TREND MICRO™

6.0 TREND MICRO™ Control Manager

Patch3 Manuel de l'administrateur

Gestion centralisée de la sécurité pour l'entreprise

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

Numéro de partie du document : CMEM65910/130321

Date de sortie : Mars 2013

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

Chapitre 3: Configuration des accès utilisateurs

Chapitre 4: Principes du répertoire Produits

Chapitre 5: Téléchargement et déploiement de composants

Partie II: Surveillance du réseau Control Manager

Chapitre 6: Utilisation du tableau de bord et des widgets

Chapitre 7: Utilisation du suivi des commandes

Chapitre 8: Utilisation des notifications

Chapitre 9: Utilisation des journaux

Chapitre 10: Utilisation des rapports

Partie III: Administration de Control Manager

Chapitre 11: Agents MCP et Control Manager

Chapitre 12: Administration des produits gérés

Chapitre 13: Activation de Control Manager et des produits gérés

Chapitre 14: Gestion des serveurs enfants

Chapitre 15: Gestion des stratégies

Chapitre 16: Investigation sur les incidents de prévention contre la perte de données

Chapitre 17: Administration de la base de données

Partie IV: Services et outils

Chapitre 18: Utilisation des services Trend Micro

Chapitre 19: Utilisation des outils de Control Manager

Partie V: Suppression de Control Manager et contact de l'assistance technique

Chapitre 20: Suppression de Trend Micro Control Manager

Chapitre 21: Obtenir de l'assistance

Annexes

Annexe A: Journal système de Control Manager

Annexe B: Affichages des données

Annexe C: Prise en charge d'IPv6 dans Control Manager

Annexe D: Vérification de l'état de la stratégie

Index

Préface

Préface

Ce manuel de l'administrateur présente Trend Micro™Control Manager™6.0 et parcourt la configuration pour le fonctionnement de Control Manager en fonction de vos besoins.

Cette préface traite les rubriques suivantes :

Nouveautés de cette version

Cette section répertorie les nouvelles fonctions et améliorations disponibles dans chaque version.

Fonctions et améliorations de Control Manager 6.0 Patch 3

De nouvelles fonctions et améliorations liées au service Command-and-Control Contact Alert (CCCA) sont disponibles dans la version 6.0 Patch 3.

FONCTION	DESCRIPTION
Widgets	• Événements de rappel C&C • Hôtes compromis uniques au fil du temps
Notification	• Alerte de rappel C&C • Alerte d'épidémie de rappel C&C
Journaux	Affichage de données d'informations de rappel C&C disponibles sous Informations sur les menaces de sécurité
Composants	Modèles disponibles pour les mises à jour : • Modèle d'informations C&C • Modèle avancé de programme malveillant

Fonctions et améliorations de Control Manager 6.0 Patch 2

Les nouvelles fonctions et améliorations de la version 6.0 Patch 2 sont les suivantes.

Fonction	Description
Rôles utilisateurs	Les rôles utilisateur DLP sont disponibles pour les investigations sur les incidents de DLP : • Responsable de conformité DLP • Réviseur d'incidents DLP
Notification	Les notifications DLP sont disponibles pour les investigations sur les incidents de DLP : • Résumé d'incidents programmé • Informations détaillées des incidents mises à jour
Niveaux de sévérité des modèles de DLP	Niveaux de sévérité des modèles de DLP visibles : • Élevé • Moyen • Faible • D'information • Indéfini
Investigation sur les incidents de DLP	• Les widgets du tableau de bord DLP sont disponibles pour la surveillance et la révision d'incidents DLP en fonction des niveaux de gravité et des utilisateurs gérés • Affichage d'une liste de résumés d'incidents DLP déclenchés par les utilisateurs gérés • Révision et mise à jour des informations détaillées sur l'incident
Journaux d'audit DLP	Exportation des journaux d'audit DLP

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	• 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	• 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)	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. Control Manager a intégré les fonctionnalités DLP suivantes : • 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	Documentation accessible en ligne à partir de la console Web de Control Manager. 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.
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	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.
Guide d'installation	Documentation PDF accessible sur le DVD Trend Micro Enterprise ou téléchargeable à partir du site Web de Trend Micro. Le guide d'installation explique en détail comment installer Control Manager et configurer les paramètres de base pour une prise en main rapide.
Manuel de l'administrateur	Document PDF accessible sur le DVD Solutions Trend Micro de Control Manager ou téléchargeable sur le site internet de Trend Micro. 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.

Document	Description
Didacticiel	Document PDF accessible sur le DVD Solutions Trend Micro de Control Manager ou téléchargeable sur le site internet de Trend Micro. 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.

Conventions typographiques

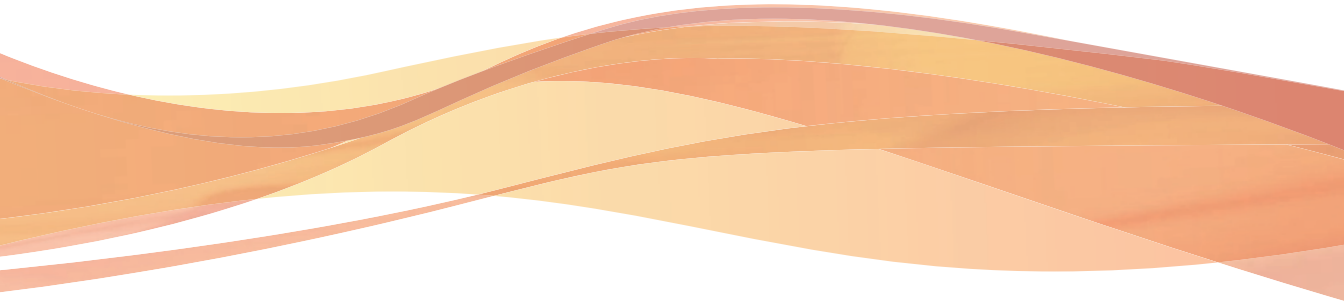
Pour faciliter la recherche et la compréhension des informations, cette documentation utilise les conventions suivantes.

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.
Italique	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.

Partie I

Démarrage



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.

Control Manager permet aux administrateurs système de surveiller et de signaler des activités telles que des infections, violations de sécurité et points d'entrée de virus/programmes malveillants. Les administrateurs système peuvent télécharger et déployer des composants de mise à jour sur le réseau, contribuant ainsi à garantir une protection homogène et actualisée. Les composants de mise à jour comprennent, par exemple, les fichiers de signatures de virus, les moteurs de scan et les règles de filtrage de courrier indésirable. Control Manager permet de réaliser à la fois des mises à jour manuelles et programmées. Il permet de configurer et de gérer des produits, en groupe ou séparément, pour une flexibilité accrue.

Ce chapitre traite les rubriques suivantes :

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 fonctions 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.

TABLEAU 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	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. 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.
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	Control Manager utilise une infrastructure de communication reposant sur le protocole SSL (Secure Socket Layer). Selon les paramètres de sécurité utilisés, Control Manager peut chiffrer des messages avec ou sans authentification.
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	Les administrateurs système peuvent définir des comptes personnalisés avec des privilèges individualisés pour les utilisateurs de la console Web de Control Manager. 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.

FONCTION	DESCRIPTION
Suivi des commandes	Cette fonction permet de contrôler toutes les commandes exécutées à l'aide de la console Web de Control Manager. 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.
Contrôle de produits à la demande	Cette fonction permet de contrôler des produits gérés en temps réel. 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.
Contrôle centralisé des mises à jour	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.
Journalisation centralisée	Des journaux et des rapports complets permettent d'avoir une vue d'ensemble sur le fonctionnement des produits antivirus et de sécurité de contenu. Control Manager collecte des journaux de tous les produits gérés. Vous n'avez plus à vérifier le journal de chaque produit.

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.

TABLEAU 1-2. Composants de Control Manager

COMPOSANT	DESCRIPTION
Serveur Control Manager	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 : • Une base de données SQL qui stocke les configurations et les journaux des produits gérés. Control Manager stocke dans la base de données Microsoft SQL Server (`db_ControlManager.mdf`) 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. • Un serveur Web qui héberge la console Web de Control Manager. • Un serveur de messagerie qui envoie des notifications d'événement par courrier électronique. 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. • Un serveur de rapports, présent uniquement dans la version Advanced Edition, qui génère des rapports sur les produits antivirus et de sécurité de contenu. 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.

COMPOSANT	DESCRIPTION
Trend Micro Management Communication Protocol (MCP)	MCP gère les interactions entre le serveur Control Manager et les produits gérés qui prennent en charge les agents MCP de la dernière génération. MCP constitue la nouvelle épine dorsale du système Control Manager. 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.
Trend Micro Management Infrastructure	Gère les interactions du serveur Control Manager avec les produits gérés antérieurs. 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.
Agents Control Manager 2.x	Un agent reçoit des commandes du serveur Control Manager et lui renvoie des informations d'état et des journaux. 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.

COMPOSANT	DESCRIPTION
Console d'administration à interface Web	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™ 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.
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

Prise en main de Control Manager

La console d'administration à interface Web de Control Manager permet d'administrer des produits gérés et d'autres serveurs Control Manager.

Ce chapitre traite les rubriques suivantes :

Utilisation de la console d'administration

La console d'administration de Control Manager est une console à interface Web publiée sur Internet ou l'intranet via Microsoft™ Internet Information Server (IIS) et hébergée par le serveur Control Manager. Elle permet d'administrer le réseau Control Manager à l'aide d'un navigateur Web compatible à partir de n'importe quel ordinateur.

Remarque

Utilisez une résolution d'écran de 1024 x 768 pixels pour afficher la console Web.

La console Web contient les éléments suivants : menu principal, menus déroulants, zone de travail et menu Aide.

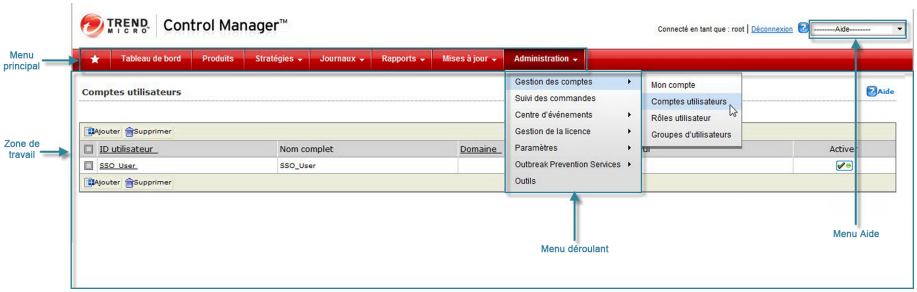


FIGURE 2-1. Console d'administration de Control Manager

Menu principal

Le menu principal de la console Web inclut des liens vers les fonctions Control Manager suivantes.

TABLEAU 2-1. Options du menu principal de Control Manager

ÉLÉMENT DU MENU PRINCIPAL	DESCRIPTION
Préférés (*)	Permet aux utilisateurs d'ajouter des raccourcis du menu pour un accès rapide

ÉLÉMENT DU MENU PRINCIPAL	DESCRIPTION
Tableau de bord	Permet d'ajouter des widgets pour obtenir des résumés de votre réseau lisibles en un coup d'œil. Les widgets incluent également des raccourcis vers des écrans d'informations détaillées et des requêtes ad hoc.
Produits	Contient des options permettant d'administrer des produits gérés, des communicateurs et des serveurs enfants.
Stratégies	Contient des options permettant de gérer des stratégies et de mettre à jour des modèles de stratégie.
Journaux	Contient des options permettant d'afficher les journaux de tous les produits enregistrés dans le serveur de Control Manager.
Rapports	Contient des options permettant de gérer des produits gérés Control Manager et des rapports de serveur enfant.
Mises à jour	Contient des options pour la configuration des mises à jour manuelles et programmées et des plans de déploiement de composants.
Administration	Contient les options Gestion des comptes, Suivi des commandes, Centre d'événements, Gestion de la licence, Paramètres, Outbreak Prevention Services et Outils.

Menu déroulant

Lorsque vous déplacez le pointeur de la souris sur chaque élément du menu principal, les menus déroulants correspondants s'affichent. Seuls les éléments de menu Tableau de bord et Produits n'ont pas de menu déroulant.

Zone de travail

Utilisez la zone de travail pour gérer le réseau Control Manager. Elle vous permet d'administrer les produits gérés ou les paramètres d'un serveur enfant, d'invoquer des tâches ou d'afficher l'état du système, les journaux et les rapports.

Menu Aide

Le menu Aide comporte les éléments suivants :

- Descriptions détaillées des fonctions avancées et informations détaillées sur la configuration.
- Informations sur les produits et procédures élaborées par l'équipe d'assistance de Trend Micro.
- Conseils sur les programmes malveillants les plus récents et liste des 10 menaces de sécurité les plus sévères du moment.
- Version et numéro de compilation de Control Manager, mention sur les droits d'auteur

Description du mécanisme de verrouillage de fonction

Le mécanisme de verrouillage de fonction de la console Web empêche que deux utilisateurs accèdent en même temps au même écran Gestionnaire des répertoires.

En d'autres termes, lorsque l'utilisateur A classe des produits gérés à l'aide du Gestionnaire des répertoires, l'utilisateur B, qui est également connecté à la console Web, ne peut accéder à l'écran Gestionnaire des répertoires.

Si vous tentez d'accéder à une option déjà utilisée, une fenêtre de message indiquant que l'option est verrouillée s'affiche. Control Manager permet uniquement l'accès à cette fonction par un utilisateur à la fois.

Pour vérifier si la fonction est toujours utilisée, cliquez régulièrement sur **Recharger**.

Pour déverrouiller, cliquez sur **Interrompre**.

Remarque

La fonction de déverrouillage est disponible pour les utilisateurs disposant des privilèges de gestion des dossiers de produits.

Accès à la console d'administration

Vous pouvez accéder à la console Web de deux manières :

- Accès local sur le serveur Control Manager
- Accès à distance à l'aide d'un navigateur compatible

Accès à la console Web localement à partir du serveur Control Manager

Procédure

1. Cliquez sur **Démarrer** > **Programmes** > **Trend Micro Control Manager** > **Trend Micro Control Manager**.
2. Complétez les champs Nom d'utilisateur et Mot de passe.
3. Cliquez sur **Connexion**.

Accès à la console à distance

Procédure

1. Entrez l'adresse suivante dans la barre d'adresse de votre navigateur pour afficher l'écran de connexion :

   `http(s)://{nom_hôte}/WebApp/login.aspx`

   Où `nom_hôte` est le nom de domaine complet (FQDN), l'adresse IP ou le nom du serveur Control Manager.
2. Complétez les champs Nom d'utilisateur et Mot de passe.
3. Cliquez sur **Connexion**.

