



TREND MICRO™

Control Manager 6.0

Gestion centralisée de la sécurité pour l'entreprise

Guide d'installation

Trend Micro Incorporated se réserve le droit de modifier ce document et les produits décrits ici sans préavis. Avant d'installer et d'utiliser votre logiciel, veuillez consulter les fichiers Lisez-moi, les notes de mise à jour et la dernière version de la documentation utilisateur applicable que vous trouverez sur le site Web de Trend Micro à l'adresse suivante :

<http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx>

Trend Micro, le logo t-ball de Trend Micro, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, et TrendLabs sont des marques commerciales ou des marques déposées de Trend Micro Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 1998-2012 Trend Micro Incorporated. Tous droits réservés.

N° de référence du document : CMEM65332/120203

Date de sortie : Mai 2012

Protégé par les brevets américains n° 5,623,600; 5,889,943; 5,951,698 et 6,119,165

La documentation utilisateur pour Trend Micro Control Manager présente les fonctions principales du logiciel et les instructions d'installation pour votre environnement de production. Lisez attentivement ce manuel avant d'installer ou d'utiliser le logiciel.

Vous trouverez des informations détaillées sur l'utilisation des fonctions spécifiques du logiciel dans le fichier d'aide en ligne et dans la Base de connaissances en ligne sur le site Web de 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.

Veuillez évaluer cette documentation sur le site Web suivant :

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

Table des matières

Préface

Préface	1
Nouveautés de cette version	2
Fonctions et améliorations de Control Manager 6.0	2
Documentation de Control Manager	3
Conventions typographiques	5

Chapitre 1: Présentation de Trend Micro Control Manager

Control Manager Standard et Advanced	1-2
Présentation des fonctionnalités de Control Manager	1-2
Définition de Trend Micro Management Communication Protocol	1-4
Réduction de la charge du réseau et de la taille de paquet	1-5
Prise en charge transversale du NAT et des pare-feu	1-6
Prise en charge du protocole HTTPS	1-7
Communications en mode unidirectionnel	1-7
Communications en mode bidirectionnel	1-8
Prise en charge du système de signature unique (SSO)	1-8
Architecture de Control Manager	1-8
Trend Micro Smart Protection Network	1-11
Réputation des e-mails	1-11
Services de File Reputation	1-12
Services de réputation de sites Web	1-12
Smart Feedback	1-12

Chapitre 2: Planification et implémentation du déploiement de Control Manager

Identification de l'architecture et de la stratégie de déploiement	2-3
Définition du déploiement sur site unique	2-4
Définition du déploiement sur plusieurs sites	2-6

Prévision du trafic réseau	2-11
Déroulement de l'installation de Control Manager	2-12
Test de Control Manager sur un site	2-12
Préparation du déploiement test	2-13
Sélection d'un site de test	2-14
Création d'un plan de rétrogradation	2-14
Initialisation du déploiement test	2-14
Évaluation du déploiement test	2-14
Plan de distribution des serveurs	2-15
Définition des modèles d'administration	2-15
Définition de la distribution des serveurs Control Manager	2-16
Topologie à un seul serveur	2-16
Topologie à plusieurs serveurs	2-17
Plan de trafic réseau	2-17
Définition du trafic généré sur un réseau Control Manager	2-17
Source du trafic réseau	2-19
Trafic généré par les journaux	2-19
Stratégies Trend Micro Management Communication Protocol ..	2-20
Stratégies Trend Micro Management Infrastructure	2-21
Trafic généré par l'enregistrement de produits	2-22
Déploiement de stratégies	2-22
Déploiement des mises à jour	2-23
Plan de stockage des données	2-24
Recommandations pour la base de données	2-24
Pilotes ODBC	2-25
Authentification	2-25
Plan de serveur Web	2-25

Chapitre 3: Première installation de Trend Micro Control Manager

Configuration système requise	3-2
Installation des composants pré-requis	3-2

À propos de l'installation d'un serveur Control Manager	3-3
Déroulement de l'installation de Control Manager	3-4
Installation de tous les composants nécessaires	3-5
Spécification de l'emplacement d'installation	3-8
Enregistrement et activation du produit et des services	3-10
Spécification des paramètres de sécurité et de serveur Web de Control Manager	3-12
Spécification des paramètres de sauvegarde	3-15
Configuration des paramètres de notification	3-16
Configuration des informations relatives à la base de données	3-18
Installation du compte racine	3-21
Vérification de l'installation correcte du serveur Control Manager	3-23
Configuration après l'installation	3-26
Enregistrement et activation de Control Manager	3-27
Configuration des comptes utilisateurs	3-27
Téléchargement des composants les plus récents	3-27
Paramètres de notification :	3-28
Enregistrement et activation de votre logiciel	3-28
À propos de l'activation de Control Manager	3-28

Chapitre 4: Mise à niveau de serveurs ou migration d'agents vers Control Manager

Mise à niveau vers Control Manager 6.0	4-2
Mise à niveau des serveurs Control Manager 5.0 / 5.5	4-2
Mises à niveau et migrations : cas de figure	4-3
Rétablissement des serveurs Control Manager 5.0/5.5	4-10
Scénario 1 : Rétrogradation d'un serveur Control Manager 6.0 vers Control Manager 5.0/5.5	4-10
Scénario 2 : Rétrogradation d'un environnement en cascade	4-11
Planification de la migration des agents Control Manager	4-12
Mise à niveau rapide	4-12
Mise à niveau progressive	4-13
Scénarios de migration pour les agents Control Manager 2.x	4-13
Migration d'agents Control Manager 2.5x et MCP	4-17

Migration de la base de données de Control Manager	4-19
Migration d'une base de données Control Manager SQL 2005 vers un autre serveur SQL Server 2005	4-19

Chapitre 5: Suppression de Trend Micro Control Manager

Suppression d'un serveur Control Manager	5-2
Suppression manuelle de Control Manager	5-3
Suppression de l'application Control Manager	5-4
Suppression d'un agent Control Manager 2.x sur Windows	5-11

Chapitre 6: Obtenir de l'assistance

Avant de contacter l'assistance technique	6-2
Comment contacter l'assistance technique	6-2
Résolution plus rapide des problèmes	6-3
TrendLabs	6-3
Autres ressources utiles	6-4

Annexe A: Journal système de Control Manager

Liste de contrôle de l'adresse du serveur	A-2
Liste de contrôle des ports	A-3
Liste de contrôle d'installation de l'agent Control Manager 2.x	A-4
Conventions relatives à Control Manager	A-5
Processus principal et fichiers de configuration	A-6
Ports de communication et d'écoute	A-8
Comparaison des versions de Control Manager	A-9

Index

Index	IN-1
-------------	------

Préface

Préface

Ce guide d'installation présente Trend Micro™Control Manager™6.0 et parcourt la planification d'installation et l'installation de Control Manager en fonction de vos besoins.

Cette préface traite les rubriques suivantes :

- *Nouveautés de cette version à la page 2*
- *Documentation de Control Manager à la page 3*
- *Conventions typographiques à la page 5*

Nouveautés de cette version

Trend Micro Control Manager 6.0 est un produit particulièrement innovant en termes de fonctions de gestion, grâce à l'introduction de la gestion de stratégies pour déployer directement des paramètres de produits vers des points finaux à partir d'une console unique.

Fonctions et améliorations de Control Manager 6.0

Les nouvelles fonctions et améliorations de la version 6.0 sont les suivantes.

FONCTION	DESCRIPTION
Gestion des stratégies	<ul style="list-style-type: none">• Déploiement de paramètres de produits vers des produits gérés à l'aide de stratégies• Types de stratégies flexibles• Administration basée sur les rôles• Mise à jour simple de modèles de stratégies à partir de la console Web
Widget du tableau de bord d'état des stratégies	<ul style="list-style-type: none">• État de déploiement à jour des paramètres de produits• Surveillance du nombre de cibles déployées et en attente• Vérification de l'état détaillé des cibles en attente
Mise à jour de modèles de stratégies	Lorsque de nouveaux modèles ou de nouvelles versions de modèles existants sont disponibles, les administrateurs peuvent effectuer la mise à jour simplement depuis la console Web.

FONCTION	DESCRIPTION
Intégration de la prévention contre la perte de données (DLP)	<p>DLP est une fonctionnalité du module Protection des données qui contrôle la transmission des actifs numériques. La fonctionnalité DLP peut minimiser le risque de perte d'informations et améliorer la visibilité des modèles d'utilisation des données et des processus d'entreprise à risque.</p> <p>Control Manager a intégré les fonctionnalités DLP suivantes :</p> <ul style="list-style-type: none"> • Modèles DLP gérables et identificateurs de données • Déploiement de paramètres DLP vers des produits gérés à l'aide de la gestion des stratégies, des modèles DLP et des identificateurs de données • Collecte des journaux DLP pour l'établissement de rapports et les notifications d'événements • 22 modèles de rapport DLP prédéfinis • Cinq notifications d'événements DLP • Quatre widgets de tableau de bord • Prise en charge des produits : OfficeScan, IMSVA et ScanMail pour Microsoft Exchange
Préférés	Permet aux administrateurs d'ajouter des raccourcis au menu Préférés pour un accès rapide.

Documentation de Control Manager

Ce manuel suppose que vous avez acquis des connaissances élémentaires en matière de systèmes de sécurité. Il renvoie à des versions précédentes de Control Manager pour aider les administrateurs système et les utilisateurs qui sont familiarisés avec ces versions. Si ce n'est pas votre cas, ces renvois vous permettront de mieux comprendre les concepts de Control Manager.



TABLEAU 1. Documentation de Control Manager


DOCUMENT	DESCRIPTION
Aide en ligne	<p>Documentation accessible en ligne à partir de la console Web de Control Manager.</p> <p>L'aide en ligne fournit des explications sur les composants et les fonctions de Control Manager, ainsi que sur les procédures de configuration de Control Manager.</p>
Trend Micro Online Help Center (http://docs.trendmicro.com/fr-fr/home.aspx)	Trend Micro Online Help Center fournit les dernières documentations produit.
Fichier Lisez-moi	<p>Le fichier Lisez-moi contient des informations de dernière minute sur le produit qui ne se trouvent pas dans la documentation en ligne ou imprimée. Il décrit notamment les nouvelles fonctionnalités, fournit des conseils d'installation, recense les problèmes connus et rappelle l'historique des différentes versions du produit.</p>
Guide d'installation	<p>Documentation PDF accessible sur le DVD Trend Micro Enterprise ou téléchargeable à partir du site Web de Trend Micro.</p> <p>Le guide d'installation explique en détail comment installer Control Manager et configurer les paramètres de base pour une prise en main rapide.</p>
Manuel de l'administrateur	<p>Document PDF accessible sur le DVD Solutions Trend Micro de Control Manager ou téléchargeable sur le site internet de Trend Micro.</p> <p>Le manuel de l'administrateur explique en détail comment configurer et gérer Control Manager et les produits gérés, et expose les concepts et les fonctions de Control Manager.</p>

DOCUMENT	DESCRIPTION
Didacticiel	<p>Document PDF accessible sur le DVD Solutions Trend Micro de Control Manager ou téléchargeable sur le site internet de Trend Micro.</p> <p>Le didacticiel donne des instructions relatives au déploiement, à l'installation, à la configuration et à la gestion de Control Manager et des produits gérés enregistrés sur Control Manager.</p>

Conventions typographiques

Pour faciliter la recherche et la compréhension des informations, cette documentation utilise les conventions suivantes.

CONVENTION/TERME	DESCRIPTION
MAJUSCULE	Acronymes, abréviations, noms de certaines commandes et touches du clavier.
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches.
<i>Italique</i>	Références à d'autres documents.
Monospace	Échantillons de lignes de commande, code du programme, URL Web, noms de fichiers et sortie d'un programme.
 Remarque	Remarques de configuration.
 Conseil	Recommandations ou suggestions.

CONVENTION/TERME	DESCRIPTION
 AVERTISSEMENT!	Actions critiques et options de configuration.
Chemin > de navigation	Le chemin de navigation permettant d'atteindre un écran spécifique. Par exemple, Scans > Scans manuels , implique de cliquer sur Scans , puis de cliquer sur Scans manuels dans l'interface.

Chapitre 1

Présentation de Trend Micro™ Control Manager™

Trend Micro Control Manager est une console d'administration centralisée qui gère les produits et services Trend Micro, au niveau de la passerelle, du serveur de messagerie, du serveur de fichiers et des postes de travail de l'entreprise. Les administrateurs peuvent utiliser la fonctionnalité de gestion des stratégies pour configurer et déployer les paramètres du produit dans les produits gérés et les points finaux. La console d'administration à interface Web de Control Manager fournit un point de surveillance unique pour les produits et les services antivirus et de sécurité de contenu sur tout le réseau.

Ce chapitre traite les rubriques suivantes :

- *Control Manager Standard et Advanced à la page 1-2*
- *Présentation des fonctionnalités de Control Manager à la page 1-2*
- *Définition de Trend Micro Management Communication Protocol à la page 1-4*
- *Architecture de Control Manager à la page 1-8*
- *Trend Micro™ Smart Protection Network™ à la page 1-11*

Control Manager Standard et Advanced

Il existe deux versions de Control Manager : la version Standard et la version Advanced. Control Manager Advanced inclut des fonctionnalités dont la version Standard ne dispose pas. Par exemple, Control Manager Advanced prend en charge la structure de gestion en cascade. Cela signifie que le réseau Control Manager peut être géré par un serveur Control Manager Advanced parent avec plusieurs serveurs Control Manager Advanced enfants soumis au serveur Control Manager Advanced parent. Le serveur parent est le cœur de l'ensemble du réseau.



Remarque

Control Manager Advanced prend en charge les produits suivants en tant que serveurs Control Manager enfants :

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Les serveurs Control Manager 5.0/5.5/6.0 Standard ne peuvent pas être des serveurs enfants.

Pour une liste complète des fonctionnalités prises en charge par les serveurs Control Manager Standard et Advanced, consultez la section [Comparaison des versions de Control Manager à la page A-9](#).

Présentation des fonctionnalités de Control Manager

Trend Micro a conçu Control Manager pour gérer des produits et services antivirus et de sécurité de contenu déployés sur les réseaux locaux et étendus d'une entreprise.

TABEAU 1-1. Fonctions de Control Manager

FONCTION	DESCRIPTION
Gestion des stratégies	Les administrateurs système peuvent utiliser les stratégies pour configurer et déployer les paramètres du produit dans les produits gérés et les points finaux à partir d'une seule console d'administration.
Configuration centralisée	<p>Le répertoire Produits et la structure de gestion en cascade permettent de coordonner vos actions en matière de protection anti-virus et de sécurité de contenu à partir d'une seule console d'administration.</p> <p>Grâce à ces fonctions, vous pouvez appliquer de façon homogène les stratégies relatives aux virus/programmes malveillants et à la sécurité de contenu de votre entreprise.</p>
Prévention proactive des épidémies	Les services OPS (Outbreak Prevention Services) permettent de prendre des mesures proactives pour protéger le réseau contre toute menace d'épidémie de virus/programmes malveillants.
Infrastructure de communication sécurisée	<p>Control Manager utilise une infrastructure de communication reposant sur le protocole SSL (Secure Socket Layer).</p> <p>Selon les paramètres de sécurité utilisés, Control Manager peut chiffrer des messages avec ou sans authentification.</p>
Configuration et téléchargement de composants sécurisés	Ces fonctions permettent de configurer l'accès à la console Web et le téléchargement de composants de façon sécurisée.
Délégation de tâches	<p>Les administrateurs système peuvent définir des comptes personnalisés avec des privilèges individualisés pour les utilisateurs de la console Web de Control Manager.</p> <p>Un compte utilisateur définit les objets visibles et les actions réalisables par un utilisateur sur un réseau Control Manager. Vous pouvez contrôler l'utilisation faite par un utilisateur de son compte via un journal d'utilisateur.</p>

FONCTION	DESCRIPTION
Suivi des commandes	<p>Cette fonction permet de contrôler toutes les commandes exécutées à l'aide de la console Web de Control Manager.</p> <p>Elle permet ainsi de vérifier si Control Manager a pu mener à bien des opérations particulièrement longues, telles que la mise à jour et le déploiement de fichiers de signatures de virus.</p>
Contrôle de produits à la demande	<p>Cette fonction permet de contrôler des produits gérés en temps réel.</p> <p>Control Manager envoie immédiatement aux produits gérés les modifications de configuration effectuées sur la console Web. Les administrateurs système peuvent exécuter des scans manuels à partir de la console Web. Cette commande système est indispensable en cas d'épidémie de virus/programmes malveillants.</p>
Contrôle centralisé des mises à jour	<p>Cette fonction permet de mettre à jour des fichiers de signatures de virus, des règles anti-spam, des moteurs de scan et d'autres composants antivirus et de sécurité de contenu, afin que tous les produits gérés soient à jour.</p>
Journalisation centralisée	<p>Des journaux et des rapports complets permettent d'avoir une vue d'ensemble sur le fonctionnement des produits antivirus et de sécurité de contenu.</p> <p>Control Manager collecte des journaux de tous les produits gérés. Vous n'avez plus à vérifier le journal de chaque produit.</p>

Définition de Trend Micro Management Communication Protocol

Les agents MCP (Management Communication Protocol) sont les tout derniers agents développés par Trend Micro pour les produits gérés. MCP remplace TMI (Trend Micro Management Infrastructure) pour les communications entre Control Manager et les produits gérés. MCP dispose de diverses fonctions :

- Réduction de la charge du réseau et de la taille de paquet

- Prise en charge transversale du NAT et des pare-feu
- Prise en charge du protocole HTTPS
- Prise en charge des communications unidirectionnelles et bidirectionnelles
- Prise en charge du système de signature unique (SSO)

Réduction de la charge du réseau et de la taille de paquet

TMI utilise un protocole d'application utilisant le XML. Bien que le XML offre des possibilités de développement et un certain niveau de souplesse dans la conception du protocole, l'application du XML en tant que norme de format de données pour le protocole de communication présente les inconvénients suivants :

- L'analyse XML absorbe plus de ressources système que d'autres formats de données comme la paire nom-valeur CGI et la structure binaire (le programme laisse un volume important sur votre serveur ou dispositif).
- Le volume utilisé par l'agent pour transférer des informations est plus important en XML qu'avec d'autres formats de données.
- Les données sont traitées moins rapidement en raison du volume plus important occupé par les données.
- Les transferts de paquets prennent plus de temps et la vitesse de transmission est plus faible que pour d'autres formats de paquets.

Le format de données de MCP est conçu pour résoudre ces problèmes. Le format de données de MCP est un flux (binaire) de type BLOB dont chaque élément comporte un ID nom, un type, une longueur et une valeur. Le format BLOB présente les avantages suivants :

- **Moindre taille de transfert des données par rapport au XML :** Un nombre limité d'octets suffit à stocker les informations pour chaque type de données. (entier, entier non signé, booléen, virgule flottante).
- **Vitesse d'analyse plus élevée :** Le format binaire fixe permet d'analyser individuellement chaque élément de données. L'analyse est en effet plusieurs fois plus rapide qu'en XML.

- **Conception plus souple :** La souplesse de conception a également été prise en compte dans la mesure où chaque élément comporte un ID nom, un type, une longueur et une valeur. L'ordre des éléments n'est pas imposé et des éléments complémentaires peuvent être présents dans le protocole de communication uniquement en cas de besoin.

Non seulement ces éléments s'appliquent au format de flux binaire pour le transfert de données, mais plusieurs types de données peuvent être regroupés sous forme de paquet dans une connexion, avec ou sans compression. Ce type de stratégie de transfert de données permet de préserver la bande passante du réseau et d'étendre les possibilités de développement.

Prise en charge transversale du NAT et des pare-feu

Les dispositifs NAT (Network Address Translation), disposant d'adresses IP adressables limitées sur le réseau IPv4, se sont largement répandus pour permettre à davantage d'ordinateurs de points finaux de se connecter à Internet. Pour ce faire, les dispositifs NAT forment un réseau privé virtuel pour les ordinateurs qui y sont reliés. Chaque ordinateur connecté à un dispositif NAT dispose d'une adresse IP virtuelle privée qui lui est propre. Le dispositif NAT convertit cette adresse IP en une adresse IP universelle avant d'envoyer une requête sur Internet. Cela pose toutefois certains problèmes car chaque ordinateur qui se connecte utilise une adresse IP virtuelle alors que de nombreuses applications de réseau ignorent ce comportement. Des dysfonctionnements de programme et des problèmes de connexion au réseau peuvent alors survenir.

Pour les produits fonctionnant avec les agents Control Manager 2.5/3.0, on suppose la condition préalable suivante : le serveur considère que l'agent est accessible en établissant une connexion du serveur vers l'agent. Il s'agit d'un produit de communication en « mode bidirectionnel » car chaque partie peut établir une connexion réseau avec l'autre partie. Cette supposition n'est plus valable lorsque l'agent (ou le serveur Control Manager) se trouve derrière un dispositif NAT car la connexion ne peut envoyer les données que vers le dispositif NAT, et non vers le produit situé derrière le dispositif NAT (ni vers un serveur Control Manager dans la même situation). Une solution couramment utilisée consiste à établir une relation de correspondance spécifique sur le dispositif NAT pour lui demander de rediriger automatiquement la requête entrante vers l'agent respectif. Toutefois, cette solution exige l'intervention de l'utilisateur et n'est pas adaptée à un déploiement de produit à grande échelle.

Le modèle de communication en mode unidirectionnel introduit par MCP permet de résoudre ce problème. Dans ce type de communication, seul l'agent établit la connexion réseau sur le serveur. Le serveur ne peut pas établir de connexion sur l'agent. La communication unidirectionnelle convient particulièrement aux transferts de journaux. Toutefois, la distribution des commandes du serveur s'effectue en mode passif. En d'autres termes, le déploiement de commandes suppose que l'agent demande au serveur les commandes disponibles.

