanium.

Si vous prévoyez d'effectuer une mise à niveau vers cette version à partir d'OfficeScan 10.x et si vous disposez d'agents OfficeScan 10.x exécutant ces systèmes d'exploitation :

- Ne mettez pas à niveau tous les serveurs OfficeScan 10.x vers cette version d'OfficeScan.
- Désignez au moins un serveur OfficeScan 10.x (serveur parent) pour gérer les agents exécutant les systèmes d'exploitation non pris en charge.
- Avant de mettre à niveau les autres serveurs :
    - Connectez-vous à la console Web et, dans le menu principal, cliquez sur **Ordinateurs en réseau** > **Gestion des clients**.
    - Dans l'arborescence des agents, sélectionnez les agents que vous souhaitez déplacer, puis cliquez sur **Gérer l'arborescence client** > **Déplacer client**.
    - Spécifiez le nom/l'adresse IP du endpoint du serveur parent et le port d'écoute du serveur sous **Déplacer le(s) client(s) sélectionné(s) vers un autre serveur OfficeScan**.
    - Cliquez sur **Déplacer**.

Paramètres et configurations d'OfficeScan

Sauvegardez la base de données OfficeScan et les fichiers de configuration importants avant de mettre à niveau le serveur OfficeScan. Sauvegardez la base de donnés du serveur OfficeScan à un emplacement situé à l'extérieur du répertoire du programme OfficeScan.

Conseil

Cette version d'OfficeScan offre un mécanisme de sauvegarde à des fins de restauration. Effectuez une sauvegarde manuelle de la base de données si vous ne prévoyez pas d'utiliser la sauvegarde automatique pendant l'installation.

Sauvegarde et restauration de la base de données et des fichiers de configuration OfficeScan

Procédure

1. Sauvegardez la base de données à partir de la console Web d'OfficeScan 10.x en accédant à **Administration** > **Sauvegarde de la base de données**.

   Pour des instructions détaillées, consultez le *Manuel de l'administrateur* ou l'*aide du serveur* de ces versions de produit.

   AVERTISSEMENT!

   N'utilisez aucun autre type d'outil ou d'application de sauvegarde.

2. Arrêtez le service principal d'OfficeScan à partir de Microsoft Management Console.

3. Sauvegardez manuellement les fichiers et dossiers suivants figurant dans le `<dossier d'installation du serveur>\PCCSRV:`

   Remarque

   Sauvegardez ces fichiers et ces dossiers afin de pouvoir rétrograder OfficeScan si vous rencontrez des problèmes de mise à niveau.

   - `ofcscan.ini` : contient les paramètres d'agent généraux
   - `ous.ini` : contient la table source de mise à jour pour le déploiement des composants antivirus
   - `Dossier` privé : contient les paramètres du pare-feu et de la source de mise à jour

- Dossier `Web\tmOPP` : contient les paramètres de prévention des épidémies
- `Pccnt\Common\OfcPfw*.dat` : contient les paramètres du pare-feu
- `Download\OfcPfw*.dat` : contient les paramètres de déploiement du pare-feu
- Dossier de `journaux` : contient les événements système et les journaux de vérification de la connexion
- Dossier `Virus` : contient les fichiers mis en quarantaine
- Dossier `HTTPDB` : contient la base de données OfficeScan

4. Mettez à niveau le serveur OfficeScan.

Remarque

Si vous rencontrez des problèmes de mise à niveau, copiez les fichiers de sauvegarde obtenus à l'étape 3 dans le `<dossier d'installation du serveur>\PCCSRV` du endpoint cible et redémarrez le service principal d'OfficeScan.

Déploiement de la méthode de scan pendant la mise à niveau

Dans cette version d'OfficeScan, les administrateurs peuvent configurer les agents pour qu'ils utilisent le mode Smart Scan ou le scan traditionnel.

Lorsque vous mettez à niveau OfficeScan à partir d'une version antérieure, vous pouvez conserver ou personnaliser la méthode de scan pour chaque domaine en fonction de la méthode de mise à niveau choisie. Tenez compte de ce qui suit :

- Lorsque vous prévoyez de mettre à niveau le serveur OfficeScan 10.x directement sur l'ordinateur serveur, il n'est pas nécessaire de changer de méthode de scan à partir de la console Web car les agents conservent leurs paramètres de méthode de scan après leur mise à niveau.
- Lorsque vous prévoyez de mettre à niveau les agents OfficeScan 10.x en les déplaçant vers le serveur OfficeScan 11.0 :

- Dans le serveur OfficeScan 11.0, choisissez le regroupement manuel d'agents. Cette méthode permet la création de domaines.

Remarque

Lorsque vous utilisez le regroupement automatique des agents, activez cette option uniquement après la mise à niveau de tous les agents afin de garantir que tous les paramètres de méthode de scan sont conservés durant la mise à niveau des agents.

- Dupliquez les paramètres de structure de domaine et de méthode de scan du serveur OfficeScan 10.x dans le serveur OfficeScan 11,0. Si les paramètres de structure de domaine et de méthode de scan des deux serveurs ne sont pas identiques, il se peut que certains agents déplacés vers le serveur OfficeScan 11.0 n'appliquent pas leurs paramètres de méthode de scan initiaux.

Liste de contrôle de l'installation et de la mise à niveau

Le programme d'installation vous invite à fournir les informations suivantes lorsque vous installez ou mettez à niveau le serveur OfficeScan.

TABLEAU 1-2. Liste de contrôle de l'installation et de la mise à niveau

INFORMATIONS SUR L'INSTALLATION	INFORMATIONS NÉCESSAIRES			
	NOUVELLE INSTALLATION LOCALE/EN MODE SILENCIEUX	NOUVELLE INSTALLATION À DISTANCE	MISE À NIVEAU LOCALE/EN MODE SILENCIEUX	MISE À NIVEAU À DISTANCE
Chemin d'installation d'OfficeScan Le chemin d'installation par défaut du serveur est le suivant : • `C:\Program Files\Trend Micro\OfficeScan` • `C:\Program Files (x86)\Trend Micro\OfficeScan` (pour les plates-formes de type x64) Identifiez le chemin d'installation ou utilisez le chemin par défaut. Si le chemin n'existe pas, le programme d'installation le crée automatiquement.	Oui	Oui	Non	Oui
Paramètres du serveur proxy Si le serveur OfficeScan se connecte à Internet via un serveur proxy, spécifiez les éléments suivants : • Type de proxy (HTTP ou SOCKS 4) • Nom ou adresse IP de l'ordinateur • Port • Informations d'authentification du serveur proxy	Oui	Oui	Non	Oui

Informations sur l'installation	Informations nécessaires			
	Nouvelle installation locale/en mode silencieux	Nouvelle installation à distance	Mise à niveau locale/en mode silencieux	Mise à niveau à distance
Paramètres du serveur Web Le serveur Web (Apache ou IIS) exécute des scripts CGI de console Web et accepte des commandes des agents. Indiquez ce qui suit : • Port HTTP : Le port par défaut est 8080. Si vous utilisez le site Web par défaut IIS, vérifiez le port TCP du serveur HTTP. **AVERTISSEMENT!** De nombreux piratages et attaques de virus/programmes malveillants diffusés sur HTTP utilisent les ports 80 et/ou 8080. La plupart des entreprises utilisent ces numéros de port comme ports TCP par défaut pour les communications HTTP. Si les numéros de port par défaut sont actuellement en cours d'utilisation, choisissez-en d'autres. Si vous activez les connexions sécurisées : • Période de validité du certificat SSL • Port SSL (par défaut : 4343)	Oui	Oui	Non	Oui

Informations sur l'installation	Informations nécessaires			
	Nouvelle installation locale/en mode silencieux	Nouvelle installation à distance	Mise à niveau locale/en mode silencieux	Mise à niveau à distance

Enregistrement
 	
Enregistrez le produit pour recevoir les codes d'activation. Les informations suivantes sont requises pour l'enregistrement du produit :
• Pour les clients existants :
  • Compte d'enregistrement en ligne (nom et mot de passe de connexion)
• Pour les utilisateurs ne possédant pas de compte :
  • Clé d'enregistrement
	Oui	Oui	Oui	Oui

Activation Procurez-vous les codes d'activation pour les services suivants du produit : • Antivirus • Damage Cleanup Services • Réputation de sites Web et anti-spyware	Oui	Oui	Oui	Oui

Informations sur l'installation	Informations nécessaires			
	Nouvelle installation locale/en mode silencieux	Nouvelle installation à distance	Mise à niveau locale/en mode silencieux	Mise à niveau à distance
Installation du serveur Smart Protection Server intégré Lorsque vous installez le serveur intégré, indiquez ce qui suit : • Période de validité du certificat SSL • Port SSL	Oui	Oui	Oui	Oui

Destination de l'installation à distance
 	
Identifiez les endpoints sur lesquels vous installez/mettez à niveau le serveur OfficeScan. Préparez ce qui suit :
• Liste des noms ou des adresses IP des endpoints
• (Facultatif) Un fichier texte avec une liste de endpoints ou d'adresses IP cible
 	
Exemple de contenu du fichier texte :
 	
`us-user_01`
 	
`us-admin_01`
 	
`123.12.12.123`
	Non	Oui	Non	Oui

Informations sur l'installation	Informations nécessaires			
	Nouvelle installation locale/en mode silencieux	Nouvelle installation à distance	Mise à niveau locale/en mode silencieux	Mise à niveau à distance
Analyse du endpoint pour une installation à distance Le programme d'installation vous invite à fournir les informations suivantes avant d'effectuer l'analyse du endpoint cible : • Nom d'utilisateur et mot de passe pour un compte administrateur disposant du privilège de « connexion en tant que service » sur le endpoint cible.	Non	Oui	Non	Oui
Installer l'agent OfficeScan	Oui	Non	Non	Non
Mot de passe du compte administrateur Le programme d'installation crée un compte racine pour la connexion à la console Web. Indiquez ce qui suit : • Mot de passe du compte racine Empêchez la désinstallation ou le déchargement non autorisé de l'agent OfficeScan en spécifiant ce qui suit : • Mot de passe de déchargement et de désinstallation de l'agent OfficeScan	Oui	Oui	Non	Non

Informations sur l'installation	Informations nécessaires			
	Nouvelle installation locale/en mode silencieux	Nouvelle installation à distance	Mise à niveau locale/en mode silencieux	Mise à niveau à distance
Chemin d'installation de l'agent OfficeScan Spécifiez le répertoire du endpoint d'agent sur lequel l'agent OfficeScan sera installé. Indiquez ce qui suit : • Chemin d'installation : Le chemin d'installation par défaut de l'agent est `$ProgramFiles\Trend Micro\OfficeScan Client`. Identifiez le chemin d'installation ou utilisez le chemin par défaut. Si le chemin n'existe pas, le programme d'installation le crée pendant l'installation de l'agent. • Numéro de port de communication de l'agent OfficeScan : OfficeScan génère le numéro de port de manière aléatoire. Acceptez le numéro de port généré ou spécifiez-en un nouveau.	Oui	Oui	Non	Non
Raccourci du dossier du programme Le raccourci vers le dossier d'installation du serveur OfficeScan s'affiche dans le menu Démarrer de Windows. Le nom du raccourci par défaut est Trend Micro OfficeScan Server-<Nom_serveur>. Modifiez ce nom ou utilisez celui défini par défaut.	Oui	Non	Non	Non

Préparation au déploiement pilote

Avant d'effectuer un déploiement à grande échelle, procédez à un déploiement pilote dans un environnement contrôlé. Un déploiement pilote vous permet de tester les différentes fonctions et d'évaluer le niveau d'assistance nécessaire après le déploiement complet. Il offre à votre équipe d'installation la possibilité de répéter et d'affiner le processus de déploiement. Il permet également aux administrateurs de vérifier si le plan de déploiement répond aux initiatives de sécurité de l'entreprise.

Pour un exemple de déploiement d'OfficeScan, voir *Exemple de déploiement à la page A-1*.

Choix d'un site pilote

Choisissez un site pilote qui correspond à l'environnement de production. Essayez de simuler un type de topologie réseau constituant une représentation adéquate de l'environnement de production.

Création d'un plan de rétrogradation

Mettez au point un plan de restauration ou de rétrogradation, au cas où vous rencontreriez des problèmes lors du processus d'installation ou de mise à niveau.

Évaluation du déploiement pilote

Établissez une liste des réussites et des échecs rencontrés pendant le processus pilote. Identifiez les pièges potentiels et établissez un plan en conséquence. Intégrez ce plan d'évaluation pilote dans le plan de déploiement général du produit.

Problèmes de comptabilité connus

Cette section présente les problèmes de compatibilité qui peuvent survenir si vous installez le serveur OfficeScan sur un endpoint équipé de certaines applications tierces. Consultez la documentation des applications tierces pour plus de détails.

Microsoft Lockdown Tools et URLScan

Lorsque vous utilisez l'outil Microsoft IIS Lockdown Tool ou URLScan, le verrouillage des fichiers OfficeScan suivants risque de bloquer les communications de l'agent et du serveur OfficeScan :

- Fichiers de configuration (`.ini`)
- Fichiers de données (`.dat`)
- Fichiers Dynamic Link Library (`.dll`)
- Fichiers exécutables (`.exe`)

Empêchement de toute interférence entre URLScan et la communication agent/serveur

Procédure

1. Arrêtez le service World Wide Web Publishing sur l'ordinateur du serveur OfficeScan.
2. Modifiez le fichier de configuration d'URLScan pour autoriser les types de fichier spécifiés ci-dessus.
3. Redémarrez le service World Wide Web Publishing.

Microsoft Exchange Server

Lorsque vous installez l'agent OfficeScan pendant l'installation du serveur, OfficeScan doit avoir accès à tous les fichiers scannés par l'agent. Étant donné que Microsoft Exchange Server place les messages en file d'attente dans les répertoires locaux, ces répertoires doivent être exclus du scan autorisant Exchange Server à traiter les messages électroniques.

OfficeScan exclut automatiquement du scan tous les répertoires Microsoft Exchange 2000/2003. Ce paramètre peut être configuré dans la console Web (**Agents** >

Paramètres généraux de l'agent > Paramètres de scan). Pour plus d'informations sur les exclusions de scan de Microsoft Exchange 2007, reportez-vous à :

http://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx

Serveurs de base de données

Les administrateurs peuvent scanner les serveurs de base de données mais cela peut affecter les performances des applications qui accèdent à ces bases de données. Envisagez d'exclure du scan en temps réel les bases de données et leurs dossiers de sauvegarde. Effectuez un scan manuel en dehors des heures de pointe pour limiter son impact.

Pare-feu de connexion Internet (ICF)

Windows Server 2003 dispose d'un pare-feu intégré appelé Pare-feu de connexion Internet (Internet Connection Firewall - ICF). Lorsque vous exécutez ICF, ajoutez les ports d'écoute d'OfficeScan à la liste d'exceptions ICF. Consultez la documentation du pare-feu pour plus de détails sur la configuration de listes d'exceptions.

Chapitre 2

Installation d'OfficeScan

Ce chapitre décrit la procédure à suivre pour installer Trend Micro™ OfficeScan™.

Sujets abordés dans ce chapitre :

Exécution d'une nouvelle installation du serveur OfficeScan

Pour effectuer une nouvelle installation, exécutez le programme d'installation sur un endpoint répondant aux critères d'installation et de mise à niveau requis pour le serveur OfficeScan (pour plus d'informations, reportez-vous à *Configuration requise pour une nouvelle installation et une mise à niveau à la page 1-2*). Le programme d'installation installe le serveur OfficeScan et Plug-in Manager 2.1. Cette version de Plug-in Manager fournit les fonctionnalités de widget dans OfficeScan. Pour plus d'informations sur les écrans d'installation et les options de configuration, reportez-vous à *Écrans du programme d'installation à la page 2-5*.

Pour connaître les instructions et les méthodes pour une nouvelle installation, consultez le *Manuel de l'administrateur*.

Installation en mode silencieux

Vous pouvez installer ou mettre à niveau plusieurs serveurs OfficeScan en mode silencieux si ceux-ci utilisent des paramètres d'installation identiques.

Lorsque l'installation en mode silencieux s'exécute sur le endpoint cible, le programme d'installation installe OfficeScan 11.0 et Plug-in Manager 2.1. Plug-in Manager 2,1 fournit les fonctionnalités de widget dans OfficeScan.

Préparation de l'installation en mode silencieux

Procédure

1. Créez un fichier de réponse en exécutant le programme d'installation et en enregistrant les paramètres d'installation dans un fichier `.iss`. Tous les serveurs installés en mode silencieux à l'aide du fichier de réponse utilisent les mêmes paramètres.

Important

- Les écrans du programme d'installation ne s'affichent que pour l'installation locale.
- Pour les nouvelles installations, créez un fichier de réponse depuis un endpoint sur lequel un serveur OfficeScan n'est pas installé.

2. Exécutez le programme d'installation depuis une invite de commande et dirigez le programme d'installation vers l'emplacement du fichier de réponse à utiliser pour l'installation en mode silencieux.

Enregistrement de la configuration du programme d'installation dans un fichier de réponse

Cette procédure n'installe pas OfficeScan. Elle ne fait qu'enregistrer la configuration du programme d'installation dans un fichier de réponse.

Procédure

1. Ouvrez une invite de commande et accédez au répertoire du fichier `setup.exe` d'OfficeScan.

   Par exemple, « `CD C:\OfficeScan Installer\setup.exe` ».

2. Entrez ce qui suit :

   ```
   setup.exe -r
   ```

   Le paramètre `-r` déclenche le lancement du programme d'installation et enregistre les détails de l'installation dans un fichier de réponse.

3. Suivez les étapes du programme d'installation.

4. Après avoir effectué toutes les étapes, contrôlez le fichier de réponse `setup.iss` dans `%windir%`.

Exécution de l'installation en mode silencieux

Procédure

1. Copiez le pack d'installation et `setup.iss` sur le endpoint cible.
2. Sur le endpoint cible, ouvrez une invite de commande et accédez au répertoire du pack d'installation.
3. Entrez ce qui suit :

   ```
   setup.exe -s <-f1path>setup.iss <-f2path>setup.log.
   ```

   Par exemple : `C:\setup.exe -s -f1C:\setup.iss -f2C:\setup.log`

   Où :

   - `-s` : demande au programme d'installation de procéder à une installation en mode silencieux.
   - `<-f1path>setup.iss`: emplacement du fichier de réponse. Si le chemin contient des espaces, placez-le entre guillemets doubles ("). Par exemple, `-f1"C:\osce script\setup.iss"`.
   - `<-f2path>setup.log`: emplacement du fichier journal que le programme d'installation crée après l'installation. Si le chemin contient des espaces, placez-le entre guillemets doubles ("). Par exemple, `-f2"C:\osce log \setup.log"`.
4. Appuyez sur la touche Entrée :

   Le programme d'installation procède à l'installation du serveur sur le endpoint en mode silencieux.
5. Pour vérifier si l'installation a été correctement exécutée :
   - Vérifiez OfficeScan Program Shortcuts sur le endpoint cible. Si ces raccourcis ne sont pas disponibles, procédez à une nouvelle installation.
   - Connectez-vous à OfficeScan Web console.

Écrans du programme d'installation

La liste ci-dessous présente les écrans d'installation (dans l'ordre successif) qui s'affichent lorsque vous effectuez une nouvelle installation du serveur OfficeScan localement, à distance ou en mode silencieux.

TABLEAU 2-1. Écrans et tâches d'installation

ÉCRANS	NOUVELLE INSTALLATION LOCALE/EN MODE SILENCIEUX	NOUVELLE INSTALLATION À DISTANCE
Conditions préalables à l'installation d'OfficeScan	✓	✓
Bienvenue	✓	✓
Contrat de licence à la page 2-8	✓	✓
Destination de l'installation à la page 2-9	✓	✓
Pré-scan du Endpoint à la page 2-10	✓	✓
État de l'installation (analyse du endpoint) **Remarque** L'analyse peut prendre un certain temps, notamment pendant l'initialisation du serveur HTTP.	✓	
Chemin d'installation à la page 2-12	✓	✓
Serveur proxy à la page 2-13	✓	✓
Serveur Web à la page 2-14	✓	✓

ÉCRANS	NOUVELLE INSTALLATION LOCALE/EN MODE SILENCIEUX	NOUVELLE INSTALLATION À DISTANCE
Identification du serveur à la page 2-18	✓	✓
Enregistrement et activation à la page 2-20	✓	✓
Déploiement de l'agent OfficeScan à la page 2-22	✓	✓
Installer le serveur Smart Protection intégré à la page 2-23	✓	✓
Activer les services de réputation de sites Web à la page 2-27	✓	✓
Destination de l'installation à la page 2-29		✓
Analyse du endpoint cible à la page 2-31		✓
Installer l'agent OfficeScan à la page 2-32	✓	✓
Smart Protection Network à la page 2-34	✓	✓
Mot de passe du compte administrateur à la page 2-36	✓	✓
Installation de l'agent OfficeScan à la page 2-38	✓	✓
Pare-feu OfficeScan à la page 2-40	✓	✓
Fonction anti-spyware à la page 2-42	✓	✓
Fonction Réputation de sites Web à la page 2-43	✓	✓

ÉCRANS	NOUVELLE INSTALLATION LOCALE/EN MODE SILENCIEUX	NOUVELLE INSTALLATION À DISTANCE
Certificat d'authentification serveur à la page 2-45		
OfficeScan Program Shortcuts à la page 2-47		
Informations sur l'installation à la page 2-48		
Installation du serveur OfficeScan		
Assistant InstallShield terminé à la page 2-49		

Contrat de licence

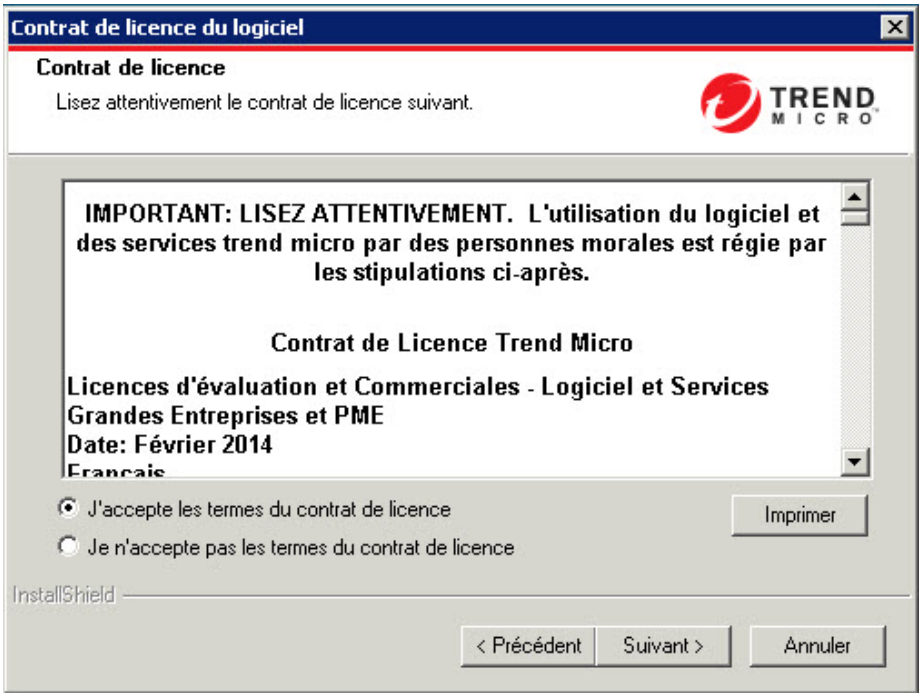

FIGURE 2-1. Écran Contrat de licence

Lisez attentivement le contrat de licence et confirmez votre acceptation avant de procéder à l'installation. Il est impossible de continuer l'installation sans accepter les termes du contrat de licence.

Destination de l'installation

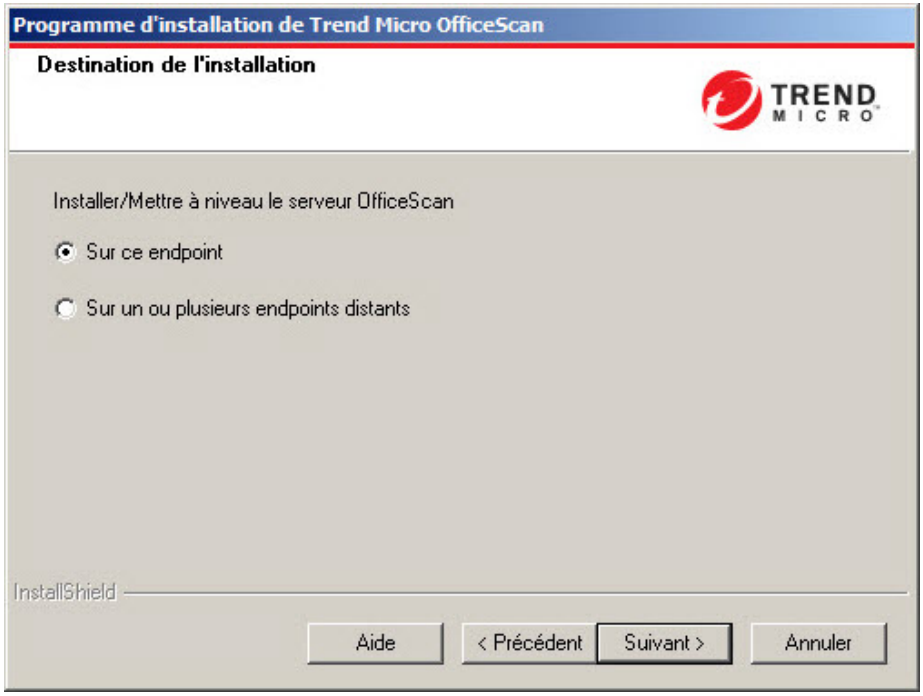

FIGURE 2-2. Écran Destination de l'installation

Exécutez le programme d'installation et installez le serveur OfficeScan sur le endpoint sur lequel vous êtes occupé ou sur d'autres endpoints du réseau.

Remarques sur l'installation à distance

Lorsque vous effectuez une installation à distance, le programme d'installation vérifie si le endpoint cible dispose de la configuration requise pour l'installation du serveur. Avant de continuer :

- Vous devez obtenir les droits d'administration de ce endpoint.

- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que les endpoints cible présentent la configuration minimale requise en vue de l'installation du serveur OfficeScan.
- Assurez-vous que le endpoint soit équipé de Microsoft IIS Server 6,0 ou d'une version supérieure s'il est utilisé comme serveur Web. Lorsque vous utilisez le serveur Web Apache, le programme d'installation installe automatiquement ce serveur s'il n'est pas déjà présent sur le endpoint cible.

Pré-scan du Endpoint

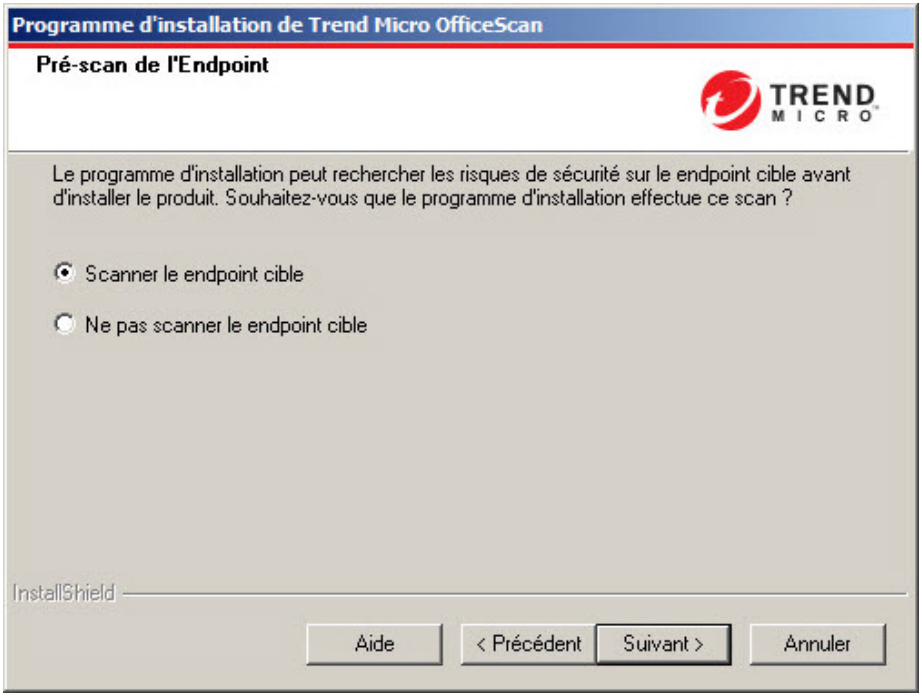

FIGURE 2-3. Écran Pré-scan du Endpoint

Avant de procéder à l'installation du serveur OfficeScan, le programme d'installation peut scanner le endpoint cible pour détecter des virus ou des programmes malveillants. Le programme d'installation scanne les zones les plus vulnérables du endpoint, parmi lesquelles :

- La zone et le répertoire d'amorçage (contre les virus d'amorce)
- Le dossier Windows
- Le dossier Program files

Le programme d'installation peut entreprendre les actions suivantes contre les virus/programmes malveillants et les chevaux de Troie détectés :

- **Supprimer** : Supprime un fichier infecté
- **Nettoyer** : Nettoie un fichier nettoyable avant d'autoriser l'accès complet au fichier ou laisse à l'action suivante spécifiée le soin de traiter un fichier non nettoyable.
- **Renommer** : remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier. 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** : Autorise l'accès complet au fichier infecté sans entreprendre d'action contre le fichier. Un utilisateur peut copier/supprimer/ouvrir le fichier.

En cas d'installation locale, le scan est effectué en cliquant sur **Suivant**. En cas d'installation à distance, le scan est effectué juste avant l'installation effective.

Chemin d'installation

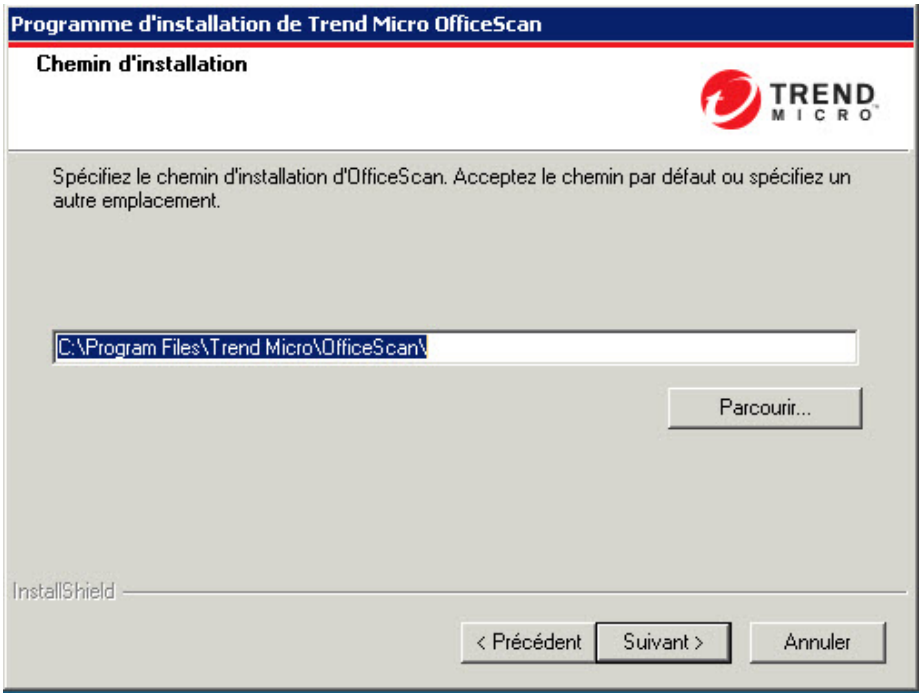

FIGURE 2-4. Écran Chemin d'installation

Acceptez le chemin d'installation par défaut ou spécifiez-en un nouveau.

Le chemin d'installation spécifié ne s'applique que lorsque l'on procède à une nouvelle installation à distance. Pour les mises à niveau à distance, OfficeScan utilise les paramètres de la version précédente

Serveur proxy

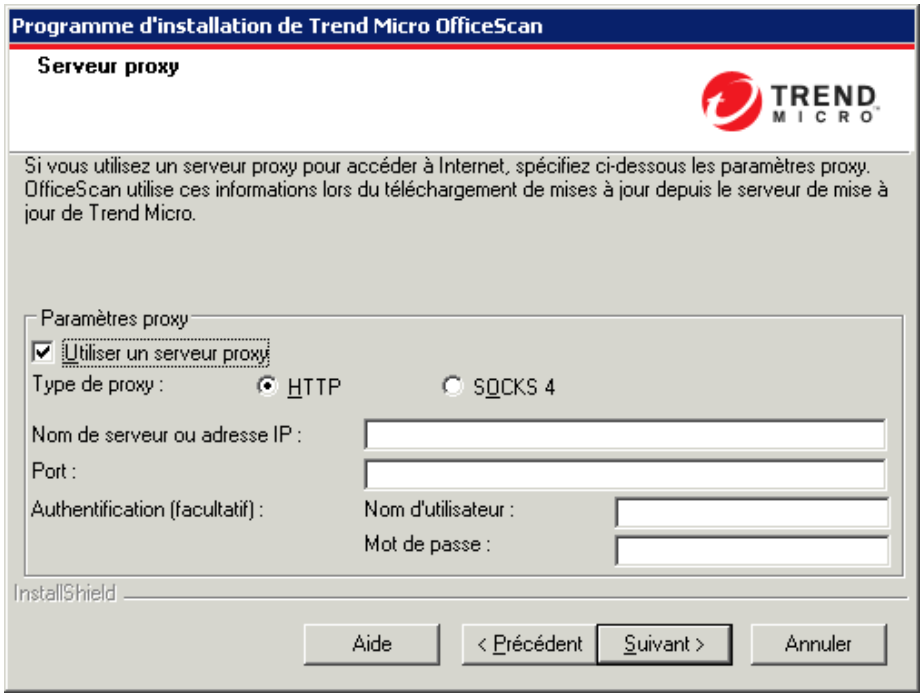

FIGURE 2-5. Écran Serveur proxy

Le serveur OfficeScan utilise le protocole HTTP pour la communication agent-serveur et pour la connexion à Trend Micro ActiveUpdate Server afin de télécharger les mises à jour. Si un serveur proxy gère le trafic Internet sur le réseau, OfficeScan doit disposer des paramètres proxy pour permettre au serveur de télécharger les mises à jour depuis le serveur ActiveUpdate.

Les administrateurs peuvent décider de ne pas spécifier les paramètres proxy pendant l'installation et de le faire après à partir d'OfficeScan Web Console.

Les paramètres proxy ne s'appliquent que lors d'une nouvelle installation à distance. Pour une mise à niveau à distance, OfficeScan utilise les paramètres de la version précédente

Remarque

Lorsque vous installez le serveur OfficeScan sur un endpoint utilisant exclusivement le protocole IPv6, installez un serveur proxy double pile qui peut convertir les adresses IP. Cela permet au serveur de se connecter au serveur ActiveUpdate.

Serveur Web

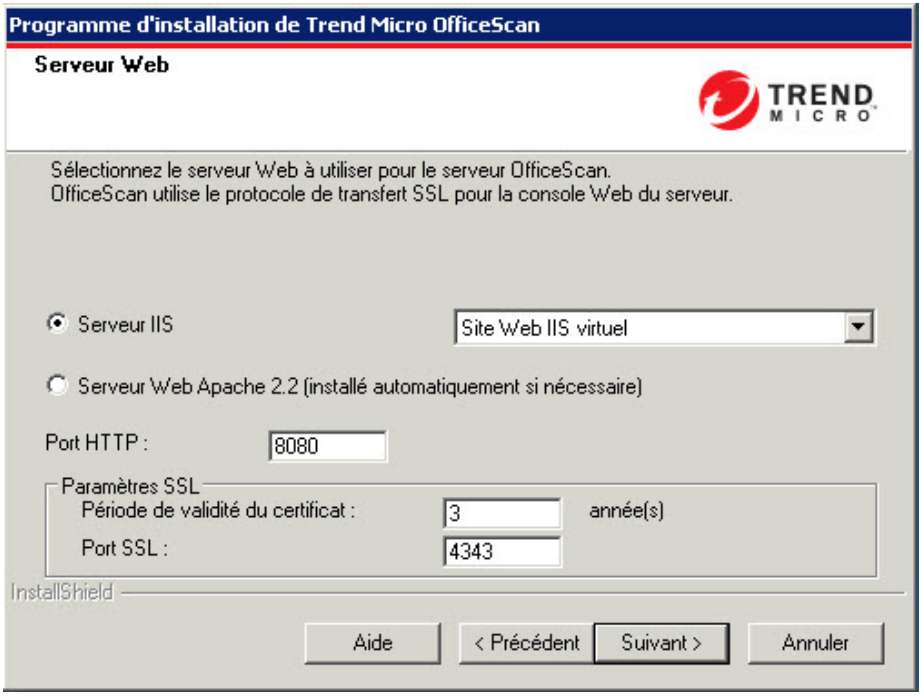

FIGURE 2-6. Écran Serveur Web

Le serveur Web OfficeScan abrite la console Web, permet à l'administrateur d'exécuter des CGI (Common Gateway Interfaces) depuis la console et accepte les commandes provenant des agents. Le serveur Web convertit ces commandes en CGI d'agents et les transmet au service principal d'OfficeScan.