À l'ouverture de la console Web, le tableau de bord affiche le résumé de l'état de l'ensemble du réseau Control Manager. Ce résumé est identique au résumé d'état généré

à partir du répertoire Produits. Les droits d'utilisateur déterminent les fonctions de Control Manager auxquelles un utilisateur a accès.

Remarque

Il est impossible de charger la console Web de Control Manager dans plusieurs navigateurs sur le même ordinateur avec les mêmes nom d'utilisateur et mot de passe. En revanche, l'exécution de plusieurs instances sur des ordinateurs différents avec les mêmes nom d'utilisateur et mot de passe est prise en charge.

Modification de l'accès à la console d'administration

Durant l'installation de Control Manager, vous pouvez choisir le niveau de sécurité pour l'accès à la console d'administration. Le niveau le moins sécurisé requiert uniquement une connexion HTTP. Le niveau le plus sécurisé requiert une connexion HTTPS. Si vous avez sélectionné le niveau le moins sécurisé durant l'installation, vous pouvez passer au niveau le plus sécurisé une fois l'installation terminée.

Vous devez obtenir un certificat et configurer le répertoire virtuel Control Manager avant de pouvoir échanger des informations chiffrées ou signées numériquement avec le serveur Control Manager.

Affectation de l'accès HTTPS à la console Web de Control Manager

Procédure

1. Obtenez un **certificat de site Web** auprès d'un fournisseur de certificats (comme Thawte.com ou VeriSign.com).
2. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Gestionnaires des services Internet** pour ouvrir la console IIS MMC (Microsoft Management Console).

3. Cliquez sur le signe **+** en regard du serveur IIS pour développer la liste des sites virtuels.

4. Sélectionnez **Site Web par défaut**, puis cliquez avec le bouton droit de la souris sur **Propriétés**.

5. Dans l'écran Propriétés du site Web par défaut, sélectionnez l'onglet **Sécurité du répertoire**, puis cliquez sur **Certificat de serveur** pour créer une demande de certificat de serveur à l'aide de l'assistant Nouveau Certificat.

   a. Cliquez sur **Suivant**.

   b. Dans l'écran Méthode de certificat de serveur, sélectionnez **Importer un certificat à partir d'un fichier de sauvegarde Key Manager**, puis cliquez sur **Suivant**.

   c. Entrez le **chemin d'accès complet** et le **nom de fichier** de la clé (par exemple, cm_cert.key), puis cliquez sur **Suivant**.

   d. Spécifiez le **mot de passe** de la clé, puis cliquez sur **Suivant**.

   e. Dans l'écran Résumé du certificat importé, cliquez sur **Suivant** pour implémenter le certificat de serveur ou cliquez sur **Retour** pour modifier des options.

6. Cliquez sur **OK** pour appliquer le certificat du serveur de site Web par défaut et revenir à la liste Site Web par défaut.

7. Sélectionnez le répertoire virtuel **Control Manager** dans la liste Site Web par défaut, puis cliquez avec le bouton droit de la souris sur **Propriétés**.

8. Cliquez sur l'onglet **Sécurité de répertoire**, puis cliquez sur **Modifier** sous Communications sécurisées. La fenêtre Communications sécurisées apparaît.

   a. Sélectionnez **Requérir un canal sécurisé (SSL)** et **Requérir le cryptage 128 bits**.

   b. Cliquez sur **OK** pour fermer cette fenêtre.

9. Cliquez sur **OK** pour appliquer les modifications et revenir à la liste Site Web par défaut.

   La prochaine fois que vous accéderez à la console Web à l'aide de HTTPS, le message suivant apparaîtra :

Cette page doit être affichée sur un canal sécurisé.

Configuration des paramètres de la console Web

Dans l'écran **Paramètres de la console Web**, configurez les paramètres de délai et d'actualisation automatique de la console. L'activation de la fonction d'actualisation automatique permet à la console Web de mettre à jour l'écran périodiquement. Lorsque la console est hors délai, Control Manager exige une authentification de l'utilisateur (connexion) pour l'accès à la console Web.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres de la console Web**.

   L'écran **Paramètres de la console Web** apparaît.

2. Dans la zone de travail, dans Actualisation automatique de la console Web, sélectionnez **Activer l'actualisation automatique**.

3. Spécifiez la fréquence d'actualisation automatique de **10** à **300** secondes.

4. Dans la zone de travail, dans Paramètre de délai d'expiration de la console, sélectionnez **Activer la déconnexion automatique de la console Web**.

5. Spécifiez le paramètre de délai d'expiration de la console de **10** à **30** minutes.

6. Cliquez sur **Enregistrer**.

Configuration des paramètres du délai d'attente des commandes

Dans l'écran **Paramètres du délai d'attente de communication**, configurez les paramètres du délai d'attente de la commande. Lorsqu'une commande est hors délai,

Control Manager ne tente plus de l'exécuter (par exemple, une commande de déploiement de composants sur des serveurs OfficeScan).

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres du délai d'attente de communication**.

   L'écran **Paramètres du délai d'attente de communication** s'affiche.

2. Dans la zone de travail sous Paramètres du délai d'attente de communication, spécifiez le paramètre de délai des commandes :

   - **24** heures
   - **48** heures
   - **72** heures

3. Cliquez sur **Enregistrer**.

Déconnexion de la console d'administration

Pour vous déconnecter de la console d'administration, procédez de l'une des façons suivantes :

Procédure

- Cliquez sur **Déconnexion** dans le coin supérieur droit de la console Web.
- Appuyez en même temps sur les touches **CTRL** et **W**.

Chapitre 3

Configuration des accès utilisateurs

Les administrateurs peuvent déterminer quels écrans de la console Web sont accessibles à un utilisateur et les accès aux produits gérés enregistrés sur le serveur Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition des accès utilisateur

Le contrôle des accès de Control Manager comporte les quatre sections suivantes :

TABLEAU 3-1. Options d'accès des utilisateurs de Control Manager

SECTION	DESCRIPTION
Mon compte	L'écran **Mon compte** contient toutes les informations dont dispose Control Manager sur le compte d'un utilisateur spécifique. Les informations de l'écran **Mon compte** varient selon l'utilisateur.
Comptes utilisateurs	L'écran **Comptes utilisateurs** affiche tous les utilisateurs de Control Manager. Cet écran offre également les options permettant aux utilisateurs de créer et gérer des comptes utilisateurs de Control Manager. Utilisez ces fonctions pour définir des domaines de responsabilités clairs pour les utilisateurs, en limitant leurs droits d'accès à certains produits gérés ainsi que les actions qu'ils peuvent effectuer sur les produits gérés. Les fonctions sont les suivantes : • Exécuter • Configurer • Modifier le répertoire

SECTION	DESCRIPTION
Rôles utilisateurs	L'écran **Rôles d'utilisateurs** affiche tous les rôles d'utilisateurs de Control Manager. Cet écran offre également les options permettant aux utilisateurs de créer et gérer des rôles d'utilisateurs de Control Manager. Les rôles d'utilisateurs définissent les zones de la console Web de Control Manager auxquelles un utilisateur a accès.
Groupes d'utilisateurs	L'écran **Comptes de groupe** contient les groupes de Control Manager et permet la création de groupes. Control Manager utilise les groupes afin de permettre l'envoi groupé de notifications à plusieurs utilisateurs. Les groupes de Control Manager ne permettent pas aux administrateurs de créer un groupe partageant les mêmes droits d'accès.

Remarque

Attribuez aux utilisateurs différents droits d'accès et privilèges pour déléguer certaines tâches de gestion sans compromettre la sécurité.

Informations sur le compte racine

Control Manager crée le compte racine lors de l'installation. Les comptes racine et administrateur permettent d'afficher toutes les fonctions du menu, d'utiliser tous les services disponibles et, sur les produits gérés plus anciens, d'installer des agents.

Les autres privilèges du compte racine sont les suivants :

- Seul le compte racine peut afficher tous les comptes utilisateurs sur le serveur. Les autres comptes peuvent uniquement afficher leurs comptes enfants.
- Le compte racine peut déverrouiller une fonction en déconnectant automatiquement l'utilisateur qui l'a activée.

Remarque

Les comptes de Control Manager se connectent uniquement à Control Manager et non à l'ensemble du réseau. Les comptes utilisateurs de Control Manager ne sont pas les mêmes que les comptes de domaine de réseau.

Définition des rôles utilisateurs

Control Manager utilise les rôles utilisateur par défaut suivants. Les administrateurs ne peuvent pas modifier les autorisations d'accès des rôles d'utilisateur par défaut.

- Administrateur/Racine
- Responsable de conformité DLP
- Réviseur d'incidents DLP
- Opérateur
- Utilisateur expérimenté

Control Manager ne prend pas en charge les rôles d'utilisateur personnalisés. Les rôles d'utilisateur personnalisés permettent aux administrateurs de Control Manager de spécifier les éléments du menu de la console Web de Control Manager auxquels les autres utilisateurs peuvent accéder.

Remarque

Trend Micro recommande de configurer les rôles d'utilisateur et les paramètres de comptes utilisateurs dans l'ordre suivant :

1. Spécifiez les produits/répertoires auxquels l'utilisateur peut accéder. (Étape 8 de la section *Modification d'un compte utilisateur à la page 3-19*.)
2. Spécifiez les éléments du menu auxquels l'utilisateur peut accéder. (Si les rôles utilisateurs par défaut ne suffisent pas, consultez la section *Ajout d'un rôle utilisateur à la page 3-5* ou *Modification d'un rôle utilisateur à la page 3-8*).
3. Spécifiez le rôle utilisateur pour le compte utilisateur. (Étape 7 de la section *Modification d'un compte utilisateur à la page 3-19*)

À propos de l'ajout de rôles utilisateurs

Chaque rôle utilisateur par défaut dispose d'autorisations spécifiques sur certains éléments de menu de la console Web de Control Manager. Les administrateurs peuvent ajouter des autorisations supplémentaires sur des éléments de menu, mais ne peuvent pas retirer d'autorisations prédéfinies pour les rôles utilisateurs par défaut.

Si les rôles utilisateurs par défaut ne sont pas assez flexibles pour répondre aux besoins d'un administrateur, celui-ci peut à présent créer ses propres rôles utilisateurs. Les rôles utilisateurs définis par l'utilisateur permettent aux administrateurs de personnaliser les autorisations de n'importe quel élément de la console Web de Control Manager.

Remarque

Les informations sur les produits gérés affichées sur les éléments de menu accessibles dépendent des autorisations sur les produits gérés/répertoires que les administrateurs du Control Manager définissent dans le compte de chaque individu.

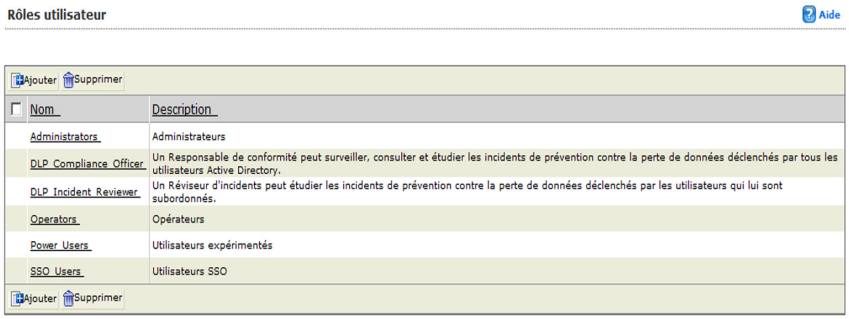
Exemple : Paul et Marie sont tous deux administrateurs OfficeScan. Ils ont des autorisations identiques pour leur rôle utilisateur (ils ont accès aux mêmes éléments de menu de la console Web). Toutefois, Marie est en charge des opérations sur tous les serveurs OfficeScan. En revanche, Paul ne s'occupe que des opérations sur les serveurs OfficeScan protégeant les postes de travail du service Marketing. Les informations auxquelles ils ont accès sur la console Web sont donc très différentes. En se connectant, Paul ne peut voir que les informations concernant les serveurs OfficeScan dont l'accès lui est accordé par son compte d'utilisateur Control Manager, c'est-à-dire les serveurs OfficeScan du service Marketing. Lorsque Marie se connecte, elle dispose des informations concernant tous les serveurs OfficeScan, car son compte utilisateur Control Manager lui autorise l'accès à tous les serveurs OfficeScan enregistrés sur Control Manager.

Ajout d'un rôle utilisateur

Procédure

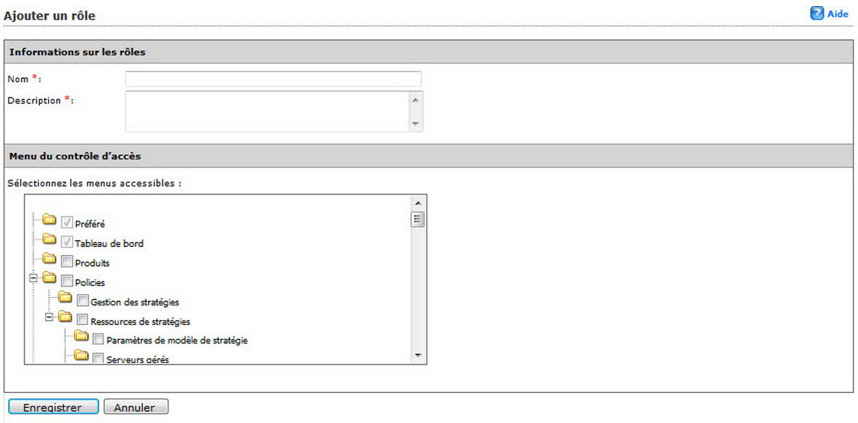
1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**.

   L'écran **Rôles utilisateurs** s'affiche.



2. Dans la zone de travail, cliquez sur **Ajouter**.

   L'écran **Ajouter un rôle** apparaît alors.



3. Dans la zone de travail, dans Informations sur les rôles, saisissez un nom de rôle utilisateur unique dans le champ **Nom**.

4. Saisissez une description pertinente du rôle utilisateur dans le champ **Description**.

Remarque

La description apparaîtra dans la liste des rôles utilisateurs. Quand le nom du rôle utilisateur ne suffit pas à exprimer clairement son utilité, fournir une description pertinente de celui-ci permet aux administrateurs de l'identifier rapidement.

---

5. Dans la zone de travail, dans Contrôle d'accès au menu, sélectionnez les éléments du menu qui seront accessibles pour le rôle utilisateur. Les éléments de menu suivants sont accessibles à tous les rôles utilisateurs : **Tableau de bord**, **Mes favoris** et **Aide**.