Prise en charge du protocole HTTPS

Le protocole d'intégration MCP applique le protocole de communication HTTP/HTTPS, couramment utilisé. Les avantages du HTTP/HTTPS sur TMI sont les suivants :

- Une large majorité de la communauté des informaticiens connaît le protocole HTTP/HTTPS. Il est donc plus facile d'identifier les problèmes de communication et de les résoudre.
- Pour la plupart des environnements d'entreprise, il est inutile d'ouvrir d'autres ports dans le pare-feu pour permettre le passage des paquets.
- Des mécanismes de sécurité existants créés pour HTTP/HTTPS (comme SSL/TLS et HTTP Digest Authentication) peuvent être utilisés.

Le protocole MCP de Control Manager définit trois niveaux de sécurité :

- **Niveau normal** : Control Manager utilise HTTP pour les communications.
- **Niveau moyen** : Control Manager utilise HTTPS pour les communications s'il est pris en charge. Si ce n'est pas le cas, Control Manager utilise alors HTTP.
- **Niveau élevé** : Control Manager utilise HTTPS pour les communications.

Communications en mode unidirectionnel

La prise en charge transversale du NAT est un problème dont l'importance prend de l'ampleur dans l'environnement de réseau actuel réel. MCP utilise des communications en mode unidirectionnel pour faire face à ce problème. Dans ce mode, le client MCP établit la connexion au serveur et lui demande les commandes. Chaque requête est une

interrogation de commande de type CGI ou une transmission de journal. Afin de réduire l'impact sur le réseau, la connexion reste active et ouverte autant que possible. Une autre requête utilise une connexion ouverte existante. Même en cas d'interruption de la connexion, toutes les connexions impliquant SSL sur le même hôte bénéficient de la mise en cache de l'ID de session, ce qui réduit considérablement le temps de reconnexion.

Communications en mode bidirectionnel

Les communications en mode unidirectionnel peuvent être remplacées par les communications en mode bidirectionnel. Le mode bidirectionnel repose sur des communications unidirectionnelles et utilise un canal supplémentaire pour la réception des notifications du serveur. Ce canal supplémentaire utilise également le protocole HTTP. Le mode bidirectionnel peut améliorer la distribution en temps réel et le traitement des commandes du serveur par l'agent MCP. L'agent MCP doit passer par un serveur Web ou un programme compatible CGI capable de traiter des requêtes de type CGI pour recevoir les notifications du serveur Control Manager.

Prise en charge du système de signature unique (SSO)

MCP permet désormais à Control Manager de prendre en charge la fonctionnalité SSO (Single Sign-On) pour les produits Trend Micro. Les utilisateurs peuvent ainsi s'enregistrer sur Control Manager et accéder aux ressources d'autres produits Trend Micro sans avoir à s'enregistrer aussi pour ces produits.

Architecture de Control Manager

Trend Micro Control Manager permet de contrôler les produits et services Trend Micro depuis un point central. Cette application simplifie la gestion de la stratégie d'une entreprise en matière de lutte contre les virus/programmes malveillants et de sécurité du contenu. Le tableau suivant fournit une liste des composants utilisés par Control Manager.

TABEAU 1-2. Composants de Control Manager

COMPOSANT	DESCRIPTION
Serveur Control Manager	<p>Sert de référentiel pour toutes les données collectées par les agents. Il peut s'agir d'un serveur Standard ou Advanced. Les fonctions d'un serveur Control Manager sont les suivantes :</p> <ul style="list-style-type: none"> • Une base de données SQL qui stocke les configurations et les journaux des produits gérés. <p>Control Manager stocke dans la base de données Microsoft SQL Server (<code>db_ControlManager.mdf</code>) les données des journaux, la programmation des communicateurs, les informations sur les produits gérés et les serveurs enfants, ainsi que les paramètres des comptes utilisateurs, de l'environnement réseau et des notifications.</p> <ul style="list-style-type: none"> • Un serveur Web qui héberge la console Web de Control Manager. • Un serveur de messagerie qui envoie des notifications d'événement par courrier électronique. <p>Control Manager peut envoyer des notifications à des individus ou à des groupes de destinataires pour leur signaler des événements qui se produisent sur le réseau Control Manager. Configurez le Centre d'événements pour envoyer des notifications par courrier électronique, le journal des événements Windows, MSN Messenger, SNMP, Syslog, un pageur ou toute autre application développée en interne ou largement répandue dans l'industrie, que votre entreprise a adoptée pour envoyer des notifications.</p> <ul style="list-style-type: none"> • Un serveur de rapports, présent uniquement dans la version Advanced Edition, qui génère des rapports sur les produits antivirus et de sécurité de contenu. <p>Un rapport Control Manager est un ensemble de données chiffrées collectées sur le réseau qui sont liées aux événements impliqués dans la protection antivirus et la sécurité de contenu sur le réseau Control Manager.</p>

COMPOSANT	DESCRIPTION
Trend Micro Management Communication Protocol (MCP)	<p>MCP gère les interactions entre le serveur Control Manager et les produits gérés qui prennent en charge les agents MCP de la dernière génération.</p> <p>MCP constitue la nouvelle épine dorsale du système Control Manager.</p> <p>Les agents MCP sont installés en même temps que les produits gérés et communiquent en mode unidirectionnel ou bidirectionnel avec Control Manager. Les agents MCP demandent des instructions et des mises à jour à Control Manager.</p>
Trend Micro Management Infrastructure	<p>Gère les interactions du serveur Control Manager avec les produits gérés antérieurs.</p> <p>Le communicateur ou le module Message Routing Framework correspond à la dorsale de communication de l'ancien système Control Manager. Il s'agit d'un composant de TMI (Trend Micro Management Infrastructure). Les communicateurs gèrent toutes les communications entre le serveur Control Manager et les produits gérés plus anciens. Ils interagissent avec les agents Control Manager 2.x pour communiquer avec les produits gérés plus anciens.</p>
Agents Control Manager 2.x	<p>Un agent reçoit des commandes du serveur Control Manager et lui renvoie des informations d'état et des journaux.</p> <p>L'agent Control Manager est une application installée sur un serveur de produits gérés qui permet à Control Manager de gérer le produit auquel il est associé. Les agents interagissent avec le produit géré et le communicateur. Un agent sert de « pont » entre un produit géré et le communicateur. Vous devez donc installer les agents sur le même ordinateur que les produits gérés.</p>

COMPOSANT	DESCRIPTION
Console d'administration à interface Web	<p>Elle permet à un administrateur de gérer Control Manager depuis pratiquement n'importe quel ordinateur disposant d'une connexion Internet et du navigateur Windows™ Internet Explorer™</p> <p>La console d'administration de Control Manager est une console à interface Web publiée sur Internet via Microsoft Internet Information Server (IIS) et hébergée par le serveur Control Manager. Elle vous permet d'administrer le réseau Control Manager à l'aide d'un navigateur Web compatible à partir de n'importe quel ordinateur.</p>
Infrastructure de widgets	Permet à l'administrateur de créer un tableau de bord personnalisé afin de surveiller le réseau Control Manager.

Trend Micro™ Smart Protection Network™

Trend Micro™ Smart Protection Network™ est une infrastructure de sécurité du contenu en ligne de nouvelle génération conçue pour protéger les clients contre les risques de sécurité et les menaces Web. Il repose sur des solutions à la fois sur site et Trend Micro hébergées pour protéger les utilisateurs, qu'ils se trouvent sur le réseau, chez eux ou en voyage. Smart Protection Network utilise des clients légers pour accéder à un ensemble unique de technologies en ligne de corrélation d'e-mail, de réputation de fichiers de sites Web et de bases de données de menaces. La protection des clients est automatiquement mise à jour et renforcée, au fur et à mesure que le nombre de produits, services et utilisateurs accédant au réseau augmente. Elle constitue ainsi un service de protection de voisinage en temps réel pour ses utilisateurs.

Réputation des e-mails

La technologie de réputation des e-mails Trend Micro valide les adresses IP en les vérifiant par rapport à une base de données de réputation contenant des sources de spams connues et en utilisant un service dynamique capable d'évaluer la réputation de l'expéditeur d'un e-mail en temps réel. L'évaluation de la réputation est affinée grâce à une analyse en continu du « comportement » des adresses IP, de leur champ d'activité et de leur historique. La réputation des e-mails bloque les messages électroniques

malveillants sur Internet en fonction de l'adresse IP de l'expéditeur, en empêchant les menaces d'accéder au réseau ou à l'ordinateur de l'utilisateur.

Services de File Reputation

Les services de File Reputation vérifient la réputation de chaque fichier par rapport à une base de données en ligne étendue. Les informations sur les programmes malveillants étant stockées en ligne, elles sont immédiatement disponibles pour tous les utilisateurs. Les réseaux fournisseurs de contenu et les serveurs de cache locaux hautes performances garantissent un temps de latence minimum lors du processus de vérification. L'architecture de client en ligne procure une protection immédiate et élimine la contrainte liée au déploiement de fichiers de signatures tout en réduisant sensiblement l'encombrement sur le client.

Services de réputation de sites Web

Dotée de l'une des plus grandes bases de données de réputation de domaine du monde, la technologie de réputation de sites Web de Trend Micro assure le suivi de la crédibilité des domaines Web en attribuant un score de réputation dépendant de facteurs tels que l'ancienneté du site Web concerné, l'historique de ses changements d'emplacement et les indications d'activités suspectes mises en lumière par l'analyse de comportement des programmes malveillants. La fonction Réputation de sites Web continue ensuite à scanner les sites et à bloquer l'accès des utilisateurs aux sites infectés. Les fonctionnalités de réputation de sites Web permettent de garantir que les pages consultées par les utilisateurs sont sûres et exemptes de menaces Web, telles que les programmes malveillants, les spywares et les attaques de phishing visant à duper les utilisateurs afin de leur faire divulguer des informations personnelles. Pour augmenter la précision et réduire le nombre de faux positifs, la technologie de réputation de sites Web Trend Micro affecte des scores de réputation à des pages ou des liens spécifiques au sein même des sites, au lieu de classer ou de bloquer l'intégralité des sites. En effet, il arrive souvent que seules des parties de sites légitimes soient piratées et que les réputations puissent changer dynamiquement au cours du temps.

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 24 heures sur 24 et 7 jours sur 7. Chaque nouvelle menace identifiée par un contrôle de réputation de routine d'un seul client met automatiquement à jour toutes les bases de données de menaces de Trend Micro, et empêche que cette menace ne survienne à nouveau chez un autre client.

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

Chapitre 2

Planification et implémentation du déploiement de Control Manager

Les administrateurs doivent tenir compte de plusieurs facteurs avant de déployer Control Manager sur leur réseau. Ce chapitre explique comment planifier le déploiement de Control Manager et gérer un déploiement de test.

Ce chapitre traite les rubriques suivantes :

- *Identification de l'architecture et de la stratégie de déploiement à la page 2-3*
- *Définition du déploiement sur site unique à la page 2-4*
- *Définition du déploiement sur plusieurs sites à la page 2-6*
- *Déroulement de l'installation de Control Manager à la page 2-12*
- *Test de Control Manager sur un site à la page 2-12*
- *Plan de distribution des serveurs à la page 2-15*
- *Plan de trafic réseau à la page 2-17*
- *Sources du trafic réseau à la page 2-17*
- *Déploiement des mises à jour à la page 2-23*
- *Plan de stockage des données à la page 2-24*

- *Plan de serveur Web à la page 2-25*

Identification de l'architecture et de la stratégie de déploiement

Le déploiement consiste à distribuer stratégiquement des serveurs Control Manager dans votre environnement de réseau pour faciliter et gérer de façon optimale des produits antivirus et de sécurité de contenu.

Le déploiement de logiciels client-serveur, tels que Control Manager, à l'échelle de l'entreprise au sein d'un réseau, exige une planification et une évaluation correctes.

Pour faciliter la planification, Trend Micro recommande deux architectures de déploiement.

- **Déploiement sur site unique** : Suppose la distribution et la gestion de serveurs enfants, de produits gérés et de points finaux à partir d'un seul Control Manager situé dans un bureau central. Si votre entreprise possède plusieurs bureaux et que les connexions de réseau local ou de réseau étendu entre les sites correspondants sont rapides et fiables, le déploiement sur site unique s'applique quand même à votre environnement.
- **Déploiement sur plusieurs sites** : Suppose la distribution et la gestion de serveurs Control Manager dans une entreprise dont les principaux bureaux sont répartis sur différents sites géographiques.



Conseil

Si vous utilisez Control Manager pour la première fois, Trend Micro recommande d'utiliser un serveur Control Manager Advanced parent pour gérer les déploiements sur site unique et sur plusieurs sites.

Définition du déploiement sur site unique

Le déploiement sur site unique suppose la distribution et la gestion de serveurs enfants, de produits gérés et de points finaux à partir d'un seul Control Manager situé dans un bureau central.

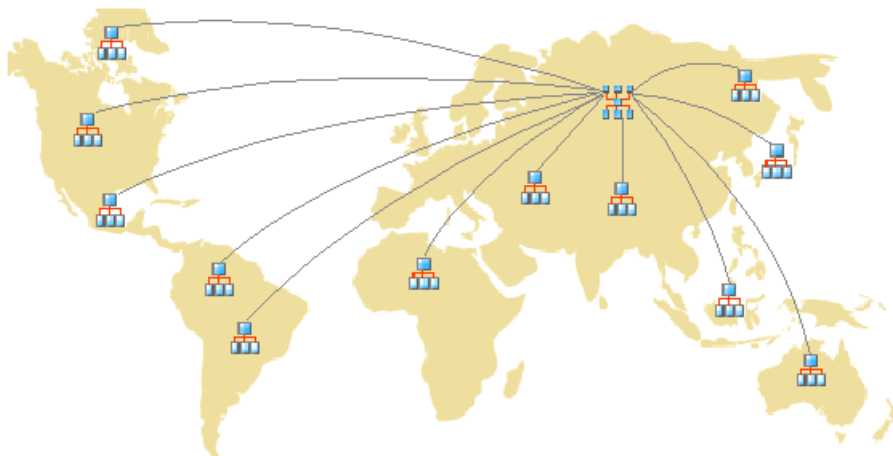


FIGURE 2-1. Déploiement mono-serveur à l'aide d'un serveur Control Manager Advanced parent et de serveurs enfants mixtes

Avant de déployer Control Manager sur un site unique, effectuez les tâches suivantes :

1. Déterminez le nombre de produits gérés, de points finaux et de structures en cascade
2. Planifiez les ratios optimaux pour :
 - Produits gérés par le serveur vers des structures en cascade
 - Points finaux du serveur vers des structures en cascade
3. Sélectionnez le serveur Control Manager Standard ou Control Manager Advanced.

**Remarque**

Control Manager 6.0 Advanced prend en charge les produits suivants en tant que serveurs Control Manager enfants :

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Les serveurs Control Manager 5.0/5.5/6.0 Standard ne peuvent pas être des serveurs enfants.

Détermination du nombre de produits gérés, de points finaux et de structures en cascade

Déterminez le nombre de produits gérés, de points finaux et de structures en cascade que vous envisagez de gérer avec Control Manager. Cette information vous sera utile pour décider quel type et quel nombre de serveurs Control Manager vous devrez déployer et à quel endroit les installer sur votre réseau pour optimiser la communication et la gestion.

Planification afin d'obtenir des ratios optimaux entre les produits gérés par le serveur/points finaux du serveur et les structures en cascade

Lorsque vous déterminez le nombre de produits gérés, de points finaux et de structures en cascade qu'un serveur Control Manager peut gérer sur un réseau local, la communication entre agent et serveur ou entre serveur parent et serveur enfant est le facteur le plus important à prendre en compte.

Basez-vous sur la configuration système recommandée pour déterminer l'unité centrale et la mémoire vive nécessaires à votre réseau Control Manager.

Désignation des serveurs Control Manager

Selon le nombre de produits gérés, de points finaux et de structures en cascade que vous avez définis, décidez quel serveur vous allez utiliser comme serveur Control Manager. Sélectionnez un serveur Standard ou Advanced.

Repérez où se trouvent vos serveurs Windows, puis sélectionnez ceux que vous voulez définir comme serveurs Control Manager. Vous devez également déterminer si vous devez installer un serveur dédié.

Lorsque vous sélectionnez un serveur pour héberger Control Manager, tenez compte de ce qui suit :

- La charge du processeur
- D'autres fonctions assumées par le serveur

Si vous installez Control Manager sur un serveur qui est utilisé à d'autres fins (par exemple un serveur d'application), Trend Micro vous conseille de réaliser l'installation sur un serveur qui n'exécute pas d'applications critiques ou qui ne nécessite pas de ressources importantes.

Selon la typologie de votre réseau, vous devrez éventuellement effectuer d'autres tâches propres à votre site.

Définition du déploiement sur plusieurs sites

Comme pour un déploiement sur un seul site, collectez les informations pertinentes sur le réseau et retenez celles qui vous seront utiles pour déployer Control Manager sur les différents sites.

Chaque réseau ayant ses caractéristiques propres, évaluez au mieux le nombre optimal de serveurs Control Manager.

Déployez les serveurs Control Manager sur plusieurs sites, y compris sur la zone DMZ (ou zone démilitarisée) ou le réseau privé. Placez le serveur Control Manager dans la zone démilitarisée sur le réseau public pour administrer les produits gérés, les points

finaux ou les serveurs enfants et accéder à la console Web de Control Manager à l'aide d'Internet Explorer sur Internet.

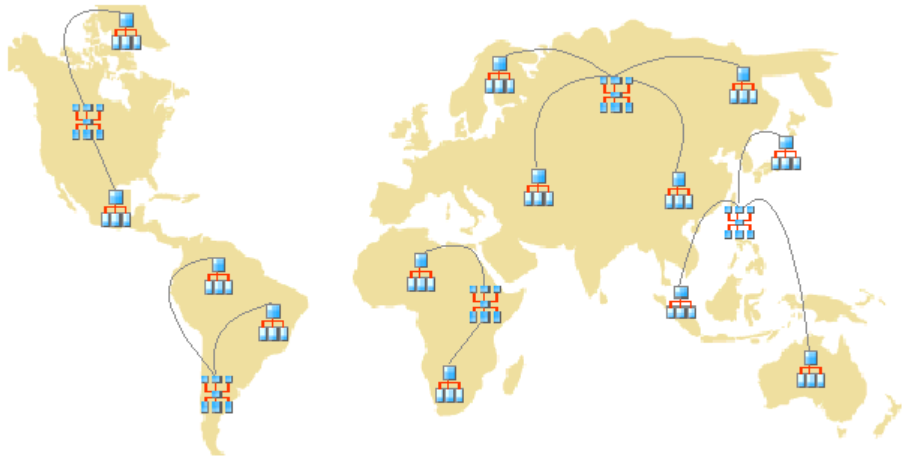


FIGURE 2-2. Déploiement sur plusieurs sites à l'aide de plusieurs serveurs Control Manager Advanced parents et de serveurs enfants mixtes

Tenez compte des points suivants lors d'un déploiement sur plusieurs sites :

- Regroupez des produits gérés, des points finaux ou des serveurs enfants
- Déterminez le nombre de sites.
- Déterminez le nombre de produits gérés, de points finaux et de serveurs enfants
- Prévoyez le trafic réseau.
- Planifiez les ratios optimaux pour :
 - Produits gérés par le serveur vers des structures en cascade
 - Points finaux du serveur vers des structures en cascade
- Décidez de l'emplacement où vous allez installer le serveur Control Manager.

Regroupement de produits gérés, de points finaux ou de serveurs enfants

Tenez compte des éléments suivants lorsque vous regroupez des produits gérés et des serveurs enfants :

TABLEAU 2-1. Éléments à prendre en compte pour regrouper des produits gérés ou des serveurs enfants

ÉLÉMENT	DESCRIPTION
Réseau et stratégies de sécurité de l'entreprise	Si des droits d'accès et de partage différents s'appliquent au réseau de l'entreprise, regroupez les produits gérés, les points finaux et les serveurs enfants en fonction du réseau et des stratégies de sécurité de l'entreprise.
Organisation et fonction	Regroupez les produits gérés, les points finaux et les serveurs enfants en fonction de la structure organisationnelle et fonctionnelle de l'entreprise. Par exemple, définissez deux serveurs Control Manager pour gérer les groupes de production et de test.
Emplacement géographique	Utilisez l'emplacement géographique comme critère de regroupement si l'emplacement des produits gérés, des points finaux et des serveurs enfants a un impact sur la communication entre le serveur Control Manager et ses produits gérés ou ses serveurs enfants.
Responsabilité administrative	Regroupez les produits gérés, les points finaux et les serveurs enfants en fonction du système ou du personnel de sécurité qui lui est affecté. Cela permet une configuration de groupes.

Détermination du nombre de sites

Déterminez le nombre de sites couverts par votre déploiement Control Manager. Cette information vous permettra de déterminer le nombre de serveurs à installer et les emplacements où vous devrez les installer.

Vous pourrez trouver cette information dans les schémas de topologie de réseau étendu (WAN) ou réseau local (LAN) de votre entreprise.

Détermination du nombre de produits gérés, de points finaux et de serveurs enfants

Vous devez également connaître le nombre de produits gérés, de points finaux et de serveurs enfants qui seront gérés par le serveur Control Manager. Trend Micro conseille de réunir des données sur la population des produits gérés, des points finaux et des serveurs enfants site par site. Si vous ne pouvez pas obtenir cette information, des estimations même approximatives seront utiles. Cette information vous permettra de déterminer le nombre de serveurs à installer.

Planification afin d'obtenir un ratio optimal entre les produits gérés par le serveur/ points finaux du serveur et la structure en cascade

Lorsque Control Manager est déployé sur un réseau étendu, le serveur Control Manager du bureau principal administre les produits gérés, les points finaux et les serveurs enfants du bureau distant. Si vous souhaitez que des produits gérés, des points finaux ou des serveurs enfants du bureau distant communiquent des informations au serveur du bureau principal sur le réseau étendu, vous devez tenir compte de la diversité de la bande passante du réseau dans l'environnement du réseau étendu. La coexistence de plusieurs bandes passantes de réseau dans cet environnement peut présenter certains avantages pour Control Manager. Si des produits gérés, des points finaux ou des serveurs enfants figurant à la fois sur le réseau local et le réseau étendu communiquent leurs données au même serveur, ces communications sont échelonnées naturellement. En effet, le serveur donne la priorité à ceux dont la connexion est plus rapide, ce qui est le cas, la plupart du temps, pour les produits gérés ou les serveurs enfants sur le réseau local.