Les paramètres du serveur Web ne s'appliquent que lors d'une nouvelle installation à distance. Lorsque l'on effectue une mise à niveau à distance, OfficeScan utilise les paramètres de la version précédente.

Prise en charge d'IPv6

Pour les nouvelles installations, sélectionnez le serveur IIS pour activer la prise en charge d'IPv6. Le serveur Web Apache ne prend pas en charge l'adressage IPv6. Si le endpoint cible n'a qu'une adresse IPv6 et que vous choisissez Apache comme serveur Web, vous ne pourrez pas procéder à l'installation. Si le endpoint cible a une adresse IPv6 et une adresse IPv4, les administrateurs peuvent choisir Apache mais la prise en charge d'IPv6 ne sera pas activée après l'installation du serveur.

Lorsque vous effectuez une mise à niveau vers cette version d'OfficeScan, le serveur OfficeScan à mettre à niveau doit déjà utiliser IIS. Si le serveur utilise Apache, configurez-le pour IIS avant de mettre à niveau.

Serveur Web

Si le programme d'installation détecte à la fois les serveurs Web IIS et Apache sur le endpoint cible, les administrateurs peuvent choisir l'un de ces deux serveurs Web. Si aucun d'eux n'est installé sur le endpoint cible, les administrateurs ne peuvent pas choisir IIS et OfficeScan installe alors automatiquement le serveur Web Apache 2.2.

Si vous utilisez un serveur Web Apache :

- Le serveur Web Apache 2.2 est requis. Si le serveur Web Apache existe sur le endpoint mais que la version n'est pas 2.2, OfficeScan installe et utilise la version 2.2. OfficeScan ne supprime pas le serveur Web Apache existant.
- En cas d'activation du protocole SSL et si le serveur Web Apache 2.2 est installé, des paramètres SSL doivent être préconfigurés sur ce dernier.
- Par défaut, le compte administrateur est le seul compte créé sur le serveur Web Apache.

Conseil

Trend Micro recommande de créer un autre compte à utiliser pour faire tourner le serveur Web. Sinon, le serveur OfficeScan risque d'être victime d'activités malveillantes si un pirate parvient à prendre le contrôle du serveur Apache.

- Avant d'installer le serveur Web Apache, consultez le site Web Apache pour obtenir les informations les plus récentes sur les mises à niveau, les patchs et les problèmes de sécurité.

Si vous utilisez un serveur Web IIS :

- Les versions suivantes de Microsoft Internet Information Server (IIS) sont requises :
  - Version 6.0 sous Windows Server 2003
  - Version 7.0 sous Windows Server 2008
  - Version 7.5 sous Windows Server 2008 R2
  - Version 8.0 sous Windows Server 2012

  N'installez pas le serveur Web sur des endpoints exécutant des applications bloquant IIS. Cela risquerait d'entraîner l'échec de l'installation. Pour obtenir des informations complémentaires, consultez la documentation relative à IIS.

Port HTTP

Le serveur Web écoute les requêtes des agents sur le port HTTP et les transmet au service principal d'OfficeScan. Ce service renvoie les informations aux agents via le port de communication d'agent déterminé. Le programme d'installation génère de façon aléatoire le numéro de port de communication de l'agent pendant l'installation.

Support technique SSL

OfficeScan utilise le protocole Secure Sockets Layer (SSL) pour sécuriser la communication entre la console Web et le serveur. Le protocole SSL offre une couche supplémentaire de protection contre les pirates. Bien qu'OfficeScan chiffre les mots de passe spécifiés sur la console Web avant de les envoyer au serveur OfficeScan, cela

n'empêche pas les pirates de capturer le paquet correspondant et, sans avoir à déchiffrer ce paquet, de l'utiliser pour accéder à la console. La tunnelisation SSL empêche les pirates de capturer les paquets traversant le réseau.

La version SSL utilisée dépend de la version prise en charge par le serveur Web.

Lorsque vous sélectionnez le protocole SSL, le programme d'installation crée automatiquement un certificat SSL, obligatoire pour les connexions SSL. Le certificat contient des informations relatives au serveur, la clé publique et la clé privée.

La période de validité du certificat SSL doit être comprise entre 1 et 20 ans. L'administrateur peut toujours utiliser le certificat après son expiration. Cependant, un message d'avertissement apparaît chaque fois qu'une connexion SSL est appelée à l'aide du même certificat.

Fonctionnement de la communication SSL :

1. L'administrateur envoie des informations de la console Web vers le serveur Web via une connexion SSL.
2. Le serveur Web répond à la console Web avec le certificat requis.
3. Le navigateur effectue l'échange des clés à l'aide du chiffrement RSA.
4. La console Web envoie les données au serveur Web à l'aide du chiffrement RC4.

Bien que le chiffrement RSA soit plus sécurisé, il occasionne un ralentissement du flux de communication. C'est pourquoi il n'est utilisé que pour l'échange des clés alors que RC4, une alternative plus rapide, est utilisé pour le transfert de données.

Ports du serveur Web

Le tableau suivant répertorie les numéros de port par défaut pour le serveur Web

TABLEAU 2-2. Numéros de port pour OfficeScan Web Server

SERVEUR WEB ET PARAMÈTRES	PORTS	
	HTTP	HTTPS (SSL)
Serveur Web Apache sur lequel SSL est activé	8080 (configurable)	4343 (configurable)

Serveur Web et paramètres	Ports	
	HTTP	HTTPS (SSL)
Site Web par défaut IIS sur lequel SSL est activé	80 (non configurable)	443 (non configurable)
Site Web virtuel IIS sur lequel SSL est activé	8080 (configurable)	4343 (configurable)

Identification du serveur

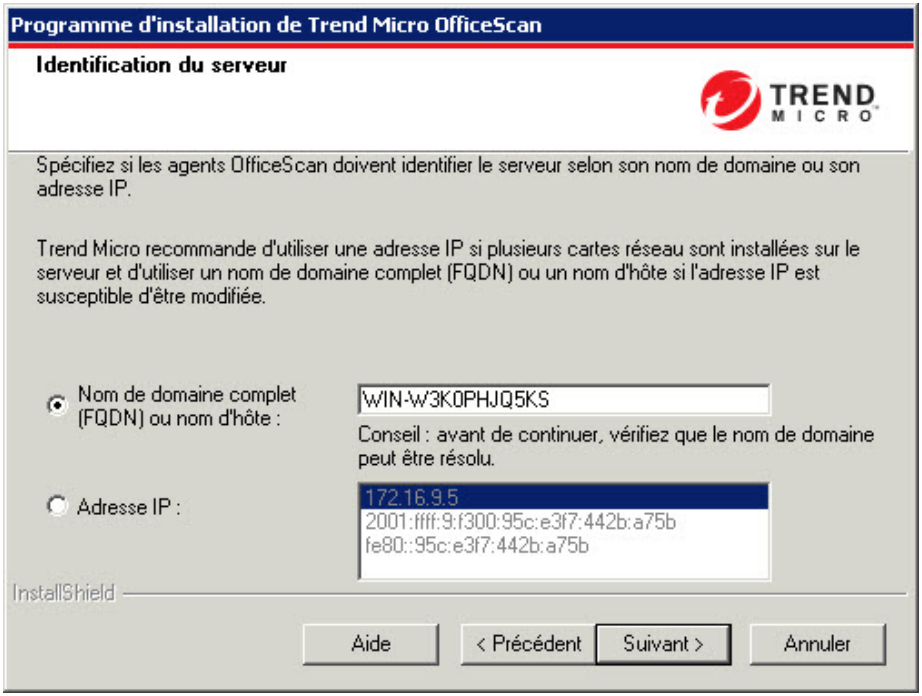

Figure 2-7. Écran Identification du serveur

L'option sélectionnée sur cet écran s'applique uniquement lors d'une nouvelle installation à distance.

Indiquez si les agents OfficeScan doivent identifier le serveur selon son nom de domaine complet (FQDN), nom d'hôte (domaine) ou adresse IP.

La communication entre le serveur et les agents dépend de l'adresse IP spécifiée. Une modification de l'adresse IP peut entraîner un problème de communication entre les agents et le serveur OfficeScan. Le seul moyen de rétablir la communication est de redéployer tous les agents. Cela vaut aussi lorsque le serveur est identifié au moyen d'un nom d'hôte et que celui-ci est modifié.

Pour la plupart des réseaux, l'adresse IP de l'ordinateur du serveur est davantage susceptible d'être modifiée que son nom d'hôte. Il est donc préférable d'identifier l'ordinateur serveur en fonction du nom d'hôte.

Conseil

Pour les administrateurs qui utilisent une adresse IP plutôt qu'un nom d'hôte, Trend Micro recommande de ne pas modifier l'adresse IP (obtenue du serveur DHCP) après l'installation. Les administrateurs peuvent éviter d'autres problèmes de communication avec les agents OfficeScan en configurant l'adresse IP sur Statique (sur le serveur DHCP) en utilisant la même adresse IP obtenue du serveur DHCP.

Une autre manière de préserver la configuration de l'adresse IP est de conserver l'adresse IP pour le serveur OfficeScan uniquement. Le serveur DHCP attribue ainsi obligatoirement la même adresse IP à OfficeScan, même lorsque DHCP est activé.

Si vous utilisez des adresses IP statiques, identifiez le serveur au moyen de son adresse IP. En outre, si l'ordinateur du serveur dispose de plusieurs cartes d'interface réseau (NIC), il est recommandé d'utiliser l'une des adresses IP plutôt que le nom d'hôte afin de garantir le bon fonctionnement de la communication agent-serveur.

Prise en charge d'IPv6

Si le serveur gère des agents IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et les administrateurs doivent l'identifier par son nom d'hôte. Si les administrateurs identifient le serveur par son adresse IPv4, les agents IPv6 ne peuvent pas s'y connecter. Le même problème se pose lorsque des agents IPv4 purs se connectent à un serveur identifié par son adresse IPv6.

Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6.

Lorsque les administrateurs identifient le serveur par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.

Remarque

Le nom de domaine complet ne peut être spécifié que lors de l'installation locale du serveur. Il n'y a pas de prise en charge du nom de domaine complet pour les installations à distance.

Enregistrement et activation

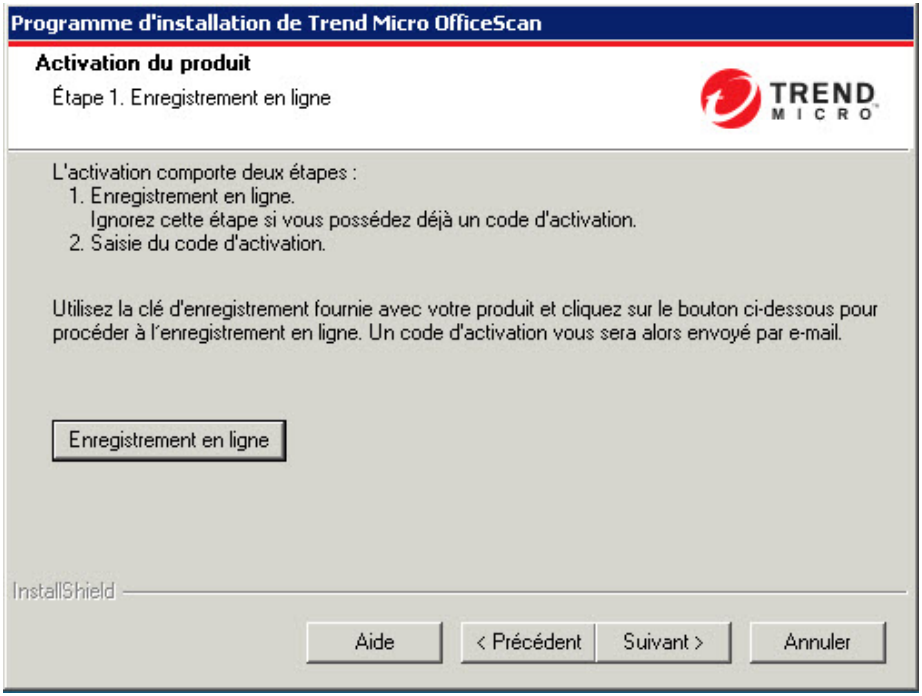

FIGURE 2-8. Activation du produit - Écran de l'étape 1

Enregistrez OfficeScan à l'aide de la clé d'enregistrement livrée avec le produit, puis munissez-vous des codes d'activation. Si les codes d'activation dont déjà disponibles, ignorez cette étape.

Pour obtenir les codes d'activation, cliquez sur **Enregistrement en ligne**. Le programme d'installation ouvre le site Web d'enregistrement de Trend Micro. Une fois le formulaire d'enregistrement rempli, Trend Micro envoie un e-mail contenant les codes d'activation. Lorsque vous recevez les codes, poursuivez le processus d'installation.

Lorsque vous installez le serveur OfficeScan sur un endpoint utilisant exclusivement le protocole IPv6, installez un serveur proxy double pile qui peut convertir les adresses IP. Cela permet au serveur de se connecter au site Web d'enregistrement de Trend Micro.

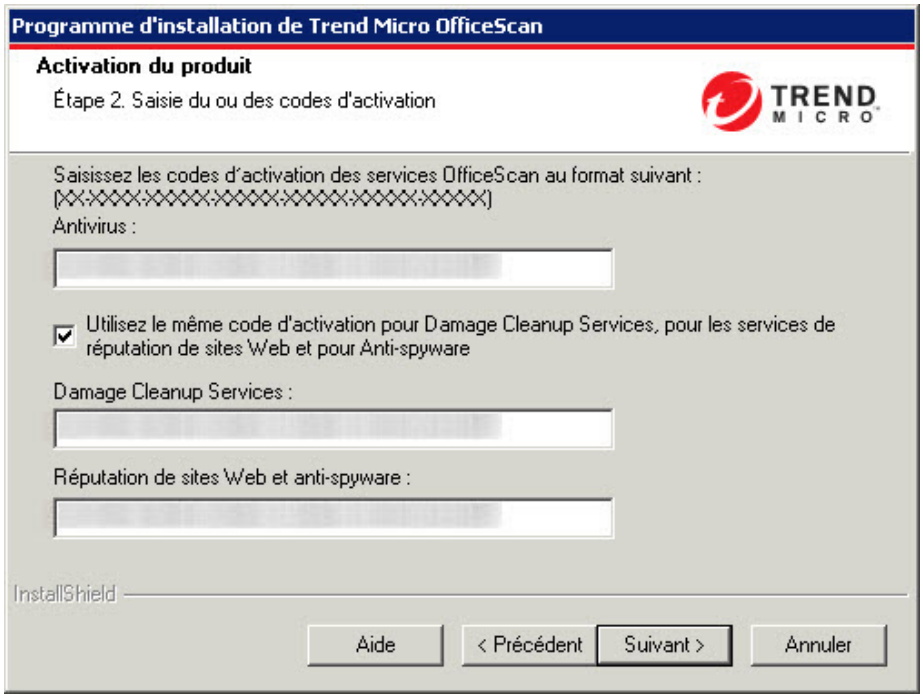

FIGURE 2-9. Activation du produit - Écran de l'étape 2

Indiquez les codes d'activation. Les codes d'activation sont sensibles à la casse.

Si le code d'activation est valide pour tous les services :

1. Entrez le code d'activation dans la zone de texte **Antivirus**.
2. Sélectionnez **Utilisez le même code d'activation pour Damage Cleanup Services, pour la réputation de sites Web et pour Anti-spyware**.
3. Cliquez sur **Suivant** et vérifiez les informations sur les licences.

Déploiement de l'agent OfficeScan

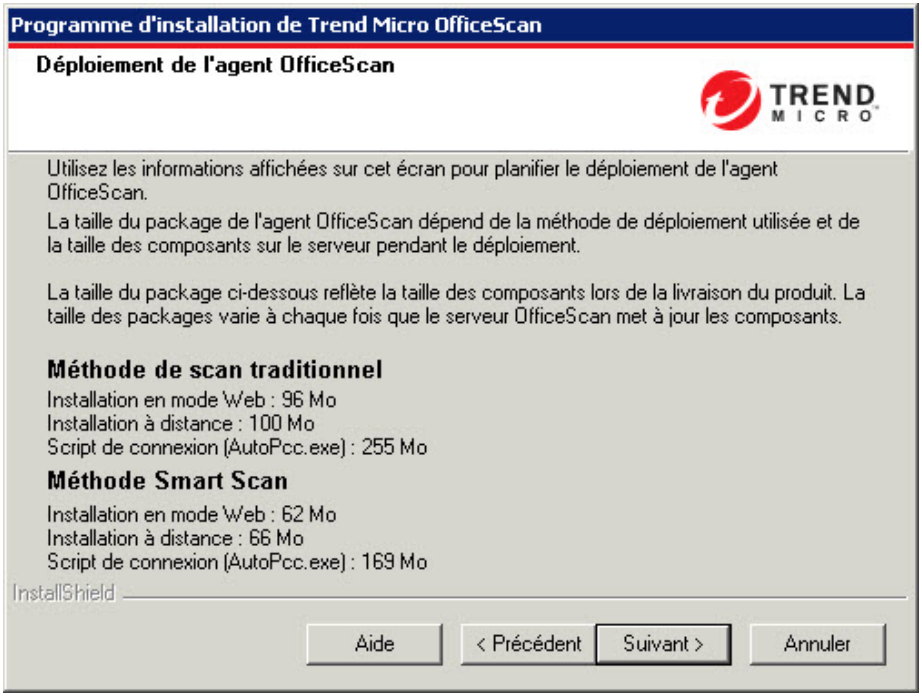

FIGURE 2-10. Écran Déploiement de l'agent OfficeScan

Différentes méthodes sont disponibles pour installer ou mettre à niveau les agents OfficeScan. Cet écran répertorie les différentes méthodes de déploiement et la bande passante du réseau approximative requise.

Cet écran permet d'estimer l'espace requis sur les serveurs et la bande passante consommée lors du déploiement des agents sur les endpoints cible.

Remarque

Toutes ces méthodes d'installation requièrent des droits d'administrateur local ou d'administrateur de domaine sur les endpoints cible.

Installer le serveur Smart Protection intégré

Remarque

Cet écran ne s'affiche pas lors de l'utilisation d'un site Web IIS virtuel pendant les installations de mises à niveaux locales.

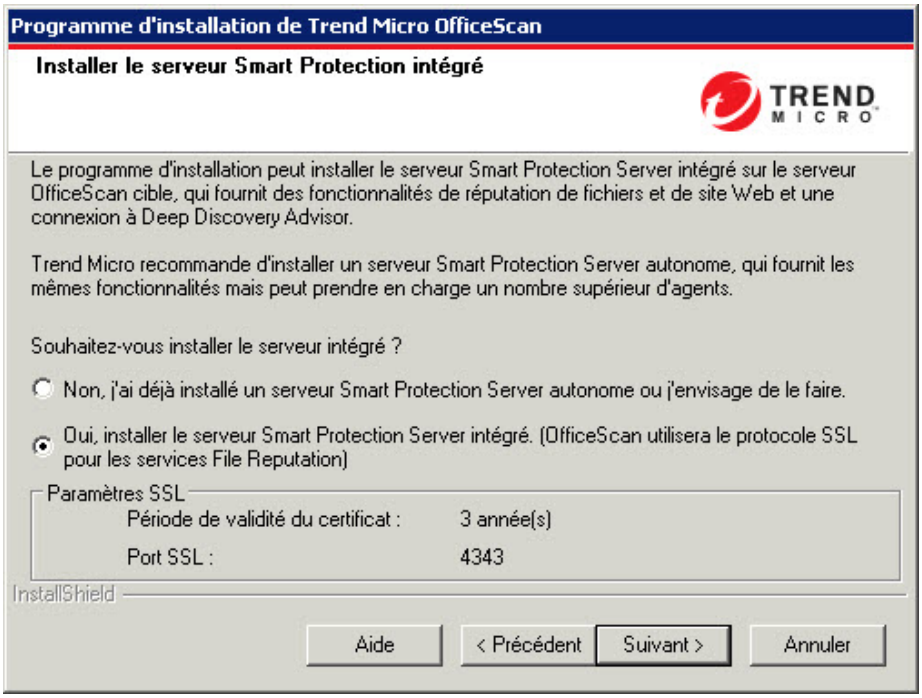

FIGURE 2-11. Écran d'installation du serveur Smart Protection Server intégré

Le programme d'installation peut installer le serveur Smart Protection Server intégré sur le endpoint cible. Le serveur intégré fournit les services de File Reputation aux agents qui utilisent Smart Scan et les services de réputation de sites Web aux agents soumis aux stratégies de réputation de sites Web. Gérez le serveur intégré à partir d'OfficeScan Web Console.

Trend Micro recommande d'installer le serveur Smart Protection Server autonome qui a les mêmes fonctions que le serveur intégré mais qui peut desservir davantage d'agents. Le serveur autonome est installé séparément et dispose de sa propre console de gestion. Consultez le *Manuel de l'administrateur Trend Micro Smart Protection Server* pour plus d'informations sur le serveur autonome.

Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même endpoint, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours. Consultez le *Manuel de l'administrateur* pour plus d'informations sur la configuration des sources Smart Protection pour les agents.

Protocoles de connexion des agents pour les services de File Reputation

Les agents OfficeScan peuvent se connecter aux services de File Reputation du serveur Smart Protection Server intégré à l'aide des protocoles HTTP et HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

Remarque

Si des agents se connectent au serveur intégré via un serveur proxy, vous devez configurer des paramètres proxy internes depuis la console Web. Consultez le *Manuel de l'administrateur* pour obtenir des informations sur la configuration des paramètres proxy.

Les numéros de port utilisés pour les services de File Reputation dépendent du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

Le port HTTP ne s'affiche pas sur l'écran d'installation. Le port HTTPS s'affiche mais la configuration est facultative.

TABLEAU 2-3. Ports pour les services de File Reputation du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORTS POUR LES SERVICES DE FILE REPUTATION	
	HTTP	HTTPS (SSL)
Serveur Web Apache	8082	4345
Site Web IIS par défaut	80	443

Serveur Web et paramètres	Ports pour les services de File Reputation	
	HTTP	HTTPS (SSL)
Site Web IIS virtuel	8080	4343

Serveur intégré non installé

Si vous effectuez une nouvelle installation et ne choisissez pas d'installer le serveur intégré :

- Le scan traditionnel devient la méthode de scan par défaut.
- Lorsque vous activez les stratégies de réputation de sites Web dans un écran d'installation différent (pour plus d'informations, voir *Fonction Réputation de sites Web à la page 2-43*), les agents ne peuvent pas envoyer de requêtes de réputation de sites Web car OfficeScan présume que le serveur Smart Protection Server n'est pas installé.

Si un serveur autonome est disponible après avoir installé OfficeScan, effectuez les tâches suivantes depuis OfficeScan Web Console :

- Changez la méthode de scan en Smart Scan.
- Ajoutez le serveur autonome à la liste des sources Smart Protection afin que les agents puissent lui envoyer des requêtes de File Reputation et de réputation de sites Web.

Lorsque vous effectuez une mise à niveau depuis des serveurs OfficeScan 10.x dans lesquels le serveur intégré a été désactivé, celui-ci n'est pas installé. Les agents OfficeScan conservent leur méthode de scan et les sources Smart Protection auxquelles ils envoient des requêtes.

Activer les services de réputation de sites Web

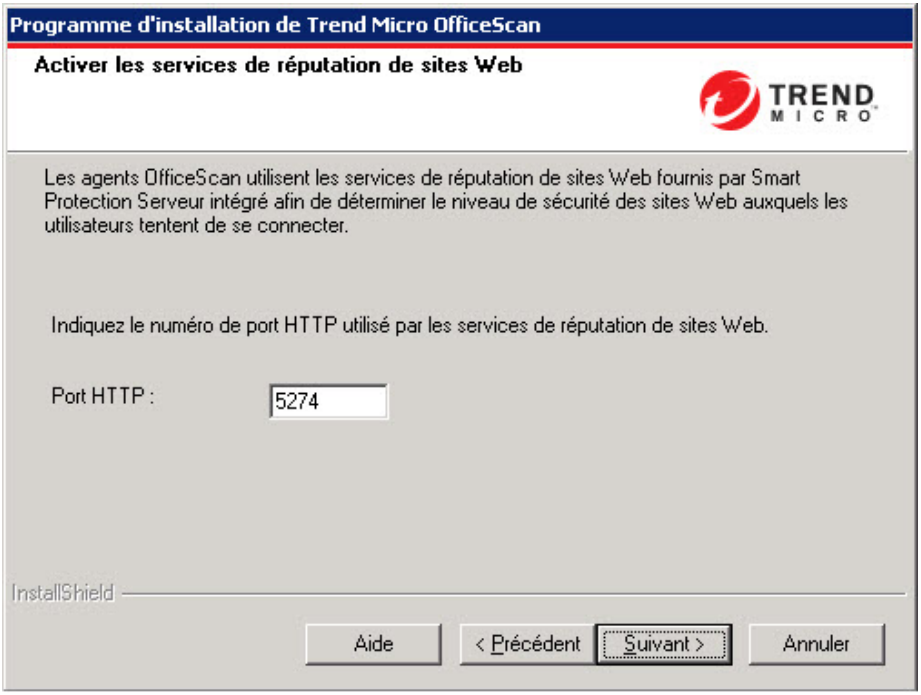

FIGURE 2-12. Activation de l'écran Services de réputation de sites Web

Les services de réputation de sites Web évaluent les risques de sécurité potentiels de toutes les URL demandées lors de l'exécution de chaque requête HTTP. Selon l'évaluation renvoyée par la base de données et le niveau de sécurité configuré, la réputation de sites Web bloque ou approuve la requête. Le serveur Smart Protection Server intégré, installé avec le serveur OfficeScan, fournit les services de réputation de sites Web.

L'activation des services de réputation de sites Web (fonctionnant sous le processus appelé `LWCSService.exe`) réduit la consommation globale de bande passante. En effet, les agents OfficeScan obtiennent les données de réputation de sites Web depuis un serveur local au lieu de se connecter à Smart Protection Network.

Protocoles de connexion des agents pour les services de réputation de sites Web

Les agents OfficeScan peuvent se connecter aux services de réputation de sites Web du serveur Smart Protection Server intégré à l'aide du protocole HTTP.

Le numéro de port HTTP utilisé pour les services de réputation de sites Web dépend du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

TABLEAU 2-4. Ports pour les services de réputation de sites Web du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORT HTTP POUR LES SERVICES DE RÉPUTATION DE SITES WEB
Serveur Web Apache sur lequel SSL est activé	5274
Site Web par défaut IIS sur lequel SSL est activé	80 (non configurable)
Site Web virtuel IIS sur lequel SSL est activé	8080 (non configurable)

Destination de l'installation

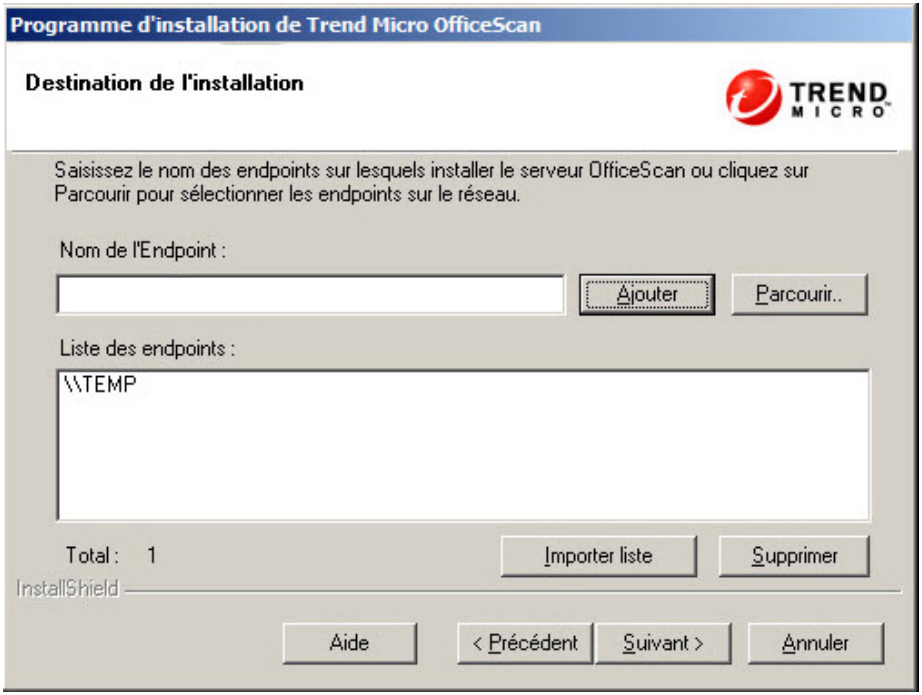

FIGURE 2-13. Écran Destination de l'installation

Spécifiez le endpoint cible sur lequel vous installerez OfficeScan. Entrez manuellement le nom d'hôte du endpoint ou son adresse IP. Cliquez sur **Parcourir** pour rechercher des endpoints sur le réseau.

Importez le(s) nom(s) de endpoint depuis un fichier texte en cliquant sur **Importer liste**. Lorsque vous procédez à une installation sur plusieurs endpoints simultanément et que tous les endpoints sont approuvés après l'analyse, le programme d'installation installe le serveur OfficeScan dans leur ordre d'apparition sur la liste du fichier texte.

Dans le fichier texte :

- Spécifiez un nom de endpoint par ligne.

- Utilisez le format de convention universelle de dénomination (Unified Naming Convention ou UNC), par exemple `\\test`.
- Utilisez uniquement les caractères suivants : a-z, A-Z, 0-9, points (.) et tirets (-).

Par exemple :

```
\\domain1\test-abc
```

```
\\domain2\test-123
```

Conseils pour vérifier si l'installation à distance peut être réalisée :

- Vous devez obtenir les droits d'administration de ce endpoint.
- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que les endpoints cible présentent la configuration système minimale requise en vue de l'installation du serveur OfficeScan.
- Assurez-vous que le endpoint soit équipé de Microsoft IIS Server 6,0 ou d'une version supérieure s'il est utilisé comme serveur Web. Si vous choisissez d'utiliser le serveur Web Apache, le programme d'installation installe automatiquement ce serveur s'il n'est pas déjà présent sur le endpoint cible.
- Ne définissez pas le endpoint sur lequel vous avez lancé le programme d'installation comme endpoint cible. Lancez plutôt une installation locale sur le endpoint.

Une fois les endpoints cible définis, cliquez sur **Suivant**. Le programme d'installation vérifie que les endpoints sont équipés de la configuration minimale requise pour OfficeScan.

Analyse du endpoint cible

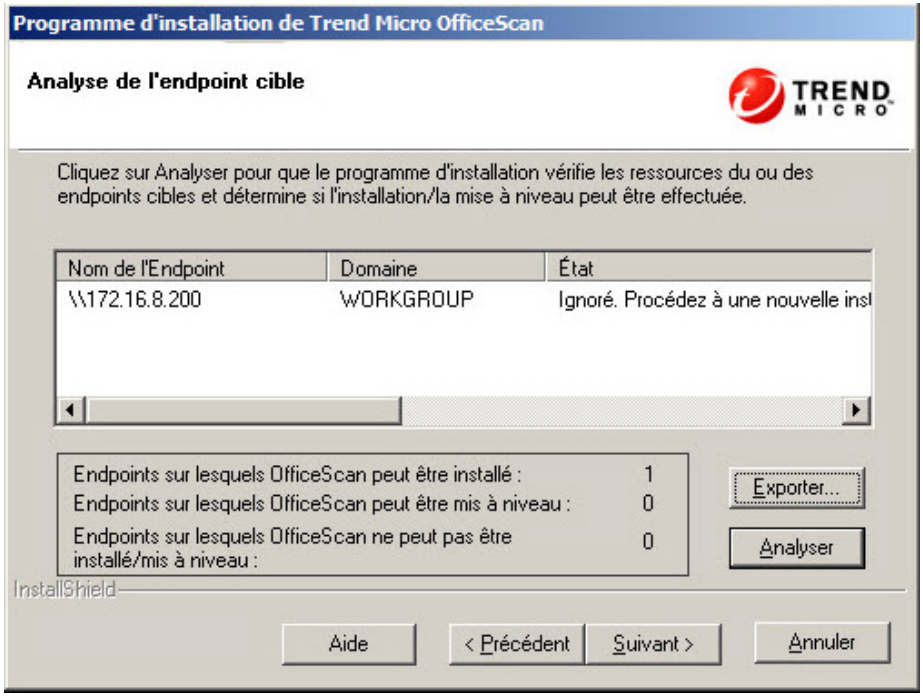

FIGURE 2-14. Écran Analyse du endpoint cible

Avant de lancer l'installation à distance, le programme d'installation doit d'abord déterminer si les endpoints cible sélectionnés peuvent installer le serveur OfficeScan. Pour démarrer l'analyse, cliquez sur **Analyser**. Le programme d'installation peut vous demander le nom d'utilisateur et le mot de passe de l'administrateur utilisés pour se connecter au endpoint cible. Après l'analyse, le programme d'installation affiche les résultats à l'écran.

Lorsque vous procédez à une installation sur plusieurs endpoints, l'installation démarrera si au moins un endpoint est approuvé après l'analyse. Le programme d'installation installe le serveur OfficeScan sur ce endpoint et ignore les endpoints refusés après l'analyse.

Pendant l'installation à distance, la progression de l'installation s'affiche uniquement sur endpoint sur lequel le programme d'installation a été lancé et pas sur les endpoints cible.

Installer l'agent OfficeScan

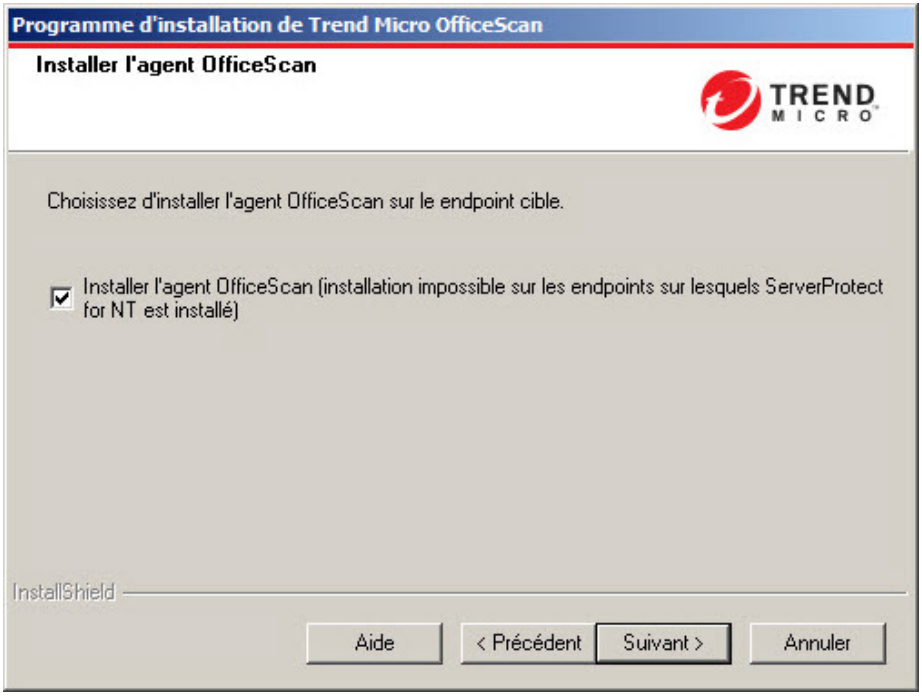

FIGURE 2-15. Écran Installer l'agent OfficeScan

Choisissez d'installer l'agent OfficeScan sur le serveur cible.