6. Cliquez sur **Enregistrer**.

   L'écran **Rôles utilisateurs** apparaît et le nouveau rôle utilisateur apparaît dans la liste des rôles utilisateurs.

À propos de la modification de rôles utilisateurs

Control Manager permet aux utilisateurs de modifier les rôles utilisateur personnalisés. Les utilisateurs peuvent modifier les noms et descriptions des rôles utilisateur par défaut, mais pas les éléments de menu qui leur sont accessibles.

Modifiez les rôles utilisateurs lorsqu'un rôle utilisateur devient obsolète ou requiert des opérations minimes de maintenance.

Conseil

Les informations sur les produits gérés affichées sur les éléments de menu accessibles dépendent des autorisations sur les produits gérés/répertoires que les administrateurs du Control Manager définissent dans le compte de chaque individu.

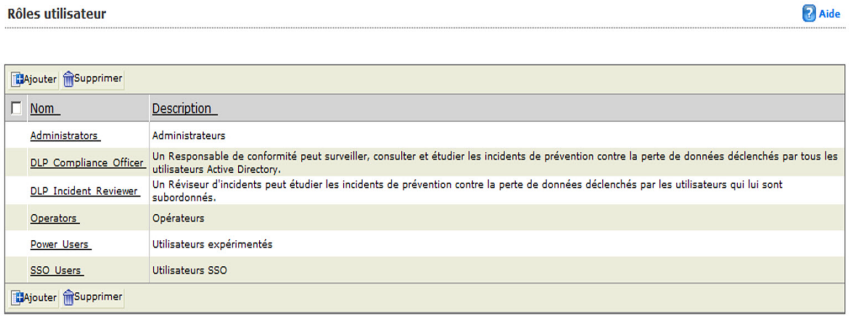
Exemple : Paul et Marie sont tous deux administrateurs OfficeScan. Ils ont des autorisations identiques pour leur rôle utilisateur (ils ont accès aux mêmes éléments de menu de la console Web). Toutefois, Marie est en charge des opérations sur tous les serveurs OfficeScan. En revanche, Paul ne s'occupe que des opérations sur les serveurs OfficeScan protégeant les postes de travail du service Marketing. Les informations auxquelles ils ont accès sur la console Web sont donc très différentes. En se connectant, Paul ne peut voir que les informations concernant les serveurs OfficeScan dont l'accès lui est accordé par son compte d'utilisateur Control Manager, c'est-à-dire les serveurs OfficeScan du service Marketing. Lorsque Marie se connecte, elle dispose des informations concernant tous les serveurs OfficeScan, car son compte utilisateur Control Manager lui autorise l'accès à tous les serveurs OfficeScan enregistrés sur Control Manager.

Modification d'un rôle utilisateur

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Rôles utilisateurs**.

   L'écran **Rôles utilisateurs** s'affiche.



2. Cliquez sur un rôle utilisateur dans la colonne Nom.

   L'écran **Modifier un rôle** apparaît.

3. Modifiez les informations requises du rôle utilisateur.

4. Cliquez sur **Enregistrer**.

   L'écran **Rôles utilisateurs** apparaît et le rôle utilisateur apparaît dans la liste des rôles utilisateurs.

Définition des comptes utilisateurs

Les administrateurs peuvent utiliser les fonctions de l'écran **Comptes utilisateurs** pour attribuer aux utilisateurs des domaines de responsabilité clairement définis, en limitant leurs droits d'accès à certains produits gérés ainsi que les opérations qu'ils peuvent réaliser.

Remarque

Lorsqu'un administrateur spécifie les produits auxquels un utilisateur a accès, l'administrateur spécifie également les informations auxquelles un utilisateur peut accéder depuis Control Manager. Les informations suivantes sont affectées : informations de composants, journaux, informations de résumé de produit, informations de sécurité et informations disponibles pour les rapports et les requêtes de journal.

Exemple : Paul et Marie sont tous deux administrateurs OfficeScan. Ils ont des autorisations identiques pour leur rôle utilisateur (ils ont accès aux mêmes éléments de menu de la console Web). Toutefois, Marie est en charge des opérations sur tous les serveurs OfficeScan. En revanche, Paul ne s'occupe que des opérations sur les serveurs OfficeScan protégeant les postes de travail du service Marketing. Les informations auxquelles ils ont accès sur la console Web sont donc très différentes. En se connectant, Paul ne peut voir que les informations concernant les serveurs OfficeScan dont l'accès lui est accordé par son compte d'utilisateur Control Manager, c'est-à-dire les serveurs OfficeScan du service Marketing. Lorsque Marie se connecte, elle dispose des informations concernant tous les serveurs OfficeScan, car son compte utilisateur Control Manager lui autorise l'accès à tous les serveurs OfficeScan enregistrés sur Control Manager.

Configuration des droits d'accès

Les droits d'accès des utilisateurs déterminent les contrôles disponibles pour les utilisateurs dans le répertoire Produits. Ainsi, lorsque vous attribuez uniquement le droit d'exécution à un utilisateur, seules les options associées à ce droit s'affichent dans le répertoire Produits.

Vous pouvez attribuer à chaque compte utilisateur les droits d'accès suivants sur un produit.

TABLEAU 3-2. Options de compte utilisateur de Control Manager

AUTORISATION	DESCRIPTION
Exécuter	Ce droit d'accès permet à l'utilisateur d'exécuter des commandes sur des produits gérés dans les dossiers attribués. Par exemple : • Démarrer le scan immédiat • Déployer les fichiers de signatures/ modèles Damage Cleanup • Activer le scan en temps réel • Déployer les fichiers programme • Déployer les moteurs • Déployer les profils de licence
Configurer	Ce droit permet à l'utilisateur d'accéder aux consoles de configuration des produits gérés dans les dossiers attribués. Les menus affichés par les utilisateurs ayant ce droit d'accès contiennent l'option Configuration de **<produit géré>** et d'autres options similaires spécifiques du produit (par exemple, les fonctions de définition de mot de passe dans OfficeScan).
Modifier le répertoire	Ce droit permet à l'utilisateur de modifier l'organisation des produits gérés/ répertoires auxquels il a accès.

Remarque

Les options qui apparaissent dépendent également du profil du produit. Par exemple, si un produit n'a pas de fonction de scan (c'est le cas d'eManager), la commande Scan immédiat est absente du menu Tâches de l'arborescence produit.

L'écran Compte utilisateurs affiche les éléments suivants.

TABLEAU 3-3. Contenu de l'écran Comptes utilisateur

INFORMATIONS DE COMPTE	DESCRIPTION
ID utilisateur	Nom d'utilisateur de l'utilisateur du compte.
Nom complet	Nom complet de l'utilisateur du compte.
Domaine	Domaine d'Active Directory (le cas échéant) auquel appartient l'utilisateur.
Rôle utilisateur	Rôle d'utilisateur affecté à l'utilisateur (par exemple : Administrateur).
Activer	État actuel du compte.

Remarque

Control Manager crée automatiquement un compte racine au cours de l'installation.

À propos de l'ajout et l'importation de comptes utilisateur

Les comptes utilisateurs de Control Manager permettent aux administrateurs de spécifier les produits ou répertoires accessibles aux autres utilisateurs.

Remarque

Lorsqu'un administrateur spécifie les produits auxquels un utilisateur a accès, l'administrateur spécifie également les informations auxquelles un utilisateur peut accéder depuis Control Manager. Les informations suivantes sont affectées : informations de composants, journaux, informations de résumé de produit, informations de sécurité et informations disponibles pour les rapports et les requêtes de journal.

Exemple : Paul et Marie sont tous deux administrateurs OfficeScan. Ils ont des autorisations identiques pour leur rôle utilisateur (ils ont accès aux mêmes éléments de menu de la console Web). Toutefois, Marie est en charge des opérations sur tous les serveurs OfficeScan. En revanche, Paul ne s'occupe que des opérations sur les serveurs OfficeScan protégeant les postes de travail du service Marketing. Les informations auxquelles ils ont accès sur la console Web sont donc très différentes. En se connectant, Paul ne peut voir que les informations concernant les serveurs OfficeScan dont l'accès lui est accordé par son compte d'utilisateur Control Manager, c'est-à-dire les serveurs OfficeScan du service Marketing. Lorsque Marie se connecte, elle dispose des informations concernant tous les serveurs OfficeScan, car son compte utilisateur Control Manager lui autorise l'accès à tous les serveurs OfficeScan enregistrés sur Control Manager.

Ajoutez des comptes utilisateurs pour :

- Permettre aux administrateurs de spécifier les produits ou répertoires accessibles aux autres utilisateurs
- Permettre aux autres utilisateurs de se connecter à la console Web de Control manager
- Permettre aux administrateurs d'inscrire l'utilisateur à la liste des destinataires de notifications
- Permettre à l'administrateur d'ajouter l'utilisateur aux groupes d'utilisateurs.

Remarque

Trend Micro vous conseille de configurer le rôle utilisateur et les paramètres de compte utilisateur dans l'ordre suivant :

1. Spécifiez les produits/répertoires auxquels l'utilisateur peut accéder. (Étape 8 de la section *Modification d'un compte utilisateur à la page 3-19*.)
2. Spécifiez les éléments du menu auxquels l'utilisateur peut accéder. (Si les rôles utilisateurs par défaut ne suffisent pas, consultez la section *Ajout d'un rôle utilisateur à la page 3-5* ou *Modification d'un rôle utilisateur à la page 3-8*).
3. Spécifiez le rôle utilisateur du compte utilisateur. (Étape 7 de la section *Modification d'un compte utilisateur à la page 3-19*.)

Lorsque vous ajoutez un compte utilisateur, vous devez indiquer les informations d'identification de l'utilisateur, lui affecter un rôle utilisateur et définir les droits d'accès aux dossiers.

Remarque

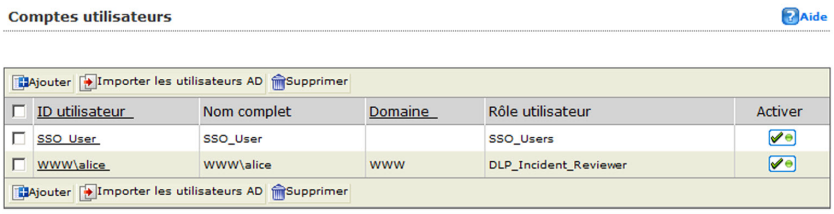
Les comptes des utilisateurs d'Active Directory ne peuvent pas être désactivés à partir de Control Manager. Pour désactiver un utilisateur d'Active Directory, vous devez désactiver son compte à partir du serveur Active Directory.

Ajout/Importation d'un compte utilisateur

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

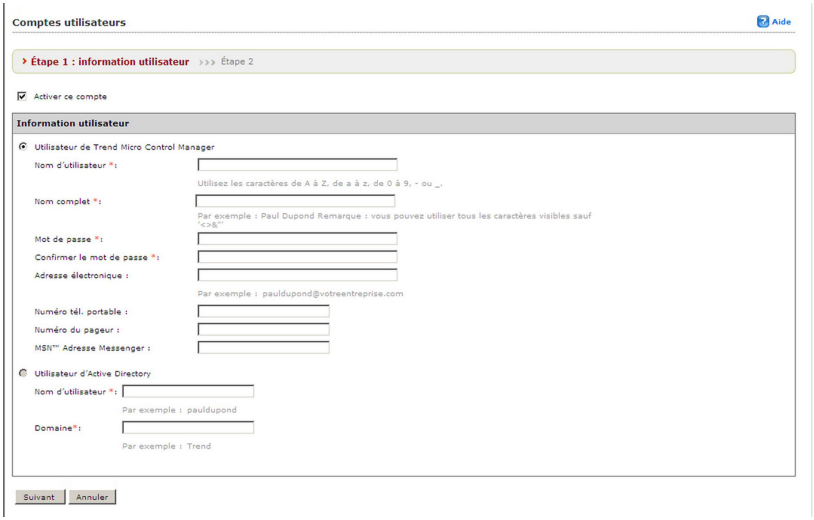
   L'écran **Comptes utilisateurs** s'affiche.



2. Cliquez sur l'un des boutons suivants pour créer le compte :

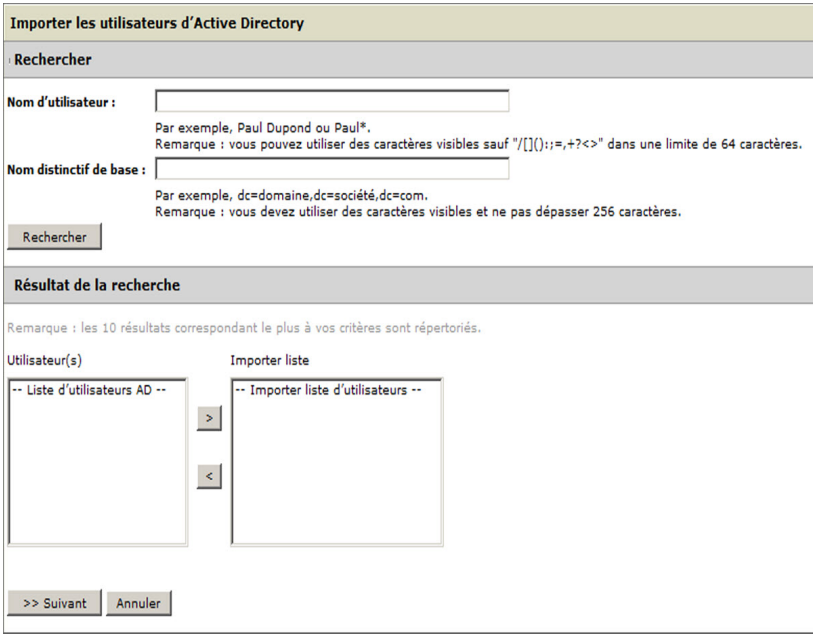
   - **Ajouter**

     L'écran **Étape 1 : Informations sur l'utilisateur** apparaît.



   - **Importer les utilisateurs AD**

L'écran **Importer les utilisateurs d'Active Directory** s'affiche. Recherchez et ajoutez des utilisateurs à **Importer liste**. Continuez vers l'étape 5.