Basez-vous sur la configuration système recommandée pour déterminer l'unité centrale et la mémoire vive nécessaires à votre réseau Control Manager.

Désignation des serveurs Control Manager

Selon le nombre de produits gérés, de points finaux et de structures en cascade que vous avez définis, décidez quel serveur vous allez utiliser comme serveur Control Manager.

Repérez où se trouvent vos serveurs Windows, puis sélectionnez ceux que vous voulez définir comme serveurs Control Manager. Vous devez également déterminer si vous devez installer un serveur dédié.

Lorsque vous sélectionnez un serveur pour héberger Control Manager, tenez compte de ce qui suit :

- La charge du processeur
- D'autres fonctions assumées par le serveur

Si vous installez Control Manager sur un serveur qui est utilisé à d'autres fins (par exemple un serveur d'application), Trend Micro vous conseille de réaliser l'installation sur un serveur qui n'exécute pas d'applications critiques ou nécessitant des ressources importantes.

Choix de l'emplacement d'installation du serveur Control Manager

Après avoir déterminé le nombre de clients et le nombre de serveurs à installer, vous devez décider de l'emplacement où vous allez installer les serveurs Control Manager. Décidez d'installer la totalité des serveurs dans le bureau central ou seulement certains d'entre eux dans des bureaux distants.

Déployez les serveurs stratégiquement sur certains segments de votre environnement pour accélérer les communications et optimiser la gestion des produits gérés, des points finaux et des serveurs enfants.

- **Bureau central** : Un bureau central est une entité physique où se trouvent la plupart des produits gérés, des points finaux et des serveurs enfants de l'entreprise. Le bureau central est parfois désigné par les termes siège, siège de la société ou

siège social. Un bureau central peut avoir d'autres bureaux plus petits ou succursales (appelés « bureaux distants » dans ce manuel) implantés sur d'autres sites géographiques.



Conseil

Trend Micro recommande d'installer un serveur parent dans le bureau central.

- **Bureau distant** : Un bureau distant correspond à une entité professionnelle de petite taille appartenant à une structure plus importante et reliée au bureau central par une connexion de réseau étendu. Si des produits gérés, des points finaux et des serveurs enfants d'un bureau distant communiquent avec le serveur du bureau central, ils risquent de rencontrer des difficultés pour s'y connecter. Des limitations de bande passante peuvent gêner la communication à partir ou à destination du serveur Control Manager.

Si la bande passante du réseau entre le bureau central et le bureau distant peut suffire pour des communications client-serveur de routine (notifications de mise à jour de paramètres de configuration, envoi d'informations d'état, par exemple), elle peut s'avérer insuffisante pour le déploiement et d'autres tâches.

Prévision du trafic réseau

Control Manager génère du trafic réseau lors des communications entre le serveur et les produits gérés/points finaux/serveurs enfants. Prenez en compte ce trafic réseau pour minimiser l'impact sur le réseau de l'entreprise.

Les sources du trafic réseau généré par Control Manager sont les suivantes :

- Battement de cœur
- Journaux
- Programmation de communicateur
- Enregistrement de produits gérés sur le serveur Control Manager

Par défaut, les serveurs Control Manager contiennent tous les profils de produits disponibles lors de la publication de Control Manager. Toutefois, si vous enregistrez une nouvelle version d'un produit dans Control Manager, et que cette

version ne correspond à aucun des profils de produits existants, le nouveau produit téléchargera son profil sur le serveur Control Manager.

Trend Micro fournit des mises à jour permettant à Control Manager d'identifier les nouveaux produits Trend Micro pour lesquels aucun profil de produit n'est disponible.

- Enregistrement d'un serveur enfant sur un serveur parent Control Manager
- Téléchargement et déploiement de mises à jour
- Déploiement de stratégies

Déroulement de l'installation de Control Manager

La procédure d'installation d'un système Control Manager comprend les étapes suivantes :

1. Planification de l'installation du système Control Manager (distribution des serveurs, trafic réseau, stockage des données, serveurs Web).
2. Installation du serveur Control Manager.



Remarque

Au cours de l'installation du serveur Control Manager, prévoyez un emplacement de sauvegarde et de restauration des fichiers.

Test de Control Manager sur un site

Un déploiement pilote permet de faire remonter les problèmes détectés lors du test des fonctionnalités du système, et de déterminer le niveau d'assistance dont vous aurez besoin après le déploiement complet.

**Conseil**

Trend Micro conseille de réaliser un déploiement pilote avant de procéder au déploiement complet.

Le déploiement pilote de Control Manager sur un site vous permettra de :

- Vous familiariser avec Control Manager et les produits gérés
- Développer ou affiner les stratégies du réseau de l'entreprise.

Un déploiement pilote permet de déterminer quelles configurations doivent être améliorées. Il donne aussi au service informatique ou à l'équipe chargée de l'installation la possibilité de répéter et d'affiner le processus de déploiement. Le déploiement pilote permet également de vérifier si votre plan de déploiement correspond aux besoins opérationnels de votre entreprise.

Le déploiement test de Control Manager implique les tâches suivantes :

- Préparation du test de déploiement
- Sélection d'un site de test
- Création d'un plan de rétrogradation
- Initialisation du déploiement test
- Évaluation du déploiement test

Préparation du déploiement test

Réalisation des activités suivantes lors de la phase de préparation.

Procédure

1. Choix du serveur Control Manager et de la configuration d'agent pour l'environnement de test.
 - Établissement de la connectivité TCP/IP entre tous les systèmes dans une configuration de test.

- Vérification des communications bidirectionnelles sur TCP/IP à l'aide d'une commande ping envoyée à chaque système agent à partir du système Control Manager et inversement.
2. Évaluation des différentes méthodes de déploiement pour déterminer celles qui conviennent à votre environnement spécifique.
 3. Réalisation d'une vérification du déploiement pilote.
-

Sélection d'un site de test

Sélectionnez un site pilote qui corresponde le mieux à votre environnement de production. Essayez de reproduire le plus fidèlement possible la topologie qui reflèterait le mieux votre environnement de production.

Création d'un plan de rétrogradation

Créez un plan anti-sinistre ou de rétrogradation (par exemple, comment revenir à un serveur Control Manager 5.0/5.5) en cas de difficultés lors de l'installation ou d'une mise à niveau. Ce processus doit tenir compte des stratégies locales de la société, ainsi que des ressources informatiques.

Initialisation du déploiement test

Après avoir effectué les étapes préparatoires et vérifié la liste de contrôle du système, installez le serveur et les agents Control Manager pour commencer le déploiement pilote.

Évaluation du déploiement test

Recensez les opérations qui ont abouti et celles qui ont échoué pendant le déploiement test. Identifiez les *pièges* potentiels et établissez un plan en conséquence afin de réussir votre déploiement.

Vous pouvez implémenter le plan d'évaluation du déploiement pilote dans le plan général de déploiement et d'installation dans l'environnement de production.

Plan de distribution des serveurs

Prenez en compte ce qui suit en planifiant la distribution des serveurs :

- Modèles d'administration
- Distribution du serveur Control Manager
- Topologie à un seul serveur
- Topologie à plusieurs serveurs

Définition des modèles d'administration

Au début du déploiement de Control Manager, déterminez le nombre exact d'utilisateurs que vous voulez autoriser à accéder au serveur Control Manager. Le nombre d'utilisateurs dépend du niveau de centralisation que vous souhaitez appliquer à la gestion. Le principe directeur étant : plus la gestion est centralisée, moins le nombre d'utilisateurs autorisés en accès est important.

Appliquez l'un des modèles d'administration suivants :

- **Gestion centralisée** : Ce modèle restreint au maximum le nombre d'utilisateurs autorisés à accéder au Control Manager. Sur un réseau fortement centralisé, un seul administrateur serait responsable de la gestion de la totalité des serveurs antivirus et de sécurité de contenu sur le réseau.

La gestion centralisée permet de contrôler de la façon la plus stricte la stratégie antivirus et de sécurité de contenu d'un réseau. Toutefois, à mesure que les réseaux deviennent plus complexes, un seul administrateur risque de ne plus suffire pour effectuer toutes les tâches administratives.

- **Gestion décentralisée** : ce modèle convient à des réseaux importants où les administrateurs système ont clairement défini et délimité leurs domaines de responsabilité. Ainsi, l'administrateur du serveur de messagerie peut également être

responsable de la protection du courrier électronique, et chaque bureau régional peut être responsable à son niveau de son domaine local.

La nomination d'un administrateur principal de Control Manager reste nécessaire. Il doit néanmoins être coresponsable de la supervision du réseau avec d'autres administrateurs de produits ou des administrateurs régionaux.

Accordez l'accès à Control Manager à tous les administrateurs, mais limitez les droits d'accès d'affichage et/ou de configuration des segments du réseau Control Manager dont ils ont la responsabilité.

Après avoir initialisé l'un de ces modèles d'administration, vous pouvez configurer le répertoire Produits et les comptes utilisateurs nécessaires à la gestion du réseau Control Manager.

Définition de la distribution des serveurs Control Manager

Control Manager peut gérer des produits indépendamment de leur emplacement physique. Il permet de gérer tous vos produits antivirus et de sécurité de contenu à partir d'un seul serveur Control Manager.

La répartition du contrôle du réseau Control Manager entre plusieurs serveurs (dont des serveurs parents et enfants pour les utilisateurs de la version Advanced) présente des avantages. Selon les caractéristiques propres à votre réseau, vous pouvez décider du nombre optimal de serveurs Control Manager.

Topologie à un seul serveur

La topologie à un seul serveur est adaptée aux petites et moyennes entreprises implantées sur un seul site. Si sa gestion par un seul administrateur est facilitée, cette topologie n'interdit pas la création d'autres comptes administrateurs tels qu'ils sont prescrits dans votre plan d'administration.

Toutefois, dans cette configuration, la charge du trafic réseau (interrogation des agents, transfert de données, déploiement de mises à jour, etc.) est concentrée sur un seul serveur et sur le réseau local qui l'héberge. L'impact sur les performances du réseau s'amplifie à mesure que le réseau se développe.

Topologie à plusieurs serveurs

Pour des entreprises plus grandes implantées sur plusieurs sites, il peut être nécessaire de créer des serveurs Control Manager régionaux pour répartir la charge du réseau.

Pour plus d'informations sur le trafic généré par un réseau Control Manager, consultez la section *Définition du trafic généré sur un réseau Control Manager à la page 2-17*.

Plan de trafic réseau

Il est important de comprendre le trafic généré sur un réseau Control Manager pour pouvoir mettre au point un plan visant à en réduire l'impact.

La section suivante explique comment le réseau Control Manager génère du trafic et comment mettre au point un plan pour en réduire son impact sur votre réseau. En outre, la section relative à la fréquence du trafic décrit les sources qui génèrent habituellement du trafic sur un réseau Control Manager.

Définition du trafic généré sur un réseau Control Manager

Il est important de comprendre le trafic généré sur un réseau Control Manager pour pouvoir mettre au point un plan visant à en réduire l'impact.

Sources du trafic réseau

Le trafic réseau est généré par les sources Control Manager suivantes :

- Trafic généré par les journaux
- Stratégies Trend Micro Management Infrastructure et MCP
- Enregistrement de produits
- Téléchargement et déploiement de mises à jour
- Déploiement des paramètres de stratégie

Fréquence du trafic

Les sources qui génèrent fréquemment du trafic sur un réseau Control Manager sont les suivantes :

- Journaux générés par les produits gérés
- Interrogation et commandes MCP
- Stratégies Trend Micro Management Infrastructure

Journaux

Les produits gérés envoient des journaux à Control Manager à différents intervalles, selon leur paramétrage respectif.

Battement de cœur de l'agent de produit géré

Par défaut, les agents de produits gérés envoient des messages de battement de cœur toutes les 60 minutes. Les administrateurs peuvent ajuster cette fréquence à une valeur comprise entre 5 et 480 minutes (soit 8 heures). Lorsque vous définissez la fréquence du battement de cœur, choisissez une valeur qui vous permette d'afficher l'état le plus récent du communicateur et de gérer les ressources système dans les meilleurs délais.

La fréquence par défaut convient à la plupart des situations. Toutefois, si vous devez redéfinir sa valeur, prenez en compte les éléments suivants :

- **Battements de cœurs à intervalle long (supérieur à 60 minutes) :** Plus l'intervalle entre les battements de cœur est long, plus le nombre d'événements susceptibles de se produire avant que la console Control Manager n'affiche l'intervalle peut être important.

Par exemple, si un problème de connexion avec un agent est résolu entre deux battements de cœur, les communications avec un agent redeviennent possibles même si la console indique que son état est *Inactif* ou *Anormal*.

- **Battements de cœurs à intervalle court (inférieur à 60 minutes) :** Les intervalles courts permettent d'obtenir un cliché plus réaliste, car mieux actualisé de l'état du réseau au niveau du serveur Control Manager. L'inconvénient est qu'ils augmentent la consommation de la bande passante de réseau.

**Remarque**

Avant de définir l'intervalle à une valeur inférieure à 15 minutes, analysez le trafic réseau existant pour comprendre l'impact d'une consommation accrue de la bande passante.

Protocoles réseau

Control Manager utilise les protocoles de communication UDP et TCP.

Source du trafic réseau

Trafic généré par les journaux

Les « journaux produit » sont des journaux que les produits gérés envoient régulièrement au serveur Control Manager. Ces journaux génèrent constamment du trafic sur un réseau Control Manager.

TABLEAU 2-2. Trafic généré par les journaux Control Manager

JOURNAL	CONTENU
Virus/programmes espions/graywares	Virus/programmes malveillants, programmes espions/graywares et autres menaces de sécurité détectés
Sécurité	Violations signalées par des produits de sécurité de contenu
Sécurité Web	Violations signalées par des produits de sécurité Web
Événement	Divers événements (mises à jour de composants et violations de sécurité d'ordre général, par exemple).

JOURNAL	CONTENU
État	Environnement d'un produit géré. L'onglet État du répertoire Produits affiche cette information.
Virus réseau	Virus détectés dans des paquets réseau.
Mesures des performances	Utilisé dans des versions de produit précédentes.
Utilisation des URL	Violations signalées par des produits de sécurité Web
Violations de sécurité	Violations signalées par des produits Network VirusWall
Conformité de sécurité	Conformités des points finaux signalées par des produits Network VirusWall
Statistiques de sécurité	Différence entre les conformités de sécurité et les violations de sécurité calculées et signalées par des produits Network VirusWall.
Point final	Violations signalées par des produits de sécurité Web

Stratégies Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) est la partie la plus récente de la dorsale de communication de Control Manager. MCP implémente les stratégies suivantes :

- Battement de cœur MCP** : Les battements de cœur MCP envoyés à Control Manager lui permettent d'afficher les informations les plus récentes et de vérifier que la connexion entre le produit géré et le serveur Control Manager fonctionne correctement.

- **Interrogation de commande MCP** : Lorsqu'un agent MCP lance une interrogation de commande à Control Manager, Control Manager demande à l'agent d'envoyer les journaux du produit géré ou envoie une commande au produit géré. Control Manager interprète également une interrogation de commande comme un battement de cœur passif en vérifiant la connexion entre Control Manager et le produit géré.

Stratégies Trend Micro Management Infrastructure

Trend Micro Management Infrastructure (TMI) fait partie de la dorsale de communication de Control Manager. Il génère son propre trafic de gestion interne. TMI implémente deux stratégies :

- **Battement de cœur du communicateur** : le communicateur, l'infrastructure d'acheminement des messages de TMI, interroge le serveur Control Manager à intervalles réguliers. Cela permet d'afficher les informations les plus récentes sur la console Control Manager et de vérifier que la connexion entre le produit géré et le serveur Control Manager fonctionne correctement.
- **Stratégie heure de travail** : La stratégie heure de travail définit quand un communicateur envoie des informations au serveur Control Manager. Définissez cette stratégie à l'aide du Programmeur de communication. L'utilisateur peut définir trois périodes d'inactivité également appelées périodes off-hour (heure creuse). Deux types d'informations ne sont pas pris en compte par le Programmeur de communication :
 - les messages d'urgence
 - les messages interdits

TMI envoie des messages d'urgence au serveur Control Manager même lorsque le communicateur est dans une période d'heure creuse. Toutefois, TMI n'envoie jamais de messages interdits à Control Manager même si le communicateur est actif.

Trafic généré par l'enregistrement de produits

Un profil de produit indique à Control Manager comment gérer le produit correspondant. Les produits gérés téléchargent des profils sur le serveur Control Manager lorsqu'ils s'enregistrent pour la première fois sur le serveur.

Chaque produit est associé à un profil et dans de nombreux cas, chaque version d'un produit a son propre profil. Un profil contient les informations suivantes :

- Catégorie (par exemple, antivirus)
- Nom du produit
- Version du produit
- Version du menu
- Format du journal
- Informations sur les mises à jour de composant - mises à jour prises en charge par le produit (par exemple, fichiers de signatures de virus)
- Informations de commandes

Par défaut, les serveurs Control Manager contiennent tous les profils des produits disponibles lors de la publication des produits gérés. Toutefois, si une nouvelle version d'un produit est enregistrée dans Control Manager, le nouveau produit télécharge son profil sur le serveur Control Manager.

Déploiement de stratégies

Control Manager génère un trafic réseau en déployant les paramètres de stratégie dans les produits gérés et les points finaux. Le trafic commence à partir des sources suivantes :

- Exécution périodique des stratégies

Control Manager exécute les paramètres de stratégie sur les produits gérés et les points finaux toutes les 60 minutes.

- Informations déployées

Une stratégie comporte les informations d'identifiants globaux uniques (GUID) pour chaque point final et les informations de configuration. Une stratégie comportant 50 000 cibles et un jeu complet de paramètres peut générer jusqu'à 1,8 Mo de trafic réseau.

Déploiement des mises à jour

La procédure de mise à jour d'un réseau Control Manager comporte deux étapes :

1. procurez-vous les composants de mise à jour les plus récents auprès de Trend Micro.

Control Manager peut télécharger des composants directement à partir du serveur de mises à jour Trend Micro ou d'un autre serveur.

2. Déployez ces composants sur les produits gérés.

Control Manager déploie les composants de mise à jour sur des produits gérés avec les éléments suivants :

- Fichiers de signatures/modèles Damage Cleanup
- des moteurs (moteurs de scan et moteurs Damage Cleanup)
- Règles anti-spam
- Programmes Plug-in d'OfficeScan Plug-in Manager
- des programmes de produits (selon le produit)



Conseil

Trend Micro recommande vivement de mettre à jour régulièrement ces composants pour que les produits gérés puissent protéger efficacement le réseau contre les menaces les plus récentes. Pour les mises à jour de programmes de produits, consultez la documentation correspondante.

Le déploiement de mises à jour sur des produits gérés consomme énormément de bande passante. Dans la mesure du possible, il est conseillé de procéder à un déploiement lorsqu'il a le moins d'impact sur le réseau.

Vous pouvez échelonner le déploiement de mises à jour de composants à l'aide de plans de déploiement.

Par ailleurs, vérifiez que la connexion réseau entre le serveur Control Manager et les produits gérés peut prendre en charge les mises à jour. Tenez compte de ce facteur lorsque vous décidez du nombre de serveurs Control Manager à installer sur le réseau.

Plan de stockage des données

Les données de Control Manager doivent être stockées dans une base de données SQL. Lorsque vous installez Control Manager sur un serveur dépourvu de base de données, le programme d'installation vous propose d'installer Microsoft SQL Express. Toutefois, en raison des capacités limitées de SQL Express, un serveur SQL Server devra être installé dans les réseaux importants.



Remarque

Control Manager utilise l'authentification Windows et SQL pour accéder au serveur SQL.

Recommandations pour la base de données

Si vous installez Control Manager et son serveur SQL sur le même ordinateur, configurez le serveur SQL de manière à ce qu'il utilise une taille de mémoire fixe équivalant à deux tiers du volume total de la mémoire sur le serveur. Par exemple, si le serveur est doté de 3Go de mémoire vive, affectez au serveur SQL Server une taille de mémoire fixe de 1Go.

Installez la base de données SQL de Control Manager directement sur le serveur Control Manager ou sur un autre serveur (un serveur SQL dédié, par exemple).

Si Control Manager gère plus de 1000 produits, Trend Micro recommande d'utiliser un serveur SQL dédié.

**Remarque**

Pour obtenir des instructions sur la gestion des ressources SQL ou d'autres recommandations sur la taille de la mémoire, consultez la documentation de Microsoft SQL.

Pilotes ODBC

Control Manager utilise un pilote ODBC pour communiquer avec le serveur SQL. La version 3.7 d'ODBC est suffisante pour la plupart des instances.

Le programme d'installation de Control Manager peut vérifier la version du pilote ODBC si le serveur SQL est installé sur l'ordinateur Control Manager. Pour les serveurs SQL distants, vérifiez le pilote manuellement pour que Control Manager puisse accéder à la base de données.

Authentification

Control Manager utilise une authentification en mode mixte et non pas l'authentification Windows pour accéder à la base de données SQL.

Plan de serveur Web

L'écran d'informations sur le serveur Web qui s'affiche dans le programme d'installation de Control Manager propose les mêmes options d'identification de serveur que l'écran de définition de l'ID hôte : nom d'hôte, nom de domaine complet, ou adresse IP. Dans les deux cas, tenez compte des éléments suivants pour choisir le nom du serveur Web :

- L'utilisation du nom d'hôte ou du nom de domaine complet permet de modifier plus facilement l'adresse IP du serveur Control Manager mais il rend le système dépendant du serveur DNS.
- L'option d'adresse IP exige un IP fixe.