Agent OfficeScan

Le programme de l'agent OfficeScan fournit la protection effective contre les risques de sécurité. C'est pourquoi, pour protéger le endpoint du serveur OfficeScan contre les risques de sécurité, celui-ci doit également être équipé du programme de l'agent

OfficeScan. Le fait de choisir d'installer l'agent OfficeScan lors de l'installation du serveur est un moyen efficace de s'assurer que le serveur est protégé automatiquement. Cela vous évite également d'avoir à installer le client après l'installation de l'agent OfficeScan.

Remarque

Installez l'agent OfficeScan sur les autres endpoints du réseau après l'installation du serveur. Consultez le *Manuel de l'administrateur* pour obtenir des informations sur les méthodes d'installation de l'agent OfficeScan.

Si un logiciel de sécurité de endpoints Trend Micro ou tiers est actuellement installé sur le serveur, il se peut qu'OfficeScan ne soit pas en mesure de désinstaller automatiquement le logiciel et de le remplacer par l'agent OfficeScan. Prenez contact avec votre service d'assistance pour obtenir une liste des logiciels désinstallés automatiquement par OfficeScan. Si le logiciel ne peut pas être désinstallé automatiquement, désinstallez-le manuellement avant de procéder à l'installation d'OfficeScan.

Smart Protection Network

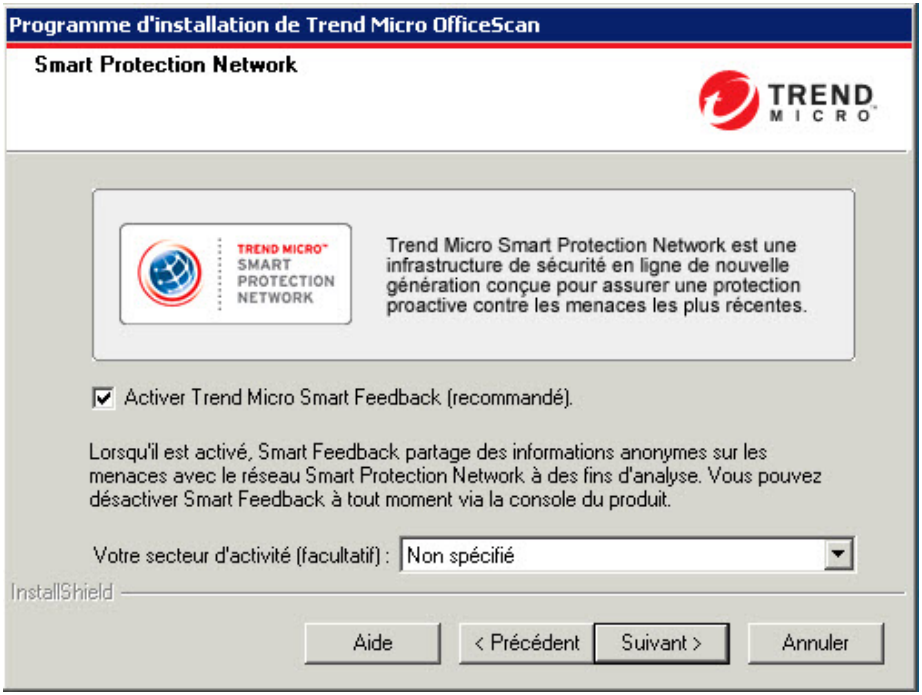

FIGURE 2-16. Écran Smart Protection Network

Trend Micro™Smart Protection Network constitue 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 locales et hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage, à l'aide d'agents légers permettant d'accéder à une combinaison unique de technologies en ligne de messagerie, File Reputation et de réputation de sites Web alliées à des bases de données de menaces. À mesure que de nouveaux produits, services et utilisateurs accèdent au réseau, la sécurité des clients est automatiquement mise à jour et renforcée, créant ainsi un service de protection de voisinage en temps réel pour les utilisateurs. La solution Smart Protection Network exploite Smart Protection Network pour une protection en ligne.

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/24h et 7 jours/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 :

- les sommes de contrôles des fichiers
- les sites Web visités
- les données relatives aux fichiers, y compris, leur taille et l'adresse de leur emplacement
- les 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 optionnelle 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 davantage d'informations à propos de Smart Protection Network, consultez :

http://fr.trendmicro.com/fr/technology/smart-protection-network/

Mot de passe du compte administrateur

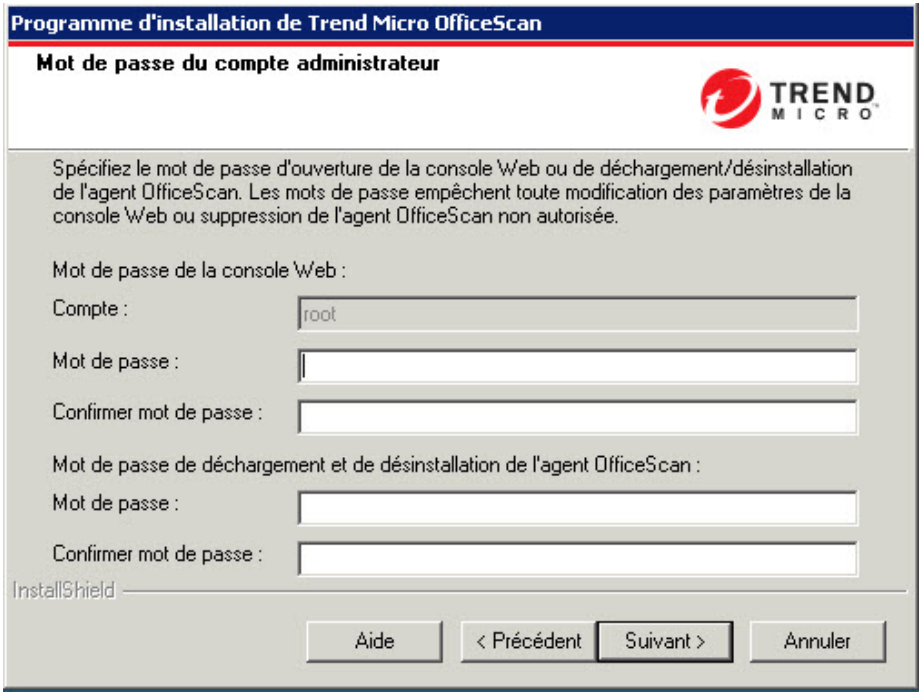

FIGURE 2-17. Écran Mot de passe du compte administrateur

Spécifiez des mots de passe pour accéder à la console Web et décharger et désinstaller l'agent OfficeScan.

Accéder à la console Web

Le programme d'installation crée un compte racine lors de l'installation. Ce compte racine dispose d'un accès complet à l'ensemble des fonctions de la console Web d'OfficeScan. Une connexion à l'aide de ce compte permet également à l'administrateur

de créer des comptes utilisateur dont les autres utilisateurs peuvent se servir pour se connecter à la console Web. Les utilisateurs peuvent configurer ou afficher une ou plusieurs fonctions de la console Web en fonction des privilèges d'accès accordés à leur compte.

Spécifiez un mot de passe que les administrateurs OfficeScan sont les seuls à connaître. Contactez votre service d'assistance pour qu'il vous aide à réinitialiser un mot de passe oublié.

Décharger et désinstaller l'agent OfficeScan

Spécifiez un mot de passe pour empêcher toute désinstallation ou tout déchargement non autorisé de l'agent OfficeScan. Ne désinstallez ni ne déchargez l'agent qu'en cas de problème lié aux fonctions de celui-ci et installez/rechargez-le dès que possible.

Installation de l'agent OfficeScan

FIGURE 2-18. Écran Installation de l'agent OfficeScan

Acceptez les paramètres par défaut d'installation de l'agent ou modifiez le chemin d'installation de l'agent OfficeScan. Modifiez le chemin si le répertoire d'installation ne dispose pas d'un espace disque suffisant.

Conseil

Trend Micro recommande l'utilisation des paramètres par défaut.

Si vous modifiez le chemin d'installation, saisissez un emplacement statique ou utilisez des variables. Si le chemin spécifié inclut un répertoire qui n'existe pas sur l'agent, celui-

ci est automatiquement créé lors de l'installation de l'agent par le programme d'installation.

Pour saisir un emplacement d'installation statique de l'agent OfficeScan, entrez l'emplacement du lecteur, y compris la lettre de lecteur. Par exemple, `C:\Program Files\Trend Micro\OfficeScan Agent`.

Remarque

Il est impossible de modifier le chemin d'installation de l'agent OfficeScan lorsque l'installation du serveur OfficeScan est terminée. Tous les agents OfficeScan installés utilisent le même chemin d'installation.

Pour spécifier des variables dans le chemin d'installation de l'agent OfficeScan, utilisez les éléments suivants :

- `$BOOTDISK` : la lettre du lecteur du disque dur d'amorçage du endpoint, par défaut `C:\`
- `$WINDIR` : le répertoire Windows, par défaut `C:\Windows`
- `$ProgramFiles`: le répertoire Program Files configuré automatiquement sous Windows et habituellement utilisé pour installer les logiciels, par défaut `C:\Program Files`

Sur cet écran, configurez les informations suivantes :

- **Numéro de port** : le programme d'installation génère de façon aléatoire ce numéro de port utilisé par le serveur OfficeScan pour communiquer avec les agents. Acceptez le numéro de port par défaut ou modifiez-le.
- **Niveau de sécurité** : Après l'installation d'OfficeScan, modifiez le niveau de sécurité depuis la console OfficeScan.

  Accédez à **Agents** > **Gestion des agents**. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

  - **Normal** : Cette autorisation donne à tous les utilisateurs (le groupe d'utilisateurs « Tous ») les pleins droits sur le répertoire du programme de l'agent et les entrées de registre de l'agent.

- **Élevé** : Le répertoire d'installation de l'agent hérite des droits du dossier `Program Files` et les entrées de registre de l'agent héritent des autorisations de la clé `HKLM\Software`. Pour la plupart des configurations d'Active Directory, les utilisateurs « normaux » (qui ne disposent pas de privilèges d'administrateur) sont dès lors limités à un accès en lecture seule.

Pare-feu OfficeScan

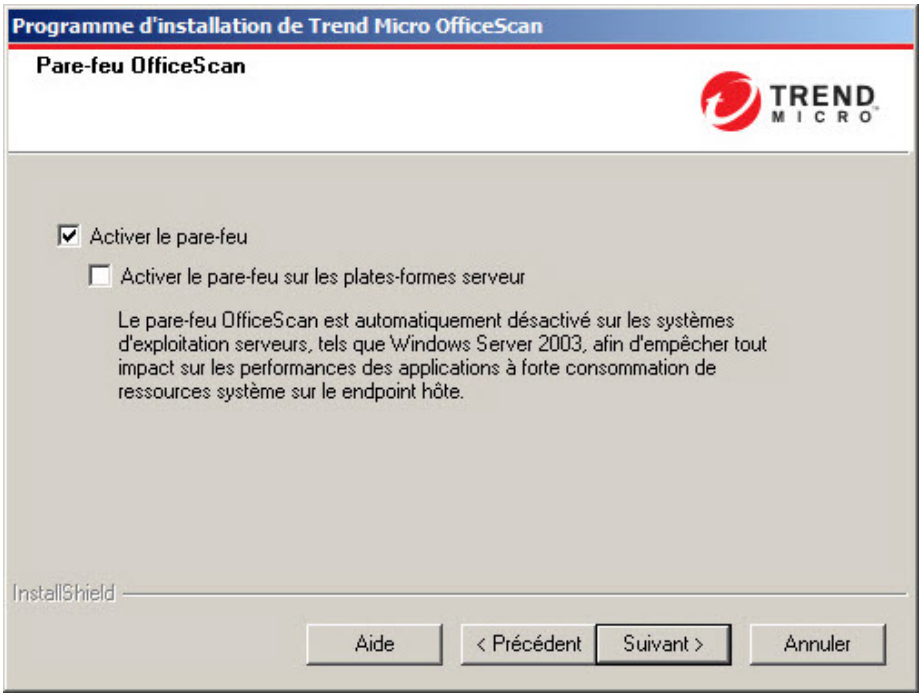

FIGURE 2-19. Écran Pare-feu OfficeScan

Cet écran ne s'affiche qu'après avoir activé le service antivirus.

Pare-feu OfficeScan

Le pare-feu OfficeScan protège les agents et les serveurs du réseau grâce à une fonction « Stateful inspection », à un scan antivirus de réseau hautes performances et à l'élimination des virus de réseau. Créez des règles pour filtrer les connexions par adresse IP, numéro de port ou protocole, puis appliquez-les à différents groupes d'utilisateurs.

Il est possible de désactiver le pare-feu et de le réactiver ultérieurement depuis la console Web du serveur OfficeScan.

Vous pouvez activer de manière facultative le pare-feu sur les plates-formes serveur. Lorsque vous faites une mise à niveau et que le service de pare-feu est activé sur les plates-formes serveur, sélectionnez **Activer le pare-feu sur les plates-formes serveur** afin que OfficeScan ne désactive pas le service de pare-feu après la mise à niveau.

Fonction anti-spyware

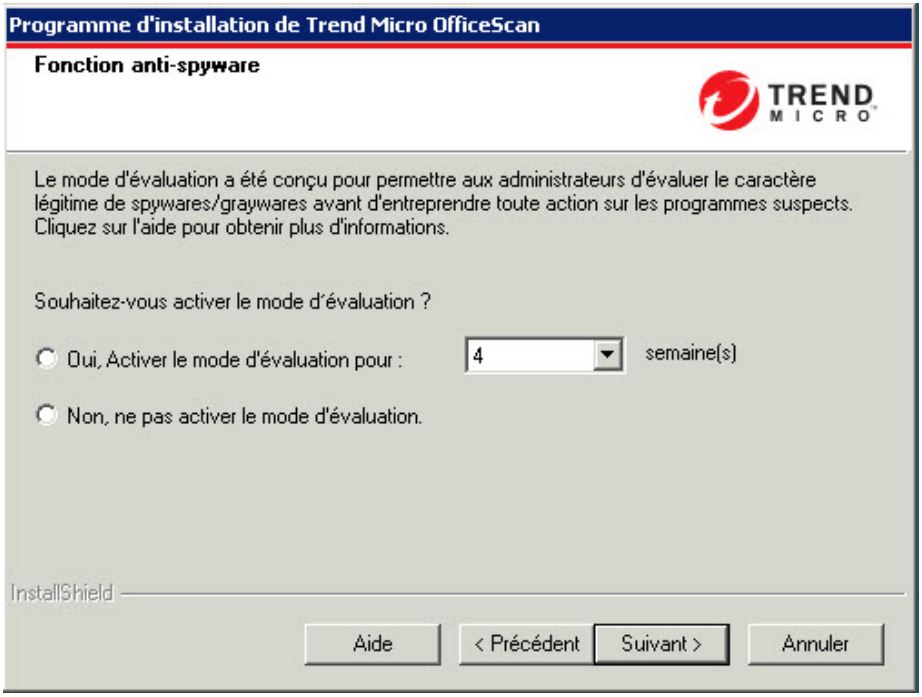

FIGURE 2-20. Écran Fonction anti-spyware

Cet écran ne s'affiche qu'après avoir activé les services de réputation de sites Web et Anti-spyware.

En mode d'évaluation, tous les agents gérés par le serveur enregistrent dans le journal les spywares/graywares détectés pendant le scan manuel, programmé, en temps réel et immédiat, mais ne nettoient pas les composants des spywares/graywares. Le nettoyage met fin aux processus ou supprime les répertoires, fichiers, cookies et raccourcis.

Le mode d'évaluation de Trend Micro a été conçu pour vous permettre d'évaluer les éléments que Trend Micro détecte comme étant des spywares/graywares. Les administrateurs peuvent alors configurer l'action appropriée. Par exemple, ajouter les

spywares/graywares, détectés comme risque de sécurité, à la liste des spywares/graywares approuvés.

Après l'installation, consultez le *Manuel de l'administrateur* pour savoir quelles actions sont recommandées en mode d'évaluation.

Configurez le mode d'évaluation pour que celui-ci ne s'applique que pour une durée déterminée en spécifiant le nombre de semaines dans cet écran. Après l'installation, modifiez les paramètres de mode d'évaluation à partir de la console Web (**Agents** > **Paramètres généraux de l'agent**, section **Paramètres de spywares/graywares**).

Fonction Réputation de sites Web

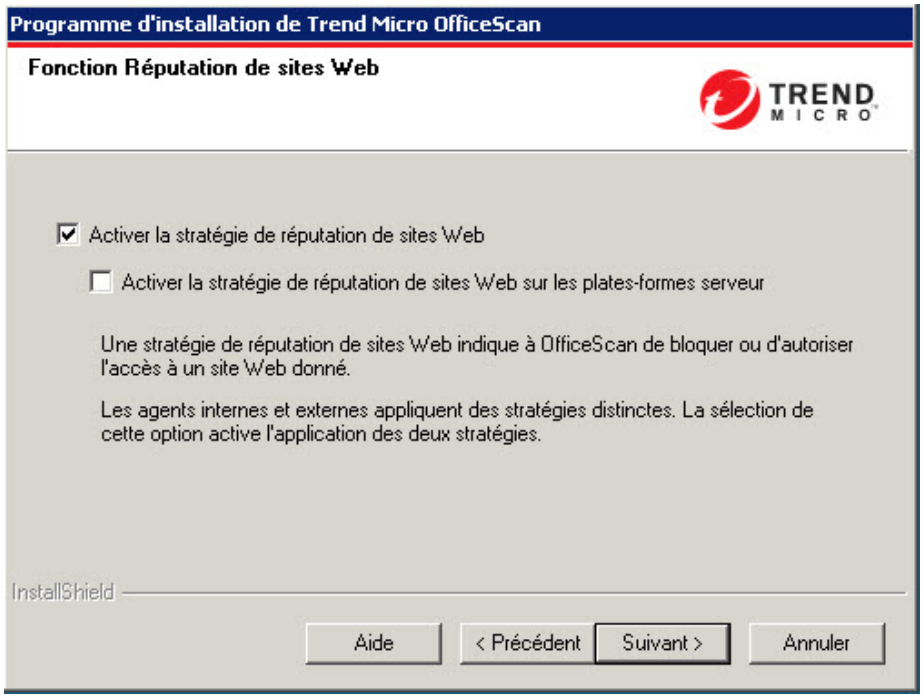

FIGURE 2-21. Écran Fonction Réputation de sites Web

Les stratégies de réputation de sites Web indiquent à OfficeScan de bloquer ou d'autoriser l'accès à un site Web donné. Pour plus de détails sur les stratégies, consultez le *Manuel de l'administrateur*.

La sélection de l'option **Activer la stratégie de réputation de sites Web** active les stratégies pour les clients internes et externes installés sur les plates-formes de postes de travail, telles que Windows XP, Windows Vista, Windows 7, Windows 8 et Windows 8.1. Sélectionnez **Activer la stratégie de réputation de sites Web sur les plates-formes serveur** si celles-ci, par exemple Windows Server 2003, Windows Server 2008 et Windows Server 2012 requièrent le même niveau de protection contre les menaces Web que les plates-formes de postes de travail.

Les agents OfficeScan utilisent les critères d'emplacement que vous avez définis dans l'écran **Emplacement du Endpoint** de la console Web afin de déterminer leur emplacement et la stratégie à appliquer. Les agents OfficeScan changent de stratégie à chaque fois que l'emplacement change.

Vous pouvez configurer les paramètres de stratégie de réputation de sites Web depuis la console Web après l'installation. Les administrateurs OfficeScan configurent généralement une stratégie plus stricte pour les agents externes.

Les stratégies de réputation de sites Web sont des paramètres détaillés de l'arborescence des agents OfficeScan. Vous pouvez appliquer des stratégies spécifiques à tous les agents, à des groupes d'agents ou à des agents individuels.

Lorsque vous activez les stratégies de réputation de sites Web, assurez-vous d'installer les serveurs Smart Protection Server (intégrés ou autonomes) et de les ajouter à la liste des sources Smart Protection dans OfficeScan web console. Les agents OfficeScan envoient des requêtes de réputation de sites Web aux serveurs afin de vérifier le niveau de sécurité des sites Web auxquels les utilisateurs se connectent.

Remarque

Le serveur intégré est installé avec le serveur OfficeScan. Pour obtenir des informations détaillées, voir *Installer le serveur Smart Protection intégré à la page 2-23*. Le serveur autonome est installé séparément.

Certificat d'authentification serveur

Le programme d'installation tente de détecter la présence de certificats d'authentification existants pendant l'installation. Si un tel certificat existe, OfficeScan mappe automatiquement le fichier sur l'écran **Certificat d'authentification serveur**. Si aucun certificat n'existe, OfficeScan applique par défaut l'option **Générer un certificat d'authentification**.

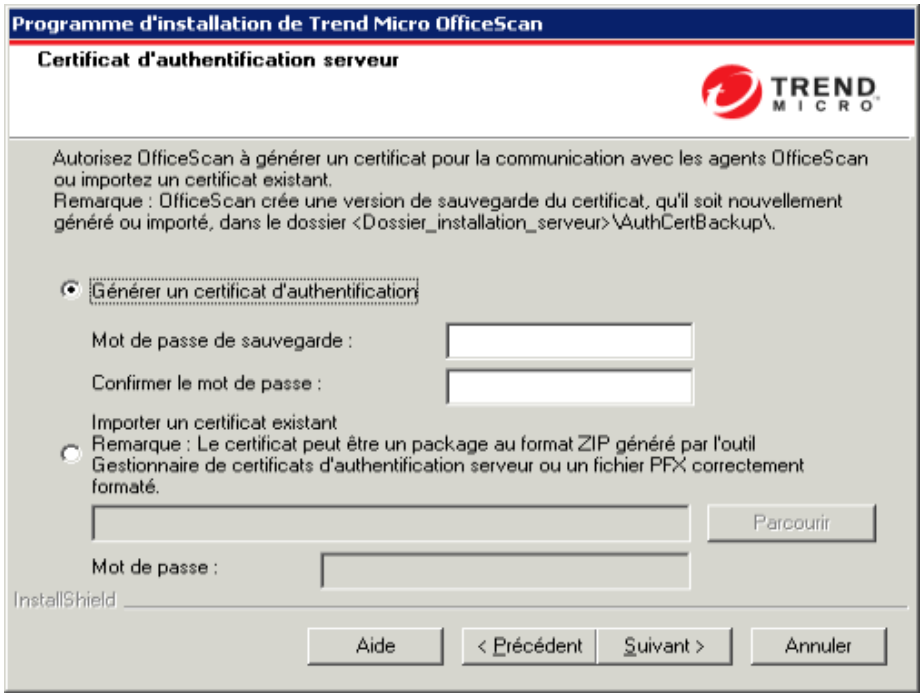

FIGURE 2-22. Écran Certificat d'authentification serveur pour les nouveaux certificats

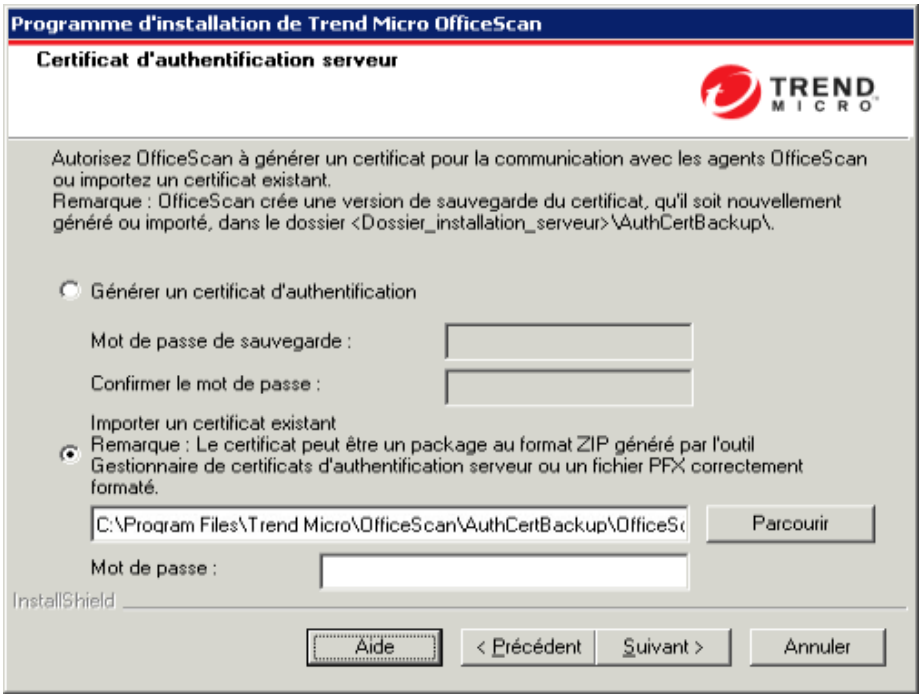

FIGURE 2-23. Écran Certificat d'authentification serveur pour les certificats existants

OfficeScan utilise le chiffrement à clé publique pour authentifier les communications du serveur OfficeScan vers les agents. Grâce à cette technologie, le serveur conserve une clé privée et déploie une clé publique sur tous les agents. Les agents utilisent la clé publique pour vérifier que les communications entrantes proviennent bien du serveur et sont valides. Les agents répondent au serveur si cette vérification réussit.

Remarque

OfficeScan n'authentifie pas les communications vers le serveur provenant des agents.

OfficeScan peut générer le certificat d'authentification pendant l'installation ou les administrateurs peuvent importer un certificat d'authentification préexistant depuis un autre serveur OfficeScan.

Conseil

Lors de la sauvegarde du certificat, Trend Micro recommande le chiffrement du certificat à l'aide d'un mot de passe.

OfficeScan Program Shortcuts

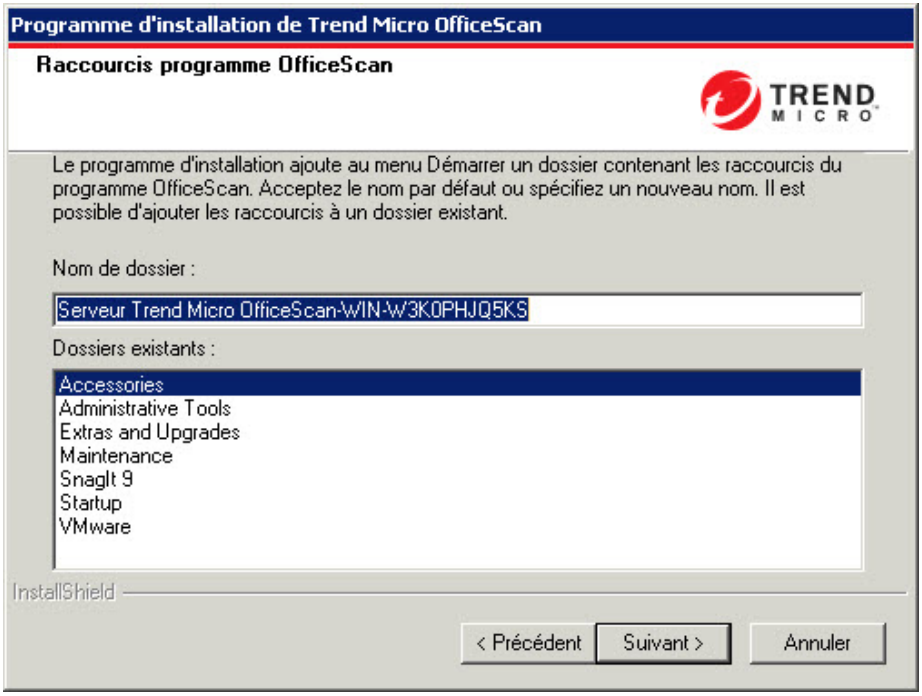

FIGURE 2-24. Écran d'OfficeScan Program Shortcuts

Acceptez le nom du dossier par défaut, indiquez-en un ou sélectionnez un dossier existant auquel le programme d'installation ajoute les raccourcis de programme.

Informations sur l'installation

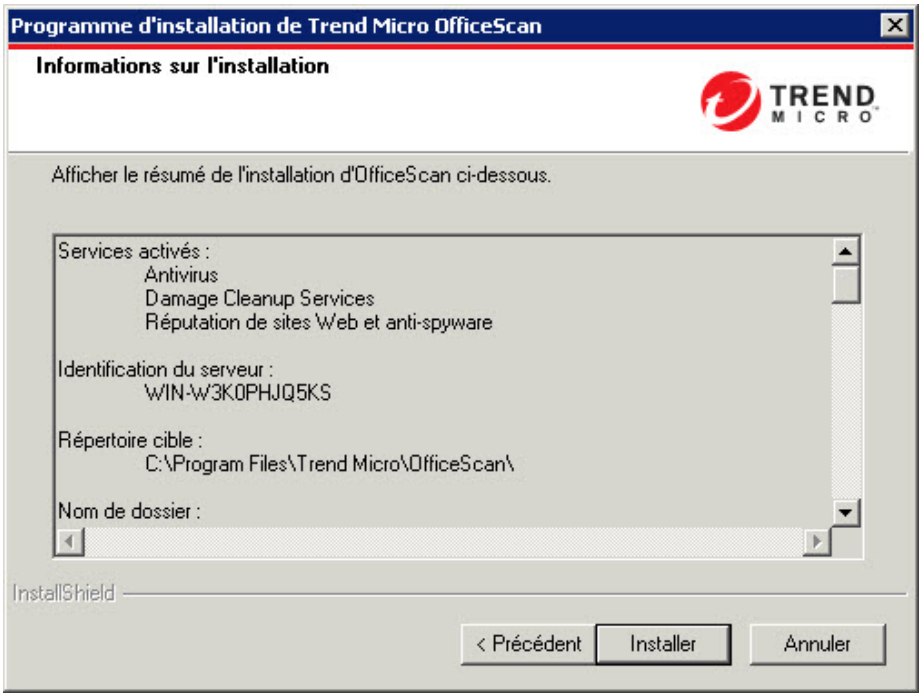

FIGURE 2-25. Écran Informations sur l'installation

Cet écran contient un récapitulatif des paramètres d'installation. Vérifiez les informations relatives à l'installation et cliquez sur **Précédent** pour modifier les paramètres ou les options, le cas échéant. Pour lancer l'installation, cliquez sur **Installer**.

Assistant InstallShield terminé

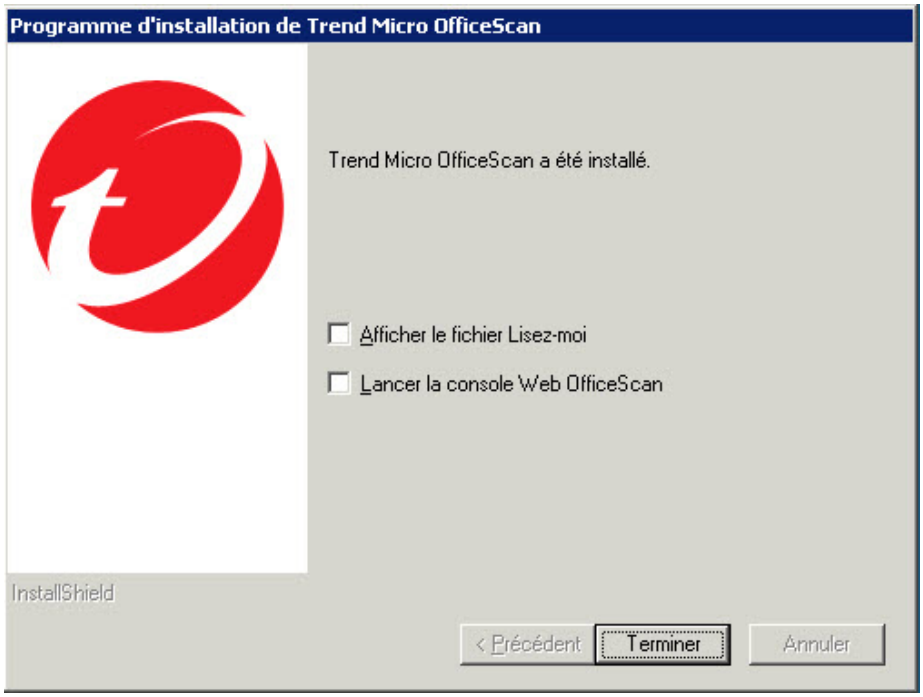

FIGURE 2-26. Écran indiquant que l'Assistant InstallShield est terminé

Une fois l'installation terminée, lisez le fichier Lisez-moi pour prendre connaissance des informations de base relatives au produit et aux problèmes connus.

Les administrateurs peuvent démarrer la console Web pour commencer à configurer les paramètres d'OfficeScan.

Chapitre 3

Mise à niveau d'OfficeScan

Ce chapitre décrit la procédure à suivre pour mettre à niveau Trend Micro™ OfficeScan™.

Sujets abordés dans ce chapitre :

Mise à niveau du serveur OfficeScan et des agents

L'exécution du programme d'installation sur un serveur OfficeScan 10.x précédemment configuré met à niveau le serveur. Si Plug-in Manager est installé sur le endpoint, le programme d'installation met également à niveau Plug-in Manager vers la version 2.1. Si Plug-in Manager n'est pas installé, la version 2.1 sera automatiquement installée. Cette version de Plug-in Manager fournit les fonctionnalités de widget dans OfficeScan.

Si le serveur OfficeScan permet aux agents de mettre à niveau le programme de l'agent OfficeScan, le pack d'installation met immédiatement à niveau tous les agents lorsque l'installation est terminée.

Si le serveur OfficeScan bloque les mises à niveau de l'agent, selon la bande passante du réseau et le nombre d'agents gérés par le serveur OfficeScan, effectuez une mise à niveau échelonnée des agents par groupes.

Conseil

Trend Micro vous recommande vivement de redémarrer les agents OfficeScan après la mise à niveau pour garantir la mise à jour de tous les composants OfficeScan.

Avant la mise à niveau du serveur OfficeScan et des agents

Avant de mettre à niveau le serveur OfficeScan et les agents, tenez compte de ce qui suit :

1. Le pack d'installation inclut des mises à jour de pilotes du pare-feu OfficeScan. Si vous avez activé le pare-feu OfficeScan de votre version OfficeScan actuelle, le déploiement de ce pack peut provoquer les anomalies suivantes sur le endpoint de l'agent :

    - Lorsque la mise à jour du pilote du pare-feu commun démarre, les endpoints de l'agent sont temporairement déconnectés du réseau. Les utilisateurs ne sont pas notifiés avant la déconnexion.

Une option, activée par défaut, de la console Web OfficeScan 10 SP1 ou version supérieure, retarde la mise à jour du pilote du pare-feu commun jusqu'au redémarrage d'un endpoint de l'agent. Pour éviter toute déconnexion, assurez-vous que cette option soit bien activée. Pour vérifier le statut de cette option, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux** puis à la section **Paramètres du pare-feu**. Cette option est **Mettre à jour le pilote du pare-feu OfficeScan uniquement après le redémarrage du système**.

- Une fois le pack déployé, la version antérieure du pilote TDI d'OfficeScan reste sur le endpoint de l'agent et la nouvelle version n'est pas chargée avant le redémarrage du endpoint. Les utilisateurs sont susceptibles de rencontrer des problèmes avec l'agent OfficeScan s'ils ne redémarrent pas immédiatement.

  Si l'option d'affichage du message de notification de redémarrage est activée sur la console Web, il est demandé aux utilisateurs de redémarrer. Cependant, pour les utilisateurs qui décident de différer le redémarrage, la notification ne sera plus affichée. Si l'option est désactivée, les utilisateurs ne sont pas notifiés du tout.

  L'option d'affichage de la notification de redémarrage est activée par défaut. Pour vérifier le statut de cette option, accédez à **Ordinateurs en réseau** > **Paramètres clients généraux** puis à la section **Paramètres d'alerte**. Cette option est **Afficher un message de notification si l'ordinateur client doit être redémarré pour charger un pilote de noyau**.