3. Sélectionnez **Activer ce compte** pour activer l'utilisateur de Control Manager.
4. Sélectionnez le type d'utilisateur à ajouter :
   - Pour ajouter un utilisateur de Trend Micro Control Manager :

   a. Sélectionnez **Utilisateur de Trend Micro Control Manager**.

   b. Indiquez les informations requises suivantes pour créer un compte :
      - **Nom d'utilisateur** : Nom utilisé par l'utilisateur pour se connecter à la console Web de Control Manager. Par exemple, OfficeScan_Admin.
      - **Nom complet** : Nom complet de l'utilisateur. Par exemple, Paul Durand
      - **Mot de passe** et **Confirmation du mot de passe** : Saisissez et confirmez votre mot de passe dans les champs fournis. Tous les

utilisateurs peuvent modifier leur mot de passe de connexion dans l'écran **Mon compte**.

c. Les informations suivantes sont facultatives. Tous les utilisateurs peuvent également modifier ces paramètres dans l'écran **Mon compte**.

- **Adresse électronique** : Adresse électronique à laquelle les notifications de l'utilisateur sont envoyées.
- **Numéro de téléphone portable** : Numéro du téléphone portable auquel les notifications de l'utilisateur sont envoyées.
- **Numéro de pageur** : Numéro du pageur auquel les notifications sont envoyées à l'utilisateur. (Faites précéder le numéro du pageur d'un 9 et d'une virgule « , » [chaque virgule correspond à une pause de 2 secondes])
- **Adresse MSN Messenger** : Adresse de messagerie instantanée à laquelle les notifications à l'utilisateur sont envoyées.

- Pour ajouter un utilisateur d'Active Directory :

Remarque

Les comptes des utilisateurs d'Active Directory ne peuvent pas être désactivés à partir de Control Manager. Pour désactiver un utilisateur d'Active Directory, vous devez désactiver son compte à partir du serveur Active Directory.

a. Sélectionnez **Utilisateur d'Active Directory**.

b. Indiquez les informations requises suivantes pour créer un compte :

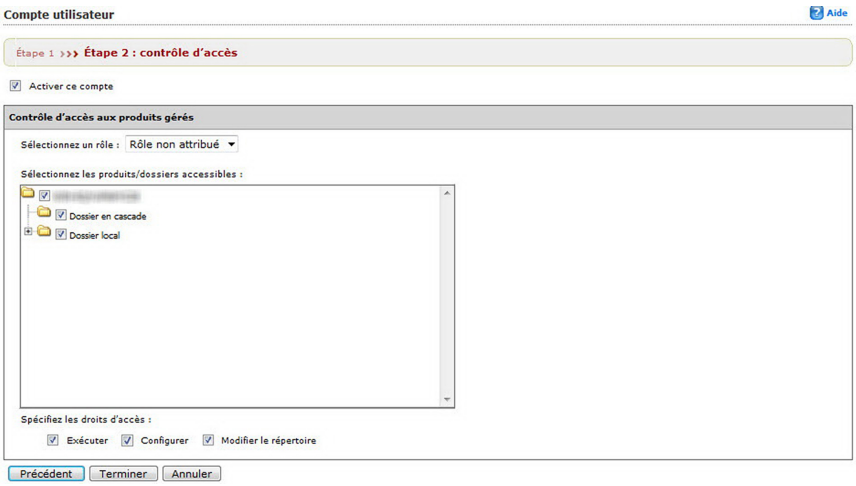
- **Nom d'utilisateur** : identification Active Directory de l'utilisateur
- **Domaine** : domaine auquel appartient l'utilisateur

Remarque

Les noms d'utilisateurs et les noms de domaine ont une longueur maximale de 32 caractères.

5. Cliquez sur **Suivant**.

L'écran **Étape 2 : Contrôle d'accès** apparaît.



6. Sélectionnez un rôle utilisateur par défaut ou personnalisé dans la liste **Sélectionner un rôle**. Control Manager fournit les rôles utilisateur suivants par défaut :

   - **Administrateur**
   - **Responsable de conformité DLP**
   - **Réviseur d'incidents DLP**
   - **Opérateur**
   - **Utilisateur expérimenté**

   Remarque

   Les rôles Responsable de conformité DLP et Réviseur d'incidents DLP sont disponibles pour les utilisateurs d'Active Directory uniquement.

7. Sélectionnez les produits ou répertoires auxquels l'utilisateur a accès dans **Sélectionner les produits/dossiers accessibles**.

Remarque

Organisez le répertoire Produits avec soin pour faciliter son utilisation. Lorsqu'un utilisateur a accès à un dossier, il peut accéder à tous ses sous-dossiers et produits gérés. Vous pouvez restreindre l'accès d'un utilisateur à un seul produit géré.

8. Sélectionnez les droits à attribuer à l'utilisateur. Ces droits définissent les actions qu'il peut exécuter sur des produits gérés.

Remarque

Les privilèges accordés à un compte ne peuvent pas excéder les privilèges de l'utilisateur qui les lui attribue. En d'autres termes, vous ne pouvez pas attribuer à un utilisateur des droits d'accès qui sont supérieurs aux vôtres. En outre, si vous réduisez les droits d'un compte, vous réduisez également ceux de ses comptes enfants.

9. Cliquez sur **Terminer**.

À propos de la modification d'un compte utilisateur

Vous pouvez modifier les informations de n'importe quel compte utilisateur, notamment les informations de compte, le rôle de l'utilisateur et les droits d'accès aux dossiers. Si vous réduisez les droits d'un compte, vous réduisez également ceux de ses comptes enfants.

Lorsque vous modifiez un compte, tenez compte des éléments suivants :

- Les utilisateurs de comptes racines peuvent modifier tous les comptes existant sur le système. Les utilisateurs disposant de comptes **administrateur** ne peuvent toutefois modifier que ceux qu'ils ont créés eux-mêmes.
- Les droits d'un compte représentent un sous-ensemble des droits de l'utilisateur qui les attribue et sont ajustés en conséquence si les droits de cet utilisateur sont réduits.
- La modification des privilèges d'un compte met fin à toutes les sessions utilisant ce compte. Si cette modification implique une diminution des droits, les comptes enfants dont les privilèges sont concernés seront également déconnectés.

- Vous ne pouvez pas modifier le nom d'utilisateur d'un compte existant.

Modification d'un compte utilisateur

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

   L'écran **Comptes utilisateurs** s'affiche.

2. Cliquez sur le compte à modifier.

   L'écran **Modification d'un compte utilisateur** s'affiche.

3. Modifiez les informations du compte, puis cliquez sur **Suivant**.

4. Modifiez le rôle utilisateur, les dossiers accessibles et les droits d'accès.

5. Cliquez sur **Terminer**.

Désactivation d'un compte utilisateur

La désactivation temporaire d'un compte utilisateur empêche l'utilisateur correspondant d'accéder au réseau Control Manager. Les informations du compte utilisateur sont conservées et le compte utilisateur peut être réactivé à tout moment.

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

   L'écran **Comptes utilisateurs** s'affiche.

2. Choisissez l'une des options suivantes :

   - Cliquez sur l'icône d'état (coche verte) sous la colonne Activer du tableau Comptes utilisateurs. L'icône d'état apparaît alors en rouge.

   - Cochez la case **Activer ce compte** :

     a. Accédez à l'écran du compte de l'utilisateur.

b. Dans la zone de travail de l'écran Ajouter un utilisateur ou Modifier un utilisateur, décochez la case **Activer ce compte**.

c. Cliquez sur **Suivant**.

d. Cliquez sur **Terminer**.

Suppression d'un compte utilisateur

Vous pouvez supprimer définitivement un compte utilisateur pour empêcher l'utilisateur correspondant d'accéder au réseau Control Manager. Lorsque vous supprimez un compte utilisateur, Control Manager supprime le compte des groupes auxquels il appartenait, et l'utilisateur ne reçoit plus les notifications d'événements correspondant aux listes de destinataires dont il faisait partie.

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Comptes utilisateurs**.

   L'écran **Comptes utilisateurs** s'affiche.

2. Cochez la case du compte à supprimer.

3. Cliquez sur **Supprimer**.

Description de Mon compte

L'écran **Mon compte** contient toutes les informations dont dispose Control Manager sur un compte d'utilisateur spécifique. Les informations de cet écran varient en fonction de l'utilisateur.

L'écran **Mon compte** affiche les éléments suivants :

INFORMATIONS DE COMPTE	DESCRIPTION	EXEMPLES
Nom d'utilisateur	Nom d'utilisateur de l'utilisateur du compte. Ce champ est obligatoire.	Administrateur
Nom complet	Nom complet de l'utilisateur du compte. Ce champ est obligatoire.	John Smith
Mot de passe	Mot de passe de connexion à Control Manager. Ce champ est obligatoire.	MyPassword!
Confirmer le mot de passe	Confirmez le mot de passe de connexion à Control Manager. Ce champ est obligatoire.	MyPassword!
Adresse électronique	Adresse électronique de l'utilisateur du compte.	pauldupond@monentreprise.com
Numéro de téléphone portable	Numéro de téléphone portable de l'utilisateur du compte.	555-5551234
Numéro de pageur	Numéro de pageur de l'utilisateur du compte.	555-5552345
Adresse e-mail MSN™ Messenger	Adresse MSN de l'utilisateur.	johnsmith@hotmail.com

Définition des groupes d'utilisateurs

Les groupes d'utilisateurs simplifient la gestion des utilisateurs de Control Manager. Vous pouvez ainsi envoyer une notification simultanément à tous les membres d'un groupe plutôt qu'individuellement à chaque membre. L'écran **Groupes d'utilisateurs** contient les groupes Control Manager. Control Manager utilise les groupes afin de permettre l'envoi groupé de notifications à plusieurs utilisateurs.

Exemple : Plusieurs administrateurs OfficeScan souhaitent être informés des épidémies, mêmes si celles-ci ne concernent pas un serveur qu'ils gèrent.

L'écran **Groupes d'utilisateurs** affiche les éléments suivants :

TABLEAU 3-4. Table des groupes d'utilisateurs

INFORMATIONS SUR LE GROUPE	DESCRIPTION
Groupes	Nom du groupe.
Modifier	Cliquez sur le lien correspondant de cette ligne pour modifier les utilisateurs qui appartiennent au groupe.
Supprimer	Cliquez sur le lien correspondant de cette ligne pour supprimer un groupe de Control Manager.

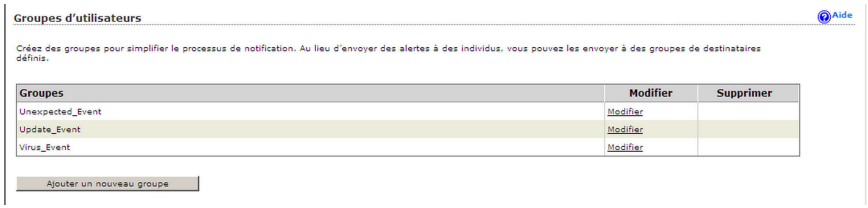
Ajout d'un groupe d'utilisateurs

Vous pouvez ajouter des utilisateurs aux groupes selon des critères similaires, notamment les types d'utilisateurs, l'emplacement ou le type de notifications qu'ils sont censés recevoir. Si un utilisateur n'a pas de compte utilisateur Control Manager, vous pouvez quand même l'ajouter à un groupe en spécifiant son adresse électronique. Toutefois, il ne recevra des notifications que si le groupe a été ajouté à la liste des destinataires concernés par certains événements.

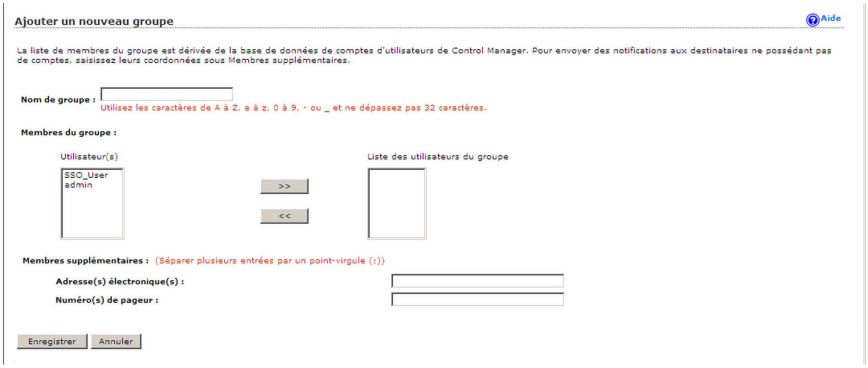
Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Groupes d'utilisateurs**.

   L'écran **Groupes d'utilisateurs** s'affiche.



2. Dans la zone de travail, cliquez sur **Ajouter un nouveau groupe**.



3. Entrez le nom descriptif du groupe dans le champ **Nom du groupe**.

4. Sous **Membres du groupe**, ajoutez ou supprimez des utilisateurs dans la liste du groupe.

   - Pour ajouter un utilisateur :

   a. Sélectionnez un utilisateur dans la liste Utilisateur(s). Pour sélectionner plusieurs utilisateurs, maintenez la touche CTRL enfoncée.

   b. Cliquez sur (>>) pour ajouter les utilisateurs sélectionnés à la liste des utilisateurs du groupe. Control Manager envoie des notifications aux utilisateurs en fonction des informations de contact qui ont été définies lors de la création de leur compte.

   - Pour supprimer un utilisateur :

   a. Sélectionnez un utilisateur dans la liste des utilisateurs du groupe. Pour sélectionner plusieurs utilisateurs, maintenez la touche CTRL enfoncée.

   b. Cliquez sur (<<) pour supprimer cet utilisateur.

5. Pour ajouter des individus qui ne possèdent pas de comptes Control Manager dans la liste des utilisateurs du groupe, indiquez les informations suivantes dans **Membres supplémentaires** :

   - Adresse(s) électronique(s)

- Numéro(s) de pageur (faites précéder le numéro de pageur par le numéro que votre entreprise utilise pour obtenir une ligne extérieure et par une virgule « , » [chaque virgule correspond à une pause de 2 secondes]). Séparez les entrées multiples par des points virgules.

6. Cliquez sur **Enregistrer**.
7. Cliquez sur **OK**.

Modification d'un groupe d'utilisateurs

Vous pouvez ajouter un utilisateur à un groupe ou l'en retirer à tout moment, même si cet utilisateur n'a pas de compte utilisateur Control Manager.

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Groupes d'utilisateurs**.

   L'écran **Groupes d'utilisateurs** s'affiche.
2. Dans la zone de travail, cliquez sur **Modifier** en regard du groupe requis.
3. Effectuez vos modifications.
4. Cliquez sur **Enregistrer**.
5. Cliquez sur **OK**.

Suppression d'un groupe d'utilisateurs

Si vous n'avez plus besoin d'un groupe d'utilisateurs, supprimez-le définitivement du réseau Control Manager. Lorsque vous supprimez un groupe d'utilisateurs, ses membres ne reçoivent plus les notifications d'événements envoyées à la liste des destinataires à laquelle le groupe était inscrit.