Utilisez l'adresse du serveur Web pour identifier la source des mises à jour de composants. Le fichier `SystemConfiguration.xml` stocke cette information et l'envoie aux agents sous forme de notification pour que ces derniers téléchargent les

mises à jour à partir du serveur Control Manager. Des instructions relatives à la source des mises à jour s'affichent comme suit :

```
Value=http://adresse serveur Web>:port>/TvcsDownload/  
ActiveUpdate/component>
```

où :

- **Port** : désigne le port qui se connecte à la source des mises à jour. Vous pouvez également spécifier cette option dans l'écran de définition de l'adresse du serveur Web (le port par défaut est le port 80).
- **TvcsDownload/ActiveUpdate** : Répertoire virtuel créé par le programme d'installation de Control Manager dans le site Web spécifié par IIS
- **Composant** : désigne le nom du composant mis à jour. Par exemple, lorsque le fichier de signatures de virus est mis à jour, la valeur ajoutée ici est la suivante :

```
Pattern/vsapi.zip
```

Pattern correspond au dossier \\ . . . Control Manager\WebUI\download\activeupdate\pattern qui se trouve sur le serveur Control Manager. Vsapi.zip désigne le fichier de signatures de virus au format compressé.

Chapitre 3

Première installation de Trend Micro Control Manager

Ce chapitre explique la procédure d'installation du serveur Control Manager. Le chapitre contient aussi des informations sur la configuration post-installation ainsi que des instructions sur la manière d'enregistrer et d'activer votre logiciel.

Ce chapitre traite les rubriques suivantes :

- *Configuration système requise à la page 3-2*
- *Installation des composants pré-requis à la page 3-2*
- *À propos de l'installation d'un serveur Control Manager à la page 3-3*
- *Vérification de l'installation correcte du serveur Control Manager à la page 3-23*
- *Configuration après l'installation à la page 3-26*
- *Enregistrement et activation de votre logiciel à la page 3-28*

Configuration système requise

Chaque réseau d'entreprise comporte ses propres caractéristiques. La configuration système requise d'un réseau dépend donc de son niveau de complexité. Cette section décrit les configurations minimale et recommandée et fournit des conseils d'ordre général et spécifique en fonction de la taille du réseau.

Pour une liste complète de la configuration requise pour une nouvelle installation, consultez le lien suivant :

<http://docs.trendmicro.com/fr-fr/enterprise/control-manager.aspx>



Remarque

Control Manager 6.0 Advanced prend en charge les produits suivants en tant que serveurs Control Manager enfants :

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Les serveurs Control Manager 5.0/5.5/6.0 Standard ne peuvent pas être des serveurs enfants.

Veillez consulter la documentation relative au produit géré pour obtenir des informations détaillées sur la configuration minimale requise d'un agent.

Installation des composants pré-requis

Le tableau suivant liste les composants requis avant de démarrer le programme d'installation de Control Manager. Sans ces composants, le processus d'installation ne peut pas être exécuté.

TABLEAU 3-1. Composants pré-requis

PLATE-FORME	COMPOSANTS
Windows 2003 Server	<ul style="list-style-type: none"> • .Net Framework 3.5 SP1* • Microsoft Message Queuing • Windows Installer 4.5*
Windows 2008 Server	<ul style="list-style-type: none"> • Composants IIS 6 Management Compatibility • Module d'authentification Windows IIS • IIS ASP.NET • .Net Framework 3.5 SP1* • Microsoft Message Queuing

Les composants ayant un astérisque (*) sont uniquement obligatoires si les administrateurs veulent utiliser SQL 2008 Express sur le serveur.

À propos de l'installation d'un serveur Control Manager

Après avoir décidé de la topologie à adopter pour votre réseau, vous pouvez commencer à installer le serveur Control Manager. Pour vous aider à recenser les informations nécessaires à l'installation, consultez la section [Liste de contrôle de l'adresse du serveur à la page A-2](#).

Vous devez réunir les informations suivantes avant de procéder à l'installation :

- Adresse et port du serveur cible concerné
- Clé d'enregistrement de Control Manager
- Niveau de sécurité à appliquer aux communications entre serveur et agent

Tenez compte des éléments suivants relatifs à la base de données :

- Décidez si vous voulez utiliser un serveur SQL avec Control Manager. Si le serveur SQL se trouve sur un autre serveur que le serveur Control Manager, recherchez

son adresse IP, son nom de domaine complet ou son nom NetBIOS. S'il existe plusieurs instances du serveur SQL, identifiez celle que vous souhaitez utiliser.

- Préparez les informations suivantes sur la base de données SQL de Control Manager :
 - Nom d'utilisateur à spécifier pour accéder à la base de données
 - Mot de passe



Remarque

Control Manager utilise les authentifications Windows et SQL pour accéder au serveur SQL.

- Déterminez le nombre de produits gérés qui seront pris en charge par Control Manager. Si un serveur SQL n'est pas détecté sur le serveur, Control Manager installera SQL Server 2008 Express, qui ne peut gérer qu'un nombre limité de connexions

Déroulement de l'installation de Control Manager

Les différentes étapes de l'installation de Control Manager sont les suivantes :

1. Installation de tous les composants nécessaires
2. spécification de l'emplacement d'installation
3. enregistrement et activation du produit et des services
4. Spécification des paramètres de sécurité et de serveur Web de Control Manager
5. Spécifiez les paramètres de sauvegarde
6. Configurez les paramètres de notification
7. Configurez les informations relatives à la base de données
8. Installez le compte racine



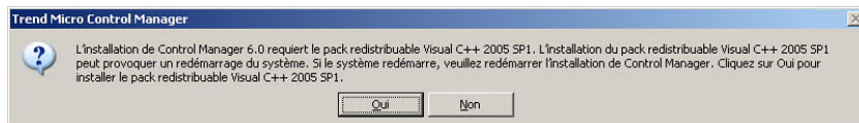
Conseil

Trend Micro vous recommande d'effectuer une mise à niveau vers la version 6.0 plutôt qu'une nouvelle installation.

Installation de tous les composants nécessaires

Procédure

1. Dans la barre des tâches Windows, cliquez sur **Démarrer** > **Exécuter**, puis localisez le programme d'installation de Control Manager (`setup.exe`). Si vous installez le logiciel à partir du DVD Trend Micro Enterprise, accédez au dossier Control Manager de celui-ci. Si vous avez téléchargé le logiciel à partir du site Web de Trend Micro, accédez au dossier correspondant sur votre ordinateur. Le programme d'installation vérifie que votre système dispose des composants nécessaires. Des boîtes de dialogue vous demandant d'installer les composants manquants apparaîtront si le programme d'installation ne détecte pas les composants suivants sur le serveur :
 - **Pack redistribuable Visual C++ 2005 SP1** : ce composant est inclus dans le paquetage d'installation de Control Manager
 - **PHP 5.3.5** : Si le serveur utilise un PHP plus ancien, supprimez-le avant de démarrer l'installation. Control Manager installe ensuite PHP 5.3.5 pendant le processus d'installation.
2. Installation de tous les composants manquants Une fenêtre de confirmation apparaît.



3. Cliquez sur **Oui** pour continuer l'installation. Une autre boîte de dialogue de confirmation apparaît.



4. Cliquez sur **Oui** pour continuer l'installation.

L'écran de **Bienvenue** apparaît.

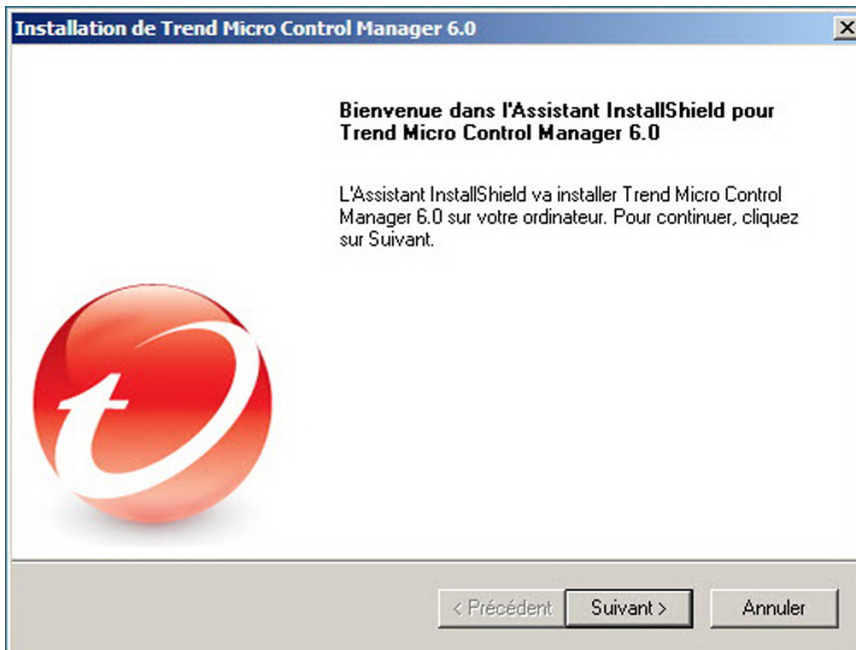


FIGURE 3-1. L'écran Bienvenue

Le programme d'installation vérifie les composants déjà installés pour votre système. Avant de procéder à l'installation, fermez toutes les instances de la console d'administration Microsoft (MMC). Pour plus d'informations sur la migration, consultez la section *Scénarios de migration pour les agents Control Manager 2.x à la page 4-13*.

5. Cliquez sur **Suivant**.

L'écran **Contrat de licence du logiciel** apparaît.

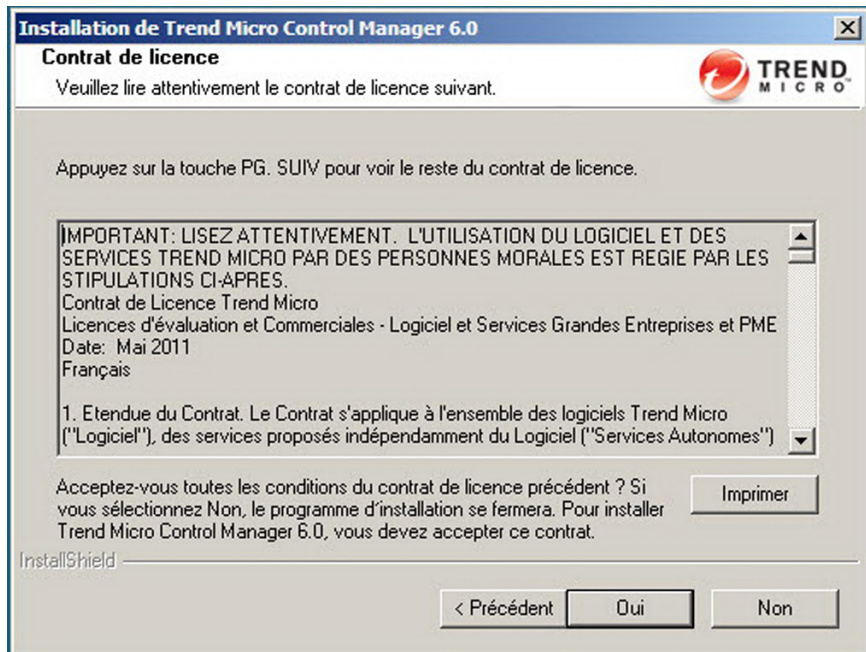


FIGURE 3-2. Acceptez le contrat de licence

6. Cliquez sur **Non** si vous refusez les termes du contrat. Dans ce cas, le programme d'installation s'interrompt. Sinon, cliquez sur **Oui**.
7. (uniquement pour une installation sous Windows 2003, 64 bits) Une boîte de dialogue de confirmation apparaît. Cliquez sur **Oui** pour passer Microsoft IIS en mode 32 bits. Cliquez sur **Non** pour arrêter l'installation.
8. Un écran affiche le récapitulatif des composants détectés.



FIGURE 3-3. Informations sur l'environnement système local

Spécification de l'emplacement d'installation

Procédure

1. Cliquez sur **Suivant**.

L'écran **Sélection d'un dossier de destination** s'affiche.

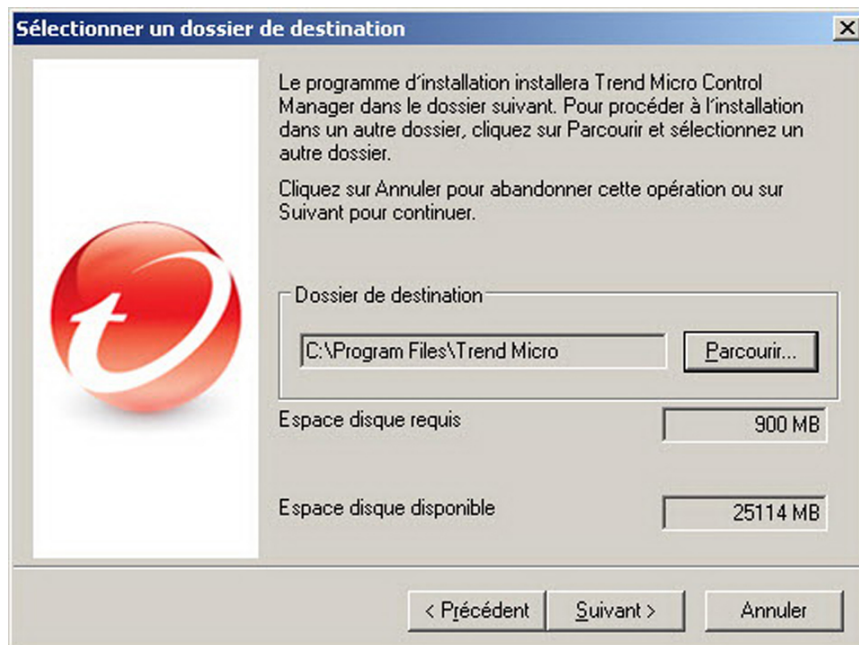


FIGURE 3-4. Sélection d'un dossier de destination

2. Spécifiez le répertoire d'installation des fichiers Control Manager. Le répertoire par défaut est `C:\Program Files\Trend Micro`. Pour changer de répertoire, cliquez sur **Parcourir** et accédez au répertoire souhaité.



Remarque

Le programme d'installation copie les fichiers des modules de communication de Control Manager (Trend Micro Management Infrastructure et MCP) dans des dossiers prédéfinis dans le dossier `Program Files`.

Enregistrement et activation du produit et des services

Procédure

1. Cliquez sur **Suivant**.

L'écran **Activation du produit** apparaît.

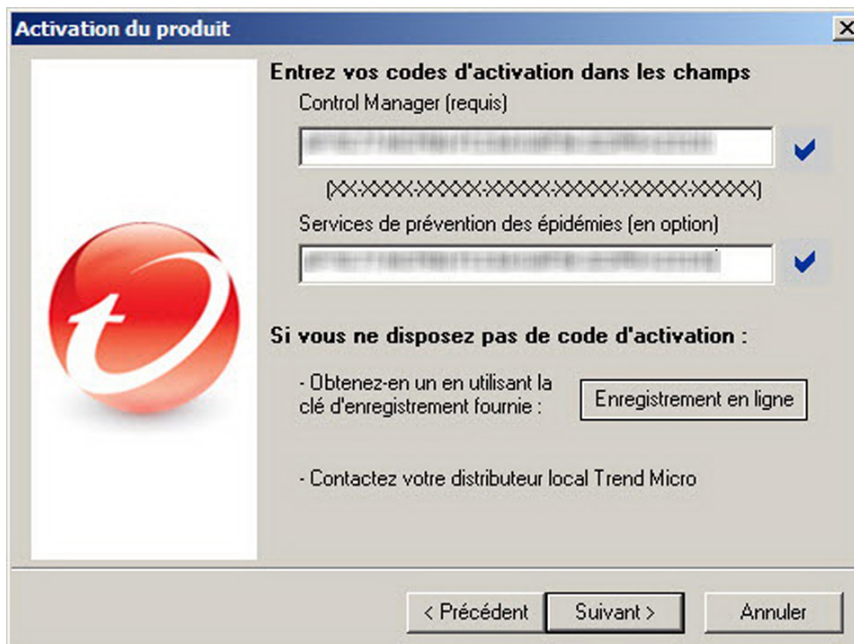


FIGURE 3-5. Indiquez le code d'activation de Control Manager et des services

2. Entrez le code d'activation de Control Manager et celui des autres services que vous avez achetés (vous pouvez également activer des services en option à partir de la console de Control Manager). Pour utiliser toutes les fonctionnalités de Control Manager et des autres services (Outbreak Prevention Services), vous devez obtenir les codes d'activation correspondants pour déverrouiller ces logiciels. Une clé d'enregistrement est fournie avec votre produit. Elle vous sera demandée lorsque vous enregistrez le produit sur le site Web d'enregistrement en ligne de Trend Micro pour obtenir un code d'activation.

3. Cliquez sur **Suivant**.

L'écran **Trend Micro Smart Feedback** s'affiche.

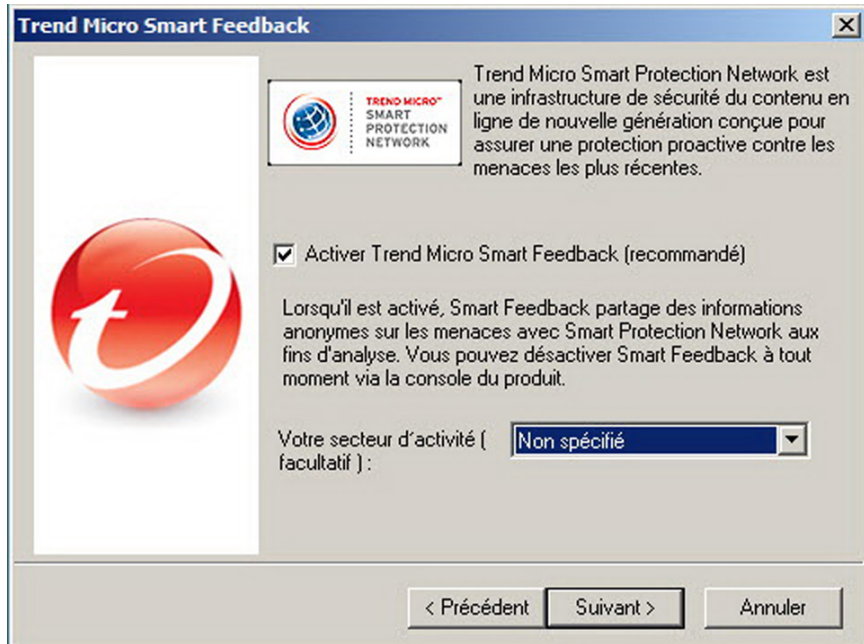


FIGURE 3-6. Paramètres de Smart Protection Network

4. Cochez la case **Activer Trend Micro Smart Feedback** pour participer au programme Smart Protection Network. Si vous choisissez de participer au programme, Control Manager envoie des informations anonymes sur les menaces aux serveurs Trend Micro Smart Protection Network. Votre réseau bénéficie ainsi d'une protection proactive. Vous pouvez vous retirer du programme à tout moment via la console Web de Control Manager.

Spécification des paramètres de sécurité et de serveur Web de Control Manager

Procédure

1. Cliquez sur **Suivant**.

L'écran **Sélectionner un niveau de sécurité et l'adresse de l'hôte** s'affiche.

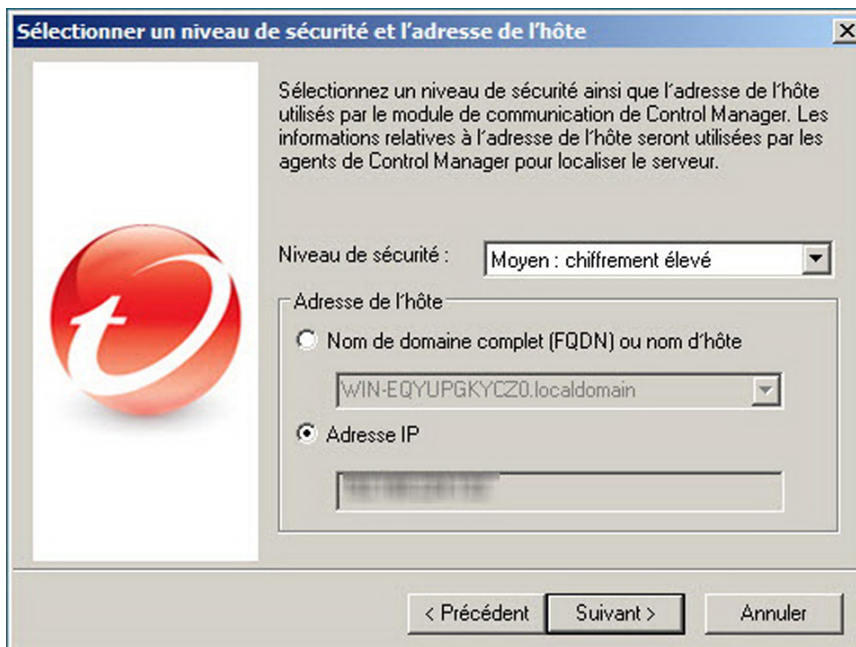


FIGURE 3-7. Sélection du niveau de sécurité

2. Dans la liste Niveau de sécurité, sélectionnez le niveau pour les communications de Control Manager avec les agents. Les options sont les suivantes :
 - **Élevé** : Toutes les communications entre Control Manager et les produits gérés utilisent le chiffrement 128 bits avec authentification. Cette option permet de sécuriser au maximum les communications entre Control Manager et les produits gérés.

- **Moyen** : Toutes les communications entre Control Manager et les produits gérés utilisent le chiffrement 128 bits. Cette option est définie par défaut lors de l'installation de Control Manager.
 - **Faible** : toutes les communications entre Control Manager et les produits gérés utilisent le chiffrement 40 bits avec authentification. Cette option correspond au niveau de sécurité le plus faible pour les communications entre Control Manager et d'autres produits.
3. Sélectionnez une adresse d'hôte pour que les agents puissent communiquer avec Control Manager :
- FDQN/Nom d'hôte
 - a. Sélectionnez **Nom de domaine complet (FQDN) ou nom d'hôte**.
 - b. Sélectionnez ou entrez un nom de domaine complet ou un nom d'hôte dans le champ correspondant.
 - Adresse IP
 - a. Sélectionnez **Adresse IP**.

Le champ de l'adresse IP affiche par défaut une adresse IPv4. Si les utilisateurs installent Control Manager sur un serveur IPv6 pur, le champ de l'adresse IP affiche l'adresse locale IPv4 (127.0.0.1).
4. Cliquez sur **Suivant**.
- L'écran **Spécifier les informations relatives au serveur Web** s'affiche.