2. La mise à niveau du serveur OfficeScan ne peut pas s'exécuter si :

   - l'agent exécute un script de connexion (`AutoPcc.exe`) au moment de la mise à niveau du serveur. Assurez-vous qu'aucun agent n'exécute le script de connexion avant d'installer le serveur.

   - Le serveur effectue des tâches liées à la base de données. Avant d'effectuer la mise à niveau, vérifiez l'état de la base de données OfficeScan (`DbServer.exe`). Par exemple, ouvrez le Gestionnaire des tâches de Windows et vérifiez que l'utilisation de l'processeur pour `DbServer.exe` est à 0. Si l'utilisation de l'processeur est supérieure, patientez jusqu'à ce qu'elle arrive à 0. Ce sera le signe que toutes les tâches liées à la base de données auront été achevées. Si vous effectuez une mise à niveau et rencontrez un problème, il est possible que les fichiers de la base de données aient été

verrouillés. Dans ce cas, redémarrez le serveur de l'ordinateur pour déverrouiller les fichiers et effectuez la mise à niveau.

Utilisez l'une des méthodes de mise à niveau suivantes :

- *Méthode de mise à niveau 1 : désactivation de la mise à niveau automatique des agents à la page 3-4*
- *Méthode de mise à niveau 2 : mise à niveau des agents de mise à jour à la page 3-6*
- *Méthode de mise à niveau 3 : Déplacez les agents vers le serveur OfficeScan 11.0. à la page 3-13*
- *Méthode de mise à niveau 4 : activation de la mise à niveau automatique des agents à la page 3-16*

Méthode de mise à niveau 1 : désactivation de la mise à niveau automatique des agents

En désactivant la mise à niveau automatique des agents, vous pouvez mettre d'abord à niveau le serveur, puis les agents par groupes. Choisissez cette méthode si vous devez mettre à niveau un grand nombre d'agents.

Première partie : configuration des paramètres de mise à niveau sur le serveur OfficeScan 10.x

Procédure

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, sélectionnez l'icône du domaine racine () pour sélectionner tous les clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
4. Sélectionnez **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hot fix**.

5. Cliquez sur **Appliquer à tous les clients**.

> **Conseil**
>
> Le déploiement des paramètres vers les clients en ligne peut prendre un certain temps si vous disposez d'un environnement de réseau complexe et d'un grand nombre de clients. Avant la mise à niveau, allouez suffisamment de temps pour que les paramètres soient déployés vers tous les clients. Les clients OfficeScan qui n'appliquent pas les paramètres sont automatiquement mis à niveau.

Deuxième partie : mise à niveau du serveur OfficeScan

Voir *Réalisation d'une mise à niveau locale à la page 3-18* ou *Réalisation d'une mise à niveau distante à la page 3-34* pour plus de détails sur la mise à niveau du serveur OfficeScan.

> **Remarque**
>
> Pour accélérer le processus de mise à niveau, déchargez l'agent OfficeScan avant de mettre à niveau un serveur OfficeScan exécutant Windows Server 2008 Standard 64 bits.

Configurez les paramètres du serveur OfficeScan en utilisant la console Web immédiatement après la fin de l'installation et avant la mise à niveau des agents.

Pour obtenir des instructions détaillées sur la méthode de configuration des paramètres d'OfficeScan, consultez le *Manuel de l'administrateur* ou l'*aide du serveur OfficeScan*.

Troisième partie : mise à niveau des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique** et assurez-vous que les options suivantes sont activées :

   - **Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan**

- **Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)**

2. Accédez à **Agents** > **Gestion des agents**.
3. Dans l'arborescence des agents, sélectionnez les agents que vous souhaitez mettre à niveau. Vous pouvez sélectionner un ou plusieurs domaines ou tout ou partie des agents d'un domaine.
4. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
5. Désactivez **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.
6. Cliquez sur **Enregistrer**.
7. Vérifiez les résultats de la mise à niveau.
   - *Agents en ligne à la page 3-11*
   - *Agents hors ligne à la page 3-13*
   - *Agents itinérants à la page 3-13*
8. Redémarrez les endpoints des agents pour terminer la mise à niveau des agents.
9. Répétez les étapes 2 à 8 jusqu'à ce que tous les agents aient été mis à niveau.

Méthode de mise à niveau 2 : mise à niveau des agents de mise à jour

Utilisez cette méthode de mise à niveau si vous avez un grand nombre d'agents qui se mettent à jour à l'aide d'agents de mise à jour. Ces agents seront mis à niveau à l'aide de leurs agents de mise à jour respectifs.

Pour les agents OfficeScan qui ne se mettent pas à jour à partir d'agents de mise à jour, la mise à niveau sera effectuée à partir du serveur OfficeScan.

Première partie : configuration des paramètres de mise à niveau sur le serveur OfficeScan 10.x

Procédure

1. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
2. Dans l'arborescence client, sélectionnez l'icône du domaine racine () pour sélectionner tous les clients.
3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
4. Sélectionnez **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hot fix**.
5. Cliquez sur **Appliquer à tous les clients**.

Conseil

Le déploiement des paramètres vers les clients en ligne peut prendre un certain temps si vous disposez d'un environnement de réseau complexe et d'un grand nombre de clients. Avant la mise à niveau, allouez suffisamment de temps pour que les paramètres soient déployés vers tous les clients. Les clients OfficeScan qui n'appliquent pas les paramètres sont automatiquement mis à niveau.

Deuxième partie : mise à niveau du serveur OfficeScan

Voir *Réalisation d'une mise à niveau locale à la page 3-18* ou *Réalisation d'une mise à niveau distante à la page 3-34* pour plus de détails sur la mise à niveau du serveur OfficeScan.

Remarque

Pour accélérer le processus de mise à niveau, déchargez l'agent OfficeScan avant de mettre à niveau un serveur OfficeScan exécutant Windows Server 2008 Standard 64 bits.

Configurez les paramètres du serveur OfficeScan en utilisant la console Web immédiatement après la fin de l'installation et avant la mise à niveau des agents.

Pour obtenir des instructions détaillées sur la méthode de configuration des paramètres d'OfficeScan, consultez le *Manuel de l'administrateur* ou l'*aide du serveur OfficeScan*.

Troisième partie : mise à niveau des agents de mise à jour

Procédure

1. Accédez à **Agents** > **Gestion des agents**.
2. Dans l'arborescence des agents, sélectionnez les agents de mise à jour à mettre à niveau.

   Conseil

   Pour localiser facilement les agents de mise à jour, sélectionnez un domaine, accédez à **Affichage de l'arborescence des agents** en haut de l'arborescence des agents, puis sélectionnez **Affichage de l'agent de mise à jour**.

3. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
4. Désactivez **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.
5. Cliquez sur **Enregistrer**.
6. Accédez à **Mises à jour** > **Agents** > **Mise à jour manuelle**.
7. Sélectionnez l'option **Sélectionner manuellement les agents** et cliquez sur **Sélectionner**.
8. Dans l'arborescence des agents qui s'ouvre, choisissez les agents de mise à jour à mettre à niveau.

   Conseil

   Pour localiser facilement les agents de mise à jour, sélectionnez un domaine, accédez à **Affichage de l'arborescence des agents** en haut de l'arborescence des agents, puis sélectionnez **Affichage de l'agent de mise à jour**.

9. Cliquez sur **Lancer la mise à jour** en haut de l'arborescence des agents.

10. Vérifiez les résultats de la mise à niveau.

    - La mise à niveau des agents de mise à jour en ligne s'opère directement après l'initialisation de la mise à jour du composant.
    - La mise à niveau des agents de mise à jour hors ligne s'opère lorsque ceux-ci passent en mode en ligne.
    - La mise à niveau des agents de mise à jour itinérants s'opère lorsque ceux-ci passent en mode en ligne ou, si l'agent de mise à jour possède des privilèges de mise à jour programmée, lors de l'exécution de cette mise à jour.

11. Redémarrez les endpoints des agents de mise à jour pour terminer la mise à niveau des agents.

12. Répétez les étapes 1 à 11 jusqu'à ce que tous les agents de mise à jour aient été mis à niveau.

Quatrième partie : Configuration des paramètres des agents de mise à jour

Procédure

1. Accédez à **Agents** > **Gestion des agents**.

2. Dans l'arborescence des agents, sélectionnez les agents de mise à jour à mettre à niveau.

   Conseil

   Pour localiser facilement les agents de mise à jour, sélectionnez un domaine, accédez à **Affichage de l'arborescence des agents** en haut de l'arborescence des agents, puis sélectionnez **Affichage de l'agent de mise à jour**.

3. Assurez-vous que les agents de mise à jour disposent des derniers composants.

4. Cliquez sur **Paramètres** > **Paramètres des agents de mise à jour**.

5. Sélectionnez les options suivantes :

- **Mises à jour des composants**
- **Paramètres de domaine**
- **Programmes et correctifs de type hot fix des agents OfficeScan**

6. Cliquez sur **Enregistrer**.

   Attendez que l'agent de mise à jour termine le téléchargement du programme de l'agent avant de passer à la cinquième partie.

7. Répétez les étapes 1 à 6 jusqu'à ce que tous les agents de mise à jour aient appliqué les paramètres nécessaires.

Cinquième partie : mise à niveau des agents OfficeScan

Procédure

1. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique** et assurez-vous que les options suivantes sont activées :

   - **Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan**
   - **Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)**

2. Accédez à **Agents** > **Gestion des agents**.

3. Dans l'arborescence des agents, sélectionnez les agents que vous souhaitez mettre à niveau. Vous pouvez sélectionner un ou plusieurs domaines ou tout ou partie des agents d'un domaine.

4. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.

5. Désactivez **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.

6. Cliquez sur **Enregistrer**.
7. Vérifiez les résultats de la mise à niveau.
   - *Agents en ligne à la page 3-11*
   - *Agents hors ligne à la page 3-13*
   - *Agents itinérants à la page 3-13*
8. Redémarrez les endpoints des agents pour terminer la mise à niveau des agents.
9. Répétez les étapes 2 à 8 jusqu'à ce que tous les agents aient été mis à niveau.

Résultats de la mise à niveau

Agents en ligne

Remarque

Redémarrez les endpoints de l'agent après la mise à niveau.

- Mise à niveau automatique

  La mise à niveau des agents en ligne commence lorsque l'un des événements suivants se produit :

  - Le serveur OfficeScan télécharge un nouveau composant et demande aux agents de se mettre à jour.
  - L'agent est rechargé.
  - L'agent redémarre et se connecte au serveur OfficeScan.
  - Un endpoint de l'agent exécutant Windows Server 2003 ou Windows XP Professionnel se connecte à un serveur dont vous avez modifié le script de connexion au moyen de l'outil Configuration du script de connexion (`AutoPcc.exe`).
  - La mise à jour programmée s'exécute sur le endpoint de l'agent (uniquement pour les agents disposant de privilèges de mise à jour programmée).

- Mise à niveau manuelle

  Si aucun des événements ci-dessous ne s'est produit, effectuez les tâches suivantes pour mettre immédiatement à niveau les agents :

  - Créez et déployez un pack agent OfficeScan EXE ou MSI.

    Remarque

    Consultez le *Manuel de l'administrateur* pour savoir comment créer un pack agent.

  - Demandez aux utilisateurs d'agents d'exécuter l'option **Mettre à jour** sur leur endpoint.
  - Si le endpoint de l'agent exécute Windows Server 2003, XP Professionnel, Server 2008, Vista™ (toutes éditions à l'exception de Vista Édition Familiale), 7™ (toutes éditions à l'exception de Windows 7 Édition Familiale), Windows 8 (Professionnel/Entreprise) ou Windows Server 2012, demandez à l'utilisateur d'effectuer les étapes suivantes :
    - Connectez-vous au serveur.
    - Accédez à `\\<nom du serveur>\ofcscan`.
    - Lancez `AutoPcc.exe`.
  - Si le endpoint de l'agent exécute Windows XP Édition Familiale, Vista Édition Familiale, Windows 7 Édition Familiale ou Windows 8, demandez à l'utilisateur de cliquer avec le bouton droit de la souris sur `AutoPcc.exe` et de sélectionner **Exécuter en tant qu'administrateur**.
  - Lancer une mise à jour manuelle de l'agent.

  Pour lancer une mise à jour manuelle de l'agent :

  1. Accédez à **Mises à jour** > **Agents** > **Mise à jour manuelle**.
  2. Sélectionnez l'option **Sélectionner manuellement les agents** et cliquez sur **Sélectionner**.
  3. Dans l'arborescence des agents qui s'ouvre, choisissez les agents à mettre à niveau.

4. Cliquez sur **Lancer la mise à jour des composants** en haut de l'arborescence des agents.

Agents hors ligne

La mise à niveau des agents hors ligne s'opère lorsque ceux-ci passent en mode en ligne.

Agents itinérants

Les agents itinérants se mettent à niveau lorsqu'ils sont en ligne ou, dans le cas des agents disposant des privilèges de mise à jour programmée, lors de l'exécution d'une mise à jour programmée.

Méthode de mise à niveau 3 : Déplacez les agents vers le serveur OfficeScan 11.0.

Effectuez une nouvelle installation du serveur OfficeScan 11.0 et déplacez les agents vers ce serveur. Lorsque vous déplacez les agents, ceux-ci sont automatiquement mis à niveau vers OfficeScan 11.0.

Première partie : exécution d'une nouvelle installation du serveur OfficeScan et configuration des paramètres de mise à jour

Procédure

1. Effectuez une nouvelle installation du serveur OfficeScan 11,0. Pour obtenir des informations détaillées, consultez la section *Écrans du programme d'installation à la page 2-5*.

2. Connectez-vous à la console Web.

3. Accédez à **Mises à jour** > **Agents** > **Mise à jour automatique** et assurez-vous que les options suivantes sont activées :

   - **Lancer la mise à jour des composants sur les agents immédiatement après le téléchargement d'un nouveau composant par le serveur OfficeScan**

- **Permettre aux agents de lancer une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les agents itinérants sont exclus)**

4. Accédez à **Agents** > **Gestion des agents**.
5. Dans l'arborescence des agents, sélectionnez l'icône du domaine racine ( ) pour sélectionner tous les agents.
6. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
7. Désactivez **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.
8. Cliquez sur **Appliquer à tous les agents**.
9. Prenez note des informations suivantes sur le serveur OfficeScan 11,0. Spécifiez ces informations sur le serveur OfficeScan10.x/8.0 SP1 lors du déplacement d'agents :
   - Nom ou adresse IP du endpoint
   - Port d'écoute du serveur

     Pour afficher le port d'écoute du serveur, accédez à **Administration** > **Paramètres** > **Connexion à l'agent**. Le numéro de port s'affiche à l'écran.

Deuxième partie : mise à niveau des agents OfficeScan

Procédure

1. Dans la console Web OfficeScan 10.x/8.0 SP1, accédez à **Mises à jour** > **Résumé**.
2. Cliquez sur **Annuler la notification**. Cette fonction efface la file d'attente des notifications du serveur, ce qui évite les problèmes lors du déplacement des clients vers le serveur OfficeScan 11,0.

AVERTISSEMENT!

Exécutez la procédure suivante immédiatement. Si la file d'attente des notifications du serveur est mise à jour avant le déplacement des clients, celui-ci risque d'échouer.

3. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
4. Dans l'arborescence client, sélectionnez les clients que vous souhaitez mettre à niveau. Sélectionnez uniquement les clients en ligne car il est impossible de déplacer les clients hors ligne et itinérants.
5. Cliquez sur **Gérer l\'arborescence des clients** > **Déplacer client**.
6. Indiquez le nom d'ordinateur/l'adresse IP du serveur OfficeScan 11,0 et son port d'écoute sous **Déplacer le ou les clients sélectionnés en ligne vers un autre serveur OfficeScan**.
7. Cliquez sur **Déplacer**.

Résultats de la mise à niveau

- Le déplacement et la mise à niveau des agents en ligne commencent.
- Conseils pour la gestion des agents hors ligne et itinérants :
  - Désactivez le mode itinérance sur les agents afin de pouvoir les mettre à niveau.
  - Pour les agents hors ligne, demandez aux utilisateurs de se connecter au réseau afin que les agents passent en mode en ligne. Pour les agents qui sont en mode hors ligne pendant une période prolongée, demandez aux utilisateurs de désinstaller l'agent du endpoint, puis d'utiliser une méthode d'installation adaptée (par exemple Agent Packager), décrite dans le *Manuel de l'administrateur*, pour installer l'agent OfficeScan.

Remarque

Redémarrez les endpoints des agents pour terminer la mise à niveau des agents.

Méthode de mise à niveau 4 : activation de la mise à niveau automatique des agents

Après la mise à niveau du serveur OfficeScan vers cette version, celui-ci demande automatiquement à tous les agents qu'il gère de se mettre à niveau.

Si le nombre d'agents que le serveur gère est peu élevé, envisagez de permettre aux agents d'effectuer immédiatement la mise à niveau. Vous pouvez également utiliser les méthodes de mise à niveau exposées auparavant.

Première partie : configuration des paramètres de mise à niveau sur le serveur OfficeScan 10.x

Procédure

1. Accédez à **Mises à jour** > **Ordinateurs en réseau** > **Mise à jour automatique** et assurez-vous que les options suivantes sont activées :
   - **Lancer la mise à jour des composants sur les clients immédiatement après le téléchargement d'un nouveau composant sur le serveur OfficeScan.**
   - **Configurer les clients pour qu'ils lancent une mise à jour des composants lorsqu'ils redémarrent et se connectent au serveur OfficeScan (les clients itinérants sont exclus)**
2. Accédez à **Ordinateurs en réseau** > **Gestion des clients**.
3. Dans l'arborescence client, sélectionnez l'icône du domaine racine () pour sélectionner tous les clients.
4. Cliquez sur **Paramètres** > **Privilèges et autres paramètres** et accédez à l'onglet **Autres paramètres**.
5. Sélectionnez **Les clients peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme client ni déployer des correctifs de type hot fix**.
6. Cliquez sur **Appliquer à tous les clients**.

Conseil

Le déploiement des paramètres vers les clients en ligne peut prendre un certain temps si vous disposez d'un environnement de réseau complexe et d'un grand nombre de clients. Avant la mise à niveau, allouez suffisamment de temps pour que les paramètres soient déployés vers tous les clients. Les clients OfficeScan qui n'appliquent pas les paramètres sont automatiquement mis à niveau.

Deuxième partie : mise à niveau du serveur OfficeScan

Voir *Réalisation d'une mise à niveau locale à la page 3-18* ou *Réalisation d'une mise à niveau distante à la page 3-34* pour plus de détails sur la mise à niveau du serveur OfficeScan.

Remarque

Pour accélérer le processus de mise à niveau, déchargez l'agent OfficeScan avant de mettre à niveau un serveur OfficeScan exécutant Windows Server 2008 Standard 64 bits.

Configurez les paramètres du serveur OfficeScan en utilisant la console Web immédiatement après la fin de l'installation et avant la mise à niveau des agents.

Pour obtenir des instructions détaillées sur la méthode de configuration des paramètres d'OfficeScan, consultez le *Manuel de l'administrateur* ou l'*aide du serveur OfficeScan*.

Résultats de la mise à niveau

- Les agents en ligne sont mis à niveau dès que la mise à niveau du serveur est terminée.
- La mise à niveau des agents hors ligne s'opère lorsque ceux-ci passent en mode en ligne.
- Les agents itinérants se mettent à niveau lorsqu'ils sont en ligne ou, dans le cas des agents disposant des privilèges de mise à jour programmée, lors de l'exécution d'une mise à jour programmée.

Remarque

Redémarrez les endpoints des agents pour terminer la mise à niveau des agents.

Réalisation d'une mise à niveau locale

Lors d'une mise à niveau locale, OfficeScan applique les paramètres utilisés par la version précédente du serveur OfficeScan. Un sous-ensemble limité d'écrans s'affichent afin de vous permettre de configurer les nouvelles fonctionnalités proposées par OfficeScan 11.0.

Contrat de licence

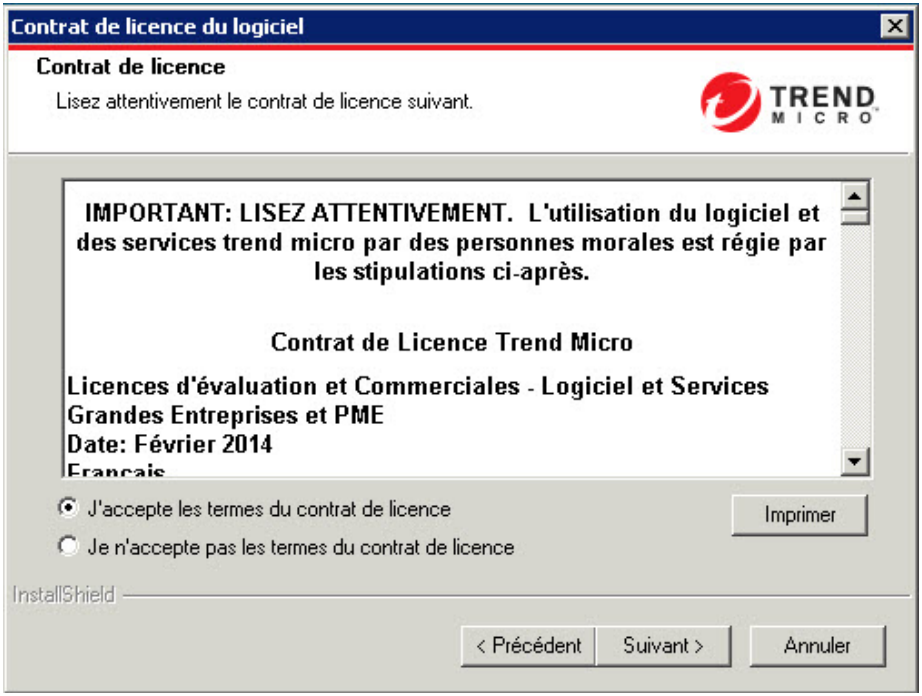

FIGURE 3-1. Écran Contrat de licence

Lisez attentivement le contrat de licence et confirmez votre acceptation avant de procéder à l'installation. Il est impossible de continuer l'installation sans accepter les termes du contrat de licence.

Destination de l'installation

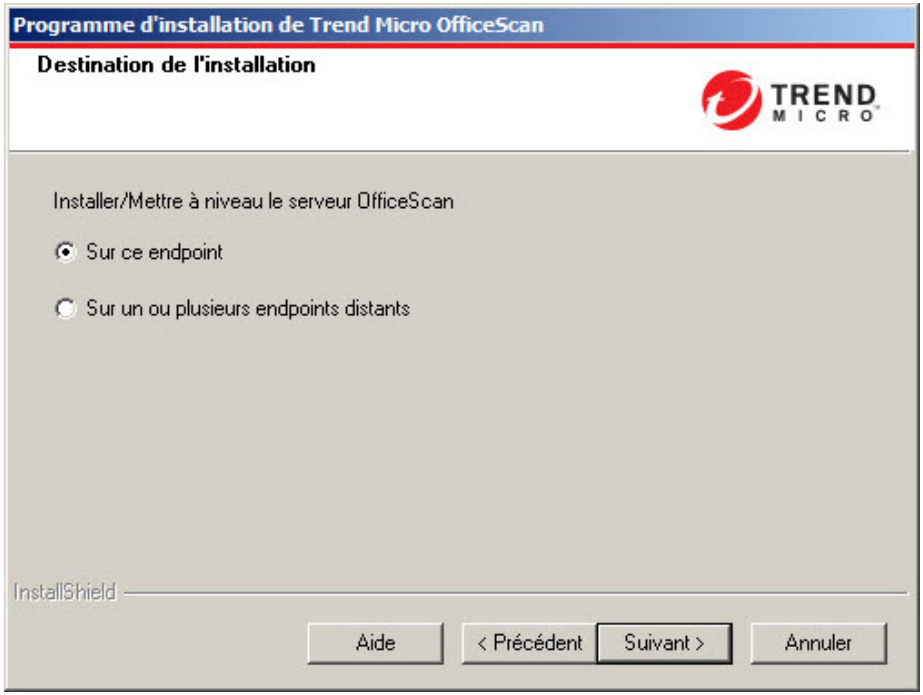

FIGURE 3-2. Écran Destination de l'installation

Exécutez le programme d'installation et installez le serveur OfficeScan sur le endpoint sur lequel vous êtes occupé ou sur d'autres endpoints du réseau.

Remarques sur la mise à niveau à distance

Lorsque vous effectuez une mise à niveau à distance, le programme d'installation vérifie si le endpoint cible dispose de la configuration requise pour la mise à niveau du serveur. Avant de continuer :

- Vous devez obtenir les droits d'administration de ce endpoint.
- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que les endpoints cible présentent la configuration minimale requise en vue de l'installation du serveur OfficeScan.
- Assurez-vous que le endpoint soit équipé de Microsoft IIS Server 6,0 ou d'une version supérieure s'il est utilisé comme serveur Web. Lorsque vous utilisez le serveur Web Apache, le programme d'installation installe automatiquement ce serveur s'il n'est pas déjà présent sur le endpoint cible.

Si vous procédez à des mises à niveau locales, OfficeScan conserve les paramètres originaux de l'installation précédente, y compris le nom du serveur, les informations relatives au serveur proxy et les numéros de port. Ces paramètres ne peuvent pas être modifiés pendant la mise à niveau. Modifiez-les après la mise à niveau depuis la console Web d'OfficeScan.

Important

Lorsque vous procédez à des mises à niveau à distance, vous devez entrer à nouveau tous les paramètres. Toutefois, ceux-ci seront ignorés après la mise à niveau du serveur puisque ce dernier utilisera les paramètres de la version précédente.

Pré-scan du Endpoint

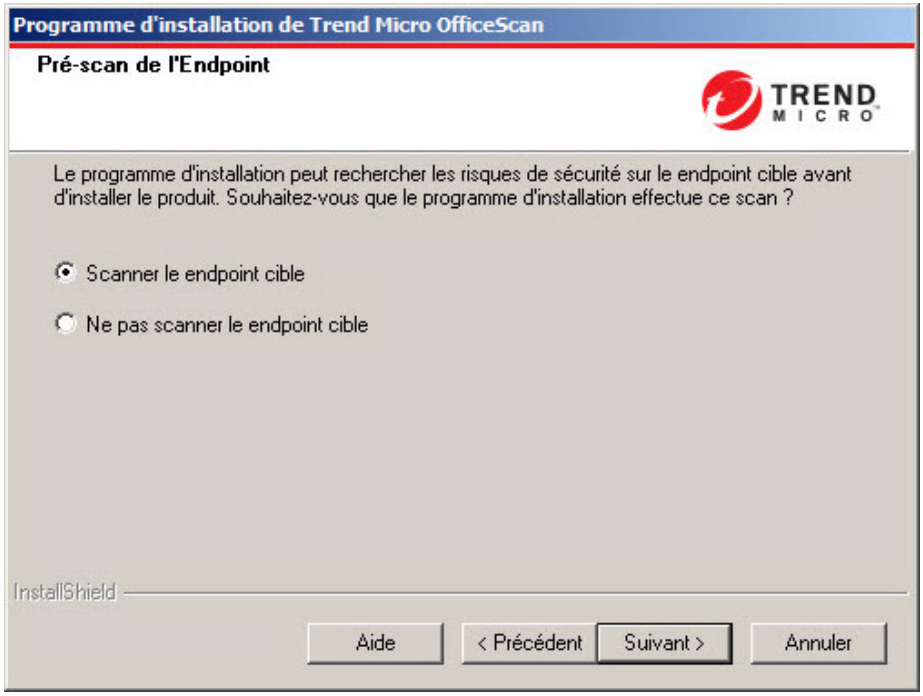

FIGURE 3-3. Écran Pré-scan du Endpoint

Avant de procéder à l'installation du serveur OfficeScan, le programme d'installation peut scanner le endpoint cible pour détecter des virus ou des programmes malveillants. Le programme d'installation scanne les zones les plus vulnérables du endpoint, parmi lesquelles :

- La zone et le répertoire d'amorçage (contre les virus d'amorce)
- Le dossier Windows
- Le dossier Program files

Le programme d'installation peut entreprendre les actions suivantes contre les virus/programmes malveillants et les chevaux de Troie détectés :

- **Supprimer** : Supprime un fichier infecté
- **Nettoyer** : Nettoie un fichier nettoyable avant d'autoriser l'accès complet au fichier ou laisse à l'action suivante spécifiée le soin de traiter un fichier non nettoyable.
- **Renommer** : remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier. 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** : Autorise l'accès complet au fichier infecté sans entreprendre d'action contre le fichier. Un utilisateur peut copier/supprimer/ouvrir le fichier.

En cas d'installation locale, le scan est effectué en cliquant sur **Suivant**. En cas d'installation à distance, le scan est effectué juste avant l'installation effective.

Alerte de redémarrage de l'agent OfficeScan

Le programme d'installation évalue les ressources sur le endpoint cible. Pendant les scénarios de mise à niveau, un écran d'avertissement apparaît si le programme de l'agent OfficeScan existe sur le endpoint cible.

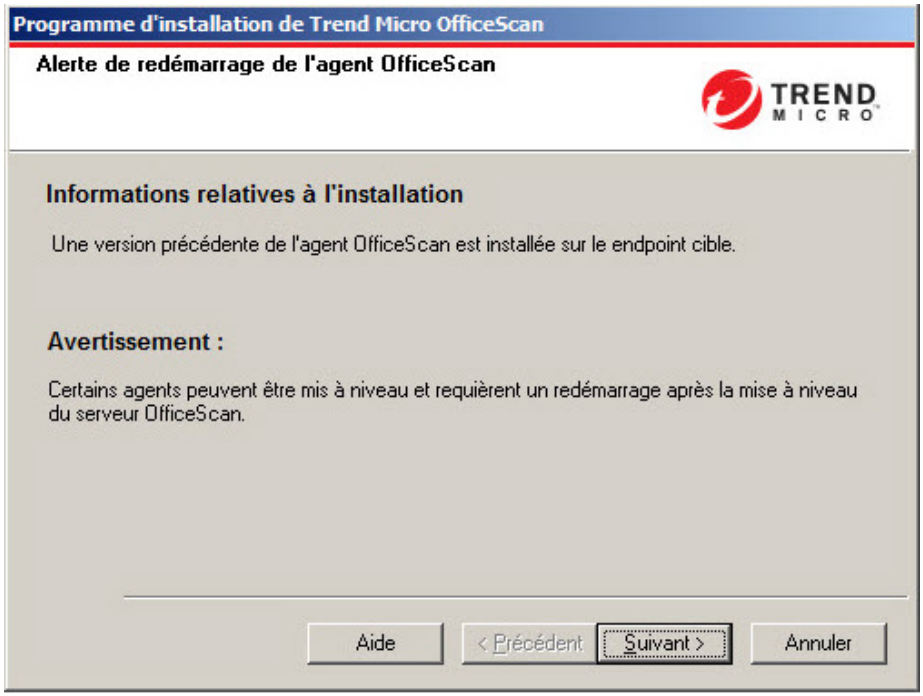

FIGURE 3-4. Alerte de redémarrage de l'agent OfficeScan

Sauvegarde de la base de données

Pendant les mises à niveau, le programme d'installation offre une option de sauvegarde de la base de données OfficeScan avant de passer à la dernière version. Vous pouvez utiliser ces informations de sauvegarde à des fins de restauration.

Remarque

Le pack de sauvegarde peut nécessiter plus de 300 Mo d'espace disque disponible.

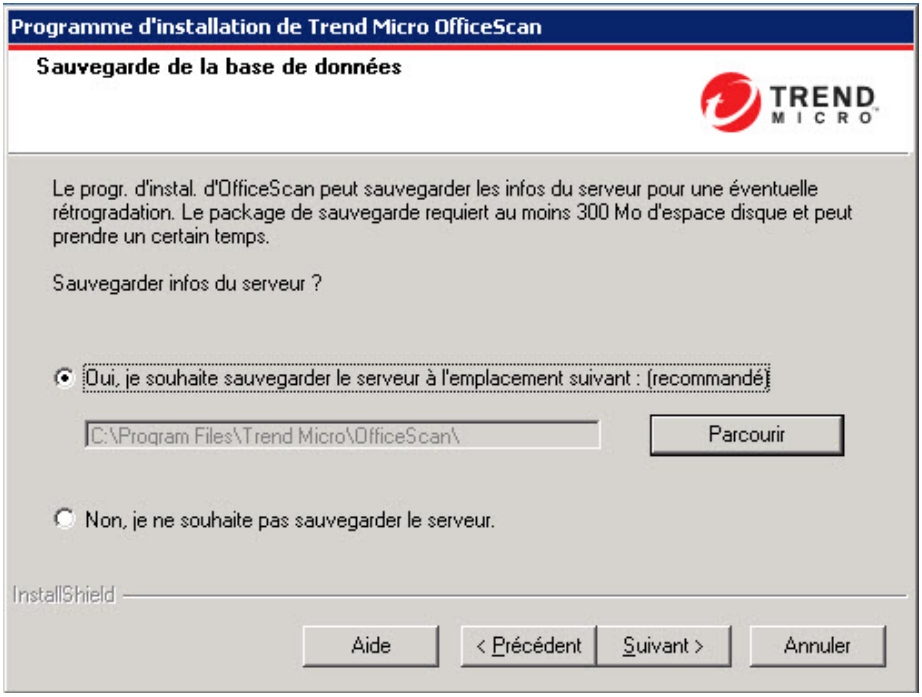

FIGURE 3-5. Écran Sauvegarde de la base de données

Déploiement de l'agent OfficeScan

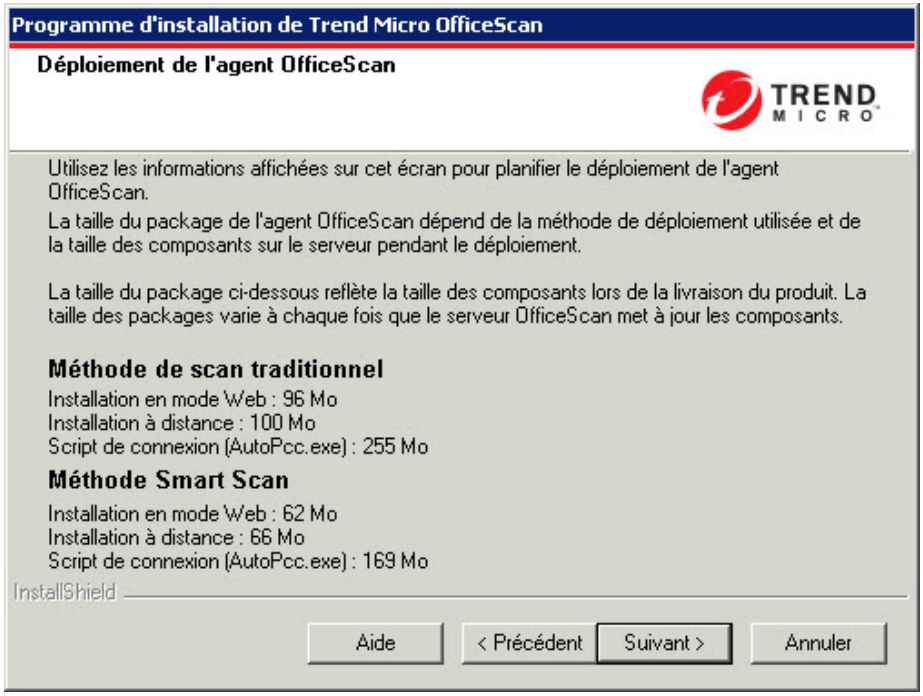

FIGURE 3-6. Écran Déploiement de l'agent OfficeScan

Différentes méthodes sont disponibles pour installer ou mettre à niveau les agents OfficeScan. Cet écran répertorie les différentes méthodes de déploiement et la bande passante du réseau approximative requise.

Cet écran permet d'estimer l'espace requis sur les serveurs et la bande passante consommée lors du déploiement des agents sur les endpoints cible.

Remarque

Toutes ces méthodes d'installation requièrent des droits d'administrateur local ou d'administrateur de domaine sur les endpoints cible.

Installer le serveur Smart Protection intégré

Remarque

Cet écran ne s'affiche pas lors de l'utilisation d'un site Web IIS virtuel pendant les installations de mises à niveaux locales.