Procédure

1. Accédez à **Administration** > **Gestion des comptes** > **Groupes d'utilisateurs**.

L'écran **Groupes d'utilisateurs** s'affiche.

2. Cliquez sur **Supprimer** en regard du groupe à supprimer.
3. Cliquez sur **OK** pour supprimer le groupe d'utilisateurs.
4. Cliquez sur **OK**.

Chapitre 4

Principes du répertoire Produits

Le répertoire Produits affiche tous les produits gérés enregistrés sur un serveur Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition du répertoire Produits

Un produit géré est un produit antivirus ou de sécurité de contenu ou un produit de protection Web présent dans le répertoire Produits. Les produits gérés sont représentés par des icônes (par exemple, () ou ()) dans la section Répertoire Produits de la console Web de Control Manager. Ces icônes représentent les produits antivirus, de sécurité de contenu et de protection Web développés par Trend Micro. Control Manager prend en charge les icônes dynamiques dont la représentation change en fonction de l'état des produits gérés. Pour plus d'informations sur les icônes et les états de votre produit géré, consultez la documentation correspondante.

Vous pouvez administrer indirectement les produits gérés, individuellement ou par groupe, à partir du répertoire Produits. Le tableau suivant présente les éléments de menu et les boutons de l'écran Répertoire Produits.

TABLEAU 4-1. Options du répertoire Produits

ÉLÉMENT DE MENU	DESCRIPTION
Recherche avancée	Cliquez sur cet élément de menu pour spécifier des critères de recherche afin d'effectuer une recherche d'un ou plusieurs produits gérés.
Configurer	Après avoir sélectionné un produit géré/ répertoire, déplacez le curseur sur cet élément de menu et sélectionnez une tâche pour vous connecter à une console Web à l'aide de SSO ou pour configurer un produit géré.

Élément de menu	Description
Tâches	Après avoir sélectionné un produit géré/répertoire, déplacez le curseur sur cet élément de menu et sélectionnez une tâche pour exécuter une fonction spécifique (telle que le déploiement des derniers composants) sur un produit géré ou un serveur enfant spécifique, ou sur des groupes de produits gérés ou de serveurs enfants. Le lancement d'une tâche depuis un répertoire entraîne l'envoi par Control Manager de requêtes à tous les produits gérés appartenant à ce répertoire.
Gestionnaire des répertoires	Cliquez sur ce bouton pour ouvrir l'écran **Gestionnaire des répertoires**. Depuis l'écran, déplacez les entités/répertoires (en procédant à des glisser/déplacer) ou créez de nouveaux répertoires.
Boutons	
Rechercher	Cliquez sur ce bouton après avoir sélectionné le nom d'un produit géré afin d'effectuer une recherche du produit géré spécifié.
État	Cliquez sur ce bouton après avoir sélectionné un produit géré/répertoire afin d'obtenir des résumés d'état sur le produit géré ou les produits gérés contenus dans le répertoire.
Dossier	Cliquez sur ce bouton après avoir sélectionné un répertoire afin d'obtenir des résumés d'état sur les produits gérés et leurs points finaux contenus dans le répertoire.

Remarque

Le serveur Control Manager parent ne peut pas envoyer de tâches aux produits gérés appartenant à des serveurs Control Manager enfants.

Regroupement de produits gérés à l'aide du Gestionnaire des répertoires

Utilisez l'écran **Gestionnaire de répertoires** pour personnaliser la structure du répertoire Produits afin qu'elle soit en phase avec votre modèle d'administration. Vous pouvez ainsi regrouper les produits par emplacement ou type de produit (sécurité de messagerie, sécurité Web, protection du stockage des fichiers).

Regroupez des produits gérés selon des critères géographiques, administratifs ou spécifiques de ces produits. Le tableau suivant indique les types de regroupement recommandés avec leurs avantages et leurs inconvénients. Il combine également les différents droits d'accès aux produits gérés ou aux dossiers dans le répertoire.

TABLEAU 4-2. Avantages et inconvénients du regroupement de produits gérés

TYPE DE REGROUPEMENT	AVANTAGE	INCONVÉNIENT
Géographique ou administratif	Structure claire	Aucune configuration de groupe pour des produits identiques
Type de produit	Configuration de groupe et état disponible	Incompatibilité possible des droits d'accès
Combinaison des deux	Configuration de groupes et gestion des droits d'accès	Structure complexe, risque d'être difficile à gérer

Recommandations relatives à l'arborescence du répertoire Produits

Trend Micro recommande les considérations suivantes pour l'élaboration de l'arborescence du répertoire Produits pour les produits gérés et les serveurs enfants :

TABLEAU 4-3. Éléments à prendre en compte pour regrouper des produits gérés ou des serveurs enfants

STRUCTURE	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 et les serveurs enfants en fonction du réseau et des stratégies de sécurité de l'entreprise.
Organisation et fonction	Regroupez les produits gérés 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 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 et les serveurs enfants en fonction du système ou du personnel de sécurité qui lui est affecté. Cela permet une configuration de groupes.

Le répertoire Produits fournit un regroupement des produits gérés spécifié par l'utilisateur qui vous permet d'effectuer ce qui suit pour administrer les produits gérés :

- Configuration des produits gérés
- Déclencher un scan immédiat sur un produit (si cette commande est prise en charge)
- Afficher des informations sur un produit et sur son environnement d'exploitation (par exemple, la version du produit, les versions du fichier de signatures de virus et du moteur de scan, des informations sur le système d'exploitation, etc.)

- Afficher des journaux de produit
- Déployer des mises à jour de fichier de signatures de virus, de moteur de scan, de règles anti-pourriel et de programme

Élaborez cette structure avec soin car elle a un impact direct sur les éléments suivants :

TABLEAU 4-4. Éléments à prendre en compte pour la structure

ÉLÉMENT À PRENDRE EN COMPTE	EFFET
Accès des utilisateurs	Lorsque vous créez un compte utilisateur, Control Manager vous demande le segment du répertoire Produits auquel l'utilisateur a accès. Par exemple, si vous attribuez l'accès au segment racine à un utilisateur, ce dernier a accès à l'ensemble du répertoire. Limitez l'accès de l'utilisateur à un produit géré donné en lui attribuant uniquement les droits correspondants.
Planification du déploiement	Control Manager déploie des composants de mise à jour (par exemple, des fichiers de signatures de virus, des moteurs de scan, des règles anti-pourriel, des mises à jour de programme) sur des produits conformément à des plans de déploiement. Ces plans s'appliquent à des dossiers du répertoire Produits et non séparément à chaque produit. Un répertoire bien structuré simplifie donc la définition des destinataires.
Déploiement d'une stratégie de prévention des épidémies (OPP) et d'un modèle Damage Cleanup (DCT)	Les déploiements de la stratégie de prévention des épidémies et du modèle Damage Cleanup reposent sur des plans de déploiement pour distribuer efficacement des tâches de stratégie de prévention des épidémies et de nettoyage.

L'écran suivant illustre un exemple de répertoire Produits :

Les produits gérés identifient le produit antivirus ou de sécurité de contenu enregistrés et indiquent l'état de connexion.

Remarque

Tous les produits gérés nouvellement enregistrés apparaissent généralement dans le dossier Nouvelle entité, quel que soit le type d'agent.

TABLEAU 4-5. Icônes des produits gérés

ICÔNE	DESCRIPTION
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	Serveur d'informations ServerProtect
	Domaine ServerProtect
NT	ServerProtect for Windows (serveur normal)

ICÔNE	DESCRIPTION
	ServerProtect for NetWare (serveur normal)
	InterScan Messaging Security Suite
	InterScan Web Security Suite
	InterScan VirusWall for Windows
	InterScan VirusWall for UNIX
	ScanMail for Microsoft Exchange
	ScanMail for Lotus Notes
	Network VirusWall
	Pare-feu NetScreen-Global PRO
	Icône d'état de la connexion des produits gérés

Organisez le répertoire Produits à l'aide du Gestionnaire de répertoires. Utilisez des noms de dossier descriptifs et regroupez les produits gérés en fonction de leur type de protection ou du modèle d'administration de réseau Control Manager.

Dossiers par défaut du répertoire Produits

Après une nouvelle installation de Control Manager, le répertoire Produits se compose initialement des répertoires suivants :

TABLEAU 4-6. Dossiers par défaut du répertoire Produits

STRUCTURE	DESCRIPTION
Racine	Tous les produits gérés et serveurs Control Manager enfants appartiennent au répertoire racine.

STRUCTURE	DESCRIPTION
Dossier en cascade	Dans un environnement en cascade, tous les serveurs enfants du serveur parent apparaissent dans le dossier en cascade.
Dossier local > Nouvelle entité	Les produits gérés nouvellement enregistrés pris en charge par les agents Control Manager apparaissent généralement dans le dossier Nouvelle entité.
Résultat de la recherche	Lors d'une recherche de base ou avancée, tous les produits gérés correspondant aux critères de recherche s'affichent dans le dossier Résultat de la recherche.

Accès au répertoire Produits

Le répertoire Produits permet d'administrer les produits gérés enregistrés sur le serveur Control Manager.

Remarque

L'affichage des dossiers et leur accès dans le répertoire Produits dépend du type de compte et des droits d'accès du compte utilisateur.

Procédure

- Cliquez sur **Produits** dans le menu principal.

  L'écran **Répertoire Produits** apparaît.

Définition de la gestion en cascade

Control Manager Advanced offre une structure de gestion en cascade permettant de contrôler plusieurs serveurs Control Manager (appelés serveurs enfants) à partir d'un seul serveur parent.

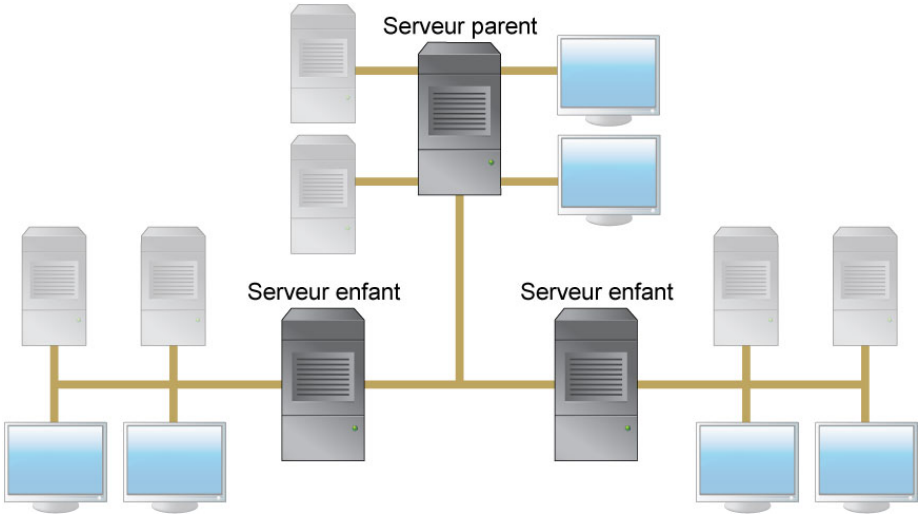


FIGURE 4-1. La structure de gestion en cascade utilise une architecture parent-enfant à deux niveaux.

Un serveur parent est un serveur Control Manager qui gère des serveurs en version Standard Edition ou Advanced Edition, également appelés « serveurs enfants ». Un serveur enfant est un serveur Control Manager géré par un serveur parent.

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.

TABLEAU 4-7. Comparaison des fonctions d'un serveur parent et d'un serveur enfant

FONCTION	DISPONIBLE SUR UN SERVEUR PARENT	DISPONIBLE SUR UN SERVEUR ENFANT
Prise en charge d'une structure en cascade à deux niveaux	●	●
Gestion des serveurs Advanced	●	
Administration de produits gérés	●	●
Gestion de plusieurs serveurs enfants	●	
Exécution de tâches générales	●	
Création de rapports généraux	●	

Remarque

Un serveur parent ne peut pas s'enregistrer sur un autre serveur parent. En outre, des serveurs parents et enfants ne peuvent pas assumer les deux rôles, c'est-à-dire être à la fois un serveur parent et un serveur enfant.

La structure du répertoire Produits, accessible à partir de la console Web de Control Manager, permet aux administrateurs système de gérer, de surveiller tous les serveurs enfants qui dépendent d'un serveur parent et d'effectuer les actions suivantes sur ces derniers :

- Surveiller les résumés des produits antivirus, de sécurité de contenu et de sécurité Web à l'aide de widgets Control Manager
- Interroger des journaux
- Exécuter des tâches
- Afficher des rapports
- Accéder à la console Web d'un serveur enfant

La structure du répertoire Produits permet de gérer efficacement les produits antivirus et de sécurité de contenu de votre entreprise au niveau national et international.

Chapitre 5

Téléchargement et déploiement de composants

Le répertoire Produits affiche tous les produits gérés enregistrés sur un serveur Control Manager.

Ce chapitre traite les rubriques suivantes :

Téléchargement et déploiement de nouveaux composants

Trend Micro recommande de mettre à jour les composants antivirus et de sécurité de contenu pour protéger le réseau des virus et des programmes malveillants les plus récents.

Par défaut, Control Manager permet de ne télécharger que les composants appartenant à des produits gérés enregistrés sur le serveur Control Manager. Control Manager active le téléchargement du fichier de signatures de virus, même si aucun produit géré n'est enregistré sur le serveur Control Manager.

Les composants suivants doivent être mis à jour (il sont classés dans l'ordre de priorité de mise à jour).

TABLEAU 5-1. Composants disponibles

COMPOSANT	DESCRIPTION
fichiers de signatures/modèles Damage Cleanup	Un produit géré tire sa capacité à détecter et à éradiquer des infections malveillantes des fichiers de signatures et des modèles Damage Cleanup qui contiennent des centaines de signatures de programmes malveillants (par exemple, des virus ou des chevaux de Troie).
Règles anti-spam	Les règles anti-spam sont des fichiers fournis par Trend Micro pour filtrer du courrier et des données indésirables.
Moteurs	Les moteurs désignent les moteurs de scan antivirus/anti-programmes malveillants, le moteur Damage Cleanup, les moteurs VirusWall, le moteur de scan de programmes espions/graywares, etc. Ces composants exécutent les fonctions de scan et de nettoyage.