Les paramètres de l'écran **Spécifier les informations relatives au serveur Web** définissent la sécurité des communications et la méthode utilisée par le réseau Control Manager pour identifier le serveur.

Spécifiez l'adresse de l'hôte pour le serveur Control Manager.

Informations sur le site Web

Site Web : Default Web Site

Adresse IP :

Port TCP : 80 Port SSL : 443

Niveau de sécurité pour la connexion Internet : Moyen : HTTPS principale

Le port SSL est requis pour les niveaux de sécurité moyen et élevé.

Si aucune adresse IP n'est attribuée dans IIS, sélectionnez une adresse IP ou un nom de domaine complet (FQDN). La sélection ne modifie pas la configuration IIS.

< Précédent Suivant > Annuler

FIGURE 3-8. Spécifier les informations relatives au serveur Web

5. Dans la liste **Site Web**, sélectionnez le site Web permettant d'accéder à Control Manager.
6. Dans la liste des adresses IP, sélectionnez l'adresse IPv6, IPv4 ou le nom de domaine complet/nom d'hôte à utiliser pour la console d'administration de Control Manager. Ce paramètre définit comment le système de communication de Control Manager identifie le serveur Control Manager. Le programme d'installation recherche le nom de domaine complet (FQDN) et l'adresse IP du serveur et les affiche dans les champs correspondants.

Si le serveur est équipé de plusieurs cartes d'interface réseau ou si vous attribuez plusieurs noms de domaine complets au serveur, les noms et les adresses IP

correspondants s'affichent ici. Sélectionnez le nom d'hôte ou l'adresse IP les plus appropriés en sélectionnant l'option correspondante dans la liste.

Si vous identifiez le serveur par son nom d'hôte ou son nom de domaine complet, vérifiez que ce nom peut être résolu sur les ordinateurs équipés des produits. Si ce n'est pas le cas, les produits ne pourront pas communiquer avec le serveur Control Manager.

7. Dans la liste Niveau de sécurité pour la connexion Internet, sélectionnez le niveau de sécurité pour les communications de Control Manager. Les options sont les suivantes :
 - **Élevé : HTTPS uniquement** : toutes les communications de Control Manager utilisent le protocole HTTPS. Cette option permet de sécuriser au maximum les communications entre Control Manager et les autres produits.
 - **Moyen : HTTPS principalement** : Toutes les communications de Control Manager utilisent le protocole HTTPS s'il est pris en charge. Si le protocole HTTPS n'est pas disponible, les agents utilisent le protocole HTTP. Cette option est définie par défaut lors de l'installation de Control Manager.
 - **Faible : basé sur HTTP** : toutes les communications de Control Manager utilisent le protocole HTTP. Cette option correspond au niveau de sécurité le plus faible pour les communications entre Control Manager et d'autres produits.
 8. Si vous avez sélectionné **Faible : basé sur HTTP** et si vous n'avez pas défini la valeur du port SSL dans la console d'administration IIS, spécifiez le port d'accès pour les communications de Control Manager dans le champ **Port SSL**.
-

Spécification des paramètres de sauvegarde

Procédure

1. Cliquez sur **Suivant**.

L'écran **Choisir l'emplacement de destination** apparaît.

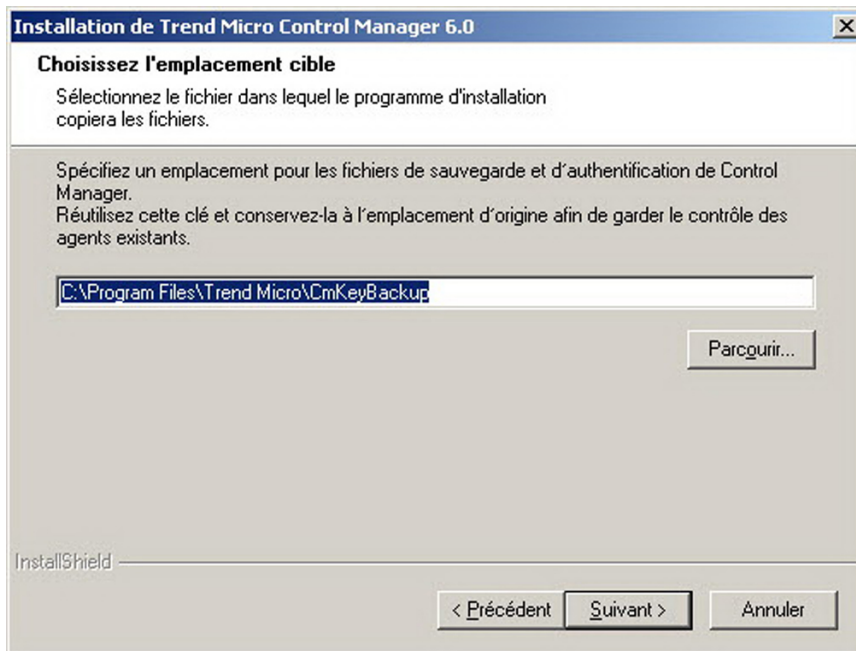


FIGURE 3-9. Sélection du répertoire de stockage des fichiers de sauvegarde et d'authentification

2. Spécifiez l'emplacement des fichiers d'authentification et de sauvegarde de Control Manager (pour obtenir plus d'informations, consultez la section [Chapitre 4, Tableau 4-2: Fichiers Control Manager devant être sauvegardés à la page 4-7](#)). Cliquez sur **Parcourir** pour sélectionner un autre répertoire.

Configuration des paramètres de notification

Procédure

1. Cliquez sur **Suivant**.

L'écran **Spécifier le chemin de routage des messages** apparaît. Cet écran s'affiche uniquement si TMI n'est pas installé sur le serveur hôte.

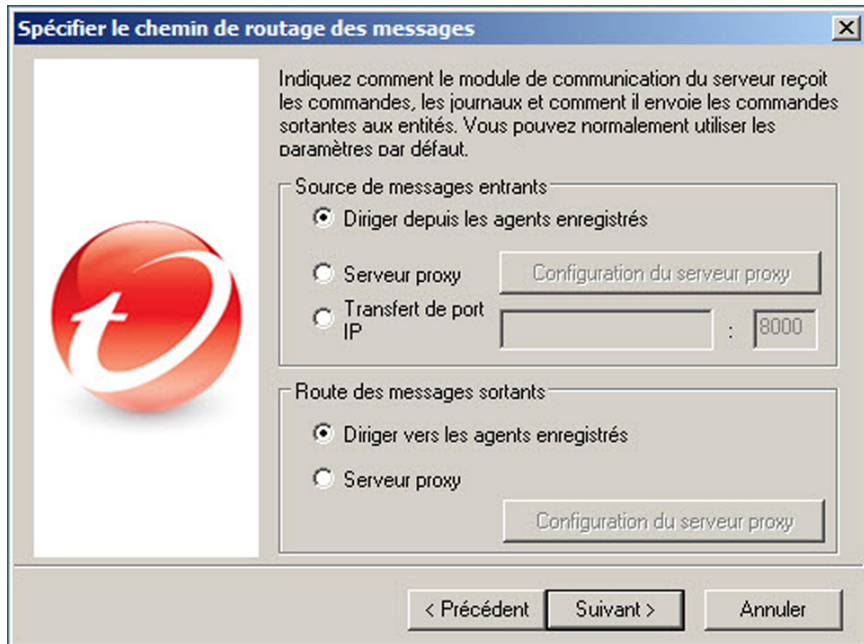


FIGURE 3-10. Définition des chemins de routage des messages ou des requêtes

2. Définissez les chemins de routage des messages entrants ou sortants ou des requêtes. Ces paramètres permettent d'adapter Control Manager aux systèmes de sécurité en place dans votre société. Sélectionnez les chemins de routage appropriés.



Remarque

Les chemins de routage peuvent être définis uniquement lors de l'installation. Les configurations proxy établies ici ne sont pas liées aux paramètres proxy utilisés pour l'accès à Internet, même si les mêmes paramètres proxy sont utilisés par défaut.

- Source de messages entrants

- **Directement depuis les agents enregistrés** : Les agents peuvent recevoir directement les messages entrants.
 - **Serveur proxy** : Utilise un serveur proxy pour la réception des messages.
 - **Transfert de port IP** : Cette fonctionnalité configure Control Manager pour qu'il utilise la fonction de transfert de port IP du pare-feu de votre entreprise. Indiquez le nom de domaine complet, l'adresse IP ou le nom NetBIOS du serveur de pare-feu, ainsi que le numéro du port que Control Manager a ouvert pour la communication.
 - Route des messages sortants
 - **Directement vers les agents enregistrés** : Control Manager envoie les messages sortants directement aux agents.
 - **Serveur proxy** : Control Manager envoie les messages sortants via un serveur proxy.
-

Configuration des informations relatives à la base de données

Procédure

1. Cliquez sur **Suivant**.

L'écran **Installer la base de données de Control Manager** apparaît.



FIGURE 3-11. Sélection de la base de données de Control Manager

2. Sélectionnez la base de données à utiliser avec Control Manager.
 - **Installer Microsoft SQL Express** : Le programme d'installation sélectionne automatiquement cette option si aucun serveur SQL n'est installé sur cet ordinateur. Pensez à spécifier un mot de passe pour cette base de données dans le champ correspondant.



Conseil

Microsoft SQL Express ne convient que si le nombre de connexions est limité. Trend Micro recommande l'utilisation d'un serveur SQL pour les réseaux Control Manager de grande taille.

- **SQL Server** : Le programme d'installation sélectionne automatiquement cette option s'il détecte un serveur SQL sur le serveur. Spécifiez les informations suivantes :

- **SQL Server (\Instance)** : Ce serveur héberge le serveur SQL que vous voulez utiliser pour Control Manager. Si le programme d'installation détecte un serveur SQL sur votre serveur, il le sélectionne automatiquement.

Pour spécifier un autre serveur, indiquez son nom de domaine complet, son adresse IPv4 ou son nom NetBIOS.

Si plusieurs instances du serveur SQL coexistent sur un serveur hôte (il peut s'agir du serveur où vous avez installé Control Manager ou d'un autre serveur), vous devez préciser quelle instance doit être utilisée. Par exemple : `your_sql_server.com\instance`



Remarque

Si les utilisateurs choisissent d'utiliser un serveur SQL distant, ne spécifiez pas d'adresse IPv6 dans le champ Serveur SQL. Control Manager ne peut pas identifier la base de données distante par son adresse IPv6.

- **Authentification du serveur SQL** : Permet de définir les informations d'identification de connexion au serveur SQL. Par défaut, le nom d'utilisateur sa est utilisé.

Si vous utilisez un compte Windows pour vous connecter au serveur SQL, saisissez le nom d'utilisateur au format suivant : **nom de domaine\nom d'utilisateur**.



AVERTISSEMENT!

Pour des raisons de sécurité, n'utilisez pas une base de données SQL non protégée par mot de passe.

3. Sous **Base de données de Trend Micro Control Manager**, indiquez le nom de la base de données de Trend Micro Control Manager. Le nom par défaut est `db_ControlManager`.

4. Cliquez sur **Suivant** pour créer la base de données requise. Si le programme d'installation détecte une base de données Control Manager existante, vous pouvez effectuer l'une des opérations suivantes :

- **Ajouter de nouveaux enregistrements à la base de données existantes :**
La version de Control Manager que vous installez conserve les mêmes paramètres, comptes et entités du répertoire Produits que le serveur précédent. En outre, Control Manager conserve le compte racine de l'installation précédente. Il est impossible de créer un nouveau compte racine.



Remarque

Lorsque vous installez Control Manager 6.0, vous ne pouvez pas sélectionner Ajouter les nouveaux enregistrements à la base de données existante pour les versions précédentes de la base de données de Control Manager.

- **Supprimer les enregistrements existants et créer une nouvelle base de données :** La base de données existante est supprimée et une autre base de données du même nom est créée.
- **Créer une nouvelle base de données portant un nouveau nom :** Vous êtes renvoyé à l'écran précédent pour pouvoir changer le nom de la base de données de Control Manager.



Remarque

Si vous ajoutez des enregistrements à la base de données en cours, vous ne pourrez pas modifier le compte racine.

Installation du compte racine

Procédure

1. Cliquez sur **Suivant**.

L'écran **Créer un compte racine** apparaît.



Créer un compte racine

Trend Micro Control Manager 6.0 doit avoir un compte racine. Utilisez des lettres, chiffres, tirets et tirets de soulignement ; les comptes racines doivent comporter moins de 32 caractères.

ID utilisateur : *

Nom complet :

Mot de passe : *

Confirmer le mot de passe : *

Adresse électronique :

< Précédent Suivant > Annuler

FIGURE 3-12. Saisissez les informations pour le compte racine de Control Manager

2. Complétez impérativement les champs suivants :
 - ID utilisateur
 - Nom complet
 - Mot de passe
 - confirmer mot de passe
 - Adresse électronique
3. Cliquez sur **Suivant**.
4. Cliquez sur **Terminer** pour achever l'installation.

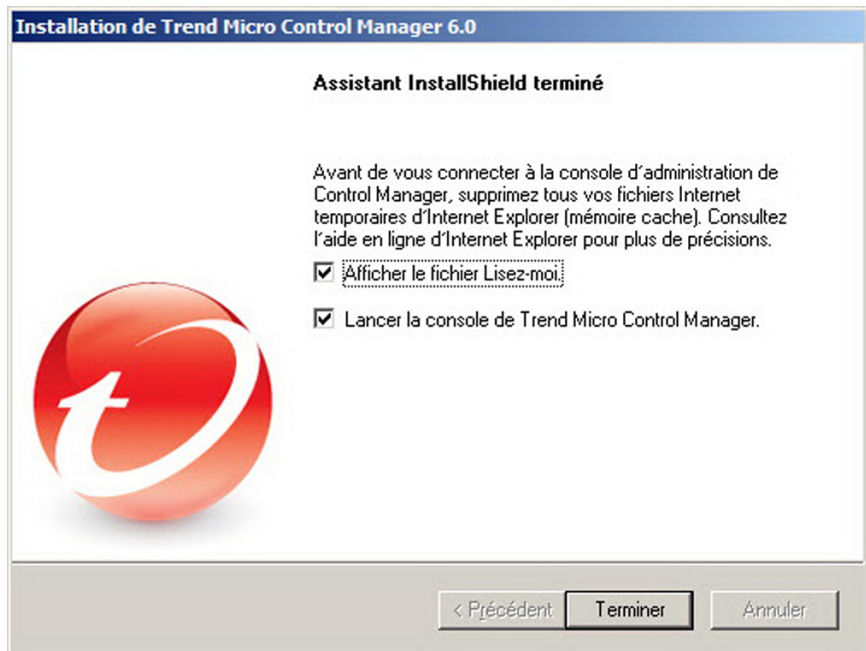



FIGURE 3-13. Installation terminée

Vérification de l'installation correcte du serveur Control Manager

Pour vérifier qu'une installation du serveur Control Manager s'est correctement déroulée, vérifiez les éléments du tableau suivant.

ÉLÉMENT	DESCRIPTION
Panneau de configuration > Ajout/ Suppression de programmes	<p>Les programmes suivants apparaissent dans la fenêtre Ajout/Suppression de programmes :</p> <ul style="list-style-type: none">• Trend Micro Common CGI• Trend Micro Control Manager• Trend Micro Management Infrastructure• Pack redistribuable Microsoft Visual C ++ 2005 (dernière version)• PHP 5.3.5• Exécution SP4 de Crystal Reports 2008• Microsoft SQL Server 2008 R2• Client natif Microsoft SQL Server 2008 R2• Configuration de Microsoft SQL Server 2008 R2• Fichier de support de configuration de Microsoft SQL Server 2008 R2• Navigateur Microsoft SQL Server• Microsoft SQL Server VSS Writer• FastCGI (figure uniquement dans Windows Server 2003)

ÉLÉMENT	DESCRIPTION
C:\Program Files	<p>Les dossiers suivants apparaissent sous le répertoire :</p> <ul style="list-style-type: none"> • Trend Micro\Common\TMI • Trend Micro\Common\CCGI • Trend Micro\Control Manager • PHP <hr/> <p> Remarque Le dossier PHP doit être créé par l'installation de Control Manager.</p>
Fichiers de base de données de Control Manager	<ul style="list-style-type: none"> • db_ControlManager.mdf • db_ControlManager_Log.LDF
Le programme d'installation crée les services et les processus suivants.	
Control Manager Services	<ul style="list-style-type: none"> • Trend Micro Control Manager • Trend Micro Common CGI • Trend Micro Management Infrastructure • Trend Micro Network Time Protocol
Processus CCGI	<ul style="list-style-type: none"> • Jk_nt_service.exe • Java.exe
Processus IIS	Inetinfo.exe (Internet Information Services)
Filtres ISAPI	<ul style="list-style-type: none"> • CCGIRedirect • ReverseProxy • TmcmRedirect

ÉLÉMENT	DESCRIPTION
Processus TMI	<ul style="list-style-type: none"> • CM.exe (TMI-CM) • MRF.exe (module Message Routing Framework) • DMServer.exe (fonction complète TMI-DM)
Processus Control Manager	<ul style="list-style-type: none"> • ProcessManager.exe • LogReceiver.exe • MsgReceiver.exe • LogRetriever.exe • CmdProcessor.exe • UIProcessor.exe • ReportServer.exe • NTPD.exe (apparaît lorsque les utilisateurs ont choisi l'activation du serveur Trend Micro NTP lors de l'installation) • DCSPprocessor.exe • Casprocessor.exe
Processus Message Queue	LogProcessor.exe

Configuration après l'installation

Une fois Control Manager correctement installé, Trend Micro recommande d'effectuer les tâches de configuration post-installation suivantes :

1. Enregistrer et activer Control Manager
2. Configurer les comptes utilisateurs et les rôles utilisateurs
3. Télécharger les composants les plus récents

4. Définir les notifications

Enregistrement et activation de Control Manager

Après avoir installé correctement Control Manager, vérifiez l'état de la licence et la date d'expiration dans la console Web. Pour ce faire, cliquez sur **Administration > Gestion des licences > Control Manager**. Si l'état n'est pas *Activé* ou s'il est expiré, demandez un code d'activation et déverrouillez votre logiciel (dans la console Web, sélectionnez **Administration > Gestion des licences > Control Manager > Spécifier un nouveau code d'activation**). Si vous rencontrez des difficultés avec votre code d'activation, veuillez contacter le service d'assistance technique. Pour plus d'informations, consultez la section *Enregistrement et activation de votre logiciel à la page 3-28*.

Configuration des comptes utilisateurs

Créez des comptes utilisateurs Control Manager en fonction de vos besoins. Tenez compte des points suivants lorsque vous créez des comptes :

- Nombre des différents rôles utilisateurs (administrateurs, utilisateurs expérimentés ou opérateurs).
- Attribuez les droits d'accès et les privilèges correspondant à chaque rôle utilisateur
- Pour que les utilisateurs puissent exploiter la structure de gestion en cascade, ils doivent au moins disposer des droits «Utilisateur expérimenté».

Téléchargement des composants les plus récents

Après l'installation, téléchargez manuellement les composants les plus récents (fichiers de signatures de virus/modèles Damage Cleanup, mises à jour de moteur) à partir de Trend Micro ActiveUpdate Server pour garantir un niveau de sécurité maximal. Si un serveur proxy est placé entre un serveur Control Manager et Internet, configurez les paramètres du serveur proxy (sur la console Web, sélectionnez **Administration > Paramètres > Paramètres proxy**).

Paramètres de notification :

Après l'installation, configurez les événements qui déclencheront les notifications permettant de surveiller les attaques virales majeures et les activités relatives à la sécurité. Vous devez définir les destinataires des notifications, choisir les canaux de notification, puis les tester pour vérifier qu'ils fonctionnent normalement (sur la console Web, sélectionnez **Administration > Centre d'événements**).

Enregistrement et activation de votre logiciel

Activez le serveur Control Manager pour maintenir à jour votre sécurité et vos mises à jour de produits. Pour ce faire, enregistrez-le en ligne et saisissez votre clé d'enregistrement afin d'obtenir un code d'activation.

Si vous installez Control Manager pour la première fois :

- Vous avez acquis la version complète auprès d'un revendeur Trend Micro. La clé d'enregistrement figure dans le coffret du produit.

Enregistrez-vous en ligne et demandez un code d'activation pour déverrouiller le logiciel.

- Vous installez une version d'évaluation

Demandez à votre revendeur une clé d'enregistrement pour la version complète, puis suivez les instructions fournies pour activer le produit.

À propos de l'activation de Control Manager

L'activation de Control Manager vous permet d'accéder à l'ensemble de ses fonctionnalités. Vous pourrez également télécharger les mises à jour des composants du programme. Vous pouvez activer Control Manager après avoir reçu un code d'activation. Pour obtenir ce code, enregistrez le produit à l'aide de la clé d'enregistrement contenu dans le coffret du produit ou procurez-vous en une auprès d'un revendeur Trend Micro.

4. Cliquez sur **Activer**, puis sur **OK**.
-

Passage à la version complète

Activez Control Manager pour continuer à l'utiliser au-delà de la période d'évaluation. Activez Control Manager pour accéder à l'ensemble de ses fonctionnalités. Vous pourrez également télécharger les mises à jour des composants du programme.

Procédure

1. Procurez-vous une clé d'enregistrement pour la version complète auprès d'un revendeur Trend Micro.
 2. Enregistrez le logiciel en ligne.
 3. Demandez un code d'activation.
 4. Activez Control Manager selon les instructions fournies dans la procédure ci-dessus.
-

Renouvellement du contrat de maintenance de votre produit

Renouvelez le contrat de maintenance de Control Manager ou de ses produits et services intégrés (Outbreak Prevention Services) à l'aide d'une des méthodes suivantes.

Pour renouveler le contrat de maintenance d'un produit ou d'un service, demandez une clé d'enregistrement mise à jour. Cette clé d'enregistrement vous permet d'obtenir un nouveau code d'activation. Les procédures de renouvellement du contrat de maintenance sont différentes selon que vous utilisez une version d'évaluation ou une version complète.