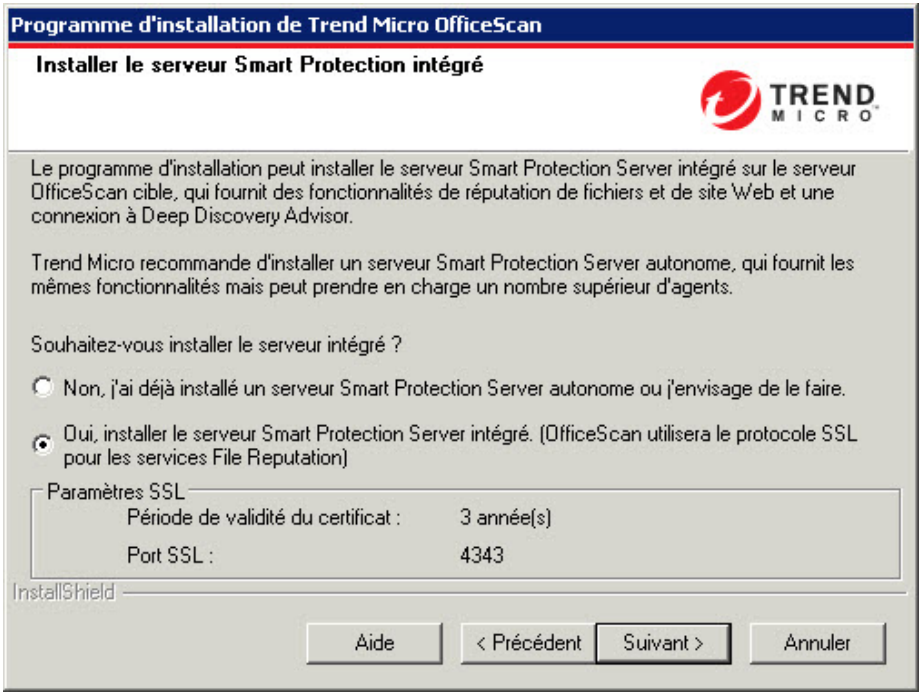

FIGURE 3-7. Écran d'installation du serveur Smart Protection Server intégré

Le programme d'installation peut installer le serveur Smart Protection Server intégré sur le endpoint cible. Le serveur intégré fournit les services de File Reputation aux agents qui utilisent Smart Scan et les services de réputation de sites Web aux agents soumis aux stratégies de réputation de sites Web. Gérez le serveur intégré à partir d'OfficeScan Web Console.

Trend Micro recommande d'installer le serveur Smart Protection Server autonome qui a les mêmes fonctions que le serveur intégré mais qui peut desservir davantage d'agents. Le serveur autonome est installé séparément et dispose de sa propre console de gestion. Consultez le *Manuel de l'administrateur Trend Micro Smart Protection Server* pour plus d'informations sur le serveur autonome.

Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même endpoint, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours. Consultez le *Manuel de l'administrateur* pour plus d'informations sur la configuration des sources Smart Protection pour les agents.

Protocoles de connexion des agents pour les services de File Reputation

Les agents OfficeScan peuvent se connecter aux services de File Reputation du serveur Smart Protection Server intégré à l'aide des protocoles HTTP et HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

Remarque

Si des agents se connectent au serveur intégré via un serveur proxy, vous devez configurer des paramètres proxy internes depuis la console Web. Consultez le *Manuel de l'administrateur* pour obtenir des informations sur la configuration des paramètres proxy.

Les numéros de port utilisés pour les services de File Reputation dépendent du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

Le port HTTP ne s'affiche pas sur l'écran d'installation. Le port HTTPS s'affiche mais la configuration est facultative.

TABLEAU 3-1. Ports pour les services de File Reputation du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORTS POUR LES SERVICES DE FILE REPUTATION	
	HTTP	HTTPS (SSL)
Serveur Web Apache	8082	4345
Site Web IIS par défaut	80	443
Site Web IIS virtuel	8080	4343

Serveur intégré non installé

Si vous effectuez une nouvelle installation et ne choisissez pas d'installer le serveur intégré :

- Le scan traditionnel devient la méthode de scan par défaut.
- Lorsque vous activez les stratégies de réputation de sites Web dans un écran d'installation différent (pour plus d'informations, voir *Fonction Réputation de sites Web à la page 2-43*), les agents ne peuvent pas envoyer de requêtes de réputation de sites Web car OfficeScan présume que le serveur Smart Protection Server n'est pas installé.

Si un serveur autonome est disponible après avoir installé OfficeScan, effectuez les tâches suivantes depuis OfficeScan Web Console :

- Changez la méthode de scan en Smart Scan.
- Ajoutez le serveur autonome à la liste des sources Smart Protection afin que les agents puissent lui envoyer des requêtes de File Reputation et de réputation de sites Web.

Lorsque vous effectuez une mise à niveau depuis des serveurs OfficeScan 10.x dans lesquels le serveur intégré a été désactivé, celui-ci n'est pas installé. Les agents OfficeScan conservent leur méthode de scan et les sources Smart Protection auxquelles ils envoient des requêtes.

Activer les services de réputation de sites Web

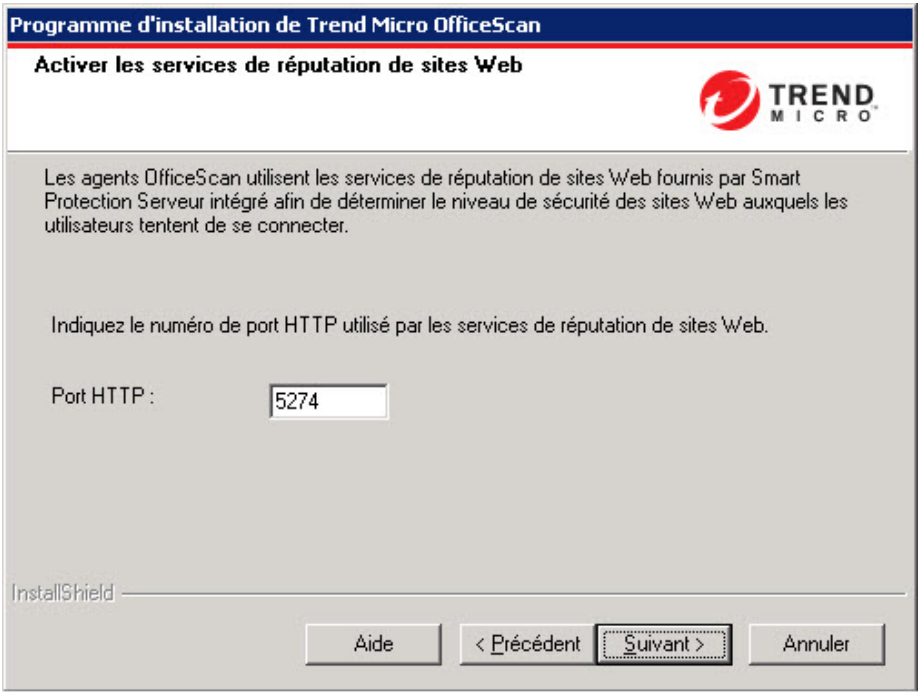

FIGURE 3-8. Activation de l'écran Services de réputation de sites Web

Les services de réputation de sites Web évaluent les risques de sécurité potentiels de toutes les URL demandées lors de l'exécution de chaque requête HTTP. Selon l'évaluation renvoyée par la base de données et le niveau de sécurité configuré, la réputation de sites Web bloque ou approuve la requête. Le serveur Smart Protection Server intégré, installé avec le serveur OfficeScan, fournit les services de réputation de sites Web.

L'activation des services de réputation de sites Web (fonctionnant sous le processus appelé `LWCSService.exe`) réduit la consommation globale de bande passante. En effet, les agents OfficeScan obtiennent les données de réputation de sites Web depuis un serveur local au lieu de se connecter à Smart Protection Network.

Protocoles de connexion des agents pour les services de réputation de sites Web

Les agents OfficeScan peuvent se connecter aux services de réputation de sites Web du serveur Smart Protection Server intégré à l'aide du protocole HTTP.

Le numéro de port HTTP utilisé pour les services de réputation de sites Web dépend du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

TABLEAU 3-2. Ports pour les services de réputation de sites Web du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORT HTTP POUR LES SERVICES DE RÉPUTATION DE SITES WEB
Serveur Web Apache sur lequel SSL est activé	5274
Site Web par défaut IIS sur lequel SSL est activé	80 (non configurable)
Site Web virtuel IIS sur lequel SSL est activé	8080 (non configurable)

Certificat d'authentification serveur

Le programme d'installation tente de détecter la présence de certificats d'authentification existants pendant l'installation. Si un tel certificat existe, OfficeScan mappe automatiquement le fichier sur l'écran **Certificat d'authentification serveur**. Si aucun

certificat n'existe, OfficeScan applique par défaut l'option **Générer un certificat d'authentification**.

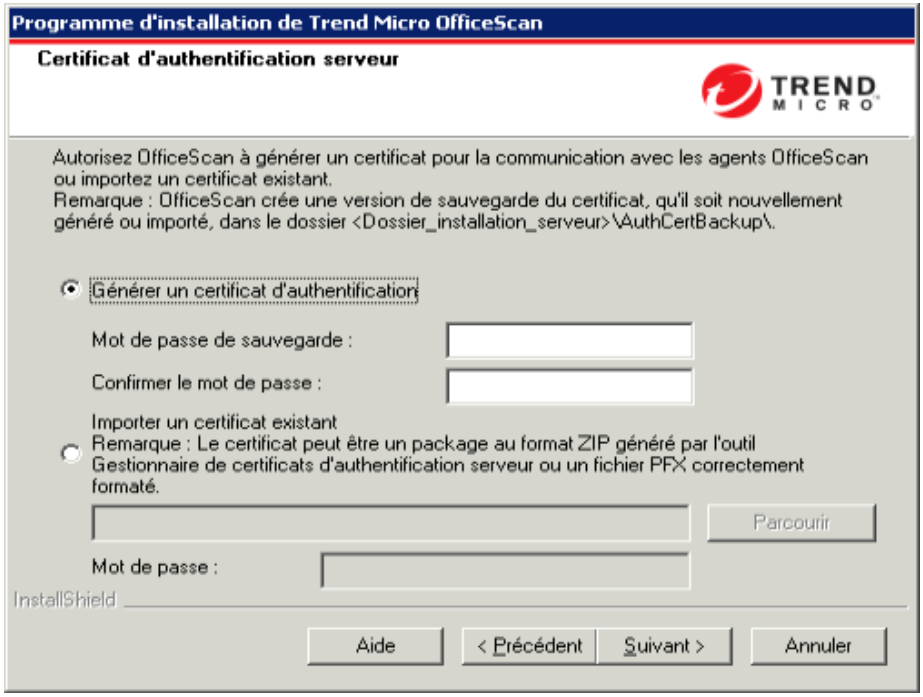

FIGURE 3-9. Écran Certificat d'authentification serveur pour les nouveaux certificats

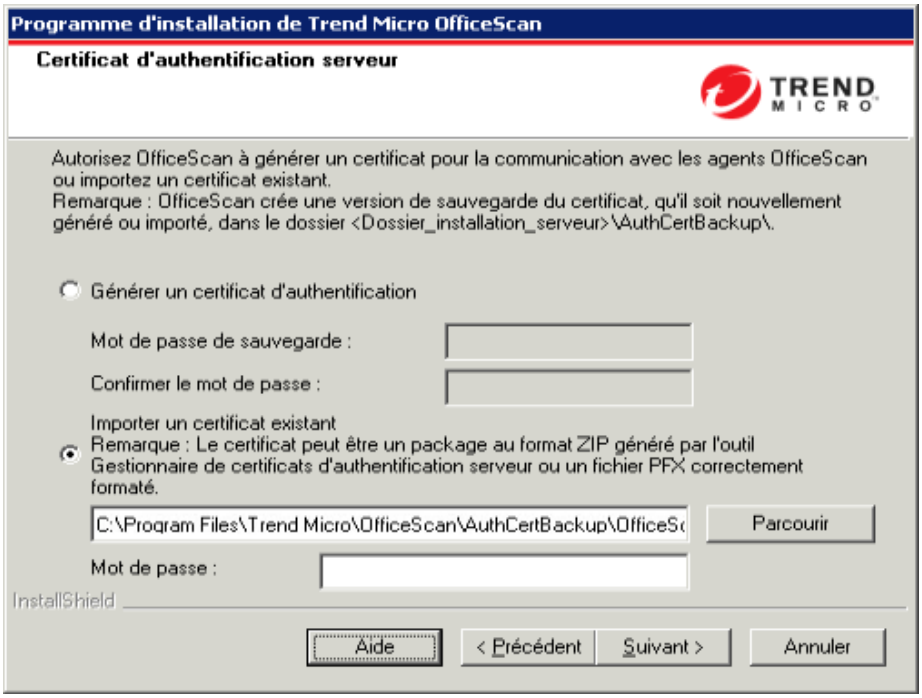

FIGURE 3-10. Écran Certificat d'authentification serveur pour les certificats existants

OfficeScan utilise le chiffrement à clé publique pour authentifier les communications du serveur OfficeScan vers les agents. Grâce à cette technologie, le serveur conserve une clé privée et déploie une clé publique sur tous les agents. Les agents utilisent la clé publique pour vérifier que les communications entrantes proviennent bien du serveur et sont valides. Les agents répondent au serveur si cette vérification réussit.

Remarque

OfficeScan n'authentifie pas les communications vers le serveur provenant des agents.

OfficeScan peut générer le certificat d'authentification pendant l'installation ou les administrateurs peuvent importer un certificat d'authentification préexistant depuis un autre serveur OfficeScan.

Conseil

Lors de la sauvegarde du certificat, Trend Micro recommande le chiffrement du certificat à l'aide d'un mot de passe.

Informations sur l'installation

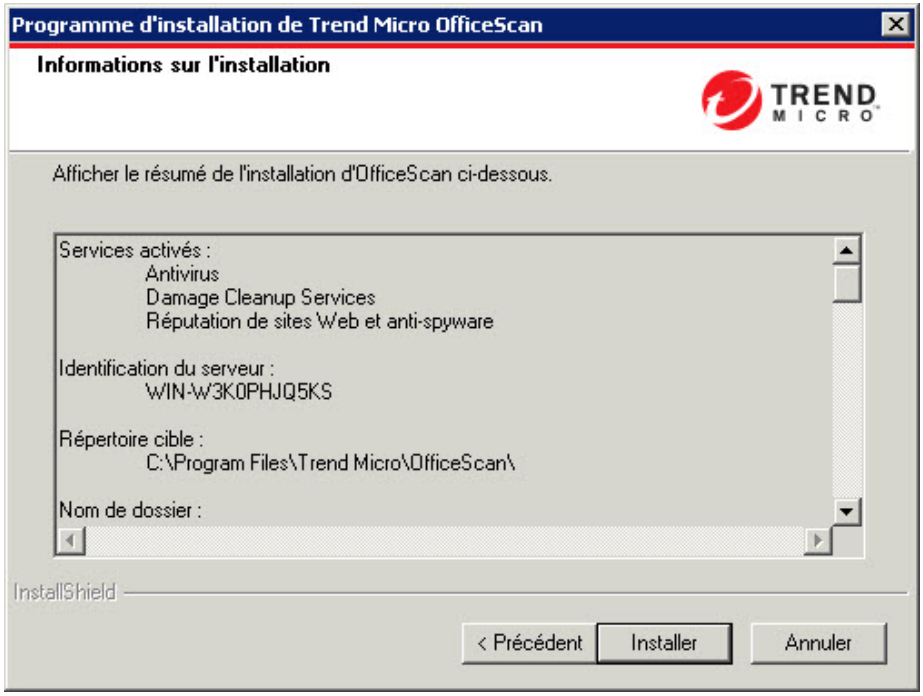

FIGURE 3-11. Écran Informations sur l'installation

Cet écran contient un récapitulatif des paramètres d'installation. Vérifiez les informations relatives à l'installation et cliquez sur **Précédent** pour modifier les paramètres ou les options, le cas échéant. Pour lancer l'installation, cliquez sur **Installer**.

Assistant InstallShield terminé

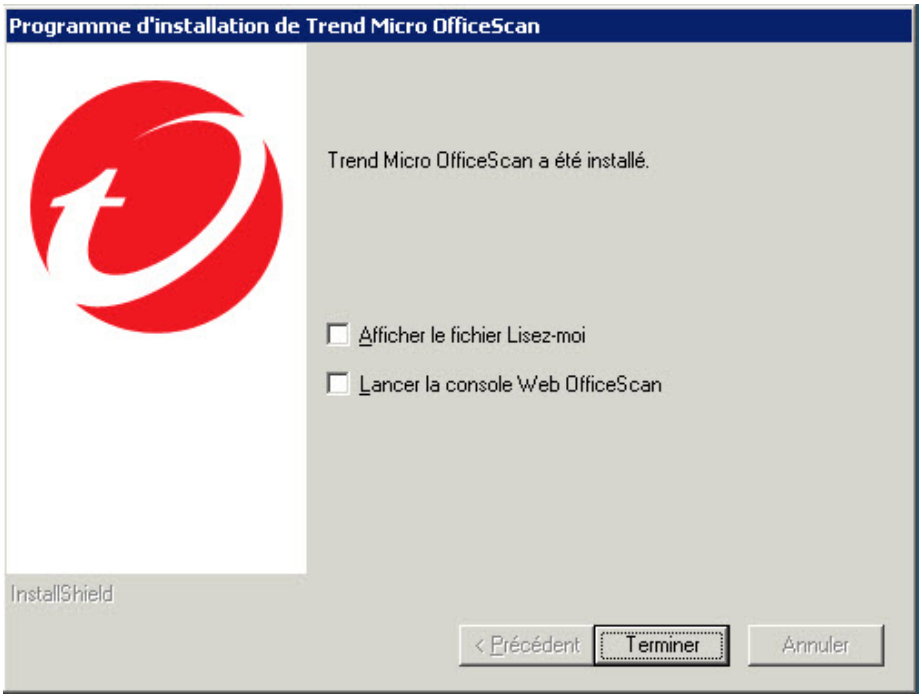

FIGURE 3-12. Écran indiquant que l'Assistant InstallShield est terminé

Une fois l'installation terminée, lisez le fichier Lisez-moi pour prendre connaissance des informations de base relatives au produit et aux problèmes connus.

Les administrateurs peuvent démarrer la console Web pour commencer à configurer les paramètres d'OfficeScan.

Réalisation d'une mise à niveau distante

Lors de la réalisation d'une mise à niveau distante, OfficeScan propose davantage d'options de configuration, car il est impossible de connaître tous les anciens paramètres

de la version précédente du serveur OfficeScan avant le lancement de la mise à niveau. Au cours de la mise à niveau, OfficeScan utilise les paramètres de configuration de la version précédente du serveur OfficeScan plutôt que ceux que vous avez définis pendant la configuration de la mise à niveau. Pour tout nouveau paramètre n'existant pas dans la version précédente du serveur OfficeScan, OfficeScan applique les paramètres que vous avez définis pendant la configuration de la mise à niveau.

Contrat de licence

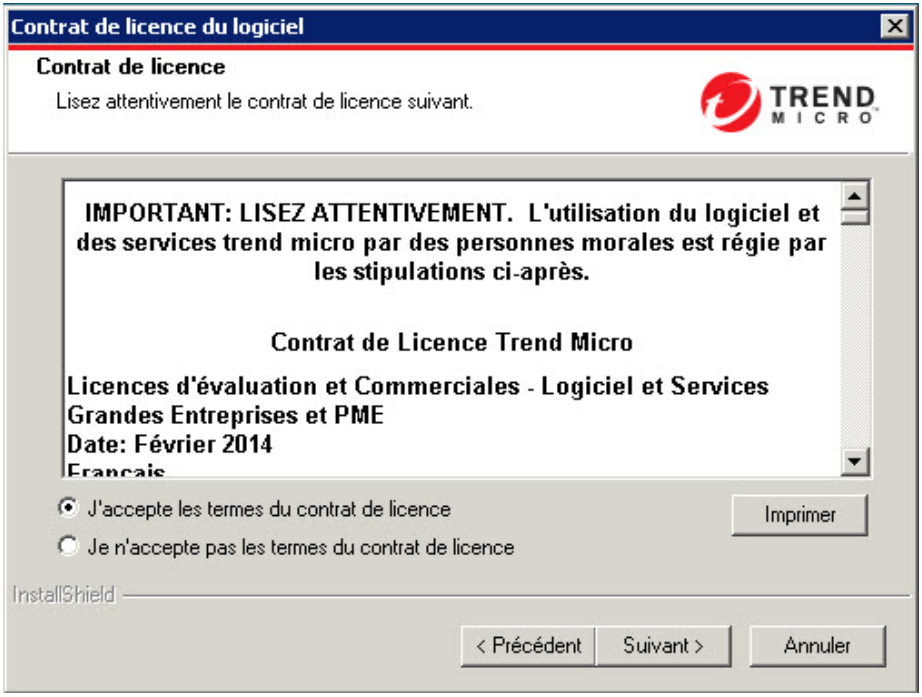

FIGURE 3-13. Écran Contrat de licence

Lisez attentivement le contrat de licence et confirmez votre acceptation avant de procéder à l'installation. Il est impossible de continuer l'installation sans accepter les termes du contrat de licence.

Destination de l'installation

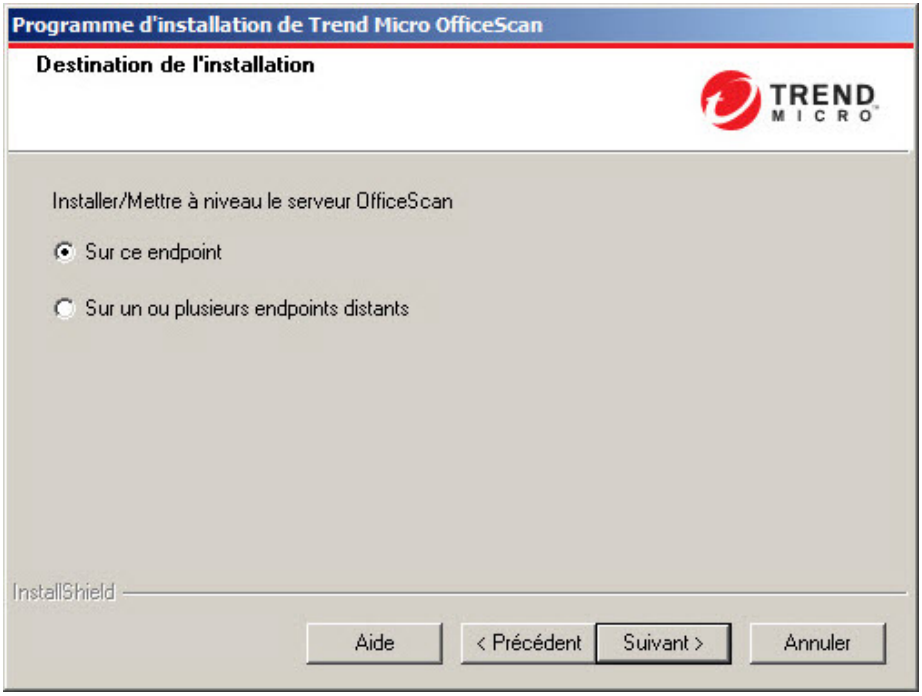

FIGURE 3-14. Écran Destination de l'installation

Exécutez le programme d'installation et installez le serveur OfficeScan sur le endpoint sur lequel vous êtes occupé ou sur d'autres endpoints du réseau.

Remarques sur la mise à niveau à distance

Lorsque vous effectuez une mise à niveau à distance, le programme d'installation vérifie si le endpoint cible dispose de la configuration requise pour la mise à niveau du serveur. Avant de continuer :

- Vous devez obtenir les droits d'administration de ce endpoint.

- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que les endpoints cible présentent la configuration minimale requise en vue de l'installation du serveur OfficeScan.
- Assurez-vous que le endpoint soit équipé de Microsoft IIS Server 6,0 ou d'une version supérieure s'il est utilisé comme serveur Web. Lorsque vous utilisez le serveur Web Apache, le programme d'installation installe automatiquement ce serveur s'il n'est pas déjà présent sur le endpoint cible.

Si vous procédez à des mises à niveau locales, OfficeScan conserve les paramètres originaux de l'installation précédente, y compris le nom du serveur, les informations relatives au serveur proxy et les numéros de port. Ces paramètres ne peuvent pas être modifiés pendant la mise à niveau. Modifiez-les après la mise à niveau depuis la console Web d'OfficeScan.

Important

Lorsque vous procédez à des mises à niveau à distance, vous devez entrer à nouveau tous les paramètres. Toutefois, ceux-ci seront ignorés après la mise à niveau du serveur puisque ce dernier utilisera les paramètres de la version précédente.

Pré-scan du Endpoint

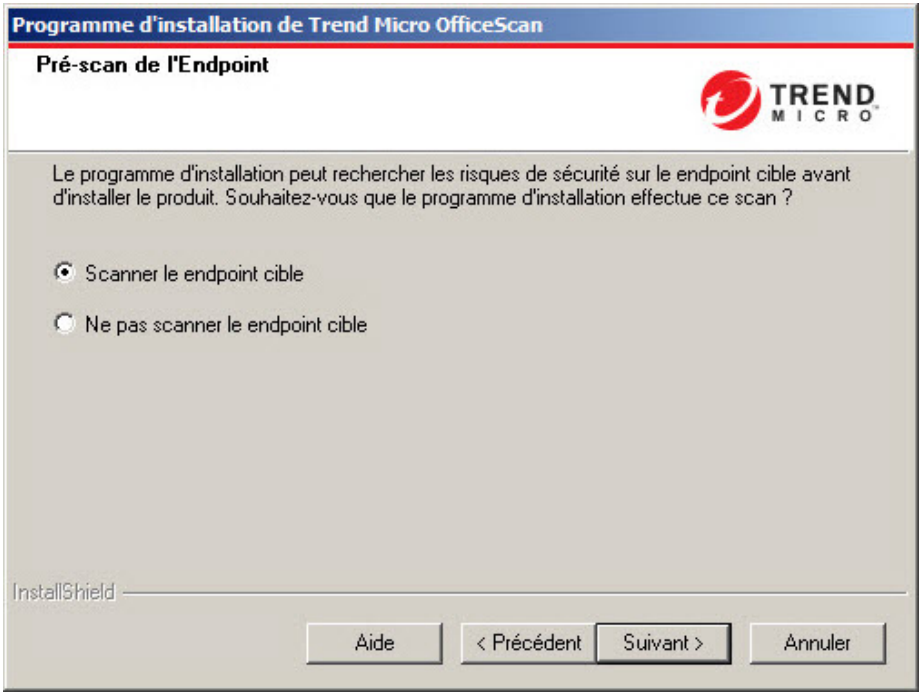

FIGURE 3-15. Écran Pré-scan du Endpoint

Avant de procéder à l'installation du serveur OfficeScan, le programme d'installation peut scanner le endpoint cible pour détecter des virus ou des programmes malveillants. Le programme d'installation scanne les zones les plus vulnérables du endpoint, parmi lesquelles :

- La zone et le répertoire d'amorçage (contre les virus d'amorce)
- Le dossier Windows
- Le dossier Program files

Le programme d'installation peut entreprendre les actions suivantes contre les virus/programmes malveillants et les chevaux de Troie détectés :

- **Supprimer** : Supprime un fichier infecté
- **Nettoyer** : Nettoie un fichier nettoyable avant d'autoriser l'accès complet au fichier ou laisse à l'action suivante spécifiée le soin de traiter un fichier non nettoyable.
- **Renommer** : remplace l'extension du fichier infecté par « `vir` ». Initialement, les utilisateurs ne peuvent pas ouvrir le fichier. 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** : Autorise l'accès complet au fichier infecté sans entreprendre d'action contre le fichier. Un utilisateur peut copier/supprimer/ouvrir le fichier.

En cas d'installation locale, le scan est effectué en cliquant sur **Suivant**. En cas d'installation à distance, le scan est effectué juste avant l'installation effective.

Chemin d'installation

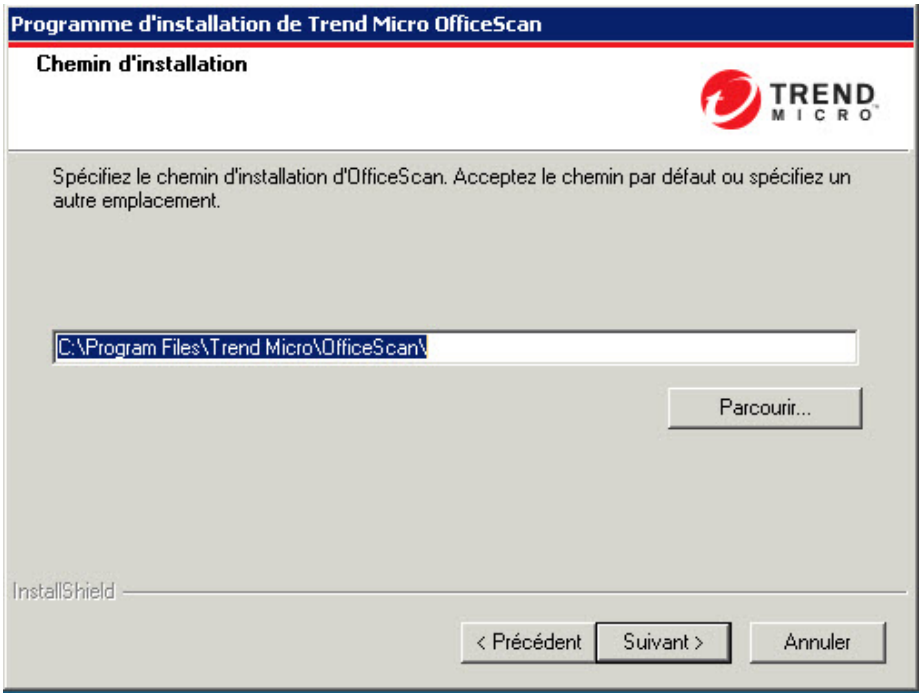

FIGURE 3-16. Écran Chemin d'installation

Acceptez le chemin d'installation par défaut ou spécifiez-en un nouveau.

Le chemin d'installation spécifié ne s'applique que lorsque l'on procède à une nouvelle installation à distance. Pour les mises à niveau à distance, OfficeScan utilise les paramètres de la version précédente

Serveur proxy

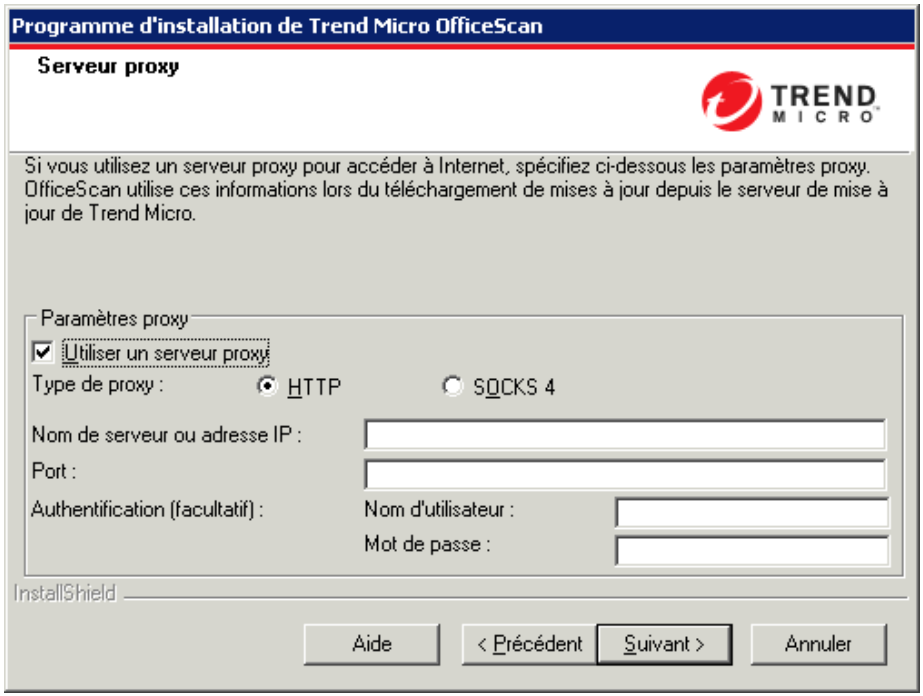

FIGURE 3-17. Écran Serveur proxy

Le serveur OfficeScan utilise le protocole HTTP pour la communication agent-serveur et pour la connexion à Trend Micro ActiveUpdate Server afin de télécharger les mises à jour. Si un serveur proxy gère le trafic Internet sur le réseau, OfficeScan doit disposer des paramètres proxy pour permettre au serveur de télécharger les mises à jour depuis le serveur ActiveUpdate.

Les administrateurs peuvent décider de ne pas spécifier les paramètres proxy pendant l'installation et de le faire après à partir d'OfficeScan Web Console.

Les paramètres proxy ne s'appliquent que lors d'une nouvelle installation à distance. Pour une mise à niveau à distance, OfficeScan utilise les paramètres de la version précédente

Remarque

Lorsque vous installez le serveur OfficeScan sur un endpoint utilisant exclusivement le protocole IPv6, installez un serveur proxy double pile qui peut convertir les adresses IP. Cela permet au serveur de se connecter au serveur ActiveUpdate.

Serveur Web

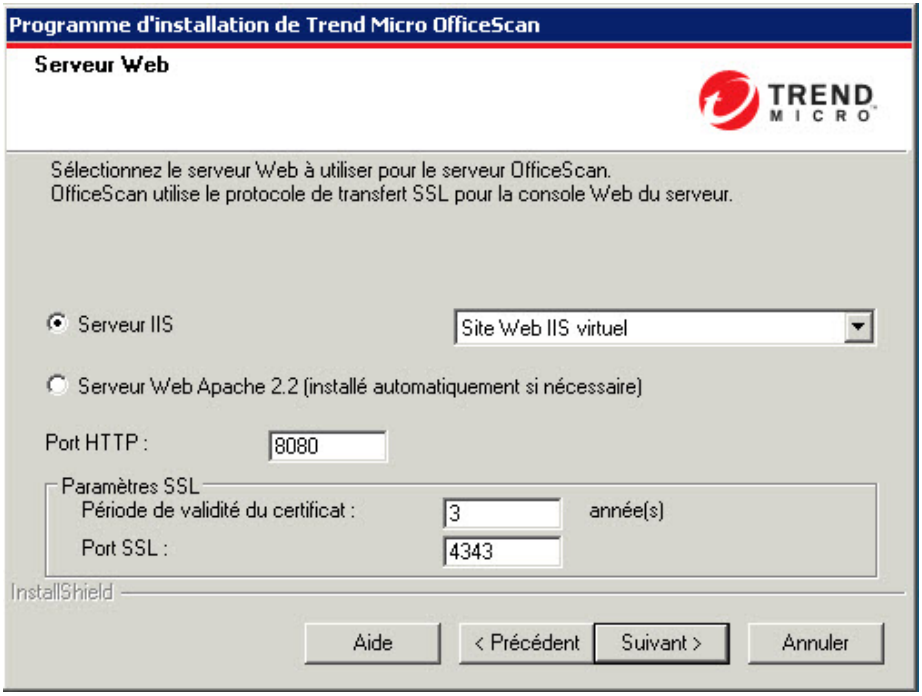

FIGURE 3-18. Écran Serveur Web

Le serveur Web OfficeScan abrite la console Web, permet à l'administrateur d'exécuter des CGI (Common Gateway Interfaces) depuis la console et accepte les commandes provenant des agents. Le serveur Web convertit ces commandes en CGI d'agents et les transmet au service principal d'OfficeScan.

Les paramètres du serveur Web ne s'appliquent que lors d'une nouvelle installation à distance. Lorsque l'on effectue une mise à niveau à distance, OfficeScan utilise les paramètres de la version précédente.

Prise en charge d'IPv6

Pour les nouvelles installations, sélectionnez le serveur IIS pour activer la prise en charge d'IPv6. Le serveur Web Apache ne prend pas en charge l'adressage IPv6. Si le endpoint cible n'a qu'une adresse IPv6 et que vous choisissez Apache comme serveur Web, vous ne pourrez pas procéder à l'installation. Si le endpoint cible a une adresse IPv6 et une adresse IPv4, les administrateurs peuvent choisir Apache mais la prise en charge d'IPv6 ne sera pas activée après l'installation du serveur.