COMPOSANT	DESCRIPTION
Programmes plug-in OfficeScan	Les programmes plug-in OfficeScan (par exemple, Trend Micro Security for Mac). **Remarque** La console Web OfficeScan affiche tous les programmes plug-in disponibles. Vous pouvez spécifier de les télécharger depuis Control Manager. Il se peut toutefois que Control Manager ne dispose pas du programme plug-in téléchargé. Dans ce cas, OfficeScan ne peut pas télécharger le programme plug-in spécifié depuis Control Manager. Avant d'indiquer un programme plug-in à télécharger vers OfficeScan, vérifiez que Control Manager l'a déjà téléchargé.
Programmes du produit et pool de widgets	Composants spécifiques au produit (les Service Packs, par exemple) et le pool de widgets de Control Manager

Remarque

Seuls les utilisateurs enregistrés bénéficient de la mise à jour des composants.

Pour minimiser le trafic du réseau Control Manager, désactivez le téléchargement des composants de produits gérés qui ne sont pas installés.

L'écran **Liste des composants** dresse la liste complète des composants de Control Manager disponibles pour les produits gérés. Cette liste indique également les

composants utilisés par les produits gérés. Sélectionnez **Mises à jour** > **Liste des composants** pour ouvrir l'écran **Liste des composants**.

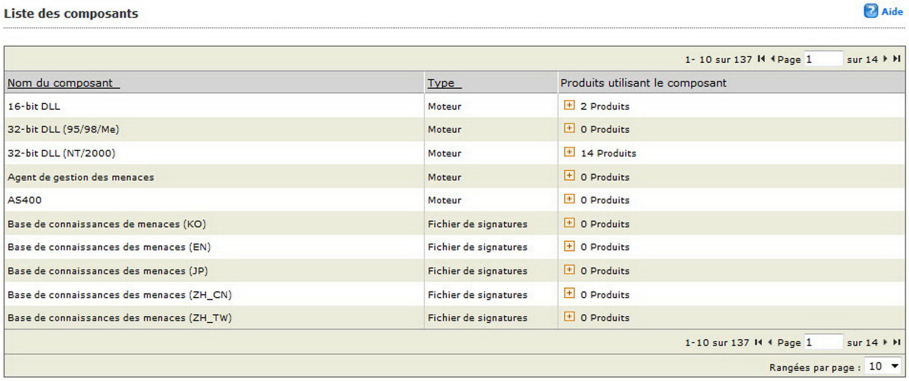


FIGURE 5-1. L'écran Liste des composants

Le serveur Control Manager conserve uniquement la version la plus récente des composants. Vous pouvez vérifier l'historique des versions d'un composant dans le fichier `racine>:\Program Files\Trend Micro\Control Manager\AU_log\TmuDump.txt`. `TmuDump.txt` est généré lorsque le débogage ActiveUpdate est activé.

Conseil

Pour minimiser le trafic du réseau Control Manager, désactivez le téléchargement des composants de produits ou de services gérés qui ne sont pas installés. Si vous enregistrez des produits gérés ou activez des services ultérieurement, veillez à configurer le téléchargement manuel ou programmé des composants correspondants.

Téléchargement manuel de composants

Téléchargez manuellement des mises à jour de composants lorsque vous installez Control Manager pour la première fois, lorsque le réseau fait l'objet d'une attaque ou lorsque vous voulez tester de nouveaux composants avant de les déployer sur le réseau.

Trend Micro recommande la méthode suivante pour configurer les téléchargements manuels. Cette procédure comporte plusieurs étapes.

Conseil

Ignorez les étapes 1 et 2 si vous avez déjà défini un plan de déploiement et les paramètres proxy.

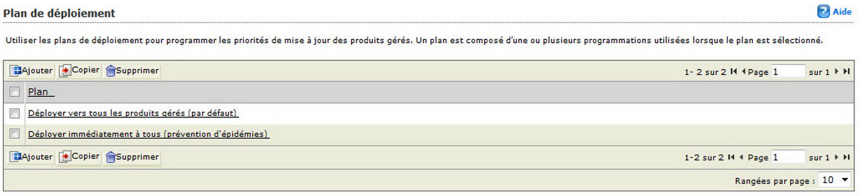
- Étape 1 : Configuration d'un plan de déploiement des composants
- Étape 2 : Configuration des paramètres du proxy (en cas d'utilisation d'un serveur proxy)
- Étape 3 : Sélection des composants à mettre à jour
- Étape 4 : Configuration des paramètres de téléchargement
- Étape 5 : Configuration des paramètres de déploiement automatique
- Étape 6 : Exécution du téléchargement manuel

Étape 1 : Configuration d'un plan de déploiement des composants

Procédure

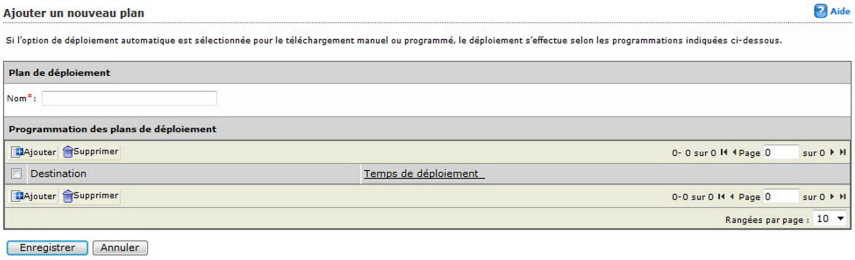
1. Accédez à **Mises à jour** > **Plan de déploiement**.

   L'écran **Plan de déploiement** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un nouveau plan** apparaît.



3. Saisissez un nom de plan de déploiement dans le champ **Nom**.

4. Cliquez sur **Ajouter** pour indiquer les détails du plan de déploiement.

   L'écran **Ajouter une nouvelle programmation** apparaît.

5. Dans l'écran **Ajouter une nouvelle programmation**, choisissez une programmation de l'heure de déploiement en sélectionnant l'une des options suivantes :

   - **Commencer à** : exécute le déploiement à l'heure indiquée

     Spécifiez l'heure choisie (heures et minutes) à l'aide des listes déroulantes.

   - **Retard** : après avoir téléchargé les composants de mise à jour, Control Manager retarde le déploiement de la durée que vous indiquez

     Spécifiez la durée (en heures et minutes) à l'aide des listes déroulantes.

6. Sélectionnez le dossier du répertoire Produits auquel vous souhaitez appliquer la programmation. Control Manager applique la programmation à tous les produits figurant dans le dossier sélectionné.

7. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un nouveau plan** apparaît.

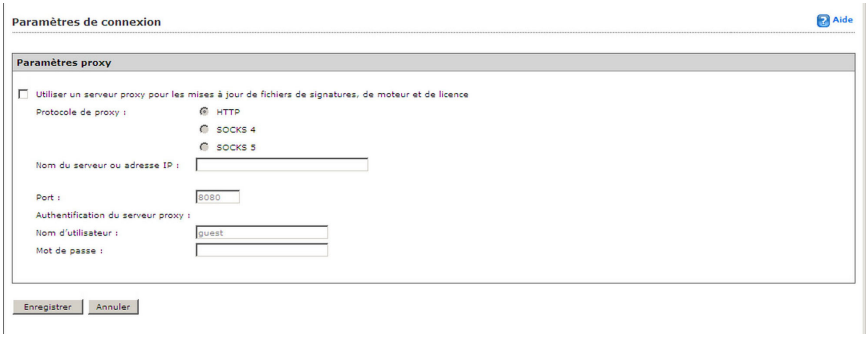
8. Cliquez sur **Enregistrer** pour appliquer le nouveau plan de déploiement.

Étape 2 : Configuration des paramètres proxy (en cas d'utilisation d'un serveur proxy)

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres proxy**.

   L'écran **Paramètres de connexion** apparaît.



2. Sélectionnez **Utiliser un serveur proxy pour les mises à jour de fichiers de signatures, de moteur et de licence**.

3. Sélectionnez le protocole :

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Saisissez le nom d'hôte ou l'adresse IP du serveur dans le champ **Nom de serveur ou adresse IP**.

5. Saisissez un numéro de port dans le champ **Port**.

6. Saisissez un nom et un mot de passe de connexion si votre serveur vous demande de vous authentifier.

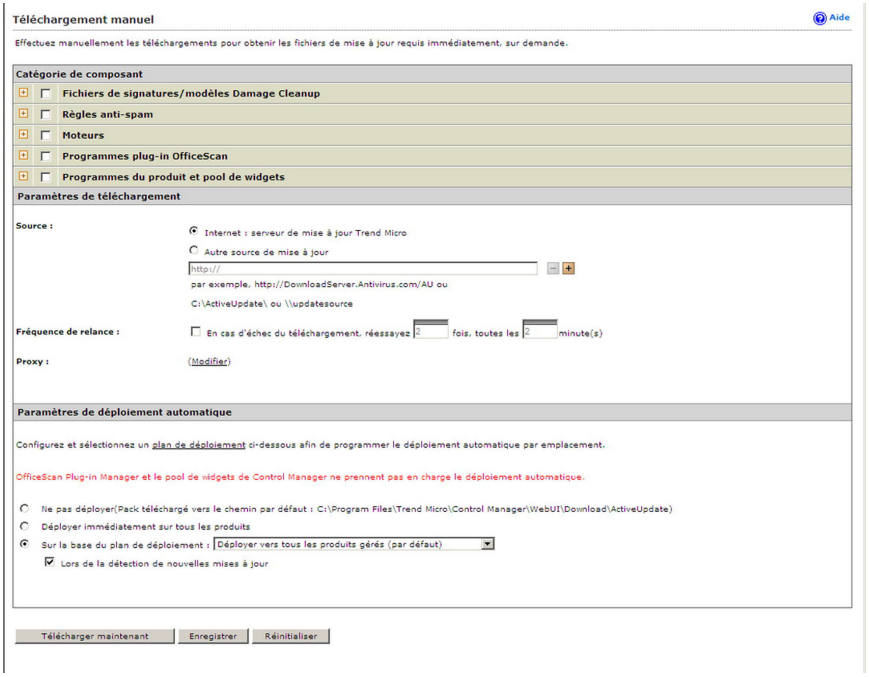
7. Cliquez sur **Enregistrer**.

Étape 3 : Sélection des composants à mettre à jour

Procédure

1. Accédez à **Mises à jour** > **Téléchargement manuel**.

   L'écran **Téléchargement manuel** apparaît.



2. Dans la zone Catégorie de composant, sélectionnez les composants à télécharger.

a. Cliquez sur l'icône + pour développer la liste des composants pour chaque groupe de composants.

b. Sélectionnez les composants à télécharger. Pour sélectionner tous les composants d'un groupe, sélectionnez :

- **Fichiers de signatures/modèles Damage Cleanup**
- **Règles anti-spam**
- **Moteurs**
- **Programmes plug-in OfficeScan**
- **Programmes du produit et pool de widgets**

Étape 4 : Configuration des paramètres de téléchargement

Procédure

1. Sélectionnez la source de mise à jour :

   - **Internet : serveur de mise à jour Trend Micro** : téléchargez les composants à partir du Trend Micro ActiveUpdate Server officiel.
   - **Autre source de mise à jour** : saisissez l'URL de la source de mise à jour dans le champ correspondant.

     Après avoir coché l'option **Autre source de mise à jour**, vous pouvez spécifier plusieurs sources de mise à jour. Cliquez sur l'icône + pour ajouter une source de mise à jour. Vous pouvez sélectionner jusqu'à cinq sources de mise à jour.

2. Sélectionnez **Fréquence de réessai** et spécifiez le nombre de nouvelles tentatives et la durée entre deux tentatives de téléchargement de composants.

Conseil

Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

3. Si vous utilisez un serveur proxy HTTP sur le réseau (si le serveur Control Manager n'a pas d'accès Internet direct), cliquez sur **Modifier** pour configurer les paramètres proxy dans l'écran **Paramètres de connexion**.

Étape 5 : Configuration des paramètres de déploiement automatique

Procédure

1. Spécifiez quand vous voulez déployer les composants téléchargés depuis la zone Paramètres de déploiement automatique. Les options sont les suivantes :

   - **Ne pas déployer** : les composants sont téléchargés sur Control Manager, mais ne sont pas déployés sur des produits gérés. Utilisez cette option dans les conditions suivantes :
     - Déploiement sur des produits gérés de façon individuelle
     - Test des composants téléchargés avant déploiement
   - **Déployer immédiatement sur tous les produits** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés.
   - **Sur la base du plan de déploiement** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés selon la programmation que vous avez sélectionnée.
   - **Lors de la détection de nouvelles mises à jour** : les composants sont téléchargés sur Control Manager lorsque de nouveaux composants sont disponibles à partir de la source de mise à jour, puis déployés sur des produits gérés selon la programmation que vous avez sélectionnée.

Conseil

Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

Étape 6 : Exécution du téléchargement manuel

Procédure

1. Cliquez sur **Télécharger maintenant**, puis cliquez sur **OK** pour confirmer.

   L'écran d'informations sur le téléchargement apparaît. La barre de progression indique l'état du téléchargement.

2. Cliquez sur **Détails sur la commande** pour afficher les informations de l'écran **Détails sur la commande**.

3. Cliquez sur **OK** pour revenir à l'écran **Téléchargement manuel**.

Description des exceptions de téléchargement programmé

Les administrateurs peuvent programmer des exceptions de téléchargement pour empêcher Control Manager de télécharger des composants de mise à jour Trend Micro pendant certains jours ou à certaines heures de la journée.

Cette fonction est particulièrement utile pour les administrateurs préférant que Control Manager ne télécharge pas de composants en dehors des jours ouvrés ou des heures d'ouverture.

Remarque

Les exceptions de programmation quotidiennes s'appliquent aux jours sélectionnés, tandis que les exceptions de programmation par heure s'appliquent à chaque jour de la semaine.

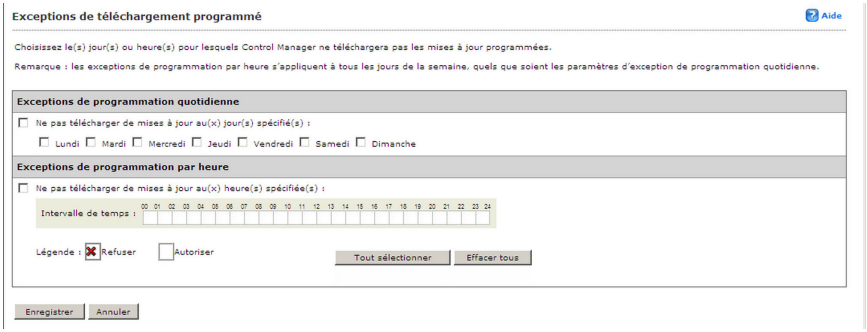
Exemple : l'administrateur souhaite que Control Manager ne télécharge pas de composants les weekends ou après les heures de travail des jours de semaine. L'administrateur active **Exception de programmation quotidienne** et sélectionne **Samedi** et **Dimanche**. L'administrateur active ensuite **Exceptions de programmation par heure** et spécifie les heures entre **00:00 et 9:00** et **18:00 et 24:00**.