Renouvellement du contrat de maintenance du produit à l'aide du service Vérifier l'état en ligne

Procédure

1. Accédez à **Administration > Gestion de la licence > Control Manager**.
L'écran **Informations sur la licence** apparaît.
 2. Dans la zone de travail sous **Informations sur la licence Control Manager**, cliquez sur le lien **Vérifier l'état en ligne**, puis cliquez sur **OK**.
 3. Déconnectez-vous et reconnectez-vous à la console Web pour que les modifications soient prises en compte.
-

Renouvellement du contrat de maintenance manuellement en saisissant un code d'activation mis à jour

Procédure

1. Accédez à **Administration > Gestion de la licence > Control Manager**.
L'écran **Informations sur la licence** apparaît.
 2. Dans la zone de travail sous **Informations sur la licence Control Manager**, cliquez sur le lien **Activer le produit**.
 3. Cliquez sur le lien **Spécifier un nouveau code d'activation** et suivez les instructions fournies sur le site Web d'enregistrement en ligne.
 4. Dans le champ **Nouveau**, saisissez votre code d'activation.
 5. Cliquez sur **Activer**.
 6. Cliquez sur **OK**.
-

Chapitre 4

Mise à niveau de serveurs ou migration d'agents vers Control Manager

La mise à niveau des serveurs existants de Control Manager 5.0 / 5.5 vers Control Manager 6.0 nécessite réflexion et préparation. La même consigne s'applique à la migration d'agents MCP ou d'anciens agents Control Manager vers un serveur Control Manager 6.0.

Ce chapitre traite les rubriques suivantes :

- *Mise à niveau vers Control Manager 6.0 à la page 4-2*
- *Rétablissement des serveurs Control Manager 5.0/5.5 à la page 4-10*
- *Planification de la migration des agents Control Manager à la page 4-12*
- *Migration de la base de données de Control Manager à la page 4-19*

Mise à niveau vers Control Manager 6.0

Le tableau suivant répertorie les éléments à prendre en compte lors d'une mise à niveau vers les versions Standard ou Advanced :

TABLEAU 4-1. Éléments à prendre en compte lors d'une mise à niveau vers Control Manager 6.0

FONCTION	STANDARD EDITION	ADVANCED EDITION
Maintien des fonctions de génération de rapports	Non	Oui
Mise à niveau de la version Standard Edition vers la version Advanced Edition Pour mettre à niveau une version Standard Edition vers la version Advanced Edition, procurez-vous un code d'activation Advanced Edition, puis modifiez-le dans l'écran Gestion de la licence .	Oui	N/A
Conversion d'une version Enterprise/Advanced en version Standard	N/A	Oui

Mise à niveau des serveurs Control Manager 5.0 / 5.5

Trend Micro recommande d'installer Control Manager 6.0 par écrasement des anciennes installations de Control Manager. De cette façon, tous les paramètres, journaux et rapports déjà existants, ainsi que le répertoire Produits resteront inchangés. Toutefois, avant d'effectuer la mise à niveau, vérifiez que le serveur où est installé Control Manager dispose de ressources système suffisantes.

Versions prises en charge pour la mise à niveau

Control Manager prend en charge la mise à niveau à partir des versions suivantes installées sur le site internet IIS par défaut :

- Control Manager 5.5 SP1
- Control Manager 5.5
- Control Manager 5.0



AVERTISSEMENT!

Effectuez toujours une sauvegarde du serveur existant avant la mise à niveau.

Mises à niveau et migrations : cas de figure

Control Manager prend en charge trois cas de figure différents pour la mise à niveau et la migration :

- *Scénario 1 : Mise à niveau d'un serveur Control Manager 5.0/5.5 vers Control Manager 6.0 à la page 4-3*
- *Scénario 2 : Migration vers une nouvelle installation de Control Manager 6.0 à l'aide de l'outil de migration d'agent à la page 4-5*
- *Scénario 3 : Mise à niveau ou migration d'un environnement en cascade à la page 4-6*

Scénario 1 : Mise à niveau d'un serveur Control Manager 5.0/5.5 vers Control Manager 6.0

Lors de la mise à niveau de Control Manager 5.0/5.5 directement vers Control Manager 6.0, les administrateurs peuvent décider d'effectuer une sauvegarde de Control Manager ou de tout le système d'exploitation sur lequel est installé Control Manager. La sauvegarde du système d'exploitation dans son ensemble représente plus de travail mais constitue une option qui assure une meilleure sécurité en matière de conservation des données.

Mise à niveau avec sauvegarde de la base de données et du serveur Control Manager antérieurs

Procédure

1. Sauvegardez la base de données Control Manager 5.0/5.5 existante.
2. Sauvegardez tous les fichiers situés à l'emplacement `\Trend Micro\CmKeyBackup*.*`.
3. Sauvegardez tous les dossiers du serveur Control Manager 5.0/5.5 actuel.
4. Sauvegardez tous les registres du serveur Control Manager 5.0/5.5 actuel.



Remarque

Voir [Tableau 4-2: Fichiers Control Manager devant être sauvegardés à la page 4-7](#) pour les étapes 2 à 4.

5. Installez Control Manager 6.0 par écrasement de Control Manager 5.0/5.5.
-

Mise à niveau en sauvegardant l'ensemble du système d'exploitation du serveur et la base de données Control Manager

Procédure

1. Sauvegardez le système d'exploitation du serveur Control Manager 5.0/5.5 existant.
 2. Sauvegardez la base de données Control Manager 5.0/5.5 existante.
 3. Installez Control Manager 6.0 par écrasement de Control Manager 5.0/5.5.
-

Déroulement de la mise à niveau

Pour mettre à niveau Control Manager 5.0/5.5 vers Control Manager 6.0, exécutez le programme d'installation (`Setup.exe`) comme décrit à l'étape 1 de [Installation de tous les composants nécessaires à la page 3-5](#). Suivez les étapes pour mettre à niveau Control Manager.

Le processus de mise à niveau est très proche de celui d'une nouvelle installation, sauf en ce qui concerne les points suivants :

- Le programme d'installation met à niveau le pack redistribuable Visual C++ 2005 SP1
- (pour une mise à niveau à partir de Control Manager 5.5 uniquement) Le programme d'installation met à niveau le fichier PHP existant à partir du serveur
- Le programme d'installation migre la base de données existante dans Control Manager 6.0.

Scénario 2 : Migration vers une nouvelle installation de Control Manager 6.0 à l'aide de l'outil de migration d'agent

Ce cas de figure implique l'installation de Control Manager 6.0 sur un serveur distinct du serveur Control Manager existant. Cette méthode vous permet de mettre petit à petit le précédent serveur hors service. Pour plus d'informations sur la migration des agents, consultez la section *Planification de la migration des agents Control Manager à la page 4-12*.

Migration d'un serveur Control Manager 5.0/5.5 vers une nouvelle installation de Control Manager 6.0

Procédure

1. Sauvegardez la base de données Control Manager 5.0/5.5 existante.
2. Effectuez une nouvelle installation de Control Manager 6.0 sur un autre ordinateur.
3. Utilisez l'outil de migration des agents pour effectuer la migration des entités du serveur Control Manager 5.0/5.5 vers le serveur Control Manager 6.0.



Remarque

L'outil de migration des agents ne prend en charge que la migration de produits gérés et les journaux de produits gérés. L'outil de migration des agents ne prend pas en charge la migration des rapports ni de la structure du répertoire Produits depuis le serveur précédent.

Scénario 3 : Mise à niveau ou migration d'un environnement en cascade

Control Manager prend en charge la mise à niveau d'un environnement en cascade. Pour mettre à niveau un environnement en cascade, annulez l'enregistrement des serveurs Control Manager enfants, puis réenregistrez-les.

Procédure

1. Désenregistrez tous les serveurs Control Manager enfants du serveur Control Manager parent.
2. Sauvegardez le serveur Control Manager parent.
3. Sauvegardez tous les serveurs Control Manager enfants.
4. Mettez à niveau le serveur Control Manager parent.
5. Mettez à niveau tous les serveurs Control Manager enfants.
6. Enregistrez tous les serveurs Control Manager enfants sur le serveur Control Manager parent.

TABLEAU 4-2. Fichiers Control Manager devant être sauvegardés

INFORMATIONS SUR CONTROL MANAGER 5.0/5.5/6.0	EMPLACEMENT
Base de données	Sauvegardez la base de données Control Manager à l'aide de SQL Enterprise Manager ou d'osql. Pour connaître la procédure détaillée, consultez les rubriques d'aide en ligne de Control Manager relatives à la sauvegarde de db_ControlManager à l'aide de SQL Enterprise Manager/osql.
Informations d'authentification (permet de garantir que les produits gérés qui communiquent avec le serveur Control Manager continuent à le faire en cas de restauration de Control Manager)	\Program Files\Trend Micro \CmKeyBackup*.*
Informations sur le GUID	Valeur GUID dans \Program files \Trend Micro\COMMON\TMI\TMI.cfg
Informations sur les produits gérés	\Program Files\Trend Micro\common \tmi\mrf_entity.dat \Program Files\Trend Micro\common \tmi\mrf_entity.bak
Fichiers ActiveUpdate	\Program Files\Trend Micro \Control Manager\webui\download \Activeupdate

INFORMATIONS SUR CONTROL MANAGER 5.0/5.5/6.0	EMPLACEMENT
Registre de Control Manager	<p>Pour systèmes d'exploitation 32 bits :</p> <pre> HKEY_LOCAL_MACHINE\SOFTWARE \TrendMicro\TVCS\ HKEY_LOCAL_MACHINE\SOFTWARE \TrendMicro\TMI\ HKEY_LOCAL_MACHINE\SOFTWARE \TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows\CurrentVersion \Uninstall\TMCM HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\Windows\CurrentVersion \Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\TMCM </pre>

INFORMATIONS SUR CONTROL MANAGER 5.0/5.5/6.0	EMPLACEMENT
Registre de Control Manager	<p>Pour systèmes d'exploitation 64 bits :</p> <pre> HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\TrendMicro\TVCS HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\TrendMicro\TMI\ HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\Microsoft\Windows \CurrentVersion\Uninstall\TCM HKEY_LOCAL_MACHINE\SOFTWARE \Wow6432Node\Microsoft\Windows \CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\TCM </pre>
Registre de Control Manager	<pre> HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services \TrendMicro_NTP HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services \TrendMicro Infrastructure\ HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services \TrendCCGI HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\MSSQL \$SQLEXPRESS </pre>

Rétablissement des serveurs Control Manager 5.0/5.5

Si la mise à niveau vers Control Manager 6.0 échoue, suivez les étapes ci-dessous pour rétablir le système Control Manager 5.0/5.5.

Scénario 1 : Rétrogradation d'un serveur Control Manager 6.0 vers Control Manager 5.0/5.5

Utilisez une des méthodes suivantes pour revenir au système Control Manager 5.0/5.5 :

- Effectuer une rétrogradation à partir d'une sauvegarde de serveur Control Manager et de base de données
- Effectuer une rétrogradation à partir d'un système d'exploitation complet du serveur et de la sauvegarde de la base de données de Control Manager

Effectuer une rétrogradation à partir d'une sauvegarde de serveur Control Manager et de base de données

Procédure

1. Supprimez le serveur Control Manager 6.0.
2. Installez le serveur Control Manager 5.0/5.5.
3. Appliquez les services packs et les correctifs hotfix requis de Control Manager 5.0/5.5.



AVERTISSEMENT!

N'appliquez que les service packs et les correctifs de type hot fix que le serveur Control Manager 5.0/5.5 d'origine avait installés.

4. Rétablissez la base de données de Control Manager 5.0/5.5 avec la base de données sauvegardée.

5. Rétablissez tous les dossiers de Control Manager 5.0/5.5 avec les dossiers sauvegardés.
 6. Rétablissez les registres de Control Manager 5.0/5.5 avec les registres sauvegardés.
 7. Restaurez tous les fichiers situés à l'emplacement `\Trend Micro\CmKeyBackup*.*`.
 8. Importez l'ancien certificat.
-

Pour effectuer une rétrogradation à partir de l'ensemble du système d'exploitation du serveur et de la sauvegarde de la base de données de Control Manager

Procédure

1. Rétablissez la base de données de Control Manager 5.0/5.5 avec la base de données sauvegardée.
 2. Rétablissez le système d'exploitation du serveur avec le système d'exploitation sauvegardé.
-

Scénario 2 : Rétrogradation d'un environnement en cascade

Procédure

1. Désenregistrez tous les serveurs Control Manager enfants du serveur Control Manager parent.
2. Rétrogradez le serveur Control Manager parent.
3. Rétrogradez tous les serveurs Control Manager enfants.
4. Appliquez les service packs et les correctifs de type hot fix de Control Manager.

5. Enregistrez tous les serveurs Control Manager enfants sur le serveur Control Manager parent.
-

Planification de la migration des agents Control Manager

Il existe deux façons de faire migrer des agents vers un serveur Control Manager 6.0 :

- Mise à niveau rapide
- Mise à niveau progressive

Mise à niveau rapide

La mise à niveau rapide s'effectue selon la méthode présentée dans le tableau ci-dessous.

TABLEAU 4-3. Mise à niveau rapide

SERVEUR/AGENT D'ORIGINE	ACTION
Control Manager 5.0/5.5 avec agents MCP	Enregistrez les agents MCP sur le serveur Control Manager 6.0 puis réorganisez la structure du répertoire Produits
Control Manager 5.0/5.5 avec agents mixtes	Enregistrez les agents MCP sur le serveur Control Manager 6.0 puis réorganisez la structure du répertoire Produits

Trend Micro recommande le recours à la mise à niveau rapide pour la migration d'agents dans un environnement de type laboratoire ou sur les réseaux de petite taille, et de préférence au cours de déploiements tests (voir [Test de Control Manager sur un site à la page 2-12](#)). Toutefois, dans la mesure où il n'est pas possible d'interrompre la migration une fois qu'elle a débuté, cette méthode est mieux adaptée aux déploiements de petite taille. Le degré de difficulté augmente avec la taille du réseau.

Mise à niveau progressive

Trend Micro recommande de procéder à la mise à niveau progressive pour les réseaux Control Manager 5.0/5.5 de grande taille à serveur unique. Pour les réseaux à serveurs multiples, celle-ci est essentielle. En effet, elle permet une migration plus structurée du système et respecte les directives suivantes :

- La migration commence sur les systèmes ayant le plus faible impact sur le réseau existant, avant de passer aux systèmes dont l'impact est progressivement plus important.
- L'ancien réseau est mis à niveau par étapes planifiées plutôt qu'en une seule fois.

Ce qui simplifie tout dépannage éventuel.

La mise à niveau progressive implique les étapes suivantes :

1. installation de Control Manager 6.0 sur un serveur sur lequel aucune version précédente de Control Manager n'a été installée (et si possible, ne contenant aucun produit géré) ;
2. Exécutez l'outil `AgentMigrateTool.exe` sur le serveur Control Manager 6.0.

Utilisez le programme d'installation de l'agent Control Manager avec l'outil de migration des agents pour planifier la mise à niveau d'agents sur des réseaux Control Manager existants. L'outil de migration des agents peut générer une liste de serveurs avec les agents Control Manager. Cette méthode vous évite d'avoir à sélectionner les serveurs manuellement.

Scénarios de migration pour les agents Control Manager 2.x

Voici les cas de figure possibles pour la migration des agents :

- Migration d'un seul serveur
- Consolidation de différents serveurs/agents

Migration d'un seul serveur



FIGURE 4-1. Migration d'agents appartenant à un même serveur

Dans ce cas de figure, vous pouvez avoir recours aux méthodes de migration rapide ou progressive. Consultez la section *Mises à niveau et migrations : cas de figure à la page 4-3*.

Consolidation de différents serveurs/agents

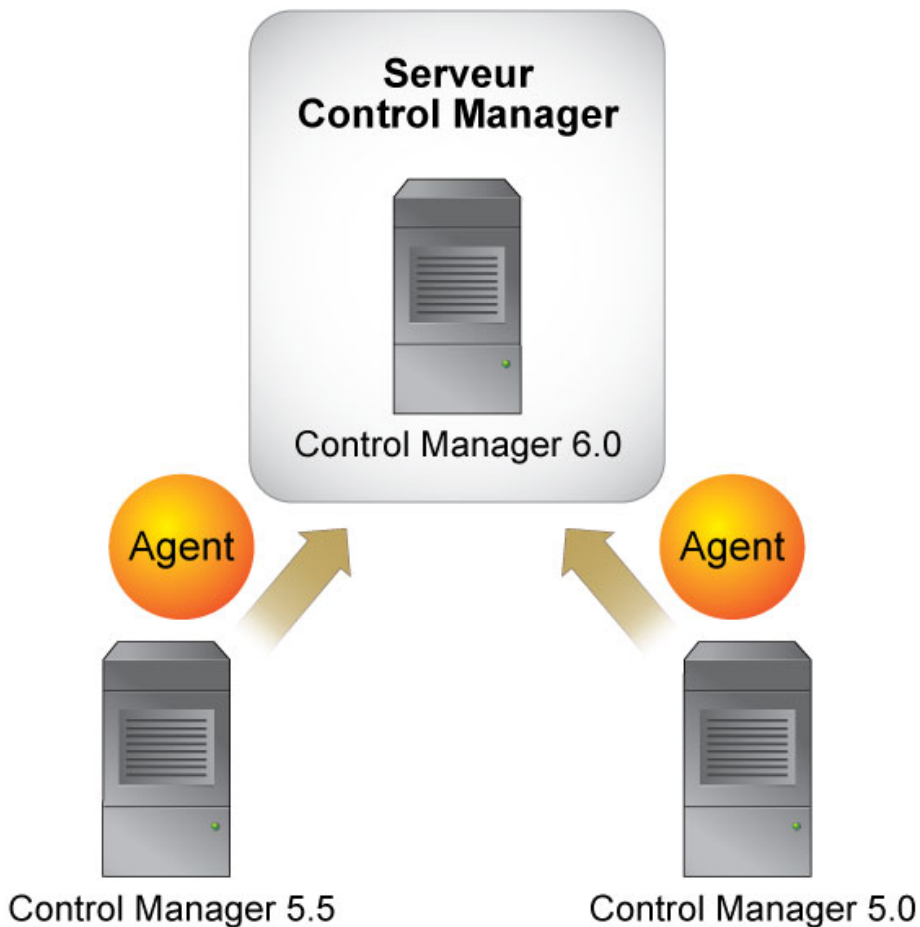


FIGURE 4-2. Migration d'agents appartenant à plusieurs serveurs

Compte tenu des nouvelles fonctions de contrôle d'accès de Control Manager, les fonctions précédemment gérées par des serveurs Control Manager distincts (pour

restreindre l'accès à des segments précis du réseau antivirus) peuvent dorénavant être regroupées sur un même serveur Control Manager.

Flux de migration des agents Control Manager 2.5x

Lors de la migration des agents Control Manager 2.5x, l'outil de migration réalise les opérations suivantes :

1. Arrête le service d'infrastructure TMI (Trend Micro Infrastructure)
2. Extrait du serveur Control Manager 5.0/5.5 les informations relatives au répertoire Produits.
3. Supprime de la base de données Control Manager 5.0/5.5 et du fichier `TMI.cfg` les informations relatives aux agents.
4. Conserve la version des agents Control Manager 2.5x (aucune mise à niveau n'a lieu).
5. Écrit dans la base de données Control Manager 6.0 et dans le fichier `TMI.cfg` les informations relatives aux agents.
6. Redémarre le service d'infrastructure TMI (Trend Micro Infrastructure).

Si l'outil `AgentMigrationTool.exe` ne peut pas achever la migration des agents Control Manager 2.5x, il supprime de la base de données Control Manager 6.0 et du fichier `TMI.cfg` les informations sur les agents, puis les réécrit dans la base de données Control Manager 5.0/5.5.

Flux de migration des agents MCP

Lors de la migration des agents MCP, l'outil de migration réalise les opérations suivantes :

1. Arrête le service d'infrastructure TMI sur le serveur de destination.
2. Extrait du serveur Control Manager les informations relatives au répertoire Produits.
3. Conserve la version des agents Control Manager (aucune mise à niveau n'a lieu).

4. Écrit les informations relatives aux agents dans la base de données du serveur de destination.
5. Redémarre le service d'infrastructure TMI sur le serveur de destination.
6. Arrête puis redémarre le service Trend Micro Control Manager sur le serveur de destination.
7. Demande au serveur source d'émettre une commande de changement de serveur et attend l'interrogation de l'agent MCP.

Migration d'agents Control Manager 2.5x et MCP

Utilisez l'outil `AgentMigrateTool.exe` pour procéder à la migration d'agents Windows initialement administrés par des serveurs Control Manager 5.0/5.5. Lors de la migration d'agents, les agents 2.5x migrent d'abord, suivis des agents MCP.

En cas d'échec de la migration :

- L'agent continue d'être géré par le serveur source.
- Les journaux des agents figurent à la fois sur le serveur source et sur le serveur de destination.

Les journaux ayant fait l'objet d'une migration n'apparaissent pas, à moins que les agents ne soient enregistrés sur le serveur de destination. Le serveur Control Manager de destination purge les journaux ayant migré lors de l'activation de la purge.



Remarque

Exécutez `AgentMigrateTool.exe` directement sur le serveur de destination, à savoir le serveur Control Manager 6.0 vers lequel les agents migrent.

Procédure

1. Dans Windows Explorer, ouvrez le dossier racine de Control Manager 6.0. Par exemple : `<racine>\Program Files\Trend Micro\Control Manager\`
2. Double-cliquez sur `AgentMigrateTool.exe`.



Remarque

N'oubliez pas de démarrer le service Registre distant sur le serveur Control Manager de destination pour que la migration des agents s'effectue correctement.

3. Cliquez sur **Configurer les paramètres du serveur source** dans le menu principal.
4. Dans l'écran de configuration, dans **Serveur source**, saisissez l'**adresse IP** du serveur source qui héberge les agents à migrer.
5. Sous **Compte administrateur système**, indiquez le **nom d'utilisateur** et le **mot de passe** de l'administrateur qui permettent d'accéder au serveur source, puis cliquez sur **Se connecter**.
6. Dans la fenêtre principale, cliquez sur **Ajouter >** ou **Ajouter tout >>** pour faire passer les agents de la liste **Source** à la liste **Destination**.
7. Choisissez une ou plusieurs options parmi les suivantes :
 - **Sauvegarder la structure arborescente** : AgentMigrateTool.exe indique au serveur de destination (un serveur Control Manager 6.0) de conserver l'arborescence du répertoire Produits pour les produits gérés sélectionnés.
 - **Migrer les journaux** : AgentMigrateTool.exe copie les journaux des produits gérés sélectionnés du serveur source au serveur de destination.
 - **Activer HTTPS** : AgentMigrateTool.exe indique aux agents en cours de migration d'utiliser HTTPS pour s'enregistrer auprès de Control Manager. Si vous ne sélectionnez pas cette option, les agents utilisent le protocole HTTP pour s'enregistrer.