Lorsque vous effectuez une mise à niveau vers cette version d'OfficeScan, le serveur OfficeScan à mettre à niveau doit déjà utiliser IIS. Si le serveur utilise Apache, configurez-le pour IIS avant de mettre à niveau.

Serveur Web

Si le programme d'installation détecte à la fois les serveurs Web IIS et Apache sur le endpoint cible, les administrateurs peuvent choisir l'un de ces deux serveurs Web. Si aucun d'eux n'est installé sur le endpoint cible, les administrateurs ne peuvent pas choisir IIS et OfficeScan installe alors automatiquement le serveur Web Apache 2.2.

Si vous utilisez un serveur Web Apache :

- Le serveur Web Apache 2.2 est requis. Si le serveur Web Apache existe sur le endpoint mais que la version n'est pas 2.2, OfficeScan installe et utilise la version 2.2. OfficeScan ne supprime pas le serveur Web Apache existant.
- En cas d'activation du protocole SSL et si le serveur Web Apache 2.2 est installé, des paramètres SSL doivent être préconfigurés sur ce dernier.
- Par défaut, le compte administrateur est le seul compte créé sur le serveur Web Apache.

Conseil

Trend Micro recommande de créer un autre compte à utiliser pour faire tourner le serveur Web. Sinon, le serveur OfficeScan risque d'être victime d'activités malveillantes si un pirate parvient à prendre le contrôle du serveur Apache.

- Avant d'installer le serveur Web Apache, consultez le site Web Apache pour obtenir les informations les plus récentes sur les mises à niveau, les patchs et les problèmes de sécurité.

Si vous utilisez un serveur Web IIS :

- Les versions suivantes de Microsoft Internet Information Server (IIS) sont requises :
  - Version 6.0 sous Windows Server 2003
  - Version 7.0 sous Windows Server 2008
  - Version 7.5 sous Windows Server 2008 R2
  - Version 8.0 sous Windows Server 2012

  N'installez pas le serveur Web sur des endpoints exécutant des applications bloquant IIS. Cela risquerait d'entraîner l'échec de l'installation. Pour obtenir des informations complémentaires, consultez la documentation relative à IIS.

Port HTTP

Le serveur Web écoute les requêtes des agents sur le port HTTP et les transmet au service principal d'OfficeScan. Ce service renvoie les informations aux agents via le port de communication d'agent déterminé. Le programme d'installation génère de façon aléatoire le numéro de port de communication de l'agent pendant l'installation.

Support technique SSL

OfficeScan utilise le protocole Secure Sockets Layer (SSL) pour sécuriser la communication entre la console Web et le serveur. Le protocole SSL offre une couche supplémentaire de protection contre les pirates. Bien qu'OfficeScan chiffre les mots de passe spécifiés sur la console Web avant de les envoyer au serveur OfficeScan, cela

n'empêche pas les pirates de capturer le paquet correspondant et, sans avoir à déchiffrer ce paquet, de l'utiliser pour accéder à la console. La tunnelisation SSL empêche les pirates de capturer les paquets traversant le réseau.

La version SSL utilisée dépend de la version prise en charge par le serveur Web.

Lorsque vous sélectionnez le protocole SSL, le programme d'installation crée automatiquement un certificat SSL, obligatoire pour les connexions SSL. Le certificat contient des informations relatives au serveur, la clé publique et la clé privée.

La période de validité du certificat SSL doit être comprise entre 1 et 20 ans. L'administrateur peut toujours utiliser le certificat après son expiration. Cependant, un message d'avertissement apparaît chaque fois qu'une connexion SSL est appelée à l'aide du même certificat.

Fonctionnement de la communication SSL :

1. L'administrateur envoie des informations de la console Web vers le serveur Web via une connexion SSL.
2. Le serveur Web répond à la console Web avec le certificat requis.
3. Le navigateur effectue l'échange des clés à l'aide du chiffrement RSA.
4. La console Web envoie les données au serveur Web à l'aide du chiffrement RC4.

Bien que le chiffrement RSA soit plus sécurisé, il occasionne un ralentissement du flux de communication. C'est pourquoi il n'est utilisé que pour l'échange des clés alors que RC4, une alternative plus rapide, est utilisé pour le transfert de données.

Ports du serveur Web

Le tableau suivant répertorie les numéros de port par défaut pour le serveur Web

TABLEAU 3-3. Numéros de port pour OfficeScan Web Server

SERVEUR WEB ET PARAMÈTRES	PORTS	
	HTTP	HTTPS (SSL)
Serveur Web Apache sur lequel SSL est activé	8080 (configurable)	4343 (configurable)

Serveur Web et paramètres	Ports	
	HTTP	HTTPS (SSL)
Site Web par défaut IIS sur lequel SSL est activé	80 (non configurable)	443 (non configurable)
Site Web virtuel IIS sur lequel SSL est activé	8080 (configurable)	4343 (configurable)

Identification du serveur

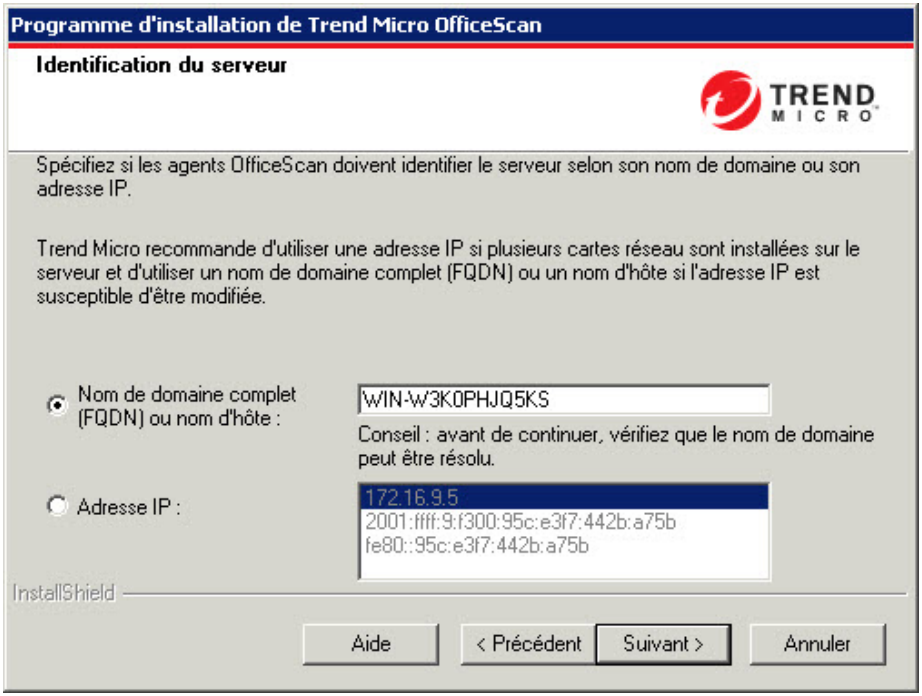

Figure 3-19. Écran Identification du serveur

L'option sélectionnée sur cet écran s'applique uniquement lors d'une nouvelle installation à distance.

Indiquez si les agents OfficeScan doivent identifier le serveur selon son nom de domaine complet (FQDN), nom d'hôte (domaine) ou adresse IP.

La communication entre le serveur et les agents dépend de l'adresse IP spécifiée. Une modification de l'adresse IP peut entraîner un problème de communication entre les agents et le serveur OfficeScan. Le seul moyen de rétablir la communication est de redéployer tous les agents. Cela vaut aussi lorsque le serveur est identifié au moyen d'un nom d'hôte et que celui-ci est modifié.

Pour la plupart des réseaux, l'adresse IP de l'ordinateur du serveur est davantage susceptible d'être modifiée que son nom d'hôte. Il est donc préférable d'identifier l'ordinateur serveur en fonction du nom d'hôte.

Conseil

Pour les administrateurs qui utilisent une adresse IP plutôt qu'un nom d'hôte, Trend Micro recommande de ne pas modifier l'adresse IP (obtenue du serveur DHCP) après l'installation. Les administrateurs peuvent éviter d'autres problèmes de communication avec les agents OfficeScan en configurant l'adresse IP sur Statique (sur le serveur DHCP) en utilisant la même adresse IP obtenue du serveur DHCP.

Une autre manière de préserver la configuration de l'adresse IP est de conserver l'adresse IP pour le serveur OfficeScan uniquement. Le serveur DHCP attribue ainsi obligatoirement la même adresse IP à OfficeScan, même lorsque DHCP est activé.

Si vous utilisez des adresses IP statiques, identifiez le serveur au moyen de son adresse IP. En outre, si l'ordinateur du serveur dispose de plusieurs cartes d'interface réseau (NIC), il est recommandé d'utiliser l'une des adresses IP plutôt que le nom d'hôte afin de garantir le bon fonctionnement de la communication agent-serveur.

Prise en charge d'IPv6

Si le serveur gère des agents IPv4 et IPv6, il doit contenir les adresses IPv4 et IPv6 et les administrateurs doivent l'identifier par son nom d'hôte. Si les administrateurs identifient le serveur par son adresse IPv4, les agents IPv6 ne peuvent pas s'y connecter. Le même problème se pose lorsque des agents IPv4 purs se connectent à un serveur identifié par son adresse IPv6.

Si le serveur ne gère que des agents IPv6, la configuration minimale requise est une adresse IPv6. Le serveur peut être identifié par son nom d'hôte ou son adresse IPv6.

Lorsque les administrateurs identifient le serveur par son nom d'hôte, il est préférable d'utiliser le nom de domaine complet (FQDN). En effet, dans un environnement exclusivement IPv6, un serveur WINS ne peut pas convertir un nom d'hôte en une adresse IPv6 correspondante.

Remarque

Le nom de domaine complet ne peut être spécifié que lors de l'installation locale du serveur. Il n'y a pas de prise en charge du nom de domaine complet pour les installations à distance.

Enregistrement et activation

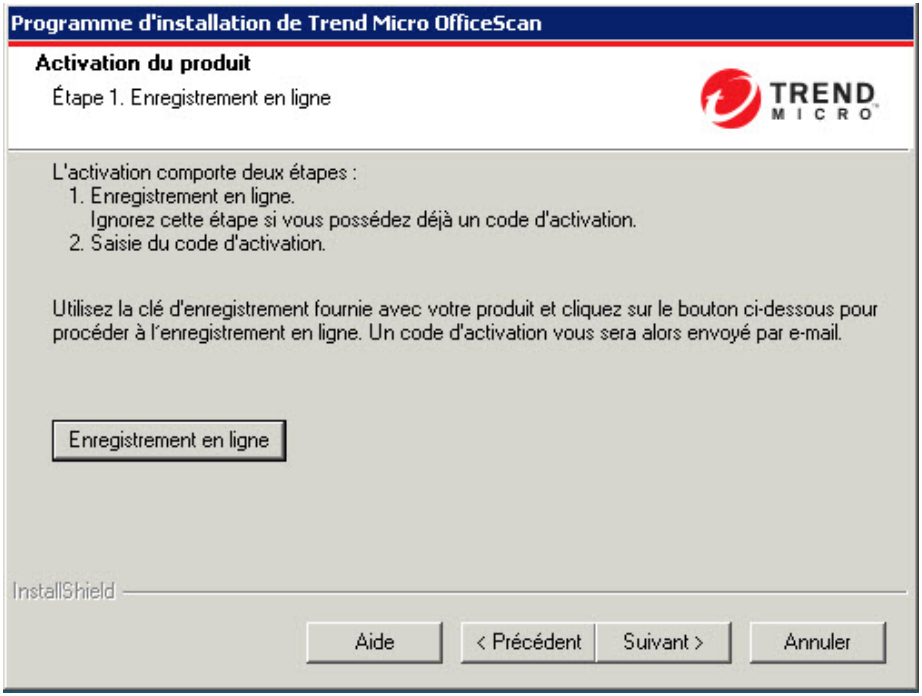

FIGURE 3-20. Activation du produit - Écran de l'étape 1

Enregistrez OfficeScan à l'aide de la clé d'enregistrement livrée avec le produit, puis munissez-vous des codes d'activation. Si les codes d'activation dont déjà disponibles, ignorez cette étape.

Pour obtenir les codes d'activation, cliquez sur **Enregistrement en ligne**. Le programme d'installation ouvre le site Web d'enregistrement de Trend Micro. Une fois le formulaire d'enregistrement rempli, Trend Micro envoie un e-mail contenant les codes d'activation. Lorsque vous recevez les codes, poursuivez le processus d'installation.

Lorsque vous installez le serveur OfficeScan sur un endpoint utilisant exclusivement le protocole IPv6, installez un serveur proxy double pile qui peut convertir les adresses IP. Cela permet au serveur de se connecter au site Web d'enregistrement de Trend Micro.

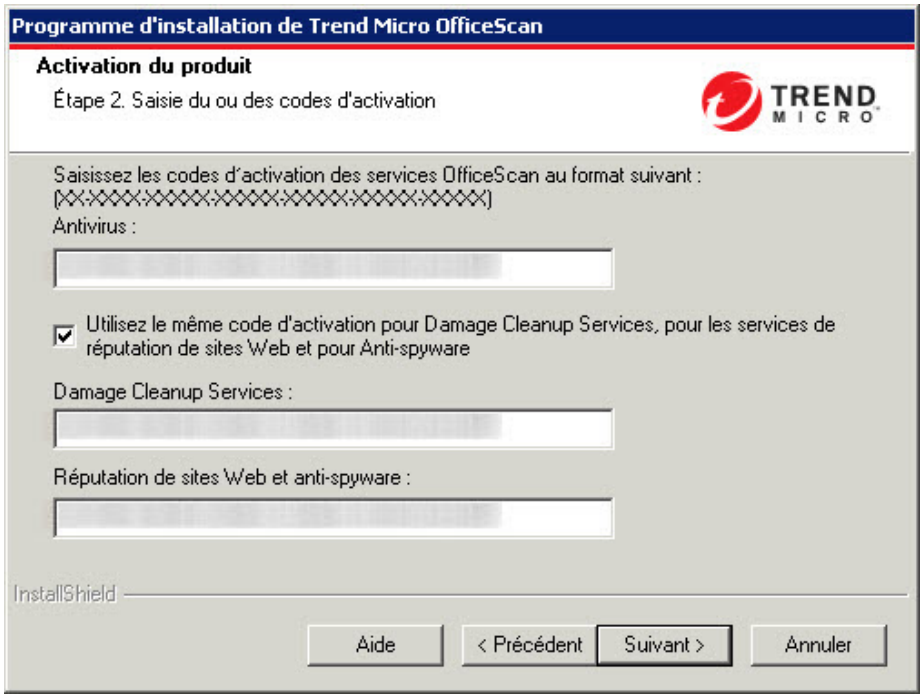

FIGURE 3-21. Activation du produit - Écran de l'étape 2

Indiquez les codes d'activation. Les codes d'activation sont sensibles à la casse.

Si le code d'activation est valide pour tous les services :

1. Entrez le code d'activation dans la zone de texte **Antivirus**.
2. Sélectionnez **Utilisez le même code d'activation pour Damage Cleanup Services, pour la réputation de sites Web et pour Anti-spyware**.
3. Cliquez sur **Suivant** et vérifiez les informations sur les licences.

Déploiement de l'agent OfficeScan

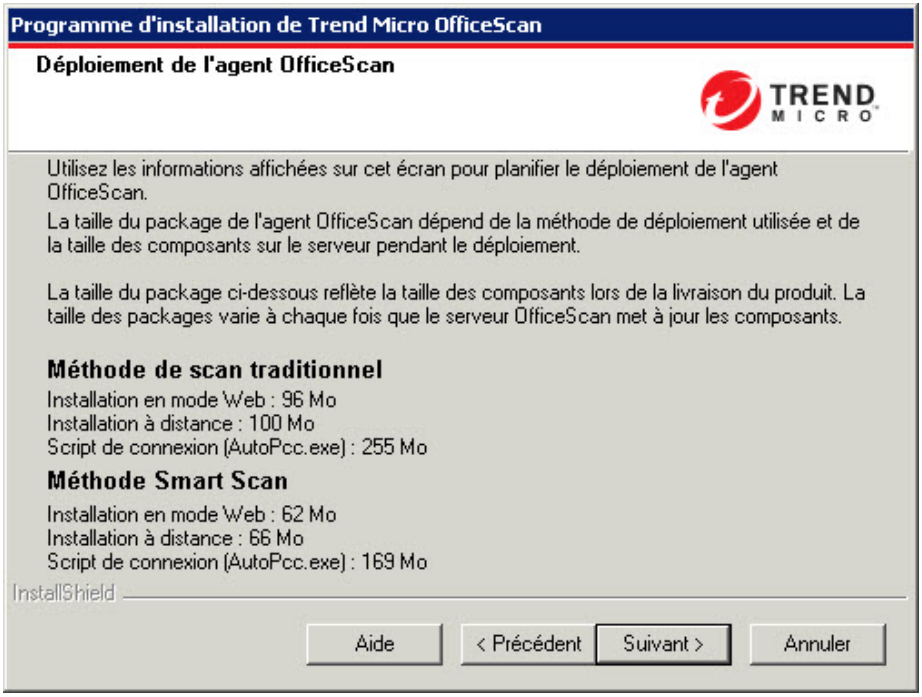

FIGURE 3-22. Écran Déploiement de l'agent OfficeScan

Différentes méthodes sont disponibles pour installer ou mettre à niveau les agents OfficeScan. Cet écran répertorie les différentes méthodes de déploiement et la bande passante du réseau approximative requise.

Cet écran permet d'estimer l'espace requis sur les serveurs et la bande passante consommée lors du déploiement des agents sur les endpoints cible.

Remarque

Toutes ces méthodes d'installation requièrent des droits d'administrateur local ou d'administrateur de domaine sur les endpoints cible.

Installer le serveur Smart Protection intégré

Remarque

Cet écran ne s'affiche pas lors de l'utilisation d'un site Web IIS virtuel pendant les installations de mises à niveaux locales.

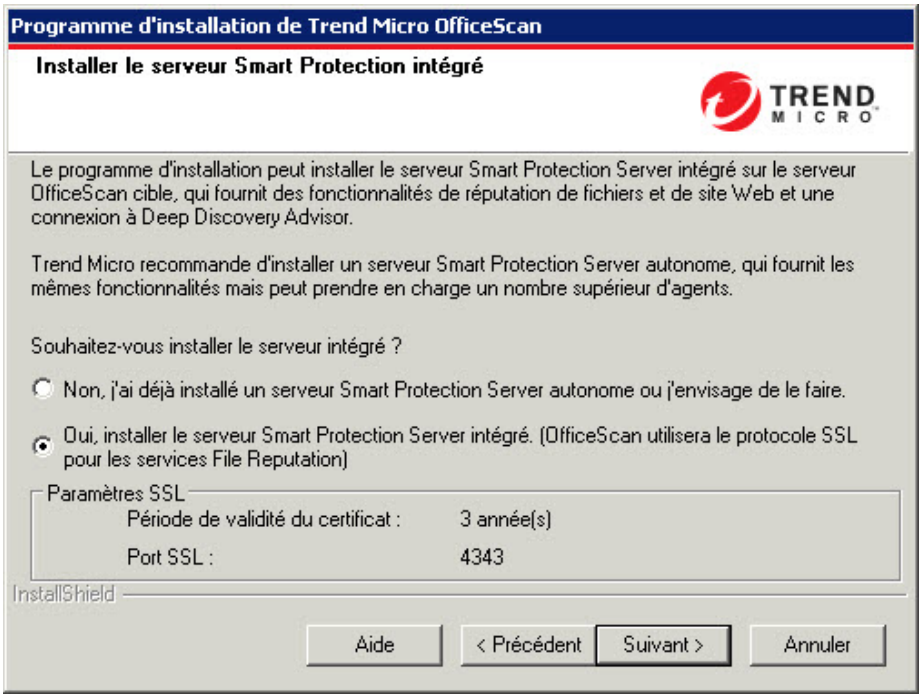

FIGURE 3-23. Écran d'installation du serveur Smart Protection Server intégré

Le programme d'installation peut installer le serveur Smart Protection Server intégré sur le endpoint cible. Le serveur intégré fournit les services de File Reputation aux agents qui utilisent Smart Scan et les services de réputation de sites Web aux agents soumis aux stratégies de réputation de sites Web. Gérez le serveur intégré à partir d'OfficeScan Web Console.

Trend Micro recommande d'installer le serveur Smart Protection Server autonome qui a les mêmes fonctions que le serveur intégré mais qui peut desservir davantage d'agents. Le serveur autonome est installé séparément et dispose de sa propre console de gestion. Consultez le *Manuel de l'administrateur Trend Micro Smart Protection Server* pour plus d'informations sur le serveur autonome.

Conseil

Du fait que le serveur Smart Protection Server intégré et le serveur OfficeScan s'exécutent sur le même endpoint, les performances de ce dernier peuvent être fortement réduites pendant les pointes de trafic des deux serveurs. Pour réduire le trafic dirigé vers l'ordinateur du serveur OfficeScan, affectez un serveur Smart Protection Server autonome comme source Smart Protection principale, et le serveur intégré comme source de secours. Consultez le *Manuel de l'administrateur* pour plus d'informations sur la configuration des sources Smart Protection pour les agents.

Protocoles de connexion des agents pour les services de File Reputation

Les agents OfficeScan peuvent se connecter aux services de File Reputation du serveur Smart Protection Server intégré à l'aide des protocoles HTTP et HTTPS. HTTPS permet une connexion plus sécurisée, tandis que HTTP utilise moins de bande passante.

Remarque

Si des agents se connectent au serveur intégré via un serveur proxy, vous devez configurer des paramètres proxy internes depuis la console Web. Consultez le *Manuel de l'administrateur* pour obtenir des informations sur la configuration des paramètres proxy.

Les numéros de port utilisés pour les services de File Reputation dépendent du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

Le port HTTP ne s'affiche pas sur l'écran d'installation. Le port HTTPS s'affiche mais la configuration est facultative.

TABLEAU 3-4. Ports pour les services de File Reputation du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORTS POUR LES SERVICES DE FILE REPUTATION	
	HTTP	HTTPS (SSL)
Serveur Web Apache	8082	4345
Site Web IIS par défaut	80	443

Serveur Web et paramètres	Ports pour les services de File Reputation	
	HTTP	HTTPS (SSL)
Site Web IIS virtuel	8080	4343

Serveur intégré non installé

Si vous effectuez une nouvelle installation et ne choisissez pas d'installer le serveur intégré :

- Le scan traditionnel devient la méthode de scan par défaut.
- Lorsque vous activez les stratégies de réputation de sites Web dans un écran d'installation différent (pour plus d'informations, voir *Fonction Réputation de sites Web à la page 2-43*), les agents ne peuvent pas envoyer de requêtes de réputation de sites Web car OfficeScan présume que le serveur Smart Protection Server n'est pas installé.

Si un serveur autonome est disponible après avoir installé OfficeScan, effectuez les tâches suivantes depuis OfficeScan Web Console :

- Changez la méthode de scan en Smart Scan.
- Ajoutez le serveur autonome à la liste des sources Smart Protection afin que les agents puissent lui envoyer des requêtes de File Reputation et de réputation de sites Web.

Lorsque vous effectuez une mise à niveau depuis des serveurs OfficeScan 10.x dans lesquels le serveur intégré a été désactivé, celui-ci n'est pas installé. Les agents OfficeScan conservent leur méthode de scan et les sources Smart Protection auxquelles ils envoient des requêtes.

Activer les services de réputation de sites Web

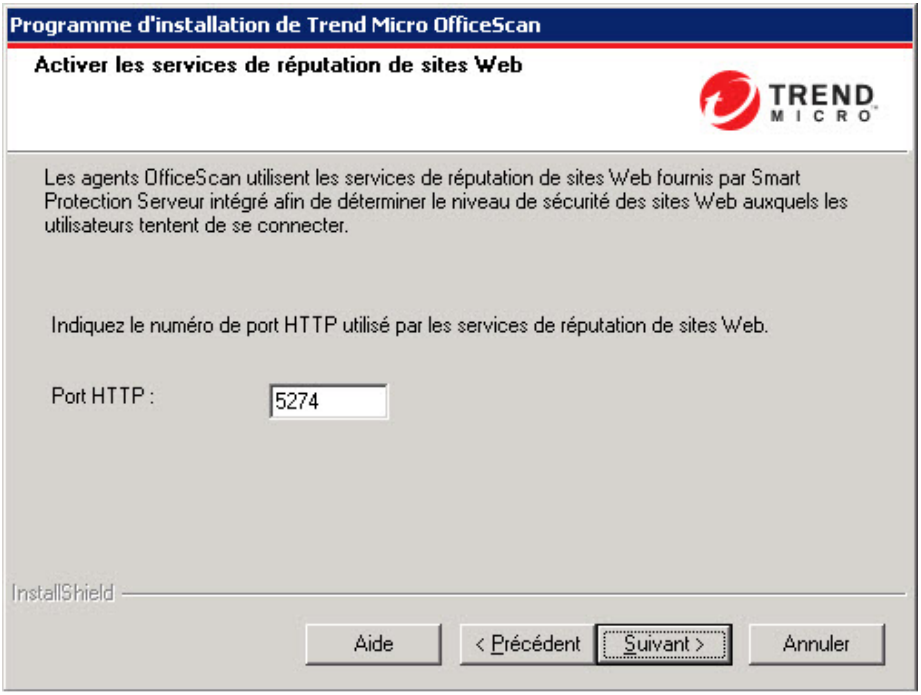

FIGURE 3-24. Activation de l'écran Services de réputation de sites Web

Les services de réputation de sites Web évaluent les risques de sécurité potentiels de toutes les URL demandées lors de l'exécution de chaque requête HTTP. Selon l'évaluation renvoyée par la base de données et le niveau de sécurité configuré, la réputation de sites Web bloque ou approuve la requête. Le serveur Smart Protection Server intégré, installé avec le serveur OfficeScan, fournit les services de réputation de sites Web.

L'activation des services de réputation de sites Web (fonctionnant sous le processus appelé `LWCSService.exe`) réduit la consommation globale de bande passante. En effet, les agents OfficeScan obtiennent les données de réputation de sites Web depuis un serveur local au lieu de se connecter à Smart Protection Network.

Protocoles de connexion des agents pour les services de réputation de sites Web

Les agents OfficeScan peuvent se connecter aux services de réputation de sites Web du serveur Smart Protection Server intégré à l'aide du protocole HTTP.

Le numéro de port HTTP utilisé pour les services de réputation de sites Web dépend du serveur Web (Apache ou IIS) utilisé par le serveur OfficeScan. Voir la *Serveur Web à la page 2-14* pour plus d'informations.

TABLEAU 3-5. Ports pour les services de réputation de sites Web du serveur Smart Protection Server intégré

SERVEUR WEB ET PARAMÈTRES	PORT HTTP POUR LES SERVICES DE RÉPUTATION DE SITES WEB
Serveur Web Apache sur lequel SSL est activé	5274
Site Web par défaut IIS sur lequel SSL est activé	80 (non configurable)
Site Web virtuel IIS sur lequel SSL est activé	8080 (non configurable)

Destination de l'installation

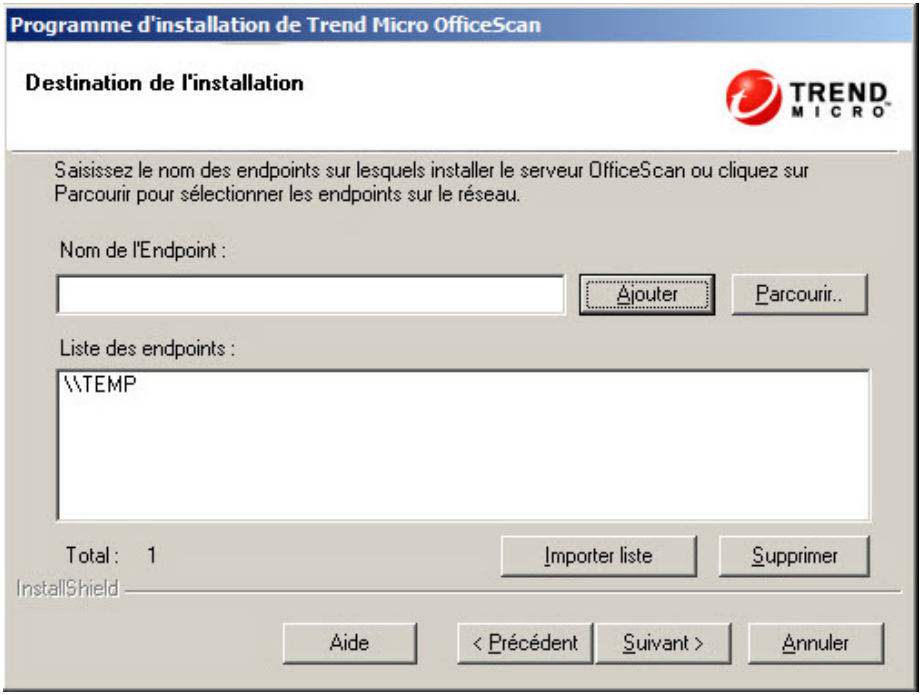

FIGURE 3-25. Écran Destination de l'installation

Spécifiez le endpoint cible sur lequel vous installerez OfficeScan. Entrez manuellement le nom d'hôte du endpoint ou son adresse IP. Cliquez sur **Parcourir** pour rechercher des endpoints sur le réseau.

Importez le(s) nom(s) de endpoint depuis un fichier texte en cliquant sur **Importer liste**. Lorsque vous procédez à une installation sur plusieurs endpoints simultanément et que tous les endpoints sont approuvés après l'analyse, le programme d'installation installe le serveur OfficeScan dans leur ordre d'apparition sur la liste du fichier texte.

Dans le fichier texte :

- Spécifiez un nom de endpoint par ligne.

- Utilisez le format de convention universelle de dénomination (Unified Naming Convention ou UNC), par exemple `\\test`.
- Utilisez uniquement les caractères suivants : a-z, A-Z, 0-9, points (.) et tirets (-).

Par exemple :

```
\\domain1\test-abc
```

```
\\domain2\test-123
```

Conseils pour vérifier si l'installation à distance peut être réalisée :

- Vous devez obtenir les droits d'administration de ce endpoint.
- Notez le nom d'hôte du endpoint et les informations d'identification de connexion (nom d'utilisateur et mot de passe).
- Vérifiez que les endpoints cible présentent la configuration système minimale requise en vue de l'installation du serveur OfficeScan.
- Assurez-vous que le endpoint soit équipé de Microsoft IIS Server 6,0 ou d'une version supérieure s'il est utilisé comme serveur Web. Si vous choisissez d'utiliser le serveur Web Apache, le programme d'installation installe automatiquement ce serveur s'il n'est pas déjà présent sur le endpoint cible.
- Ne définissez pas le endpoint sur lequel vous avez lancé le programme d'installation comme endpoint cible. Lancez plutôt une installation locale sur le endpoint.

Une fois les endpoints cible définis, cliquez sur **Suivant**. Le programme d'installation vérifie que les endpoints sont équipés de la configuration minimale requise pour OfficeScan.

Analyse du endpoint cible

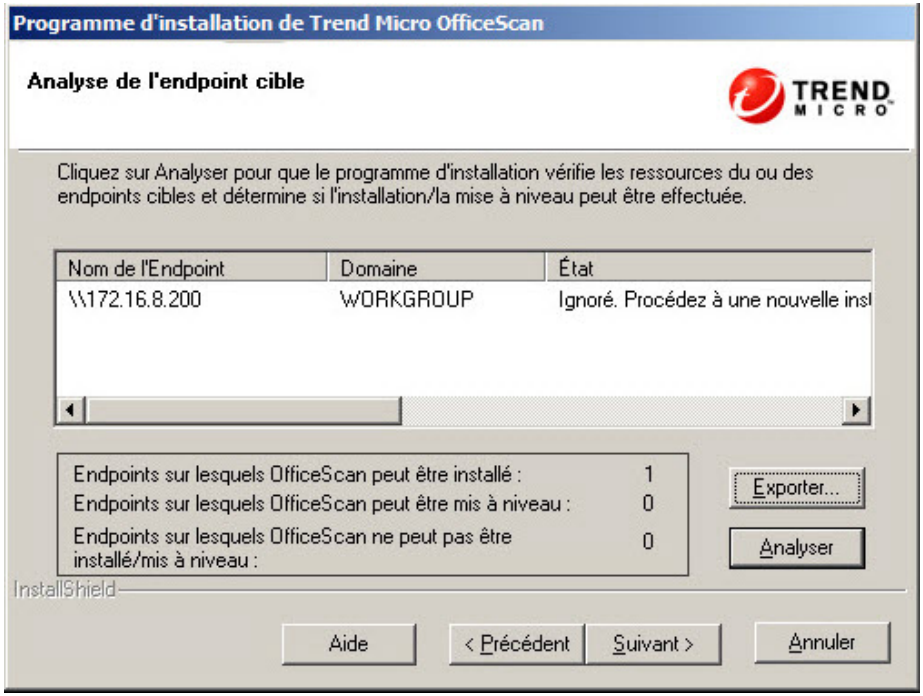

FIGURE 3-26. Écran Analyse du endpoint cible

Avant de lancer l'installation à distance, le programme d'installation doit d'abord déterminer si les endpoints cible sélectionnés peuvent installer le serveur OfficeScan. Pour démarrer l'analyse, cliquez sur **Analyser**. Le programme d'installation peut vous demander le nom d'utilisateur et le mot de passe de l'administrateur utilisés pour se connecter au endpoint cible. Après l'analyse, le programme d'installation affiche les résultats à l'écran.

Lorsque vous procédez à une installation sur plusieurs endpoints, l'installation démarrera si au moins un endpoint est approuvé après l'analyse. Le programme d'installation installe le serveur OfficeScan sur ce endpoint et ignore les endpoints refusés après l'analyse.

Pendant l'installation à distance, la progression de l'installation s'affiche uniquement sur endpoint sur lequel le programme d'installation a été lancé et pas sur les endpoints cible.

Alerte de redémarrage de l'agent OfficeScan

Le programme d'installation évalue les ressources sur le endpoint cible. Pendant les scénarios de mise à niveau, un écran d'avertissement apparaît si le programme de l'agent OfficeScan existe sur le endpoint cible.

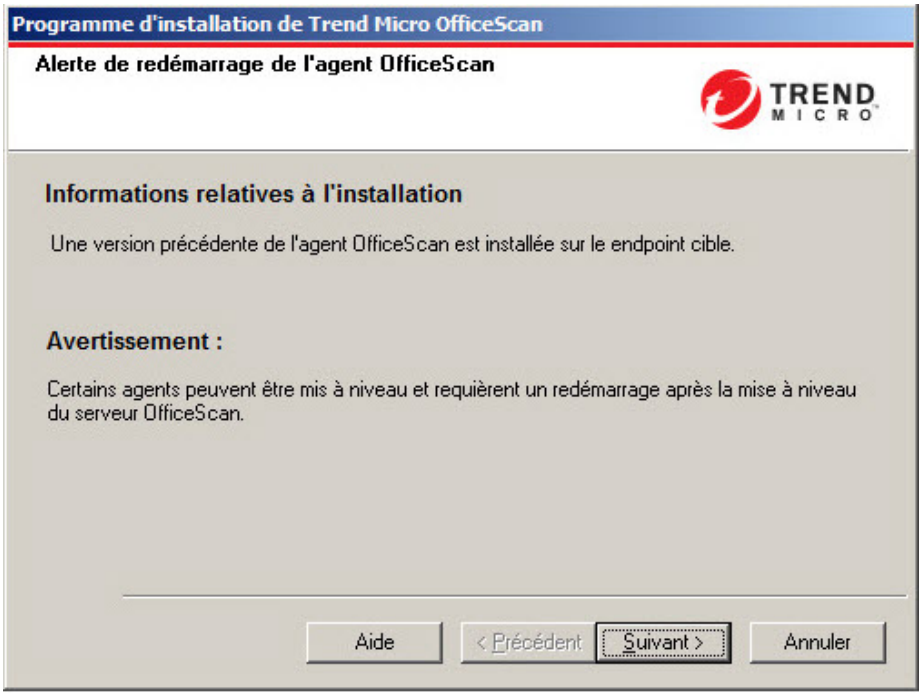

FIGURE 3-27. Alerte de redémarrage de l'agent OfficeScan

Sauvegarde de la base de données

Pendant les mises à niveau, le programme d'installation offre une option de sauvegarde de la base de données OfficeScan avant de passer à la dernière version. Vous pouvez utiliser ces informations de sauvegarde à des fins de restauration.