Configuration d'exceptions de téléchargement programmé

Procédure

1. Accédez à **Mises à jour** > **Exceptions de téléchargement programmé**.

   L'écran **Exceptions de téléchargement programmé** apparaît.



2. Effectuez une ou plusieurs des opérations suivantes :

   - Pour programmer une exception quotidienne, dans Exceptions de programmation quotidienne, spécifiez le(s) jour(s) où vous ne souhaitez pas effectuer de téléchargement, puis sélectionnez **Ne pas télécharger de mises à jour au(x) jour(s) spécifié(s)**. Chaque semaine, aux jours sélectionnés, Control Manager bloque tous les téléchargements.

- Pour programmer une exception à une heure spécifique, dans Exceptions de programmation par heure, spécifiez les heures auxquelles vous ne souhaitez pas de téléchargement, puis sélectionnez **Ne pas télécharger de mises à jour au(x) heure(s) spécifiée(s)**. Chaque jour, aux heures sélectionnées, Control Manager bloque tous les téléchargements.

3. Cliquez sur **Enregistrer**.

Configuration de téléchargements programmés

Vous pouvez programmer le téléchargement des composants pour les maintenir à jour et protéger le réseau au maximum. Control Manager prend en charge le téléchargement granulaire des composants. Vous pouvez programmer le téléchargement de composants spécifiques ou de groupes de composants. Toutes les programmations sont indépendantes les unes des autres. Lorsque vous programmez le téléchargement d'un groupe de composants, vous programmez le téléchargement de tous les composants de ce groupe.

Accédez à l'écran **Téléchargement programmé** pour obtenir les informations suivantes sur les composants actuellement installés dans votre système Control Manager :

- **Fréquence** : indique la fréquence de mise à jour des composants.
- **Activé** : indique si la programmation du composant est activée ou non.
- **Source de mise à jour** : affiche l'URL ou le chemin d'accès à la source de mise à jour.

La procédure de programmation du téléchargement de composants comporte les étapes suivantes :

- Étape 1 : Configuration d'un plan de déploiement des composants
- Étape 2 : Configuration des paramètres du proxy (en cas d'utilisation d'un serveur proxy)
- Étape 3 : Sélection des composants à mettre à jour

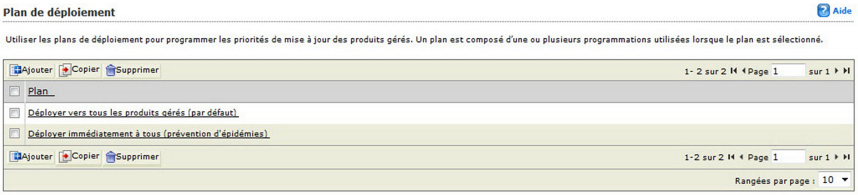
- Étape 4 : Configuration de la programmation de téléchargement
- Étape 5 : Configuration des paramètres de téléchargement
- Étape 6 : Configuration des paramètres de déploiement automatique
- Étape 7 : Activation de la programmation et enregistrement des paramètres

Étape 1 : Configuration d'un plan de déploiement des composants

Procédure

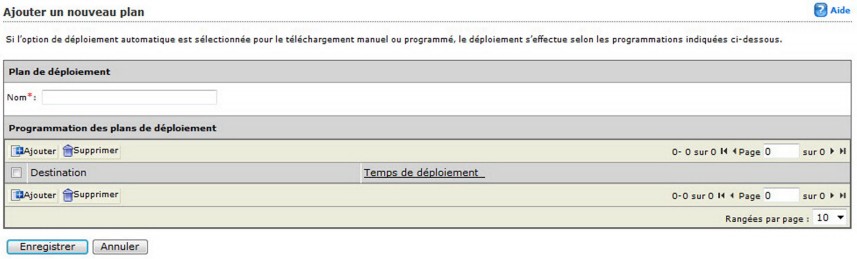
1. Accédez à **Mises à jour** > **Plan de déploiement**.

   L'écran **Plan de déploiement** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un nouveau plan** apparaît.



3. Saisissez un nom de plan de déploiement dans le champ **Nom**.

4. Cliquez sur **Ajouter** pour indiquer les détails du plan de déploiement.

   L'écran **Ajouter une nouvelle programmation** apparaît.

5. Choisissez une heure de déploiement en sélectionnant une des options suivantes :

   - **Commencer à** : exécute le déploiement à l'heure indiquée

     Spécifiez l'heure choisie (heures et minutes) à l'aide des listes déroulantes.

   - **Retard** : après avoir téléchargé les composants de mise à jour, Control Manager retarde le déploiement de la durée que vous indiquez

     Spécifiez la durée (en heures et minutes) à l'aide des listes déroulantes.

6. Sélectionnez le dossier du répertoire Produits auquel vous souhaitez appliquer la programmation. Control Manager applique la programmation à tous les produits figurant dans le dossier sélectionné.

7. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un nouveau plan** apparaît.

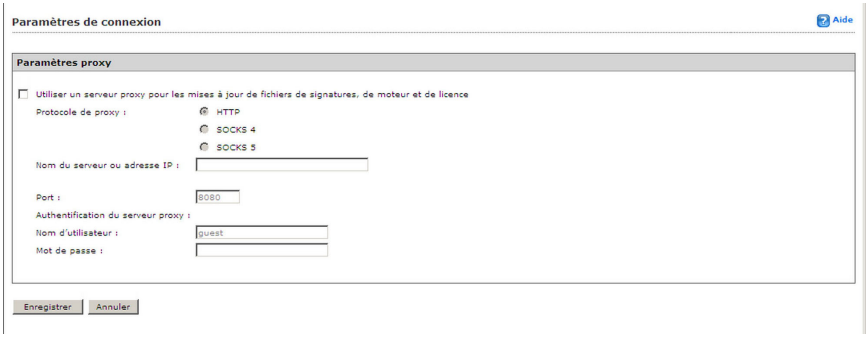
8. Cliquez sur **Enregistrer** pour appliquer le nouveau plan de déploiement.

Étape 2 : Configuration des paramètres proxy (en cas d'utilisation d'un serveur proxy)

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres proxy**.

   L'écran **Paramètres de connexion** apparaît.



2. Sélectionnez **Utiliser un serveur proxy pour les mises à jour de fichiers de signatures, de moteur et de licence**.

3. Sélectionnez le protocole :

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Saisissez le nom d'hôte ou l'adresse IP du serveur dans le champ **Nom de serveur ou adresse IP**.

5. Saisissez un numéro de port pour le serveur proxy dans le champ **Port**.

6. Saisissez un nom et un mot de passe de connexion si votre serveur vous demande de vous authentifier.

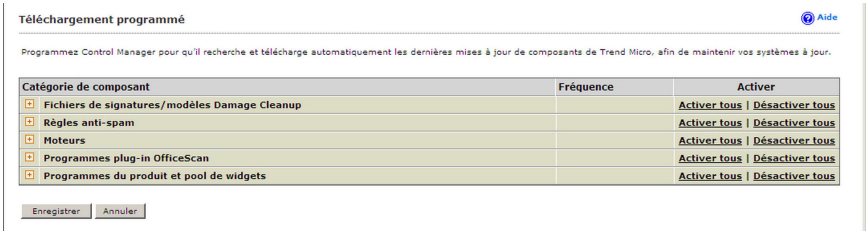
7. Cliquez sur **Enregistrer**.

Étape 3 : Sélection des composants à mettre à jour

Procédure

1. Accédez à **Mises à jour** > **Téléchargement programmé**.

   L'écran **Téléchargement programmé** apparaît.



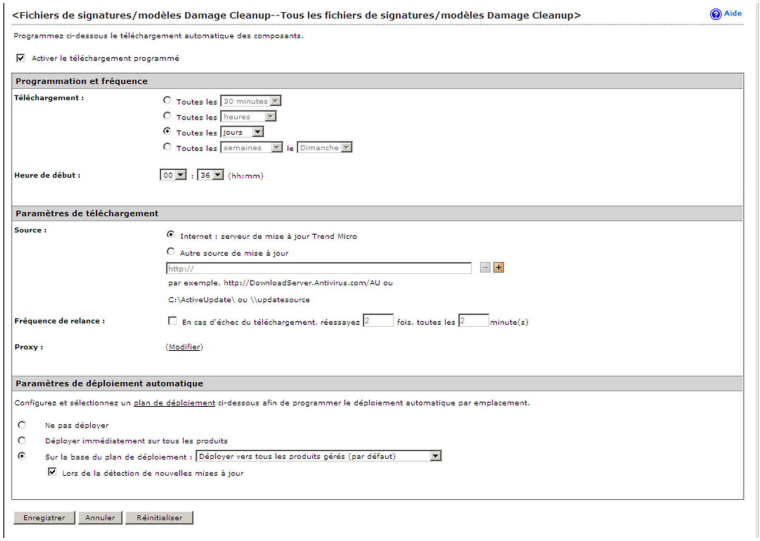
2. Dans la zone Catégorie de composant, sélectionnez les composants à télécharger.

   a. Cliquez sur l'icône **+** pour développer la liste des composants pour chaque groupe de composants.

   b. Sélectionnez les composants à télécharger. Pour sélectionner tous les composants d'un groupe, sélectionnez :

      - **Tous les fichiers de signatures/modèles Damage Cleanup**
      - **Toutes les règles anti-spam**
      - **Tous les moteurs**
      - **Programmes plug-in OfficeScan**
      - **Programmes du produit et pool de widgets**

        L'écran <Nom du composant> apparaît. Où <Nom du composant> correspond au nom du composant que vous avez sélectionné.



Étape 4 : Configuration de la programmation de téléchargement

Procédure

1. Sélectionnez la case **Activer téléchargement programmé** pour activer le téléchargement programmé du composant.

2. Définissez la programmation de téléchargement. Sélectionnez une fréquence et spécifiez la programmation requise à partir des listes déroulantes appropriées. Vous pouvez programmer un téléchargement toutes les minutes, toutes les heures, selon une fréquence quotidienne ou hebdomadaire.

3. Définissez la date et l'heure de prise en compte de la programmation à partir des listes déroulantes **Heure de début**.

Étape 5 : Configuration des paramètres de téléchargement

Procédure

1. Sélectionnez la source de mise à jour :

   - **Internet** : **serveur de mise à jour Trend Micro** : téléchargez les composants à partir du Trend Micro ActiveUpdate Server officiel.
   - **Autre source de mise à jour** : saisissez l'URL de la source de mise à jour dans le champ correspondant.

     Après avoir coché l'option **Autre source de mise à jour**, vous pouvez spécifier plusieurs sources de mise à jour. Cliquez sur l'icône **+** pour ajouter une source de mise à jour. Vous pouvez sélectionner jusqu'à cinq sources de mise à jour.

2. Sélectionnez **Fréquence de réessai** et spécifiez le nombre de nouvelles tentatives et la durée entre deux tentatives de téléchargement de composants.

   Remarque

   Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

3. Si vous utilisez un serveur proxy HTTP sur le réseau (si le serveur Control Manager n'a pas d'accès Internet direct), cliquez sur **Modifier** pour configurer les paramètres proxy dans l'écran **Paramètres de connexion**.

Étape 6 : Configuration des paramètres de déploiement automatique

Procédure

1. Spécifiez quand vous voulez déployer les composants téléchargés depuis la zone Paramètres de déploiement automatique. Les options sont les suivantes :

- **Ne pas déployer** : les composants sont téléchargés sur Control Manager, mais ne sont pas déployés sur des produits gérés. Utilisez cette option dans les conditions suivantes :
  - Déploiement sur des produits gérés de façon individuelle
  - Test des composants téléchargés avant déploiement
- **Déployer immédiatement** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés.
- **Sur la base du plan de déploiement** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés selon la programmation que vous avez sélectionnée.
- **Lors de la détection de nouvelles mises à jour** : les composants sont téléchargés sur Control Manager, puis déployés vers les produits gérés lorsque de nouveaux composants sont disponibles sur la source de mise à jour.

Remarque

Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

2. Sélectionnez un plan de déploiement une fois les composants téléchargés sur Control Manager, dans l'écran **Plan de déploiement**.
3. Cliquez sur **Enregistrer**.

Étape 7 : Activation de la programmation et enregistrement des paramètres

Procédure

1. Cliquez sur le bouton État dans la colonne **Activer**.
2. Cliquez sur **Enregistrer**.

Configuration de la programmation et de la fréquence d'un téléchargement programmé

Spécifiez la fréquence à laquelle Control Manager doit télécharger les mises à jour de composants dans le groupe Programmation et fréquence.

Procédure

1. Accédez à **Mises à jour** > **Téléchargement programmé**.

   L'écran **Téléchargement programmé** apparaît.

2. Dans la zone Catégorie de composant, sélectionnez les composants à télécharger.

   a. Cliquez sur l'icône **+** pour développer la liste des composants pour chaque groupe de composants.

   b. Sélectionnez les composants à télécharger. Pour sélectionner tous les composants d'un groupe, sélectionnez :

      - **Tous les fichiers de signatures/modèles Damage Cleanup**
      - **Toutes les règles anti-spam**
      - **Tous les moteurs**
      - **Programmes plug-in OfficeScan**
      - **Programmes du produit et pool de widgets**

        L'écran <Nom du composant> apparaît. Où Nom du composant> est le nom du composant que vous avez sélectionné.

3. Sous Programmation et fréquence :

   a. Définissez la programmation de téléchargement. Sélectionnez une fréquence et spécifiez la programmation requise à partir des listes déroulantes appropriées. Vous pouvez programmer un téléchargement toutes les minutes, toutes les heures, selon une fréquence quotidienne ou hebdomadaire.

   b. Définissez la date et l'heure de prise en compte de la programmation à partir des listes déroulantes **Heure de début**.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres de téléchargement programmé

Vous définissez les composants à télécharger automatiquement et la méthode de téléchargement dans le groupe Paramètres de téléchargement.

Procédure

1. Accédez à **Mises à jour** > **Téléchargement programmé**.

   L'écran **Téléchargement programmé** apparaît.