Ces options s'appliquent aux agents répertoriés dans la liste Destination.



Remarque

Trend Micro vous recommande d'activer les options **Sauvegarder la structure arborescente** et **Migrer les journaux** si vous effectuez la migration de tous les agents du serveur source.

8. Cliquez sur **Migrer**. `AgentMigrateTool.exe` procède alors à la migration de/des agents répertorié(s) dans la liste Destination.
-

Migration de la base de données de Control Manager

Il existe deux façons de faire migrer une base de données Control Manager 5.0/5.5 :

- Installer Control Manager 6.0 par écrasement d'un serveur Control Manager 5.0/5.5. Il s'agit de la méthode recommandée.

Le programme d'installation de Control Manager 6.0 procède automatiquement à la mise à niveau de la base de données vers la version 6.0.
- Transférez manuellement la base de données Control Manager 5.0/5.5 vers le serveur Control Manager 6.0.

Migration d'une base de données Control Manager SQL 2005 vers un autre serveur SQL Server 2005

Il est nécessaire de modifier un certain nombre de paramètres dans le fichier `TMI.cfg` pour déplacer une base de données Control Manager d'un serveur SQL Server 2005 vers un autre.

Procédure

1. À l'aide de Windows Services, arrêtez les services Control Manager suivants :
 - Trend Micro Management Infrastructure
 - Trend Micro Common CCGI
 - Trend Micro Control Manager
2. Copiez la base de données Control Manager de l'ancien serveur SQL 2005 Server vers le nouveau.



Remarque

Control Manager chiffre les valeurs de nom d'utilisateur et de mot de passe. Trend Micro vous recommande de configurer le serveur SQL cible avec le même compte d'authentification que celui qui permet d'accéder à db_ControlManager et de conserver les mêmes identifiant et mot de passe.

3. Ouvrez <racine>\Program Files\Trend Micro\COMMON\TMI\TMI.cfg dans un éditeur de texte.
-



Remarque

Sauvegardez TMI.cfg afin de pouvoir rétablir les paramètres d'origine.

4. Remplacez la valeur du paramètre
CFG_DM_DB_DSN=DSN=ControlManager_DataBase par le nom du serveur SQL de destination.
5. Conservez l'ancien identificateur et l'ancien mot de passe ou mettez à jour les valeurs des paramètres suivants :

CFG_DM_DB_ID

CFG_DM_DB_PWD
6. Enregistrez et fermez TMI.cfg.
7. Cliquez sur **Démarrer > Programmes > Outils d'administration > Sources de données (ODBC)** pour ouvrir l'administrateur de sources de données ODBC.
8. Activez l'onglet **Nom DSN système** et configurez la source de données **ControlManager_DataBase**.
9. Sur l'écran Configuration de source de données de Microsoft SQL Server, sélectionnez le **serveur de destination** pour modifier la valeur du champ **À quel serveur SQL Server voulez-vous vous connecter?**, puis cliquez sur **Suivant**. Si le serveur de destination ne figure pas dans la liste, saisissez le **nom du serveur**.
10. Dans la fenêtre suivante, sélectionnez les options **Avec l'authentification SQL Server à l'aide d'un identifiant de connexion entré par l'utilisateur** et **Se connecter à SQL Server pour obtenir les paramètres par défaut pour la configuration supplémentaire**.

11. Saisissez l'**identificateur** et le **mot de passe** qui figurent dans le fichier TMI.cfg, puis cliquez sur **Suivant**.
 12. Cliquez sur **Terminer** pour enregistrer la nouvelle configuration et fermer l'écran Configuration de source de données de Microsoft SQL Server.
 13. Cliquez sur **OK** pour fermer l'administrateur de sources de données ODBC.
 14. À l'aide de Windows Services, redémarrez tous les services Control Manager.
 15. Connectez-vous à la console Web et accédez au répertoire Produits afin de vérifier si tous les produits gérés sont enregistrés. Si c'est le cas, vous avez réussi la migration de la base de données vers le serveur SQL Server de destination.
-

Chapitre 5

Suppression de Trend Micro Control Manager

Ce chapitre contient des informations permettant de supprimer de votre réseau des composants Control Manager, dont le serveur et les agents Control Manager, ainsi que tous autres fichiers associés.

Ce chapitre contient les sections suivantes :

- *Suppression d'un serveur Control Manager à la page 5-2*
- *Suppression manuelle de Control Manager à la page 5-3*
- *Suppression d'un agent Control Manager 2.x sur Windows à la page 5-11*

Suppression d'un serveur Control Manager

Vous disposez de deux méthodes pour supprimer automatiquement Control Manager (les instructions suivantes s'appliquent à un environnement Windows 2003; les détails peuvent légèrement différer en fonction de votre plate-forme Microsoft Windows) :

Procédure

- À partir du menu Démarrer, cliquez sur **Démarrer > Programmes > Trend Micro Control Manager > Désinstallation de Trend Micro Control Manager**.
- À partir du composant Ajout/Suppression de programmes :
 - a. Cliquez sur **Démarrer > Paramètres > Panneau de configuration > Ajout/Suppression de programmes**.
 - b. Sélectionnez **Trend Micro Control Manager** et cliquez sur **Supprimer**. Cette opération entraîne la suppression automatique des autres services associés, tels que Trend Micro Management Infrastructure et l'interface de passerelle commune (CGI), ainsi que la base de données Control Manager.
 - c. Cliquez sur **Oui** pour conserver la base de données ou sur **Non** pour la supprimer.



Remarque

Conserver la base de données permet de réinstaller Control Manager sur le serveur en conservant toutes les informations système, telles que l'enregistrement des agents et les données relatives aux comptes utilisateurs.

Si vous réinstallez le serveur Control Manager alors que vous aviez supprimé la base de données d'origine, mais pas les agents qui dépendaient à l'origine de l'installation précédente, ces agents sont réenregistrés auprès du serveur lorsque :

- Les serveurs des produits gérés redémarrent les services des agents
 - Les agents Control Manager vérifient leur connexion après une période de 8 heures
-

Suppression manuelle de Control Manager

Cette section indique comment supprimer manuellement Control Manager. N'utilisez les procédures ci-dessous qu'en cas d'échec de la fonction Ajout/Suppression de programmes de Windows ou du programme de désinstallation de Control Manager.



Remarque

Les instructions relatives à Windows peuvent varier selon la version du système d'exploitation. Les procédures suivantes sont rédigées pour **Windows Server 2003**.

La suppression de Control Manager implique le retrait de composants différents. Ces composants peuvent être supprimés dans n'importe quel ordre, voire tous en même temps. Cependant, dans un souci de clarté, la désinstallation de chaque module est décrite séparément, dans des sections distinctes. Les composants sont les suivants :

- Application Control Manager
- Trend Micro Management Infrastructure
- Common CGI Modules (CGI)
- Control Manager Database (facultatif)
- PHP
- FastCGI

D'autres produits Trend Micro utilisent aussi Trend Micro Management Infrastructure et les modules de l'interface de passerelle commune (CGI), de sorte que si d'autres produits Trend Micro sont installés sur le même ordinateur, il est recommandé de ne pas supprimer ces deux composants.



Remarque

Une fois tous les composants supprimés, vous devez redémarrer le serveur. Cette opération n'est nécessaire qu'à une seule reprise, une fois la suppression effectuée.

Suppression de l'application Control Manager

La suppression manuelle de l'application Control Manager comporte les étapes suivantes :

1. *Arrêt des services Control Manager à la page 5-4*
2. *Suppression des paramètres IIS de Control Manager à la page 5-5*
3. *Suppression de Crystal Reports, PHP, FastCGI, TMI et CCGI à la page 5-7*
4. *Suppression des fichiers/répertoires et clés de registre de Control Manager à la page 5-8*
5. *Suppression des composants de base de données à la page 5-9*
6. *Suppression de Control Manager et des services NTP à la page 5-10*

Arrêt des services Control Manager

L'écran Windows Services permet de redémarrer les services de Control Manager suivants :

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager
- Trend Micro NTP



Remarque

Il s'agit des services exécutés en arrière-plan dans le système d'exploitation Windows, non pas des services Trend Micro qui nécessitent des codes d'activation (par exemple, Outbreak Prevention Services).

Arrêt des services Control Manager depuis l'écran des services Windows

Procédure

1. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Services** pour ouvrir l'écran **Services**.
 2. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Arrêter**.
-

Arrêt des services IIS et Control Manager à partir de l'invite de commande

Procédure

- Exécutez les commandes suivantes à l'invite de commande :

```
net stop w3svc
```

```
net stop tmcm
```

Suppression des paramètres IIS de Control Manager

Supprimez les paramètres Internet Information Services après avoir arrêté les services Control Manager.

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer** > **Exécuter**.
La boîte de dialogue **Exécuter** s'affiche.
2. Saisissez la ligne suivante dans le champ **Ouvrir** :

```
%SystemRoot%\System32\Inetsrv\iis.msc
```

3. Dans le menu de gauche, double-cliquez sur le nom du serveur pour développer l'arborescence de la console.
 4. Double-cliquez sur **Site Web par défaut**.
 5. Supprimez les répertoires virtuels suivants :
 - ControlManager
 - TVCSDownload
 - crystalreportviewers12
 - TVCS
 - Jakarta
 - WebApp
 6. Sur IIS 6 uniquement :
 - a. Cliquez avec le bouton droit de la souris sur le site Web IIS que vous avez défini au cours de l'installation.
 - b. Cliquez sur **Propriétés**.
 7. Cliquez sur l'onglet **Filtres ISAPI**.
 8. Supprimez les filtres ISAPI suivants :
 - TmcmRedirect
 - CCGIRedirect
 - ReverseProxy
 9. Sur IIS 6 uniquement, supprimez les extensions de service Web suivantes :
 - Filtre de redirection de Trend Micro CGI (en cas de suppression de CCGI)
 - Extensions Trend Micro Control Manager CGI
-

Suppression de Crystal Reports, PHP, FastCGI, TMI et CCGI

La suppression de PHP, FastCGI, TMI et CCGI est facultative. Utilisez la fonction Ajout/Suppression de programmes pour désinstaller Crystal Reports, PHP et FastCGI.

Suppression de Cristal Reports

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Ajouter/Supprimer des programmes**.
 2. Faites défiler la liste des programmes jusqu'aux fichiers d'exécution de Crystal Reports, puis cliquez sur **Supprimer** pour supprimer automatiquement les fichiers associés à Crystal Reports.
-

Suppression de PHP et FastCGI

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer > Paramètres > Panneau de configuration > Ajouter/Supprimer des programmes**.
 2. Faites défiler la liste jusqu'à PHP, puis cliquez sur **Supprimer** pour supprimer automatiquement les fichiers associés à PHP.
 3. Faites défiler la liste jusqu'à FastCGI, puis cliquez sur **Supprimer** pour supprimer automatiquement les fichiers associés à FastCGI.
-

Suppression de TMI et CCGI

Procédure

1. Téléchargez l'outil de service Microsoft Sc.exe vers le serveur Control Manager :
<http://support.microsoft.com/kb/251192/fr>

2. Exécutez `Sc.exe` et saisissez les commandes suivantes :

```
sc delete "TrendCGI"
```

```
sc delete "TrendMicro Infrastructure"
```

Suppression des fichiers/répertoires et clés de registre de Control Manager

Procédure

1. Supprimez les répertoires suivants :

- `.Trend Micro\Control Manager`
- `.Trend Micro\COMMON\ccgi`
- `.Trend Micro\COMMON\TMI`
- `.PHP`
- `C:\Documents and Settings\All Users\Start Menu\Programs\PHP 5`
- `C:\Documents and Settings\All Users\Start Menu\Programs\Trend Micro Control Manager`

2. Supprimez les clés de registre suivantes de Control Manager :

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPTrustPort`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS`

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro
\VulnerabilityAssessmentServices
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
\CurrentVersion\Uninstall\TMCM
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
\CurrentVersion\Uninstall\TMI
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\TMCM
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\TrendCCGI
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\TrendMicro Infrastructure
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
\TrendMicro_NTP
-

Suppression des composants de base de données

Cette section décrit la manière de supprimer les composants de base de données suivants du serveur Control Manager :

- Suppression des paramètres ODBC de Control Manager
- Suppression de la base de données Control Manager SQL Server 2008 Express

Suppression des paramètres ODBC de Control Manager

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer** > **Exécuter**.

La boîte de dialogue **Exécuter** s'affiche.

2. Saisissez la ligne suivante dans le champ Ouvrir :

`odbcad32.exe`.

3. Dans la fenêtre **Administrateur de sources de données ODBC**, cliquez sur l'onglet **Nom DSN système**.
 4. Sous **Nom**, sélectionnez **ControlManager_Database**.
 5. Cliquez sur **Supprimer**, puis cliquez sur **Oui** pour confirmer.
-

Suppression de la base de données Control Manager SQL Server 2008 Express

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer > Panneau de configuration > Ajout/Suppression de programmes**.
 2. Faites défiler la liste jusqu'à **SQL Server 2008 Express**, puis cliquez sur **Supprimer** pour supprimer automatiquement les fichiers associés.
-



Conseil

Trend Micro vous recommande de consulter le site internet de Microsoft pour obtenir des instructions sur la suppression de SQL Server 2008 Express si vous rencontrez des problèmes lors de la désinstallation :

<http://support.microsoft.com/kb/909967>

Suppression de Control Manager et des services NTP

Procédure

1. Téléchargez l'outil de service Microsoft `sc.exe` dans le serveur Control Manager : <http://support.microsoft.com/kb/251192/fr>
2. Exécutez `sc.exe` et saisissez les commandes suivantes :

```
sc delete "TMCM"
```

```
sc delete "TrendMicro_NTP"
```

Suppression d'un agent Control Manager 2.x sur Windows

Pour supprimer un ou plusieurs agents, vous devez exécuter le composant de désinstallation du programme d'installation d'agents Control Manager.

Désinstallez des agents soit à distance en exécutant le programme à partir du serveur Control Manager ou d'un autre serveur, soit localement en exécutant le programme d'installation sur l'ordinateur de chaque agent.

Procédure

1. Accédez à **Administration > Paramètres > Paramètres d'agents de produits**.
L'écran **Paramètres d'agents de produits** apparaît.
2. Cliquez sur le lien **RemoteInstall.exe** pour télécharger l'application.
3. Dans l'Explorateur Windows, accédez au dossier où vous avez enregistré le programme d'installation d'agents.
4. Cliquez deux fois sur le fichier `RemoteInstall.exe`.

L'écran **Installation d'agent de Trend Micro Control Manager** apparaît.

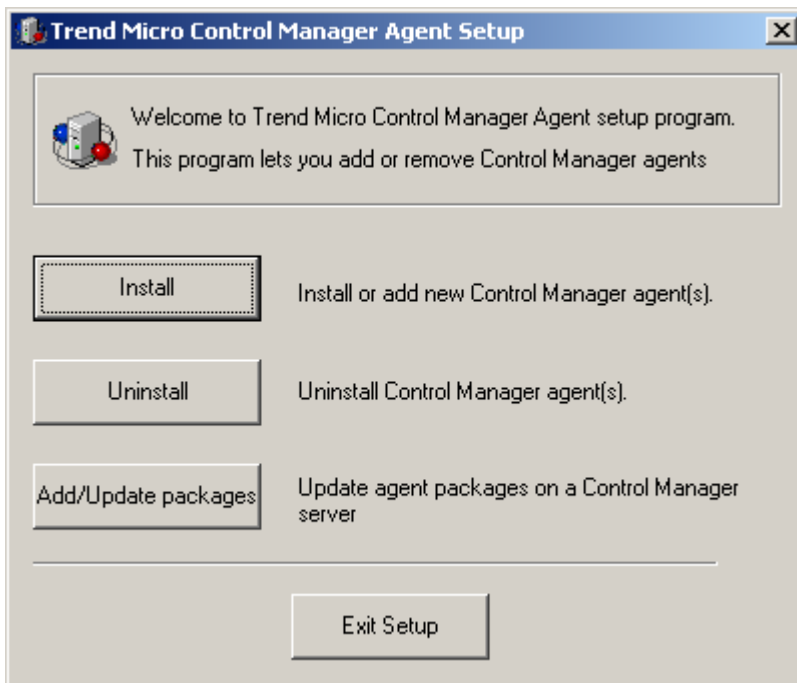


FIGURE 5-1. Programme d'installation des agents de Trend Micro Control Manager

5. Cliquez sur **Désinstaller**.

L'écran de **Bienvenue** apparaît.

6. Cliquez sur **Suivant**.

L'écran **Connexion au serveur source Control Manager** apparaît.

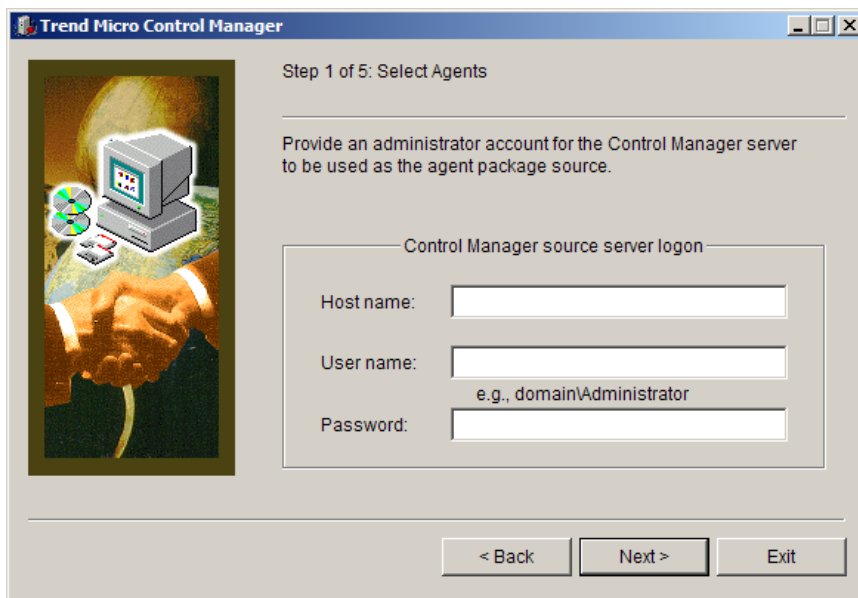


FIGURE 5-2. Connexion au serveur source Control Manager

7. Spécifiez et indiquez les informations d'identification de connexion de niveau administrateur pour le serveur Control Manager. Entrez les informations suivantes :
 - Nom d'hôte
 - Nom d'utilisateur
 - Mot de passe
8. Cliquez sur **Suivant**. Sélectionnez le produit dont vous souhaitez supprimer l'agent.
9. Cliquez sur **Suivant**. Sélectionnez les serveurs sur lesquels vous souhaitez supprimer les agents. Pour ce faire, vous pouvez procéder de deux façons :
 - Pour sélectionner un serveur dans la liste :

- a. Dans la liste de gauche, double-cliquez sur le domaine contenant les serveurs antivirus; la liste de tous les serveurs de ce domaine s'affiche.
 - b. Sélectionnez le(s) serveur(s) cible(s) dans cette liste, puis cliquez sur **Ajouter**. Le serveur que vous avez sélectionné est ajouté à la liste de droite. Cliquez sur **Ajouter tout** pour ajouter des agents à tous les serveurs du domaine sélectionné. Vous pouvez également double-cliquer sur un serveur pour l'ajouter à la liste de droite.
 - Pour spécifier le nom d'un serveur directement :
 - a. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du serveur dans le champ **Nom du serveur**.
 - b. Cliquez sur **Ajouter**. Le serveur est ajouté à la liste de droite. Pour supprimer un serveur de la liste, sélectionnez-le dans la liste de droite, puis cliquez sur **Supprimer**. Pour supprimer tous les serveurs, cliquez sur **Supprimer tout**.
10. Cliquez sur **Précédent** pour revenir à l'écran précédent, sur **Quitter** pour abandonner l'opération ou sur **Suivant** pour continuer.
 11. Indiquez les informations d'identification de connexion de niveau administrateur pour les serveurs sélectionnés. Entrez le nom d'utilisateur et le mot de passe requis dans les champs correspondants.
 12. Cliquez sur **OK**. L'écran **Analyse du serveur choisi** indique les détails suivants sur les serveurs cibles : nom du serveur, domaine et type de l'agent détecté.
 13. Cliquez sur **Suivant** pour continuer. Le tableau de cet écran affiche les informations suivantes sur les serveurs cibles : nom du serveur, version du système d'exploitation, adresse IP, nom de domaine et version de l'agent que vous allez supprimer. Cliquez sur **Précédent** pour revenir à l'écran précédent, sur **Quitter** pour abandonner l'opération ou sur **Désinstaller** pour supprimer l'agent. La désinstallation démarre.
 14. Cliquez sur **OK** puis, sur l'écran **Suppression des agents**, cliquez sur **Quitter**.
-

Chapitre 6

Obtenir de l'assistance

Trend Micro s'engage à fournir des services et une assistance dépassant les attentes des utilisateurs. Le présent chapitre indique comment faire appel à l'assistance technique. N'oubliez pas que vous devez enregistrer votre produit pour pouvoir bénéficier de cette assistance.

Ce chapitre traite les rubriques suivantes :

- *Avant de contacter l'assistance technique à la page 6-2*
- *Comment contacter l'assistance technique à la page 6-2*
- *TrendLabs à la page 6-3*
- *Autres ressources utiles à la page 6-4*

Avant de contacter l'assistance technique

Avant de contacter l'assistance technique, commencez par effectuer les deux opérations suivantes pour tenter de trouver une solution rapide à votre problème :

- **Consultez votre documentation** : le manuel et l'aide en ligne fournissent des informations exhaustives sur Control Manager. Faites une recherche dans les deux documents pour voir s'ils contiennent la solution.
- **Visitez le site Web de notre service d'assistance technique** : notre site d'assistance technique contient les dernières informations sur tous les produits Trend Micro. Il recense également les réponses aux questions précédemment posées par les utilisateurs.