Remarque

Le pack de sauvegarde peut nécessiter plus de 300 Mo d'espace disque disponible.

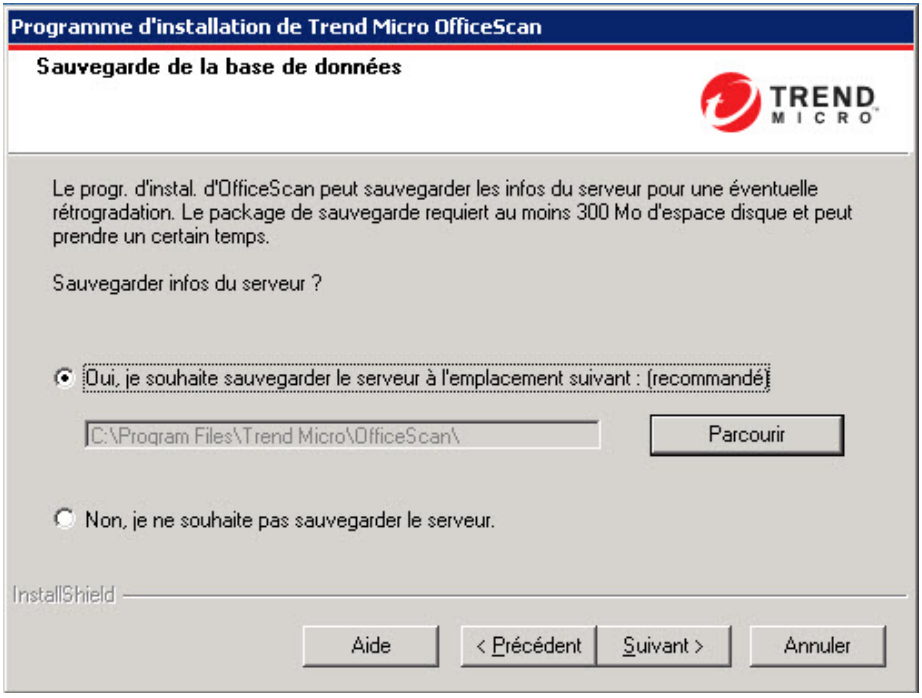

FIGURE 3-28. Écran Sauvegarde de la base de données

Certificat d'authentification serveur

Le programme d'installation tente de détecter la présence de certificats d'authentification existants pendant l'installation. Si un tel certificat existe, OfficeScan mappe

automatiquement le fichier sur l'écran **Certificat d'authentification serveur**. Si aucun certificat n'existe, OfficeScan applique par défaut l'option **Générer un certificat d'authentification**.

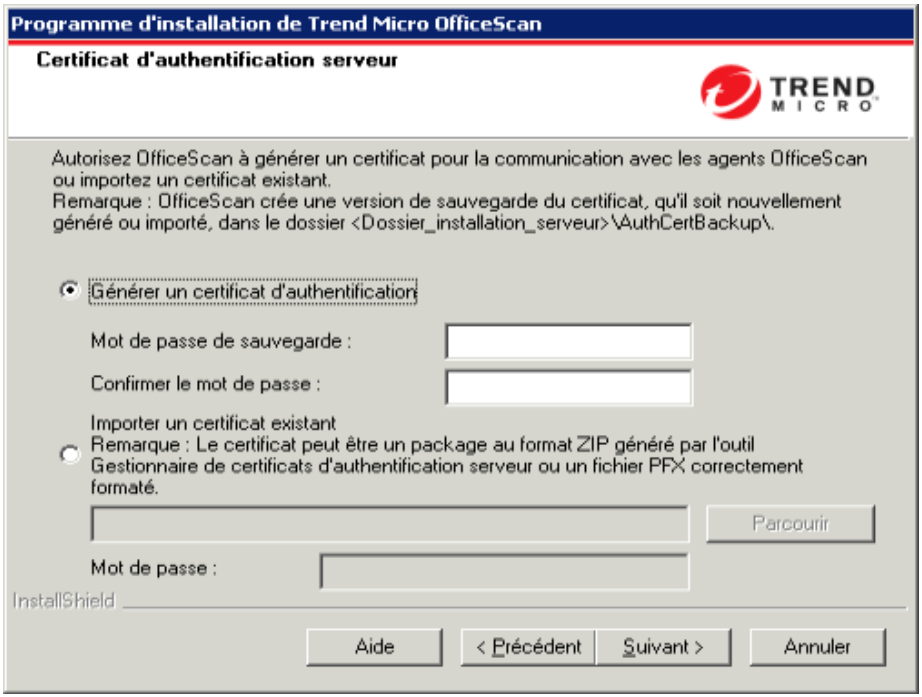

FIGURE 3-29. Écran Certificat d'authentification serveur pour les nouveaux certificats

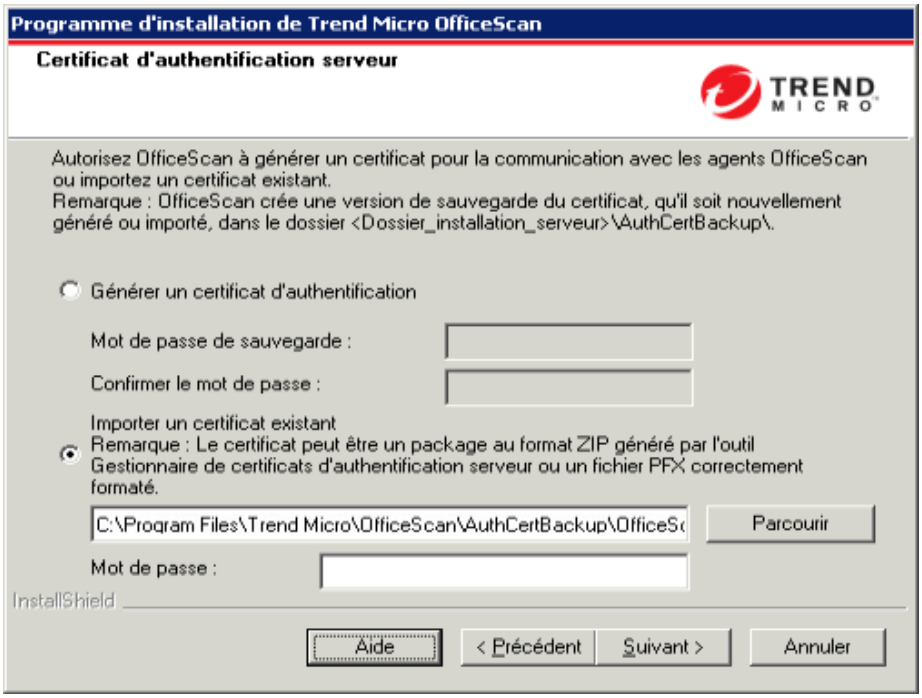

FIGURE 3-30. Écran Certificat d'authentification serveur pour les certificats existants

OfficeScan utilise le chiffrement à clé publique pour authentifier les communications du serveur OfficeScan vers les agents. Grâce à cette technologie, le serveur conserve une clé privée et déploie une clé publique sur tous les agents. Les agents utilisent la clé publique pour vérifier que les communications entrantes proviennent bien du serveur et sont valides. Les agents répondent au serveur si cette vérification réussit.

Remarque

OfficeScan n'authentifie pas les communications vers le serveur provenant des agents.

OfficeScan peut générer le certificat d'authentification pendant l'installation ou les administrateurs peuvent importer un certificat d'authentification préexistant depuis un autre serveur OfficeScan.

Conseil

Lors de la sauvegarde du certificat, Trend Micro recommande le chiffrement du certificat à l'aide d'un mot de passe.

Informations sur l'installation

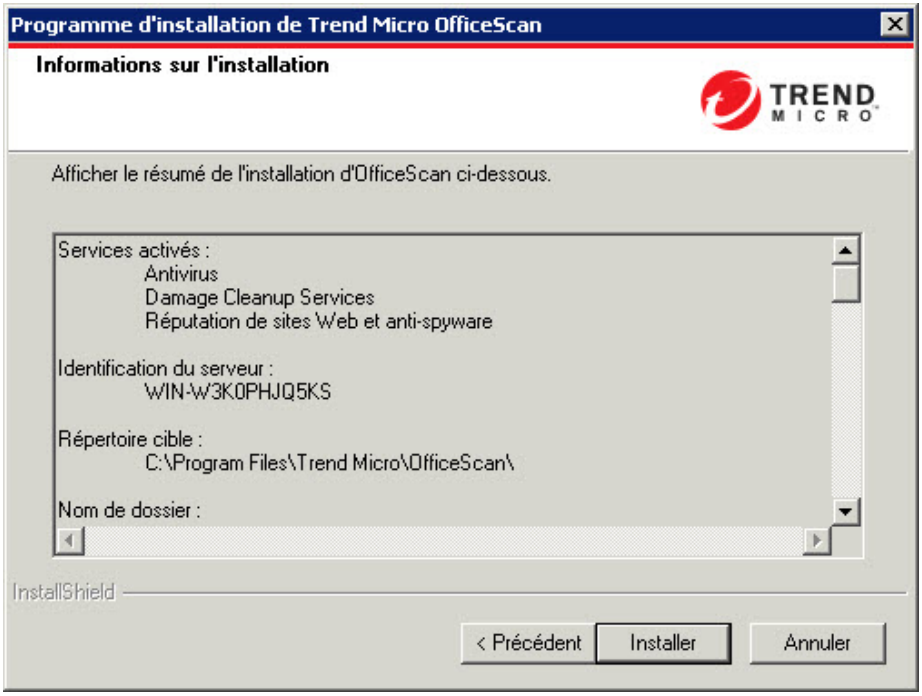

FIGURE 3-31. Écran Informations sur l'installation

Cet écran contient un récapitulatif des paramètres d'installation. Vérifiez les informations relatives à l'installation et cliquez sur **Précédent** pour modifier les paramètres ou les options, le cas échéant. Pour lancer l'installation, cliquez sur **Installer**.

Assistant InstallShield terminé

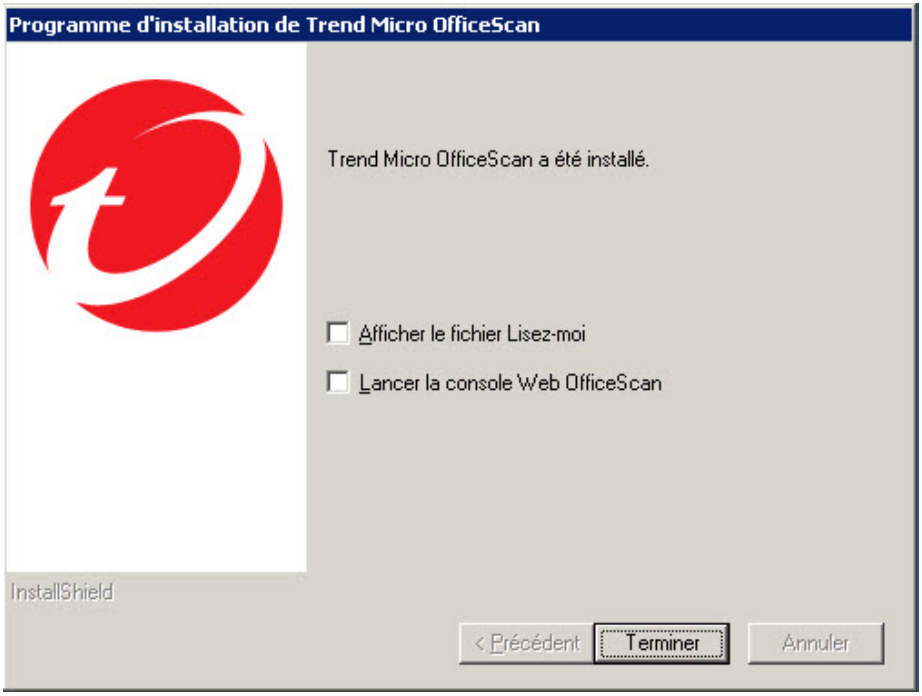

FIGURE 3-32. Écran indiquant que l'Assistant InstallShield est terminé

Une fois l'installation terminée, lisez le fichier Lisez-moi pour prendre connaissance des informations de base relatives au produit et aux problèmes connus.

Les administrateurs peuvent démarrer la console Web pour commencer à configurer les paramètres d'OfficeScan.

Chapitre 4

Tâches après l'installation

Effectuez les tâches suivantes une fois l'installation du serveur OfficeScan terminée.

Sujets abordés dans ce chapitre :

Vérification de l'installation ou de la mise à niveau du serveur

Une fois l'installation effectuée, vérifiez les éléments suivants :

TABLEAU 4-1. Éléments à vérifier après l'installation d'OfficeScan

ÉLÉMENT À VÉRIFIER	DÉTAILS
Raccourcis du serveur OfficeScan	Les raccourcis du serveur Trend Micro OfficeScan apparaissent dans le menu **Démarrer** de Windows sur l'ordinateur serveur.
Liste des programmes	Trend Micro OfficeScan Server est répertorié dans la liste **Ajout/Suppression de programmes** du Panneau de configuration du serveur.
OfficeScan web console	Saisissez les URL suivantes dans le navigateur Internet Explorer : • Connexion HTTPS : `https://<nom du serveur OfficeScan>:<numéro de port>/OfficeScan` Où `<nom du serveur OfficeScan>` est le nom ou l'adresse IP du serveur OfficeScan. L'écran de connexion à la console Web s'affiche.

Élément à vérifier	Détails
Services du serveur OfficeScan	Les services suivants du serveur OfficeScan s'affichent dans Microsoft Management Console : • Service d'intégration d'Active Directory OfficeScan : ce service s'affiche si les fonctionnalités d'intégration Active Directory et Role-based Administration fonctionnent correctement. • Agent Control Manager d'OfficeScan : l'état de ce service doit être « Démarré » si le serveur OfficeScan a été enregistré auprès de Control Manager. • Service principal d'OfficeScan : l'état de ce service doit être « Démarré ». • OfficeScan Plug-in Manager l'état de ce service doit être « Démarré ». • Trend Micro Smart Scan Server : l'état de ce service doit être « Démarré ». • Trend Micro Local Web Classification Server : l'état de ce service doit être « Démarré » si les services de réputation de sites Web ont été activés pendant l'installation.
Processus du serveur OfficeScan	Lorsque vous ouvrez le Gestionnaire de tâches Windows, DBServer.exe s'exécute.
Journal d'installation du serveur	Le journal d'installation du serveur, OFCMAS.LOG, se trouve dans `%windir%`.

Clés de registre	Les clés de registre suivantes existent :
	• Pour les plates-formes 32 bits :
	`HKEY_LOCAL_MACHINE\Software\TrendMicro\OfficeScan`
	• Pour les plates-formes 64 bits :
	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\TrendMicro\OfficeScan`

Dossier du programme	Les fichiers du serveur OfficeScan se trouvent dans le `<dossier d'installation du serveur>`.

Vérification de l'installation du serveur Smart Protection Server intégré

OfficeScan installe automatiquement le serveur Smart Protection Server intégré lors d'une nouvelle installation.

Procédure

1. Dans la console Web du serveur, accédez à **Administration** > **Smart Protection** > **Sources Smart Protection**.
2. Cliquez sur le lien **Liste standard**.
3. Dans l'écran qui s'affiche, cliquez sur **Serveur Smart Protection Server intégré**.
4. Dans l'écran qui s'affiche, cliquez sur **Tester la connexion**.

   La connexion au serveur intégré devrait réussir.

Mise à jour des composants OfficeScan

Après avoir installé OfficeScan, mettez à jour les composants sur le serveur.

Remarque

Cette section explique comment effectuer une mise à jour manuelle. Pour plus d'informations sur la mise à jour programmée et les configurations de mise à jour, consultez l'*aide du serveur OfficeScan*.

Mise à jour du serveur OfficeScan

Procédure

1. Connectez-vous à la console Web.
2. Dans le menu principal, cliquez sur **Mises à jour** > **Serveur** > **Mise à jour manuelle**.

L'écran **Mise à jour manuelle** qui s'affiche présente les composants actuels, leur numéro de version, ainsi que les dates des mises à jour les plus récentes.

3. Sélectionnez les composants à mettre à jour.

4. Cliquez sur **Mettre à jour**. Le serveur vérifie la présence de composants mis à jour sur le serveur de mise à jour. La progression et l'état de la mise à jour s'affichent.

Vérification des paramètres par défaut

OfficeScan s'installe avec les paramètres par défaut. Si ces paramètres ne correspondent pas à vos exigences en matière de sécurité, modifiez-les dans la console Web. Reportez-vous à l'*aide du serveur OfficeScan* et au *Manuel de l'administrateur* pour plus de détails sur les paramètres disponibles sur la console Web.

Paramètres de scan

OfficeScan propose différents types de scan pour protéger les endpoints contre les risques de sécurité. Modifiez les paramètres de scan depuis la console Web en accédant à **Agents** > **Gestion des agents** et en cliquant sur **Paramètres** > **{Type de scan}**.

Paramètres des agents

OfficeScan fournit différents types de paramètres qui s'appliquent à tous les agents enregistrés sur le serveur ou à tous les agents disposant d'un privilège donné. Modifiez les paramètres de l'agent depuis la console Web en accédant à **Agents** > **Paramètres généraux de l'agent**.

Privilèges de l'agent

Les privilèges par défaut de l'agent comprennent l'affichage de l'icône de la barre d'état système sur le endpoint de l'agent OfficeScan. Modifiez les privilèges par défaut de l'agent à partir de la console Web.

1. Accédez à **Agents** > **Gestion des agents**.

2. Cliquez sur **Paramètres** > **Privilèges et autres paramètres**.

Enregistrement d'OfficeScan sur Control Manager

Lorsqu'un serveur Control Manager gère les serveurs OfficeScan nouvellement installés, enregistrez OfficeScan sur Control Manager après l'installation.

Remarque

l'enregistrement sur Control Manager ne s'applique qu'à des serveurs OfficeScan nouvellement installés.

Dans OfficeScan Web Console, accédez à **Administration** > **Paramètres** > **Control Manager**.

Consultez l'*aide du serveur OfficeScan* ou le *Manuel de l'administrateur OfficeScan* pour connaître la procédure à suivre.

Chapitre 5

Désinstallation et rétrogradation d'OfficeScan

Ce chapitre décrit la procédure à suivre pour désinstaller ou rétrograder Trend Micro™ OfficeScan™.

Sujets abordés dans ce chapitre :

Remarques sur la désinstallation et la rétrogradation

En cas de problème avec OfficeScan, procédez comme suit :

- Utiliser le programme de désinstallation pour supprimer en toute sécurité le serveur OfficeScan du endpoint. Avant de désinstaller le serveur, déplacez les agents qu'il gère vers un autre serveur OfficeScan.
- Rétrogradez les agents vers une version précédente d'OfficeScan au lieu de désinstaller le serveur OfficeScan. Voir la section *Rétrogradation du serveur et des agents OfficeScan à l'aide du pack de sauvegarde du serveur à la page 5-9*.

Avant de désinstaller le serveur OfficeScan

Utilisez le programme de désinstallation pour supprimer en toute sécurité le serveur OfficeScan.

Avant de désinstaller le serveur, déplacez les agents qu'il gère vers un autre serveur OfficeScan disposant de la même version. Envisagez de sauvegarder la base de données du serveur et les fichiers de configuration afin de réinstaller le serveur par la suite.

Déplacement des agents vers un autre serveur OfficeScan

OfficeScan Web Console dispose d'une option permettant de déplacer les agents gérés par le serveur vers un autre serveur OfficeScan.

Procédure

1. Notez les informations suivantes pour l'autre serveur OfficeScan. Elles sont requises lors du déplacement des agents.
   - Nom ou adresse IP du endpoint
   - Port d'écoute du serveur

Pour afficher le port d'écoute du serveur, accédez à **Administration** > **Paramètres** > **Connexion à l'agent**. Le numéro de port s'affiche à l'écran.

2. Sur la console Web du serveur que vous souhaitez désinstaller, accédez à **Agents** > **Gestion des agents**.
3. Dans l'arborescence des agents, sélectionnez les agents que vous souhaitez mettre à niveau, puis cliquez sur **Gérer l'arborescence des agents** > **Déplacer un agent**.
4. Sous **Déplacer le(s) agent(s) sélectionné(s) vers un autre serveur OfficeScan**, spécifiez le nom/l'adresse IP de l'ordinateur serveur ainsi que le port d'écoute de l'autre serveur OfficeScan.
5. Cliquez sur **Déplacer**.

Si tous les agents ont été déplacés et sont désormais gérés par l'autre serveur OfficeScan, vous pouvez désinstaller le serveur OfficeScan en toute sécurité.

Sauvegarde et restauration de la base de données et des fichiers de configuration OfficeScan

Sauvegardez la base de données OfficeScan et les fichiers de configuration importants avant de désinstaller le serveur OfficeScan. Sauvegardez la base de donnés du serveur OfficeScan à un emplacement situé à l'extérieur du répertoire du programme OfficeScan.

Procédure

1. Sauvegardez la base de données à partir de la console Web, en accédant à **Administration** > **Paramètres** > **Sauvegarde de la base de données**. Consultez le *Manuel de l'administrateur OfficeScan* ou l'*aide du serveur OfficeScan* pour connaître la procédure à suivre.

   AVERTISSEMENT!

   N'utilisez aucun autre type d'outil ou d'application de sauvegarde.

   ---

2. Arrêtez le service principal d'OfficeScan à partir de Microsoft Management Console.

3. Sauvegardez manuellement les fichiers et dossiers suivants figurant dans le répertoire `<dossier d'installation du serveur>\PCCSRV>` :

   - `ofcscan.ini`: contient les paramètres de l'agent général
   - `ous.ini`: contient la table source de mise à jour pour le déploiement des composants antivirus
   - Dossier privé : contient les paramètres du pare-feu et de la source de mise à jour
   - `Dossier Web\tmOPP` : contient les paramètres de prévention des épidémies
   - `Pccnt\Common\OfcPfw*.dat`: contient les paramètres du pare-feu
   - `Download\OfcPfw.dat`: contient les paramètres de déploiement du pare-feu
   - Dossier Log : contient les événements système et les journaux de vérification de la connexion
   - Dossier Virus : contient les fichiers mis en quarantaine
   - Dossier HTTPDB : contient la base de données OfficeScan

4. Désinstallez le serveur OfficeScan. Pour obtenir des informations détaillées, consultez la section *Désinstallation du serveur OfficeScan à la page 5-5*.

5. Effectuez une nouvelle installation. Voir *Exécution d'une nouvelle installation du serveur OfficeScan à la page 2-2* pour obtenir des informations détaillées.

6. Une fois l'installation terminée, ouvrez Microsoft Management Console (`services.msc`).

7. Cliquez avec le bouton droit sur **Service principal d'OfficeScan**, puis cliquez sur **Arrêter**.

8. Copiez les fichiers de sauvegarde dans le répertoire `<dossier d'installation du serveur>\PCCSRV` du endpoint cible. Cette opération remplace la base de données du serveur OfficeScan ainsi que les fichiers et dossiers appropriés.

9. Redémarrez le service principal d'OfficeScan.

Désinstallation du serveur OfficeScan

Utilisez le programme de désinstallation pour désinstaller le serveur OfficeScan ainsi que le serveur Smart Protection Server intégré.

Si vous rencontrez des problèmes avec le programme de désinstallation, désinstallez manuellement le serveur.

Remarque

Pour connaître la procédure de désinstallation de l'agent OfficeScan, consultez le Manuel de l'administrateur.

Désinstallation du serveur OfficeScan à l'aide du programme de désinstallation

Procédure

1. Lancez le programme de désinstallation. Il existe deux moyens d'accéder au programme de désinstallation.

   - Méthode A

   a. Sur le endpoint du serveur OfficeScan, cliquez sur **Démarrer** > **Programmes** > **Trend Micro OfficeScan Server** > **Désinstaller OfficeScan**. Un écran de confirmation s'affiche.

   b. Cliquez sur **Oui**. Le programme de désinstallation du serveur vous invite à saisir le mot de passe de l'administrateur.

   c. Saisissez le mot de passe de l'administrateur et cliquez sur **OK**. Le programme de désinstallation du serveur commence à supprimer les fichiers du serveur. Un message de confirmation s'affiche.

   d. Cliquez sur **OK** pour fermer le programme de désinstallation.

- Méthode B

a. Double-cliquez sur le programme du serveur OfficeScan dans l'écran **Ajout/Suppression de programmes de Windows**.

b. Cliquez sur **Panneau de configuration** > **Ajout/Suppression de programmes**. Localisez «Trend Micro OfficeScan Server» et double-cliquez dessus. Suivez les instructions à l'écran jusqu'à ce que vous soyez invité à saisir le mot de passe d'administrateur.

c. Saisissez le mot de passe de l'administrateur et cliquez sur **OK**. Le programme de désinstallation du serveur commence à supprimer les fichiers du serveur. Un message de confirmation s'affiche.

d. Cliquez sur **OK** pour fermer le programme de désinstallation.

Désinstallation manuelle du serveur OfficeScan

Première partie : Désinstallation du serveur Smart Protection Server intégré

Procédure

1. Ouvrez Microsoft Management Console et arrêtez le service principal d'OfficeScan.
2. Ouvrez une invite de commande et accédez au `<dossier d'installation du serveur>\PCCSRV`.
3. Exécutez la commande suivante:

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   Cette commande désinstalle les services liés à OfficeScan, mais ne supprime pas les fichiers de configuration ou la base de données OfficeScan.
4. Accédez au `<dossier d'installation du serveur>\PCCSRV\private` et ouvrez `ofcserver.ini`.

5. Modifiez les paramètres suivants:

TABLEAU 5-1. Paramètres d'ofcserver.ini

PARAMÈTRE	INSTRUCTION
`WSS_INSTALL`	Changez 1 en 0
`WSS_ENABLE=1`	Supprimez cette ligne
`WSS_URL=https://<computer_name>:4345/tmcss/`	Supprimez cette ligne

6. Accédez au `<dossier d'installation du serveur>\PCCSRV` et ouvrez `OfUninst.ini`. Supprimez les lignes suivantes:

- Si vous utilisez un serveur Web IIS:

```
[WSS_WEB_SERVER]

ServerPort=8082

IIS_VhostName=Smart Protection Server (intégré)

IIS_VHostIdx=5
```

Remarque

La valeur pour `IIS_VHostidx` doit être identique à la valeur « isapi » indiquée sur la ligne suivante :

```
ROOT=/tmcss,C:\Program Files\Trend Micro\OfficeScan
\PCCSRV\WSS\isapi,,<valeur>
```

```
[WSS_SSL]

SSLPort=<port SSL>
```

- Si vous utilisez un serveur Web Apache:

```
[WSS_WEB_SERVER]

ServerPort=8082

[WSS_SSL]
```

```
SSLPort=<port SSL>
```

7. Ouvrez une invite de commande et accédez au <dossier d'installation du serveur>\PCCSRV.

8. Exécutez les commandes suivantes:

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. Vérifiez si les éléments suivants ont été supprimés:

   - service Trend Micro Smart Protection Server à partir de Microsoft Management Console
   - Compteurs de performances de Smart Protection Server
   - Site Web du serveur Smart Protection Server (intégré)

Deuxième partie : Désinstallation du serveur OfficeScan

Procédure

1. Ouvrez l'Éditeur du Registre et suivez cette procédure:

   AVERTISSEMENT!

   Cette procédure implique la suppression des 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.

   a. Accédez à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`.

   b. Vérifiez que la ruche `ofcservice` a été supprimée.

c. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\` et supprimez la ruche `OfficeScan`.

   Pour les endpoints 64 bits, le chemin est `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\`.

d. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\`. Supprimez le dossier `OfficeScan Management Console-<Nom du serveur>`.

2. Accédez au `<dossier d'installation du serveur>\PCCSRV` et arrêtez le partage du dossier `PCCSRV`.

3. Redémarrez l'ordinateur serveur.

4. Accédez au `<dossier d'installation du serveur>\PCCSRV` et supprimez le dossier `PCCSRV`.

5. Supprimez le site Web OfficeScan à partir de la console IIS (Internet Information Services).

   a. Ouvrez la console IIS.

   b. Développez `NomServeur`.

   c. Si vous avez installé OfficeScan sur un site Web distinct, accédez au dossier `Sites Web` et supprimez OfficeScan.

   d. Si vous avez installé des répertoires virtuels par défaut sous le site Web par défaut, accédez à `Site Web par défaut` et supprimez le répertoire virtuel OfficeScan.

Rétrogradation du serveur et des agents OfficeScan à l'aide du pack de sauvegarde du serveur

La procédure de rétrogradation d'OfficeScan implique dans un premier temps la rétrogradation des agents OfficeScan, puis celle du serveur OfficeScan dans un second.

Important

- Les administrateurs ne peuvent procéder à la rétrogradation du serveur et des agents OfficeScan à l'aide de la procédure suivante que si l'administrateur en charge du processus d'installation a choisi de sauvegarder le serveur. Si aucun fichier de sauvegarde du serveur n'est disponible, consultez les procédures manuelles de rétrogradation dans le *Guide d'installation et de mise à niveau* pour la version précédemment installée d'OfficeScan.
- Cette version d'OfficeScan prend uniquement en charge la rétrogradation à partir des versions suivantes :
  - OfficeScan 10.6 Service Pack 3
  - OfficeScan 10.6 Service Pack 2
  - OfficeScan 10.6 Service Pack 1
  - OfficeScan 10.6
  - OfficeScan 10.5
  - OfficeScan 10.0 SP1

Rétrogradation des agents OfficeScan

OfficeScan ne peut rétrograder des agents OfficeScan que vers la version du serveur subissant une restauration. Il est impossible de rétrograder des agents OfficeScan vers une version antérieure à celle du serveur.

Important

Assurez-vous de rétrograder les agents OfficeScan avant de procéder à la rétrogradation du serveur OfficeScan.

Procédure

1. Assurez-vous que les agents OfficeScan peuvent procéder à la mise à niveau de leur programme.
   a. Sur la console Web OfficeScan 11.0, accédez à **Agents** > **Gestion des agents**.

b. Sélectionnez les agents OfficeScan à rétrograder.

c. Cliquez sur l'onglet **Paramètres** > **Privilèges et autres paramètres** > **Autres paramètres**.

d. Sélectionnez **Les agents OfficeScan peuvent mettre à jour les composants, mais ne peuvent pas mettre à niveau le programme de l'agent, ni déployer des correctifs de type hot fix**.

2. Sur la console Web OfficeScan 11.0, accédez à **Mises à jour** > **Agents** > **Source de mise à jour**.

3. Sélectionnez **Source de mise à jour personnalisée**.

4. Dans la liste **Liste des sources de mise à jour personnalisée**, cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

5. Saisissez les adresses IP des agents OfficeScan à rétrograder.

6. Entrez l'URL de la source de mise à jour.

   Par exemple, entrez :

   ```
   http://<adresse IP du serveur OfficeScan>:<port>/
   OfficeScan/download/Rollback
   ```

7. Cliquez sur **Enregistrer**.

8. Cliquez sur **Notifier tous les agents**.

   Lorsque l'agent OfficeScan devant être rétrogradé se met à jour à partir de la source de mise à jour, il est désinstallé et la version précédente de l'agent est installée.

9. Une fois la version précédente de l'agent OfficeScan installée, informez l'utilisateur qu'il doit redémarrer l'ordinateur.

   Une fois le processus de rétrogradation effectué, l'agent OfficeScan continue à dépendre du même serveur OfficeScan.

Remarque

Une fois la rétrogradation de l'agent OfficeScan effectuée, tous les composants, y compris le fichier de signatures de virus, subissent également une rétrogradation vers leur version précédente. Si les administrateurs n'effectuent pas la rétrogradation du serveur OfficeScan, l'agent OfficeScan ayant subi une rétrogradation ne peut pas mettre à jour ses composants. Les administrateurs doivent rétablir la source de mise à jour standard sur l'agent OfficeScan ayant subi une rétrogradation afin de rendre possible la mise à jour des composants.

Restauration de la version précédente du serveur OfficeScan

La procédure de restauration du serveur OfficeScan nécessite que l'administrateur désinstalle le serveur OfficeScan 11.0, réinstalle la version précédente, arrête manuellement les services Windows, mette à jour le Registre système et remplace les fichiers du serveur OfficeScan dans le répertoire d'installation d'OfficeScan.

Important

Assurez-vous de rétrograder les agents OfficeScan avant de procéder à la restauration du serveur OfficeScan.

Procédure

1. Désinstallez OfficeScan 11.0.

   Pour obtenir des informations détaillées, consultez la section *Désinstallation du serveur OfficeScan à la page 5-5*.

2. Installez la version précédente du serveur OfficeScan.

Conseil

Trend Micro recommande de ne pas changer le nom d'hôte ou l'adresse IP lors de la restauration du serveur.

Pour vérifier la version précédente du serveur, accédez au `<dossier_installation_serveur>` et affichez le dossier de restauration créé lors de l'installation du serveur OfficeScan 11.0. Le nom du dossier (désigné par >version_dossier_restauration>) est l'un des suivants :

- OSCE106_SP3 : OfficeScan 10.6 Service Pack 3
- OSCE106_SP2 : OfficeScan 10.6 Service Pack 2
- OSCE106_SP1 : OfficeScan 10.6 Service Pack 1
- OSCE106 : OfficeScan 10.6
- OSCE105 : OfficeScan 10.5
- OSCE10_SP1 : OfficeScan 10.0 Service Pack 1

3. Sur l'ordinateur du serveur OfficeScan, arrêtez les services suivants :
   - Intrusion Defense Firewall (si installé)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - Service d'intégration d'Active Directory OfficeScan
   - Agent Control Manager d'OfficeScan
   - OfficeScan Plug-in Manager
   - Service principal d'OfficeScan
   - Apache 2 (si vous utilisez le serveur Web Apache)
   - World Wide Web Publishing Service (si vous utilisez le serveur Web IIS)
4. Copiez et remplacez tous les fichiers et dossiers du répertoire `<dossier_installation_serveur>\<version_dossier_restauration>\` vers le répertoire `<dossier_installation_serveur>\PCCSRV\`.

5. Restaurez le registre OfficeScan.

   a. Ouvrez l'**Éditeur de Registre** (`regedit.exe`).

   b. Dans le volet de navigation de gauche, sélectionnez l'une des clés de Registre suivantes :

      - Pour les systèmes 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
      - Pour les systèmes 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

   c. Accédez à **Fichier** > **Importer...**.

   d. Sélectionnez le fichier `.reg` général du serveur OfficeScan situé dans le répertoire `<dossier_installation_serveur>\<version_dossier_restauration>\`.

      Le nom du fichier de registre respecte le format suivant :

      `RegBak_<version_dossier_restauration>.reg`

   e. Cliquez sur **Oui** pour restaurer les versions précédentes de toutes les clés d'OfficeScan.

6. Restaurez éventuellement le programme de sauvegarde de la base de données.

   a. Ouvrez l'**Éditeur de Registre** (`regedit.exe`).

   b. Dans le volet de navigation de gauche, sélectionnez l'une des clés de Registre suivantes :

      - Pour les systèmes 32 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
      - Pour les systèmes 64 bits : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

   c. Accédez à **Fichier** > **Importer...**.

   d. Sélectionnez le fichier de base de données `.reg` situé dans le répertoire `<dossier_installation_serveur>\<version_dossier_restauration>\`.

Le nom du fichier de Registre respecte le format suivant :

```
RegBak_DBBak_<version_dossier_restauration>.reg
```

e. Cliquez sur **Oui** pour restaurer les versions précédentes de toutes les clés d'OfficeScan.

7. Ouvrez un éditeur de ligne de commande (`cmd.exe`), puis entrez les commandes suivantes afin de réinitialiser le compteur de performances du serveur Local Web Classification Server :

```
cd <dossier d'installation du serveur>\PCCSRV\LWCS

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

8. Redémarrez les services suivants :

   - Intrusion Defense Firewall (si installé)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - Service d'intégration d'Active Directory OfficeScan
   - Agent Control Manager d'OfficeScan
   - OfficeScan Plug-in Manager
   - Service principal d'OfficeScan
   - Apache 2 (si vous utilisez le serveur Web Apache)
   - World Wide Web Publishing Service (si vous utilisez le serveur Web IIS)

9. Nettoyez le cache d'Internet Explorer et supprimez manuellement les contrôles ActiveX. Pour obtenir des instructions détaillées sur la suppression des contrôles ActiveX d'Internet Explorer 9, consultez la page http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ie=ie-9.

   Les paramètres de la version précédente du serveur OfficeScan ont été restaurés.

Conseil

Les administrateurs peuvent confirmer la réussite de la rétrogradation en vérifiant le numéro de version d'OfficeScan sur l'écran **À propos de** (**Aide** > **À propos de**).

10. Enregistrez éventuellement le serveur OfficeScan auprès du serveur Control Manager à l'aide de la console Web.

11. Enregistrez éventuellement le serveur OfficeScan sur le serveur Deep Discovery Advisor à l'aide de la console Web.

Remarque

L'intégration de Deep Discovery Advisor avec le serveur OfficeScan a commencé dans OfficeScan 10.6 Service Pack 2.

12. Une fois la réussite de la rétrogradation d'OfficeScan confirmée, supprimez tous les fichiers qui se trouvent dans le répertoire `<dossier_installation_serveur>\<version_dossier_restauration>\`.

Rétrogradation manuelle vers des versions précédentes d'OfficeScan

Si vous rencontrez des problèmes lors de la mise à niveau des agents OfficeScan, il est possible de revenir à la version précédente de ces derniers.

Remarque

Procédez à une rétrogradation manuelle si vous n'avez pas sauvegardé les informations du serveur pendant l'installation. Si vous avez sauvegardé les informations du serveur pendant l'installation du serveur, suivez la procédure de rétrogradation décrite dans *Rétrogradation du serveur et des agents OfficeScan à l'aide du pack de sauvegarde du serveur à la page 5-9*.

Pour réussir la rétrogradation, préparez ce qui suit:

- Le serveur OfficeScan qui gérera les agents rétrogradés. La version du serveur peut être l'une des suivantes :

- 10.6 (y compris tous les Service Packs)
- 10,5 Patch 1
- 10.5
- 10.0 Service Pack 1
- 10.0
- 8.0 Service Pack 1

- Le endpoint qui fera fonction de source de mise à jour. Cette source de mise à jour contient les fichiers et les composants de rétrogradation. Lorsque l'agent devant être rétrogradé se met à jour à partir de cette source, l'agent OfficeScan est désinstallé et la précédente version de l'agent est installée.
- Le serveur OfficeScan 11.0 gérant les agents à rétrograder
- Les agents OfficeScan 11.0 à rétrograder

Première partie : Préparation de la précédente version du serveur OfficeScan

Procédure

1. Préparez un serveur équipé de la version précédente du serveur OfficeScan.
2. Appliquez à ce serveur les correctifs de type hotfix, les patchs ou les Services Packs de la version précédente du serveur OfficeScan.
3. Répliquez les paramètres du serveur OfficeScan 11.0 suivants sur la précédente version du serveur OfficeScan.

   a. Paramètres des agents

      Scan

      Agents de mise à jour

      Privilèges

Liste des spywares/graywares approuvés (pour OfficeScan 8.0 SP1 ou supérieur)

Liste d'exceptions de la surveillance des comportements (pour OfficeScan 10.0 SP1 ou supérieur)

b. Paramètres généraux de l'agent OfficeScan

c. Web Reputation Settings (pour OfficeScan 8.0 SP1 ou supérieur)

Emplacement du Endpoint

Stratégies

Proxy

d. Paramètres de pare-feu OfficeScan

Stratégie

Profils

e. Programme de vérification de la connexion

f. Web Reputation Settings (pour OfficeScan 8.0 SP1 ou supérieur)

Mise à jour programmée du serveur

Source de mise à jour du serveur

Mise à jour programmée de l'agent

Source de mise à jour des agents

g. Paramètres de maintenance des journaux

h. Notifications - tous les paramètres de notification

i. Paramètres d'administration

Gestionnaire de quarantaine

Control Manager

Sauvegarde de la base de données

4. Sur la version précédente du serveur OfficeScan, exécutez deux fois Client Packager pour créer deux packs d'installation de l'agent OfficeScan, un pour les endpoints x86 et un pour les endpoints x64.

   Paramètres du pack d'installation de l'agent OfficeScan pour les endpoints x86 :

   - Type de pack : Installation
   - Type de système d'exploitation Windows : 32 bits
   - Fichier de sortie : `InstNTPkg.exe`

   Paramètres du pack d'installation de l'agent OfficeScan pour les endpoints x64 :

   - Type de pack : Installation
   - Type de système d'exploitation Windows : 64 bits
   - Fichier de sortie : `InstNTPkg.exe`

   Comme les deux fichiers de sortie ont le même nom, enregistrez-les dans des emplacements distincts afin que l'un ne remplace pas l'autre.

Deuxième partie : Préparation d'une source de mise à jour pour les agents qui seront rétrogradés

Procédure

1. Préparez un endpoint qui fera fonction de source de mise à jour.
2. Sur l'ordinateur du serveur OfficeScan 11.0, accédez au `<Dossier d'installation du serveur>\PCCSRV` et copiez le dossier `Download` (y compris les sous-dossiers) sur le endpoint source de mise à jour (endpoint préparé à l'étape précédente).

   Par exemple, copiez le dossier `Download` dans le répertoire suivant sur le endpoint source de mise à jour :

   `C:\OfficeScanUpdateSource`
3. Sur l'ordinateur du serveur OfficeScan 11.0 :

a. Créez un dossier temporaire.

b. Accédez au `<Dossier d'installation du serveur>\PCCSRV\Admin` et copiez les fichiers suivants dans le dossier temporaire :

`RollbackAgent.dll`

`RollbackAgent_64x.dll`

`ClientRollback.exe`

c. Dans le dossier temporaire, compressez `RollbackAgent.dll` en `RollbackAgent.zip`.

d. Dans le dossier temporaire, compressez `RollbackAgent_64x.dll` en `RollbackAgent_64x.zip`.

e. Créez un sous-dossier dans le dossier temporaire et nommez-le `RollBackNTPkg`.

f. Copiez les fichiers suivants dans le dossier `RollBackNTPkg` :

`ClientRollback.exe`

Le pack d'installation de l'agent OfficeScan pour les endpoints x86 (`InstPkg.exe`) créé dans la première partie, étape 4

g. Compressez le dossier `RollbackNTPkg` en `RollbackNTPkg.zip`.

h. Créez un sous-dossier dans le dossier temporaire et nommez-le `RollBackNTPkgx64`.

i. Copiez les fichiers suivants dans le sous-dossier `RollBackNTPkgx64` :

`ClientRollback.exe`

Le pack d'installation de l'agent pour les endpoints x64 (`InstPkg.exe`) créé dans la première partie, étape 4

j. Compressez le sous-dossier `RollbackNTPkgx64` en `RollbackNTPkgx64.zip`.

k. Copiez les fichiers compressés suivants du dossier temporaire sur le endpoint source de mise à jour :

```
RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip
```

Remarque

Copiez les fichiers dans le dossier `\Download\Product` sur le endpoint source de mise à jour. Par exemple, copiez les fichiers dans `C:\OfficeScanUpdateSource\Download\Product`.

4. Concernant le endpoint source de mise à jour :

   a. Vérifiez que le « Compte Internet invité » dispose d'un accès en lecture aux fichiers compressés suivants dans `\Download\Product` (par exemple, `C:\OfficeScanUpdateSource\Download\Product`) :

   ```
   RollbackAgent.zip

   RollbackAgent_64x.zip

   RollbackNTPkg.zip

   RollbackNTPkgx64.zip
   ```

   Conseil

   Pour vérifier les droits d'accès, cliquez avec le bouton droit sur chaque fichier et sélectionnez Propriétés. Dans l'onglet Sécurité, l'autorisation pour le compte Internet invité doit être « Lecture ».

5. Dans le dossier `\Download\Product`, ouvrez le fichier `server.ini` en utilisant un éditeur de texte tel que le Bloc-notes.

6. Modifiez les lignes suivantes dans le fichier `server.ini`, puis enregistrez le fichier :

AVERTISSEMENT!

Ne modifiez aucun autre paramètre dans le fichier `server.ini`.

```
[All_Product]

MaxProductID=109

Product.109=OfficeScan Rollback, 3.5, <Version actuelle
d'OfficeScan>

[Info_109_35000_1_5633]

Version=<Version précédente d'OfficeScan>

Update_Path=product/RollbackAgent_64x.zip, <Taille du
fichier RollbackAgent64>

Path=product/RollBackNTPkgx64.zip, <Taille du fichier
RollBackNTPkg64>
```

Où :

```
<Taille du fichier RollbackAgent> : Taille du fichier
«RollbackAgent.zip» en octets. Par exemple, 90517.

<Taille du fichier RollBackNTPkg> : Taille du fichier
«RollbackNTPkg.zip» en octets. Par exemple, 32058256.

<Taille du fichier RollbackAgent64> : Taille du fichier
«RollbackAgent_64x.zip» en octets. Par exemple, 90517.

<Taille du fichier RollBackNTPkg64> : Taille du fichier
«RollbackNTpkgx64.zip» en octets. Par exemple, 36930773.
```

Conseil

Pour connaître la taille du fichier, cliquez avec le bouton droit de la souris sur le fichier `.zip` et cliquez sur **Propriétés**. Prenez en compte la taille du fichier, et non la taille sur le disque.

```
<Version actuelle d'OfficeScan> : Version actuelle
d'OfficeScan (11.0)
```

```
<Version précédente d'OfficeScan> : Version précédente
d'OfficeScan. Par exemple, 10.0.
```

Troisième partie : Rétrogradation des agents OfficeScan

Procédure

1. Sur la console Web OfficeScan 11.0, accédez à **Mises à jour** > **Agents** > **Source de mise à jour** :

   a. Sélectionnez **Source de mise à jour personnalisée**.

   b. Dans la liste **Liste des sources de mise à jour personnalisée**, cliquez sur **Ajouter**. Un nouvel écran s'affiche.

   c. Entrez les adresses IP des agents à rétrograder.

   d. Entrez l'URL de la source de mise à jour. Par exemple, entrez :

      ```
      http://<Adresse IP de la source de mise à jour>/
      OfficeScanUpdateSource/
      ```

   e. Cliquez sur **Enregistrer**.

      L'écran se ferme.

   f. Cliquez sur **Notifier tous les agents**.

      Lorsque des agents devant être rétrogradés se mettent à jour à partir de la source de mise à jour, l'agent OfficeScan est désinstallé et la version précédente du client est installée.

2. Une fois la version précédente du client installée, informez l'utilisateur de redémarrer le endpoint. Après le redémarrage, l'agent OfficeScan dépend du serveur OfficeScan préparé dans la première partie.

Chapitre 6

Obtenir de l'aide

Ce chapitre explique les problèmes de dépannage pouvant survenir et indique comment contacter le support.

Sujets abordés dans ce chapitre :

Ressources de dépannage d'OfficeScan

Utilisez les ressources suivantes pour trouver des solutions aux problèmes rencontrés dans cette version d'OfficeScan :

- Support Intelligence System
- Case Diagnostic Tool
- Trend Micro Performance Tuning Tool
- Journaux d'installation
- Journaux de débogage du serveur
- Journaux de débogage de l'agent

Support 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.

Case Diagnostic Tool

Trend Micro Case Diagnostic Tool (CDT) collecte les informations de débogage nécessaires issues du produit d'un client à chaque fois qu'un problème apparaît. Il active ou désactive automatiquement le débogage du produit et collecte les fichiers nécessaires en fonction des catégories de problèmes. Trend Micro utilise ces informations pour résoudre les problèmes liés au produit.

Pour obtenir cet outil et la documentation appropriée, contactez votre service d'assistance.

Trend Micro Performance Tuning Tool

Trend Micro fournit un outil autonome d'optimisation des performances pour identifier les applications susceptibles de provoquer des problèmes de performances. Trend Micro Performance Tuning Tool doit être exécuté sur une image de poste de travail autonome et/ou sur quelques postes de travail cibles durant le processus pilote pour éviter les problèmes de performances dans le déploiement réel de la surveillance des comportements et du contrôle des dispositifs.

Remarque

Trend Micro Performance Tuning Tool ne prend en charge que les plates-formes 32 bits.

Identification des applications exigeantes en ressources système

Procédure

1. Téléchargez Trend Micro Performance Tuning Tool à partir de :

   http://solutionfile.trendmicro.com/solutionfile/1054312/EN/TMPerfTool_2_90_1131.zip

2. Décompressez `TMPerfTool.zip` pour extraire `TMPerfTool.exe`.

3. Placez `TMPerfTool.exe` dans le `<Dossier d'installation du client>` ou dans le même dossier que `TMBMCLI.dll`.

4. Cliquez avec le bouton droit de la souris sur `TMPerfTool.exe` et sélectionnez **Exécuter en tant qu'administrateur**.

5. Lisez et acceptez le contrat de licence utilisateur final puis cliquez sur **OK**.

6. Cliquez sur **Analyser**. L'outil commence à surveiller l'utilisation de l'processeur et le chargement d'événements.

Un processus exigeant en ressources système est surligné en rouge.

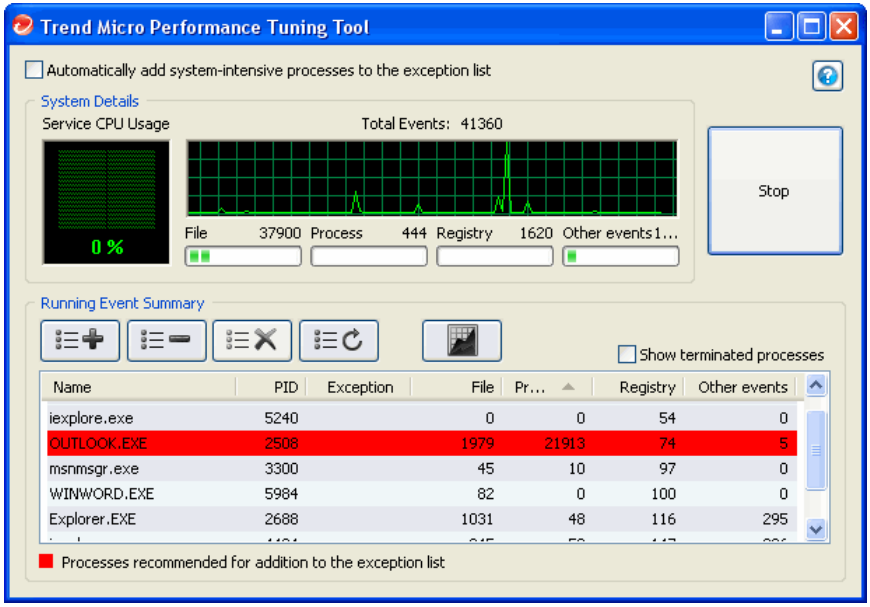

FIGURE 6-1. Processus exigeant en ressources système surligné

7. Sélectionnez un processus exigeant en ressources système puis cliquez sur le bouton **Ajouter à la liste d'exceptions (autoriser)** ( ).

8. Vérifiez si les performances du système ou des applications s'améliorent.

9. Si elles s'améliorent, sélectionnez à nouveau le processus, puis cliquez sur le bouton **Supprimer de la liste d'exceptions** ( ).

10. Si les performances baissent à nouveau, procédez comme suit :

    a. Notez le nom de l'application.

    b. Cliquez sur **Arrêter**.

    c. Cliquez sur le bouton **Générer le rapport** ( ), puis enregistrez le fichier .xml.

d. Vérifiez les applications identifiées comme conflictuelles et ajoutez-les à la liste d'exceptions de surveillance des comportements. Pour plus de détails, reportez-vous au *Manuel de l'administrateur*.

Journaux d'installation

Utilisez les fichiers journaux d'installation générés automatiquement par OfficeScan pour résoudre les problèmes liés à l'installation.

TABLEAU 6-1. Fichiers journaux d'installation

FICHIER JOURNAL	NOM DU FICHIER	EMPLACEMENT
Journal d'installation locale du serveur	OFCMAS.LOG	%windir%
Journal d'installation à distance du serveur	OFCMAS.LOG (sur le endpoint sur lequel vous avez lancé l'installation) OFCMAS.LOG (sur le endpoint cible)	%windir%
Journal d'installation de l'agent OfficeScan	OFCNT.LOG	%windir% (pour toutes les méthodes d'installation à l'exception du pack MSI) %temp% (pour la méthode d'installation à l'aide du pack MSI)

Journaux de débogage du serveur

Activez la journalisation du débogage avant d'exécuter les tâches de serveur suivantes :

- Désinstaller et réinstaller le serveur.
- Exécuter une installation à distance (la journalisation du débogage est activée sur le endpoint sur lequel vous avez lancé le programme d'installation et non sur le endpoint distant).

AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances du serveur et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si la taille du fichier devient trop volumineuse.

Activation de la journalisation du débogage sur l'ordinateur du serveur OfficeScan

Option n°1 :

Procédure

1. Connectez-vous à la console Web.
2. Dans la bannière de la console Web, cliquez sur le « **O** » d'OfficeScan. L'écran **Paramètres du journal de débogage** s'affiche alors.
3. Spécifiez les paramètres de journalisation du débogage.
4. Cliquez sur **Enregistrer**.
5. Vérifiez le fichier journal (`ofcdebug.log`) dans son emplacement par défaut : `<Dossier d'installation du serveur>\PCCSRV\Log`.

Option n°2 :

Procédure

1. Copiez dans `C:\` le dossier « LogServer » situé dans le `<dossier d'installation du serveur>>\PCCSRV\Private`.
2. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

```
[debug]

DebugLevel=9
```

```
DebugLog=C:\LogServer\ofcdebug.log

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. Enregistrez `ofcdebug.ini` dans `C:\LogServer`.
4. Exécutez la tâche appropriée (c'est-à-dire, désinstaller/réinstaller le serveur, ou effectuer une installation à distance).
5. Vérifiez le fichier `ofcdebug.log` dans `C:\LogServer`.

Remarque

Si l'agent OfficeScan est installé sur le serveur OfficeScan, il envoie également le résultat de ses propres journaux de débogage vers ceux du serveur.

Journaux de débogage de l'agent

Activez la journalisation du débogage avant d'installer l'agent OfficeScan.

AVERTISSEMENT!

Les journaux de débogage risquent de diminuer les performances des agents et utilisent une quantité considérable d'espace disque. Activez la journalisation du débogage si nécessaire et désactivez-la immédiatement si vous n'utilisez plus les données de débogage. Supprimez le fichier journal si la taille du fichier devient trop volumineuse.

Activation de la journalisation du débogage sur l'agent OfficeScan

Procédure

1. Créez un fichier nommé `ofcdebug.ini` avec le contenu suivant :

```
[Debug]

Debuglog=C:\ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. Envoyez le fichier `ofcdebug.ini` aux utilisateursde l'agent en leur demandant de l'enregistrer sous `C:\`. `LogServer.exe` s'exécute automatiquement à chaque redémarrage du endpoint de l'agent. Demandez aux utilisateurs de ne PAS fermer la fenêtre de commande `LogServer.exe` qui s'ouvre au démarrage du endpoint, car cette opération invite OfficeScan à interrompre la journalisation de débogage. Si les utilisateurs ferment la fenêtre de commande, ils peuvent relancer la journalisation du débogage en exécutant le fichier `LogServer.exe` situé dans `\Client OfficeScan`.
3. Pour chaque endpoint de l'agent, vérifiez le fichier `ofcdebug.log` dans `C:\`.
4. Pour désactiver la journalisation du débogage pour l'agent OfficeScan, supprimez `ofcdebug.ini`.

Assistance technique

Cette section explique comment trouver des solutions en ligne, utiliser le portail d'assistance et contacter Trend Micro.

Ressources de dépannage

Avant de contacter le service d'assistance technique, consultez les ressources d'aide en ligne suivantes fournies par Trend Micro.

Trend Community

Pour obtenir de l'aide, partager des expériences, poser des questions et discuter de vos inquiétudes quant aux problèmes de sécurité avec d'autres utilisateurs, des amateurs et des experts, rendez-vous sur le site :

http://community.trendmicro.com/

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 sur les problèmes courants et inhabituels pouvant être rencontrés.

Procédure

1. Accédez au site http://esupport.trendmicro.com.
2. Sélectionnez un produit ou un service dans la liste déroulante appropriée, puis indiquez toute autre information associée nécessaire.

   La page **Technical Support** (Assistance technique) du produit s'affiche.
3. Utilisez la zone **Search Support** (Lancer une recherche dans les ressources d'assistance) pour rechercher les solutions disponibles.
4. Si vous ne trouvez aucune solution, cliquez sur **Submit a Support Case** (Envoyer une demande d'assistance) dans le volet de navigation de gauche et fournissez tous les détails nécessaires. Vous avez également la possibilité de soumettre une demande d'assistance via le site ci-dessous :

   http://esupport.trendmicro.com/srf/SRFMain.aspx

Un technicien d'assistance de Trend Micro étudiera votre demande et y répondra sous 24 heures.

Communauté « Security Intelligence »

Les experts en cyber-sécurité de Trend Micro constituent une équipe spécialisée dans la sécurité dans les domaines suivants : détection et analyse des menaces, sécurité en ligne et dans les environnements virtualisés, chiffrement des données.

Rendez-vous sur le site http://www.trendmicro.com/us/security-intelligence/index.html pour en savoir plus sur les sujets suivants :

- Blogs, comptes Twitter et Facebook, chaîne YouTube et autres sites de présence de Trend Micro sur les réseaux sociaux.
- Rapports de menaces, études et articles.
- Solutions, podcasts et newsletters des acteurs principaux de la sécurité à l'échelle mondiale.
- Outils, applications et widgets gratuits.

Threat Encyclopedia

De nos jours, la plupart des programmes malveillants présentent des « menaces combinées », à savoir deux technologies (ou plus), combinées pour parvenir à contourner les protocoles de sécurité des ordinateurs. Trend Micro combat ces programmes malveillants complexes à l'aide de produits capables de générer une stratégie de défense personnalisée. L'encyclopédie des menaces fournit une liste aussi exhaustive que possible des noms et des symptômes de diverses menaces combinées connues, telles que programmes malveillants, spam, URL malveillantes et vulnérabilités connues.

Rendez-vous sur le site http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp pour en savoir plus sur les sujets suivants :

- Programmes malveillants et codes mobiles malveillants actuellement actifs ou « en circulation ».

- Pages d'informations connexes dédiées aux menaces, présentant l'historique complet d'une attaque Web.
- Avis relatifs aux menaces Internet, dédiés à des attaques et à des menaces de sécurité ciblées.
- Informations sur les tendances en matière d'attaques Web.
- Rapports hebdomadaires sur les programmes malveillants.

Comment contacter Trend Micro

Les techniciens de Trend Micro peuvent être contactés par téléphone, télécopie ou courrier électronique :

Adresse	TREND MICRO INCORPORATED Trend Micro SA 85, avenue Albert 1er 92500 Rueil Malmaison France
Téléphone	+33 (0) 1 76 68 65 00
Site Web	http://www.trendmicro.com
Adresse électronique	sales@trendmicro.fr

- Sites d'assistance à travers le monde :

  http://www.trendmicro.fr/apropos/contact/index.html

- Documentation des produits Trend Micro :

  http://docs.trendmicro.com/fr-fr/home.aspx

Accélération du traitement de votre demande d'assistance

Afin d'améliorer la résolution des problèmes, ayez les informations ci-dessous à portée de main :

- Étapes permettant de reproduire le problème

- Informations sur l'appareil et le réseau
- Marque et modèle de l'ordinateur, ainsi que de tout matériel supplémentaire connecté au endpoint
- Quantité de mémoire et d'espace disque disponibles
- Nom et version (Service Pack inclus) du système d'exploitation
- Version du client du endpoint
- 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 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 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/1055473.aspx

Services de réputation de sites Web

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.

Other Resources

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.

TrendEdge

Obtenez des informations sur les techniques novatrices non prises en charge, les outils et les bonnes pratiques liés aux produits et services Trend Micro. La base de données TrendEdge contient de nombreux documents couvrant un large éventail de sujets destinés aux employés et partenaires de Trend Micro, ainsi qu'aux autres parties intéressées.

Consultez les informations les plus récemment ajoutées à TrendEdge à l'adresse :

http://trendedge.trendmicro.com/

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://www.trendmicro.com/download/emea/?lng=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.

TrendLabs

TrendLabs℠ est un réseau mondial de centres de recherche, de développement et d'action dédiés à la surveillance des menaces, à la prévention des attaques et à la publication rapide et transparente de solutions 24 h/24 et 7 j/7. Véritable clef de voûte de l'infrastructure de services de Trend Micro, l'équipe de TrendLabs se compose de plusieurs centaines de techniciens et d'employés certifiés qui proposent un large éventail de services d'assistance technique et d'assistance produit.

TrendLabs surveille l'apparition et l'évolution des menaces à l'échelle mondiale, afin de pouvoir proposer des mesures de sécurité efficaces permettant de détecter, de bloquer et d'éliminer les attaques. La portée de ces efforts se mesure au jour le jour, par le biais des mises à jour des fichiers de signatures de virus et des ajustements apportés au moteur de scan fréquemment transmis à nos clients.

Pour en savoir plus sur TrendLabs, rendez-vous sur le site :

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Annexe A

Exemple de déploiement

Cette section indique comment déployer OfficeScan en fonction de la topologie du réseau et des ressources réseau disponibles. Utilisez-la à titre de référence lors de la planification du déploiement d'OfficeScan dans votre entreprise.

Réseau de base

La figure 1 illustre un réseau de base avec un serveur et des agents OfficeScan connectés directement. La plupart des réseaux d'entreprise disposent de cette configuration, avec une vitesse d'accès au réseau local (et/ou étendu) de 10 Mbps, 100 Mbps ou 1 Gbps. Dans ce scénario, le endpoint qui satisfait à la configuration système requise

d'OfficeScan et dispose des ressources adéquates constitue le candidat idéal pour héberger le serveur OfficeScan.

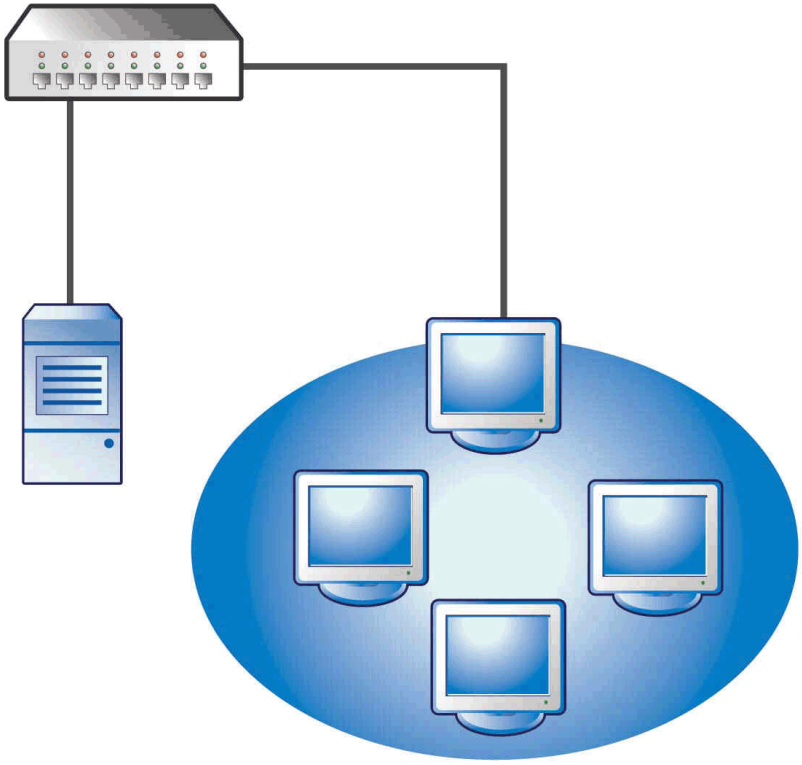

FIGURE A-1. Topologie d'un réseau de base

Réseau multisite

Pour un réseau disposant de plusieurs points d'accès et plusieurs sites distants avec différentes bandes passantes :

- Analysez les points de consolidation en termes de bureaux et de bande passante réseau.
- Déterminez l'utilisation actuelle de la bande passante pour chaque bureau.

Voici une représentation explicite de la meilleure façon de déployer OfficeScan. La Figure 1 illustre une topologie de réseau multisite.

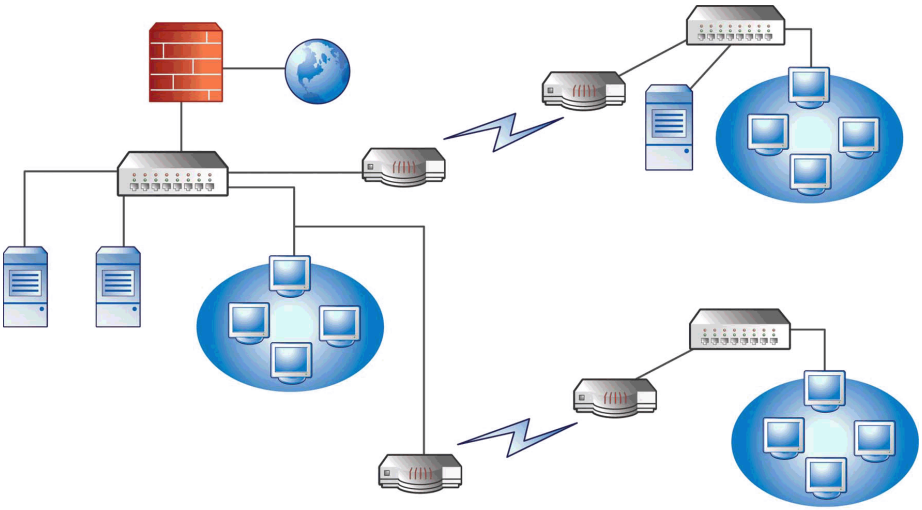

FIGURE A-2. Topologie de réseau multisite

Informations sur le réseau :

- La connexion WAN du site distant 1 présente une moyenne de 70 % d'utilisation pendant les heures de bureau. Ce site comprend 35 endpoints d'agent.
- La connexion WAN du site distant 2 présente une moyenne de 40 % d'utilisation pendant les heures de bureau. Ce site comprend 9 endpoints d'agent.
- Le serveur 3 fait office de serveur de fichiers et d'impression pour le groupe du site distant 1. Ce endpoint constitue une option pour l'installation du serveur OfficeScan, ce qui entraînerait toutefois une augmentation du temps consacré à

l'administration. Tous les serveurs sont équipés de Windows Server 2003. Le réseau utilise Active Directory, mais principalement pour l'authentification du réseau.

- Tous les endpoints d'agent du site principal, du site distant 1 et du site distant 2 sont équipés de Windows Server 2003 ou Windows XP.

Préparation d'un réseau multisite

Procédure

1. Identifiez le endpoint sur lequel vous souhaitez installer le serveur OfficeScan. Voir *Exécution d'une nouvelle installation du serveur OfficeScan à la page 2-2* pour obtenir une description de la procédure d'installation.

2. Identifiez les méthodes d'installation de l'agent disponibles et éliminez les méthodes non compatibles. Consultez le *Manuel de l'administrateur* pour plus d'informations sur les méthodes d'installation de l'agent.

   Méthodes d'installation disponibles :

   - Configuration du script de connexion

     L'outil Configuration du script de connexion fonctionne bien lorsqu'aucun réseau étendu (WAN) n'est mis en place, dans la mesure où le trafic local n'a aucune importance. Cependant, étant donné que 50 Mo de données sont transmis à chaque endpoint, cette option n'est pas viable.

   - Installation à distance depuis la console Web

     Cette méthode vaut pour tous les endpoints connectés au réseau local (LAN) sur le site principal. Dans la mesure où tous les endpoints exécutent Windows Server 2003, le déploiement du pack vers les endpoints est facile.

     En raison de la faible vitesse de connexion entre deux sites distants, cette méthode de déploiement risque d'avoir un impact sur la bande passante disponible si le déploiement d'OfficeScan est effectué pendant les heures de bureau. Utilisez toute la capacité de connexion pour déployer OfficeScan en dehors des heures de bureau, lorsque la plupart des postes de travail sont inutilisés. Cependant, si les utilisateurs éteignent leur endpoint, le déploiement d'OfficeScan vers ces endpoints ne pourra pas avoir lieu.

- Déploiement du pack de l'agent OfficeScan

  Le déploiement du pack de l'agent OfficeScan semble constituer la meilleure option pour le déploiement sur les sites distants. Cependant, sur le site distant 2, il n'existe pas de serveur local pour faciliter la mise œuvre de cette option. Après examen approfondi de toutes les options, cette option fournit la meilleure couverture pour la plupart des endpoints.

Déploiement sur le site principal

La méthode de déploiement de l'agent la plus simple à implémenter sur le site principal est l'installation à distance depuis la console Web d'OfficeScan. Consultez le *Manuel de l'administrateur* pour connaître la procédure.

Déploiement sur le site distant 1

Le déploiement sur le site distant 1 requiert la configuration du service de fichiers répartis DFS (Distributed File System) de Microsoft. Pour obtenir des informations complémentaires sur DFS, consultez le site http://support.microsoft.com/?kbid=241452. Après la configuration de DFS, le serveur 3 du site distant 1 doit activer DFS, répliquant l'environnement DFS existant ou créant un nouvel environnement DFS.

Une méthode de déploiement appropriée consiste à créer un pack d'agent au format de pack Microsoft Installer (MSI) et à déployer ce pack sur DFS. Consultez le *Manuel de l'administrateur* pour connaître la procédure. Dans la mesure où le pack d'agent sera répliqué vers le serveur 3 au cours de la prochaine mise à jour programmée, son déploiement a un impact minimum sur la bande passante.

Vous pouvez également déployer un pack d'agent via Active Directory. Consultez le *Manuel de l'administrateur* pour obtenir des informations détaillées.

Minimisation de l'impact des mises à jour des composants à travers le réseau étendu

Procédure

1. Désignez un agent devant faire fonction d'agent de mise à jour sur le site distant 1.
   a. Connectez-vous à la console Web et accédez à **Agents** > **Gestion des agents**.
   b. Dans l'arborescence des agents, sélectionnez l'agent qui fera office d'agent de mise à jour et cliquez sur **Paramètres** > **Paramètres des agents de mise à jour**.
2. Sélectionnez les agents du site distant 1 qui procèdent à la mise à jour des composants depuis l'agent de mise à jour.
   a. Accédez à **Mises à jour** > **Serveur** > **Source de mise à jour**.
   b. Sélectionnez **Sources de mise à jour personnalisées** et cliquez sur **Ajouter**.
   c. Dans l'écran qui s'affiche, saisissez la plage d'adresses IP des endpoints du site distant 1.
   d. Sélectionnez **Source de mise à jour**, puis choisissez l'agent de mise à jour désigné dans la liste déroulante.

Déploiement sur le site distant 2

Le problème clé touchant le site distant 2 est la faible bande passante. Cependant, 60 % de la bande passante est disponible pendant les heures de bureau lorsqu'environ 154 Kbits de bande passante sont disponibles.

La meilleure façon d'installer l'agent OfficeScan consiste à utiliser le même pack d'agent au format MSI utilisé sur le site distant 1. Cependant, dans la mesure où aucun serveur n'est disponible, vous ne pouvez pas utiliser un service de fichiers répartis (Distributed File System ou DFS).

Une option consiste à utiliser des outils de gestion tiers permettant aux administrateurs de configurer ou de créer des répertoires partagés sur des endpoints sans disposer d'un

accès physique à ces répertoires. Après la création de ce répertoire partagé sur un endpoint unique, la copie du pack d'agent dans le répertoire partagé requiert moins de temps de gestion que l'installation sur neuf endpoints.

Utilisez une autre stratégie Active Directory, mais veillez bien à ne pas spécifier le partage DFS en tant que source.

Grâce à ces méthodes, le trafic réseau résultant de l'installation reste local, réduisant le trafic à travers le réseau étendu.

Pour minimiser l'impact des mises à jour des composants à travers le réseau étendu, attribuez à un agent le rôle d'agent de mise à jour. Voir la *Déploiement sur le site distant 1 à la page A-6* pour plus d'informations.

Index

T

V