Pour faire une recherche dans la base de connaissances, rendez-vous sur

<http://esupport.trendmicro.com/default.aspx>

Comment contacter l'assistance technique

Trend Micro fournit une assistance technique, des téléchargements de signatures et des mises à jour de programmes à tous les utilisateurs enregistrés pendant une année. Au terme de cette période, un paiement sera exigé pour renouveler la maintenance. Si vous avez besoin d'aide ou si vous avez simplement une question, n'hésitez pas à nous contacter. Vos commentaires sont aussi toujours les bienvenus.

- Consultez la liste des centres d'assistance à travers le monde à l'adresse suivante : <http://esupport.trendmicro.com>
- Procurez-vous la documentation la plus récente concernant les produits Trend Micro à l'adresse suivante : <http://docs.trendmicro.com/fr-fr/home.aspx>

Aux États-Unis, vous pouvez contacter les revendeurs Trend Micro par téléphone, fax ou e-mail :

```
Trend Micro, Inc. 10101 North De Anza Blvd.,  
Cupertino, CA 95014  
Toll free: +1 (800) 228-5651 (sales)  
Voice: +1 (408) 257-1500 (main)
```

Fax: +1 (408) 257-2003
Web address : <http://www.trendmicro.com/>
Email : support@trendmicro.com

Résolution plus rapide des problèmes

Pour accélérer la résolution des problèmes, lorsque vous contactez notre équipe technique, veuillez fournir le plus d'informations possible :

- Numéro de série du produit
- Version de compilation de Control Manager
- Version du système d'exploitation, type de connexion Internet et version de la base de données (par exemple, SQL 2005 ou SQL 2008)
- Énoncé précis du message d'erreur (le cas échéant)
- Étapes permettant de reproduire le problème

TrendLabs

Trend Micro TrendLabsSM est un réseau mondial de centres de recherche antivirus et d'assistance qui fournit une assistance 24 heures sur 24, 7 jours sur 7 à tous les clients Trend Micro à travers le monde.

Avec des équipes de plus de 250 ingénieurs et spécialistes de l'assistance technique, les centres de services dédiés des TrendLabs répartis dans le monde entier permettent de contrecarrer rapidement toute épidémie virale ou de résoudre les problèmes urgents des clients, partout dans le monde.

Le siège social moderne des TrendLabs a obtenu la certification ISO 9002 pour ses procédures de gestion de qualité en 2000. Il constitue l'un des premiers centres d'assistance et de recherche antivirus à être ainsi agréé. Chez Trend Micro, nous pensons que les TrendLabs figurent au premier rang de l'industrie antivirus en matière de services et d'assistance.

Autres ressources utiles

Trend Micro offre de nombreux services par l'intermédiaire de son site Web, <http://www.trendmicro.com/>.

Les outils et services fournis par Internet sont les suivants :

- **Trend Micro™ Smart Protection Network™** : contrôle les incidents de menaces de sécurité dans le monde
- **HouseCall™** : scan antivirus Trend Micro en ligne

Annexe A

Journal système de Control Manager

Servez-vous des listes de contrôle fournies dans cette annexe pour consigner les informations système pertinentes en guise de référence.

Cette annexe contient les sections suivantes :

- *Liste de contrôle de l'adresse du serveur à la page A-2*
- *Liste de contrôle des ports à la page A-3*
- *Liste de contrôle d'installation de l'agent Control Manager 2.x à la page A-4*
- *Conventions relatives à Control Manager à la page A-5*
- *Processus principal et fichiers de configuration à la page A-6*
- *Ports de communication et d'écoute à la page A-8*
- *Comparaison des versions de Control Manager à la page A-9*

Liste de contrôle de l'adresse du serveur

Vous devez indiquer les informations suivantes sur l'adresse du serveur lors de l'installation et de la configuration du serveur Control Manager pour qu'il fonctionne sur votre réseau. Notez ces informations ici pour pouvoir vous y reporter facilement.

TABLEAU A-1. Liste de contrôle de l'adresse du serveur

INFORMATIONS REQUISES	ÉCHANTILLON	VOTRE VALEUR
Informations relatives au serveur Control Manager		
Adresse IP	10.1.104.255	
Nom de domaine complet (FQDN)	server.company.com	
Nom (d'hôte) NetBIOS	yourserver	
Informations relatives au serveur Web		
Adresse IP	10.1.104.225	
Nom de domaine complet (FQDN)	server.company.com	
Nom (d'hôte) NetBIOS	yourserver	
Informations relatives à la base de données SQL de Control Manager		
Adresse IP	10.1.104.225	
Nom de domaine complet (FQDN)	server.company.com	
Nom (d'hôte) NetBIOS	sqlserver	
Serveur proxy pour le téléchargement des composants		
Adresse IP	10.1.174.225	
Nom de domaine complet (FQDN)	proxy.company.com	

INFORMATIONS REQUISES	ÉCHANTILLON	VOTRE VALEUR
Nom (d'hôte) NetBIOS	proxyserver	
Informations sur le serveur SMTP (facultatif, pour les notifications par courrier électronique)		
Adresse IP	10.1.123.225	
Nom de domaine complet (FQDN)	mail.company.com	
Nom (d'hôte) NetBIOS	mailserver	
Informations sur le déROUTement SNMP (facultatif, pour les notifications par déROUTement SNMP)		
Nom de communauté	trendmicro	
Adresse IP	10.1.194.225	

Liste de contrôle des ports

Control Manager fait appel aux ports suivants pour les utilisations indiquées.

PORT	ÉCHANTILLON	VOTRE VALEUR
SMTP	25	
Proxy	8088	
Pageur COM	COM1	
Proxy pour l'agent Trend VCS (facultatif)	223	
Console Web et mise à jour/déploiement de composants	80	

PORT	ÉCHANTILLON	VOTRE VALEUR
Pare-feu, port de "transfert" (facultatif ; utilisé lors de l'installation d'agents Control Manager)	224	
Communication entre processus internes Trend Micro Management Infrastructure (TMI) (pour les produits à distance)	10198	
Communication avec les processus externes TMI	10319	
Émulateur d'entité	10329	



Remarque

Control Manager requiert l'usage exclusif des ports 10319 et 10198.

Liste de contrôle d'installation de l'agent Control Manager 2.x

Les informations suivantes sont utilisées lors de l'installation des agents.

INFORMATIONS REQUISES	ÉCHANTILLON	VOTRE VALEUR
Nom d'utilisateur du compte administrateur du serveur Control Manager	racine	
Emplacement de la clé de chiffrement	C:\Mes Documents \E2EPublic.dat	

**Remarque**

Vous pouvez utiliser un nom d'utilisateur quelconque à la place du compte racine. Toutefois, Trend Micro recommande l'utilisation du compte racine, car la suppression du nom d'utilisateur spécifié lors de l'installation de l'agent rend la gestion de l'agent très difficile.

LE NOM DU PRODUIT	COMPTE DE NIVEAU ADMINISTRATEUR	ADRESSE IP	NOM D'HÔTE
Échantillon	Admin	10.225.225.225	PH-antivirus

Conventions relatives à Control Manager

Reportez-vous aux conventions suivantes applicables à l'installation de Control Manager ou à la configuration de la console Web.

- Noms d'utilisateurs

Longueur maximale	32 caractères
Caractères admis	A à Z, a à z, 0 à 9, -, _

- Noms de dossiers

Longueur maximale	40 caractères
Caractères non admis	/ > & "

**Remarque**

Pour le nom d'hôte du serveur Control Manager, le programme d'installation prend en charge les serveurs dont le nom comporte des tirets de soulignement ("_").

Processus principal et fichiers de configuration

Control Manager enregistre les paramètres de configuration système et les fichiers temporaires au format XML.

Les tableaux suivants décrivent les fichiers de configuration et les processus utilisés par Control Manager.

TABEAU A-2. Fichiers de configuration de Control Manager

FICHIER DE CONFIGURATION	DESCRIPTION
AuthInfo.ini	Fichier de configuration qui contient des informations sur les noms de fichiers de clé privée, les noms de fichiers de clé publique, les noms de fichiers de certificat et la phrase de passe chiffrée de la clé privée, ainsi que sur l'ID et le port de l'hôte
aucfg.ini	Fichier de configuration ActiveUpdate
TVCS_Cert.pem	Certificat utilisé par l'authentification SSL
TVCS_Pri.pem	Clé privée utilisée par SSL
TVCS_Pub.pem	Clé publique utilisée par SSL
ProcessManager.xml	Utilisé par <code>ProcessManager.exe</code>
CmdProcessorEventHandler.xml	Utilisé par <code>CmdProcessor.exe</code>
UIProcessorEventHandler.xml	Utilisé par <code>UIProcessor.exe</code>
DMRegisterinfo.xml	Utilisé par <code>CasProcessor.exe</code>
DataSource.xml	Stocke les paramètres de connexion des processus Control Manager
SystemConfiguration.xml	Fichier de configuration système de Control Manager

FICHIER DE CONFIGURATION	DESCRIPTION
CascadingLogConfiguration.xml	Fichier de configuration de téléchargement des journaux utilisé pour les serveurs enfants
agent.ini	Fichier de l'agent MCP
TMI.cfg	Fichier de configuration de Trend Micro Management Infrastructure

TABLEAU A-3. Processus Control Manager

PROCESSUS	DESCRIPTION
ProcessManager.exe	Il lance et arrête les autres processus principaux Control Manager.
CmdProcessor.exe	Envoie des instructions XML formulées par d'autres processus aux produits gérés, procède à l'enregistrement de produits, envoie des alertes, effectue des tâches programmées et applique les stratégies de prévention des épidémies.
UIProcessor.exe	Traite les données entrées par les utilisateurs au niveau de la console Web de Control Manager et les transforme en commandes effectives.
LogReceiver.exe	Reçoit les journaux et messages des produits gérés.
LogProcessor.exe	Reçoit les nouveaux messages des produits gérés et les informations sur l'entité des serveurs enfants Control Manager.
LogRetriever.exe	Récupère et enregistre les journaux dans la base de données de Control Manager.
ReportServer.exe	Génère des rapports Control Manager.

PROCESSUS	DESCRIPTION
MsgReceiver.exe	Reçoit les messages provenant du serveur Control Manager, des produits gérés et des serveurs enfants.
EntityEmulator.exe	Permet à Control Manager d'utiliser des agents Trend VCS.
Casprocessor.exe	Permet à un serveur Control Manager (serveur parent) de gérer d'autres serveurs Control Manager (serveurs enfants).
DCSprocessor.exe	Exécute des fonctions Damage Cleanup Services.
Ntpd.exe	Service Network Time Protocol.
inetinfo.exe	Processus Microsoft Internet Information Service.
jk_nt_service.exe java.exe	Extensions Java côté serveur utilisées pour générer une interface utilisateur Web en la définissant au lieu de faire appel à de nombreux programmes CGI autonomes.
cm.exe	Gère dmserver.exe et mrf.exe.
mrf.exe	Processus du communicateur
dmserver.exe	Affiche la page de connexion de la console Web de Control Manager et gère le répertoire Produits (côté Control Manager).
sCloudProcessor.NET.exe	Gère les tâches liées à la gestion des stratégies.

Ports de communication et d'écoute

Les ports de communication et d'écoute par défaut de Control Manager sont les suivants.

TYPE	PORT DE COMMUNICATION
Communication interne	10198
Communication externe	10319

SERVICE	PORT DU SERVICE
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
Casprocessor.exe	20801
DcsProcessor.exe	20903

Comparaison des versions de Control Manager

Le tableau suivant fournit une comparaison des fonctions des versions de Control Manager.

TABEAU A-4. Comparaison des versions de produit

FONCTIONS	VERSION DE CONTROL MANAGER					
	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD	6.0 ADV	6.0 STD
Interfaces d'agent 2.x et MCP avec les produits gérés	●	●	●	●	●	●
Requête ad hoc	●	●	●	●	●	●
Mise à jour automatique des composants (par exemple, fichiers de signatures/règles)	●	●	●	●	●	●
Structure de la gestion en cascade	●		●		●	
Base de données centrale pour tous les événements système et du journal des virus	●	●	●	●	●	●
Solution de gestion antivirus centralisée sur le Web pour l'entreprise	●	●	●	●	●	●
Surveillance de serveurs enfants	●		●		●	
Émission de tâches de serveurs enfants	●		●		●	
Suivi des commandes	●	●	●	●	●	●
Battement de cœur du communicateur	●	●	●	●	●	●
Programmateur de communicateurs	●	●	●	●	●	●
Téléchargement granulaire des composants	●	●	●	●	●	●
Configuration par groupe	●	●	●	●	●	●

FONCTIONS	VERSION DE CONTROL MANAGER					
	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD	6.0 ADV	6.0 STD
Configuration de plusieurs sources de téléchargement	●	●	●	●	●	●
Interface utilisateur cohérente du produit géré et de Control Manager	●	●	●	●	●	●
Fichiers MIB de Control Manager (précédemment appelés MIB HP OpenView)	●	●	●	●	●	●
Types d'utilisateurs personnalisés	●	●	●	●	●	●
Plans de déploiement	●	●	●	●	●	●
Gestionnaire de répertoires	●	●	●	●	●	●
Communication avec sécurité avancée	●	●	●	●	●	●
Centre d'événements	●	●	●	●	●	●
Navigation améliorée	●	●	●	●	●	●
Interface utilisateur améliorée	●	●	●	●	●	●
Intégration d'InterScan Web Security Service	●	●	●	●	●	●
Améliorations de la journalisation	●	●	●	●	●	●
Améliorations apportées à la vitesse de traitement des journaux			●	●	●	●
Gestion des produits antivirus et de sécurité de contenu	●	●	●	●	●	●
Gestion des services	●	●	●	●	●	●

FONCTIONS	VERSION DE CONTROL MANAGER					
	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD	6.0 ADV	6.0 STD
Gestionnaire de licences des produits gérés	●		●		●	
Création de rapports de produit géré	●		●		●	
Amélioration du rendu de la console Web			●	●	●	●
Microsoft SQL Express ou Microsoft SQL 2005	●	●	●	●		
Microsoft SQL Express ou Microsoft SQL 2008					●	●
MSDE ou Microsoft SQL 7/2000	●	●				
Notification MSN Messenger	●	●	●	●	●	●
Notification et alerte d'épidémie	●	●	●	●	●	●
Améliorations de l'intégration d'OfficeScan			●	●	●	●
Outbreak Commander/Outbreak Prevention Services (OPS) <ul style="list-style-type: none"> • Téléchargement et déploiement automatiques d'OPP • Téléchargement et déploiement manuels d'OPP 	●	●	●	●	●	●
Prise en charge passive d'un produit tiers	●		●		●	
Gestion des stratégies					●	●
Installation d'agents locale et à distance	●	●	●	●	●	●

FONCTIONS	VERSION DE CONTROL MANAGER					
	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD	6.0 ADV	6.0 STD
Gestion à distance	●	●	●	●	●	●
Création de rapports	●		●		●	
Communication sécurisée entre serveur et agents	●	●	●	●	●	●
Système de signature unique (SSO, Single Sign-On) pour les produits gérés qui prennent en charge cette fonction	●	●	●	●	●	●
Intégration de Smart Protection Network			●	●	●	●
Notification par déroutement SNMP	●		●		●	
Prise en charge SSL pour ActiveUpdate	●	●	●	●	●	●
Prise en charge SSL pour la console Web	●	●	●	●	●	●
Prise en charge des agents de Control Manager 2.x	●	●	●	●	●	●
Prise en charge de la communication HTTPS entre serveur, agents et produits gérés	●	●	●	●	●	●
Prise en charge des agents MCP	●	●	●	●	●	●
Notification Syslog	●		●		●	
Tableau de bord basé sur l'intelligence des menaces			●	●	●	●

FONCTIONS	VERSION DE CONTROL MANAGER					
	5.0 ADV	5.0 STD	5.5 ADV	5.5 STD	6.0 ADV	6.0 STD
Intégration de Trend Micro InterScan for Cisco Content Security et Control Security Services Module (ISC CSC SSM)	●	●	●	●	●	●
Intégration de Trend Micro Network VirusWall 1200	●	●	●	●	●	●
Intégration de Trend Micro Network VirusWall 2500	●	●	●	●	●	●
Intégration du serveur d'enregistrement de produit Trend Micro	●	●	●	●	●	●
Tableau de messages des TrendLabs	●	●				
Gestion de compte utilisateur	●	●	●	●	●	●
Évaluation des failles	●	●	●	●	●	●
Authentification Windows	●	●	●	●	●	●
Contrôle des heures de travail	●	●	●	●	●	●

Index

A

- activation
 - Control Manager, 3-27, 3-28
- avantages de MCP
 - prise en charge du protocole HTTPS, 1-7
 - prise en charge transversale du NAT et des pare-feu, 1-6
 - réduction de la charge du réseau et de la taille de paquet, 1-5

B

- base de données
 - recommandations, 2-24
- batttement de cœur
 - MCP, 2-20
 - TMI, 2-18

C

- clé d'enregistrement, 3-30
- code d'activation, 3-28
- communication
 - mode bidirectionnel, 1-8
 - mode unidirectionnel, 1-7
- communications en mode bidirectionnel, 1-8
- communications en mode unidirectionnel, 1-7
- comprendre
 - MCP, 1-4
- comptes utilisateurs
 - configuration, 3-27
- configuration
 - comptes utilisateurs, 3-27
 - Serveur Web, 2-25
- configuration système requise, 3-2

- Control Manager, 1-1, 1-9
 - activation, 3-27, 3-28
 - agent, 1-10
 - à propos de, 1-1
 - base de données SQL, 1-9
 - comparaison des versions des fonctions, A-9
 - configuration système requise, 3-2
 - console d'administration à interface Web, 1-11
 - enregistrement, 3-27, 3-28
 - étapes d'installation, 3-4
 - Flux de migration des agents 2.5x, 4-16
 - fonctions, 1-2
 - fonctions de base, 1-2
 - infrastructure de widgets, 1-11
 - installation, 3-1, 3-3, 3-4
 - invite de commande, arrêt du service, 5-5
 - MCP, 1-10
 - migration de la base de données, 4-19
 - niveaux de sécurité, 3-12, 3-15
 - serveur de messagerie, 1-9
 - serveur de rapports, 1-9
 - Serveur Web, 1-9
 - suppression manuelle, 5-3, 5-4
 - test d'un déploiement pilote, 2-12
 - Trend Micro Management Infrastructure, 1-10
- conversion
 - version complète, 3-30

D

- définition

- déploiement sur plusieurs sites, 2-6
- déploiement sur site unique, 2-4

- déploiement
 - architecture et stratégie, 2-3
 - plusieurs sites, 2-6
 - site unique, 2-4

- déploiement pilote
 - test, 2-12

- déploiement sur plusieurs sites
 - définition, 2-6

- déploiement sur site unique
 - définition, 2-4

- désinstallation manuelle, 5-3

E

- enregistrement
 - Control Manager, 3-27, 3-28

- enregistrement de produit
 - trafic, 2-22

- étapes d'installation
 - Control Manager, 3-4

F

- flux
 - migration des agents Control Manager 2.5x, 4-16
 - migration des agents MCP, 4-16

- fonctions, 1-2

I

- installation
 - Control Manager, 3-1, 3-4
 - étapes, 3-4
 - flux, 2-12
 - vérifier la réussite, 3-23

- interrogation de commande
 - MCP, 2-21

- invite de commande
 - Control Manager, arrêt du service, 5-5

J

- journaux
 - trafic, 2-19

L

- liste de contrôle
 - adresse du serveur, A-2
 - ports, A-3

- liste de contrôle de l'adresse du serveur, A-2

M

- manuel
 - suppression de Control Manager, 5-4

- MCP, 1-10

- battement de cœur, 2-20

- comprendre, 1-4

- flux de migration, 4-16

- interrogation de commande, 2-21

- stratégies, 2-20

- migration, 4-12

- agents MCP, 4-16

- agents Trend VCS, Control Manager 2.x et MCP, 4-17

- base de données, 4-19

- Control Manager SQL 2000, 4-19

- flux de migration des agents Control Manager 2.5x, 4-16

- migration d'un seul serveur, 4-14

- mise à niveau progressive, 4-13

- mise à niveau rapide, 4-12

- scénarios, 4-13

- serveurs et agents différents, 4-15

- stratégie, 4-12

- mise à niveau, 4-2

- considérations, 4-2
- informations sur la sauvegarde de Control Manager, 4-7-4-9
- mise à niveau progressive, 4-13
- mise à niveau rapide, 4-12
- mises à jour
 - déploiement, 2-23

N

- NAT, prise en charge transversale, 1-6
- niveaux de sécurité, 3-13

O

- ODBC
 - paramètres, Control Manager, 5-9

P

- pare-feu, prise en charge transversale, 1-6
- plan de distribution des serveurs, 2-15
- plan de trafic réseau, 2-17
- port
 - liste de contrôle, A-3
- préface, 1
- prise en charge transversale
 - NAT et pare-feu, 1-6

R

- recommandations
 - base de données, 2-24
- renouvellement du contrat de maintenance, 3-30
- rétablissement
 - des serveurs Control Manager 5.0/3.5, 4-10

S

- sauvegarde de Control Manager, 4-7-4-9
- serveur

- adresse, liste de contrôle, A-2
- Serveur Web
 - configuration, 2-25
 - plan, 2-25
- SSO, 1-8
- stockage de données
 - plan, 2-24
- stratégies
 - MCP, 2-20
 - TMI, 2-21
- suppression
 - manuelle
 - Control Manager, 5-4
 - Microsoft Data Engine, 5-9
 - manuelle de Control Manager, 5-3

T

- TMI
 - battement de cœur, 2-18
 - stratégies, 2-21
- trafic réseau, 2-17
 - sources, 2-19

V

- vérifier l'installation correcte, 3-23
- version complète
 - conversion, 3-30