2. Dans la zone Catégorie de composant, sélectionnez les composants à télécharger.

   a. Cliquez sur l'icône **+** pour développer la liste des composants pour chaque groupe de composants.

   b. Sélectionnez les composants à télécharger. Pour sélectionner tous les composants d'un groupe, sélectionnez :

      - **Tous les fichiers de signatures/modèles Damage Cleanup**
      - **Toutes les règles anti-spam**
      - **Tous les moteurs**
      - **Programmes plug-in OfficeScan**
      - **Programmes du produit et pool de widgets**

        L'écran <Nom du composant> apparaît. Où <Nom du composant> correspond au nom du composant que vous avez sélectionné.

3. Dans Paramètres de téléchargement, sélectionnez une des sources de mise à jour suivantes :

   - **Internet : serveur de mise à jour Trend Micro** : Control Manager télécharge les composants les plus récents à partir de Trend Micro ActiveUpdate Server (option par défaut).

- **Autre source de mise à jour** : spécifiez l'URL de la source où se trouve la version la plus récente du composant (le serveur Intranet de votre société, par exemple).

  Après avoir coché l'option **Autre source de mise à jour**, vous pouvez spécifier plusieurs sources de mise à jour. Cliquez sur l'icône + pour ajouter une autre source de mise à jour. Vous pouvez sélectionner jusqu'à cinq sources de mise à jour.

4. Sélectionnez **Fréquence de réessai** pour que Control Manager essaye à nouveau de télécharger les composants les plus récents. Spécifiez le nombre et la fréquence des tentatives dans les champs correspondants.

Remarque

Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

5. Si vous utilisez un serveur proxy sur le réseau (si le serveur Control Manager n'a pas d'accès Internet direct), cliquez sur **Modifier** pour configurer les paramètres proxy dans l'écran **Paramètres de connexion**.

6. Cliquez sur **Enregistrer**.

Configuration des paramètres de déploiement automatique de téléchargements programmés

Utilisez le groupe de paramètres de déploiement automatique pour définir comment les mises à jour sont déployées par Control Manager.

Procédure

1. Accédez à **Mises à jour** > **Téléchargement programmé**.

   L'écran **Téléchargement programmé** apparaît.

2. Dans la zone Catégorie de composant, sélectionnez les composants à télécharger.

a. Cliquez sur l'icône **+** pour développer la liste des composants pour chaque groupe de composants.

b. Sélectionnez les composants à télécharger. Pour sélectionner tous les composants d'un groupe, sélectionnez :

- **Tous les fichiers de signatures/modèles Damage Cleanup**
- **Toutes les règles anti-spam**
- **Tous les moteurs**
- **Programmes plug-in OfficeScan**
- **Programmes du produit et pool de widgets**

L'écran <Nom du composant> apparaît. Où <Nom du composant> correspond au nom du composant que vous avez sélectionné.

3. Spécifiez quand vous voulez déployer les composants téléchargés depuis la zone Paramètres de déploiement automatique. Les options sont les suivantes :

- **Ne pas déployer** : les composants sont téléchargés sur Control Manager, mais ne sont pas déployés sur des produits gérés. Utilisez cette option dans les conditions suivantes :
  - Déploiement sur des produits gérés de façon individuelle
  - Test des composants téléchargés avant déploiement
- **Déployer immédiatement** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés.
- **Sur la base du plan de déploiement** : les composants sont téléchargés sur Control Manager, puis déployés sur des produits gérés selon la programmation que vous avez sélectionnée.
- **Lors de la détection de nouvelles mises à jour** : les composants sont téléchargés sur Control Manager lorsque de nouveaux composants sont disponibles à partir de la source de mise à jour, puis déployés sur des produits gérés selon la programmation que vous avez sélectionnée.

Remarque

Cliquez sur **Enregistrer** avant de cliquer sur **Modifier** ou **Plan de déploiement** dans cet écran. Vous perdrez vos paramètres si vous ne cliquez pas sur **Enregistrer**.

4. Sélectionnez un plan de déploiement une fois les composants téléchargés sur Control Manager, dans l'écran **Plan de déploiement**.

5. Cliquez sur **Enregistrer**.

Remarque

Les paramètres de déploiement automatique s'appliquent uniquement aux composants utilisés par des produits gérés.

Définition des plans de déploiement

Un plan de déploiement permet de définir l'ordre dans lequel Control Manager met à jour vos groupes de produits gérés. Avec Control Manager, vous pouvez appliquer plusieurs plans de déploiement à différents produits gérés lors de différentes programmations. Par exemple, pendant une épidémie virale impliquant un virus de messagerie, vous pouvez donner la priorité à la mise à jour des composants de votre logiciel de scan de messagerie, comme le dernier fichier de signatures de virus pour ScanMail for Microsoft Exchange de Trend Micro.

L'installation de Control Manager crée deux plans de déploiement :

- Déployer vers tous les produits gérés (par défaut) : plan par défaut utilisé durant les mises à jour des composants
- Déployer vers tous immédiatement (prévention des épidémies) : plan par défaut pour les Outbreak Prevention Services, étape de prévention

Par défaut, ces plans déploient immédiatement des mises à jour sur tous les produits du répertoire Produits.

Sélectionnez ou créez des plans dans les écrans de téléchargement manuel et programmé. Personnalisez ces plans ou créez-en de nouveaux, selon ce qui est requis par

votre réseau. Par exemple, créez des plans de déploiement en fonction de la nature de l'épidémie :

- Virus de messagerie
- Virus se propageant via le partage de fichier

Le déploiement de mises à jour vers le répertoire Produits est distinct du processus de téléchargement.

Control Manager télécharge les composants et réalise le plan de déploiement selon les paramètres de téléchargement manuel ou programmé.

Lors de la création ou de l'implémentation d'un plan de déploiement, soyez attentifs aux éléments suivants :

- Attribuez des programmations de déploiement aux dossiers et non à des produits spécifiques.

  La planification du contenu des dossiers du répertoire Produits est donc très importante.

- Vous ne pouvez inclure qu'un dossier pour chaque programmation de plan de déploiement.

  Toutefois, vous pouvez spécifier plus d'une programmation par plan de déploiement.

- Control Manager prend en compte l'heure de fin du téléchargement pour les retards de plans de déploiement, de façon indépendante les uns des autres.

  Par exemple, si vous souhaitez mettre à jour trois dossiers à 5 minutes d'intervalle, vous pouvez attribuer au premier dossier un retard de 5 minutes, puis définir des retards de 10 et 15 minutes pour les deux autres dossiers.

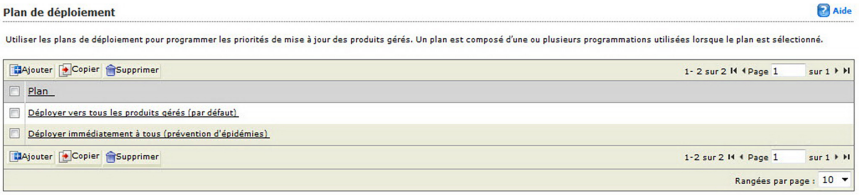
Création de plans de déploiement

Créez un nouveau plan si aucun des plans existants ne correspond à vos besoins.

Procédure

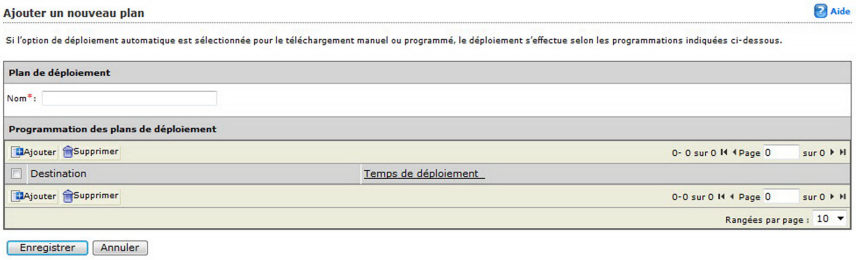
1. Accédez à **Mises à jour** > **Plan de déploiement**.

L'écran **Plan de déploiement** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un nouveau plan** apparaît.



3. Saisissez un nom de plan de déploiement dans le champ **Nom**.

4. Cliquez sur **Ajouter** pour indiquer les détails du plan de déploiement.

   L'écran **Ajouter une nouvelle programmation** apparaît.

5. Choisissez une heure de déploiement en sélectionnant une des options suivantes :

- **Commencer à** : exécute le déploiement à l'heure indiquée

  Spécifiez l'heure choisie (heures et minutes) à l'aide des listes déroulantes.

- **Retard** : après avoir téléchargé les composants de mise à jour, Control Manager retarde le déploiement de la durée que vous indiquez

  Spécifiez la durée (en heures et minutes) à l'aide des listes déroulantes.

6. Sélectionnez le dossier du répertoire Produits auquel vous souhaitez appliquer la programmation. Control Manager applique la programmation à tous les produits figurant dans le dossier sélectionné.

7. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un nouveau plan** apparaît.

8. Cliquez sur **Enregistrer** pour appliquer le nouveau plan de déploiement.

Modification d'un plan de déploiement

Utilisez l'écran **Modifier le plan** pour ajouter, modifier ou supprimer les programmations d'un plan de déploiement.

Procédure

1. Accédez à **Mises à jour** > **Plan de déploiement**.

   L'écran **Plan de déploiement** apparaît.

2. Cliquez sur le nom du plan à modifier.

   La fenêtre **Modifier le plan** s'affiche.

3. Cliquez sur le nom de la programmation à modifier.

   L'écran **Modifier la programmation** apparaît.

4. Modifiez l'heure de déploiement ou le dossier Répertoire Produits.

Remarque

Vous ne pouvez pas supprimer une programmation s'il s'agit de la seule disponible.

5. Cliquez sur **Enregistrer**.

   L'écran **Modifier un nouveau plan** s'affiche.

6. Après avoir apporté les modifications nécessaires, cliquez sur **Enregistrer**.

   L'écran **Plan de déploiement** apparaît.

Duplication d'un plan de déploiement

Créez des plans de déploiement à partir d'un plan existant.

Procédure

1. Accédez à **Mises à jour** > **Plan de déploiement**.

   L'écran **Plan de déploiement** apparaît.

2. Cochez la case correspondant au plan à copier.

3. Cliquez sur **Copier**.

   L'écran **Ajouter un nouveau plan** apparaît.

4. Saisissez un nom de plan unique. Par défaut, tous les plans copiés sont nommés *Nouveau plan*.

5. Apportez les modifications nécessaires au plan de déploiement.

Remarque

Vous ne pouvez pas supprimer une programmation s'il s'agit de la seule disponible.

6. Cliquez sur **Enregistrer**.

Suppression d'un plan de déploiement

Vous pouvez supprimer les plans obsolètes.

Procédure

1. Accédez à **Mises à jour** > **Plan de déploiement**. L'écran Plan de déploiement apparaît.
2. Cochez la case correspondant au plan à supprimer.
3. Cliquez sur **Supprimer**. Les plans sélectionnés sont supprimés de la liste des plans de déploiement.

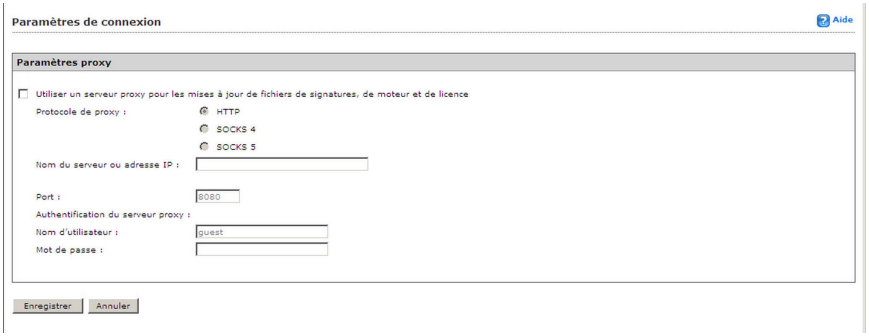
Configuration des paramètres proxy

Configurez la connexion au serveur proxy pour les téléchargements de composants et les mises à jour de licence.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres proxy**.

   L'écran **Paramètres de connexion** apparaît.



2. Sélectionnez **Utiliser un serveur proxy pour les mises à jour de fichiers de signatures, de moteur et de licence**.

3. Sélectionnez le protocole :

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Saisissez le nom d'hôte ou l'adresse IP du serveur dans le champ **Nom de serveur ou adresse IP**.

5. Saisissez un numéro de port dans le champ **Port**.

6. Saisissez un nom et un mot de passe de connexion si votre serveur vous demande de vous authentifier.

7. Cliquez sur **Enregistrer**.

Configuration des paramètres de mise à jour/déploiement

Le téléchargement de composants via HTTPS à partir de Trend Micro ActiveUpdate Server (la source de téléchargement par défaut) ou d'une autre source de mise à jour constitue une méthode de récupération des composants plus sûre.

Si vous téléchargez des composants à partir d'un répertoire partagé sur un réseau, vous devez définir l'authentification Windows locale et l'authentification UNC à distance.

L'authentification Windows locale renvoie au compte utilisateur Active Directory sur le serveur Control Manager. Vérifiez les éléments suivants pour ce compte :

- Privilège de l'administrateur
- Définition de la stratégie *Connexion en tant que travail par lots*

L'**authentification UNC à distance** utilise un compte utilisateur du serveur source de composants qui est autorisé à partager un dossier dans lequel Control Manager téléchargera les mises à jour.

Activation du téléchargement HTTPS

Procédure

1. Accédez à **Mises à jour** > **Paramètres de Mise à jour/de déploiement**.

   L'écran **Paramètres de mise à jour/de déploiement** apparaît.

2. Sélectionnez **Activer HTTPS pour la source de téléchargement de mises à jour par défaut**.
3. Cliquez sur **Enregistrer**.
4. Accédez à l'écran **Téléchargement manuel** ou **Téléchargement programmé**.
5. Dans la zone de travail sous **Paramètres de téléchargement**, sélectionnez **Internet : serveur de mise à jour Trend Micro** ou indiquez le serveur de composants de votre entreprise dans le champ **Autre source de mise à jour**.
6. Cliquez sur **Enregistrer**.

Activation du téléchargement UNC

Procédure

1. Accédez à **Mises à jour** > **Paramètres de Mise à jour/de déploiement**.

   L'écran **Paramètres de mise à jour/de déploiement** apparaît.

2. Saisissez les noms d'utilisateurs et mots de passe de l'**Authentification Windows locale** et de l'**Authentification UNC à distance**.

3. Cliquez sur **Enregistrer**.

4. Accédez à l'écran **Téléchargement manuel** ou **Téléchargement programmé**.

5. Dans la zone de travail sous le groupe **Paramètres de téléchargement**, sélectionnez **Autre source de mise à jour** et indiquez le dossier partagé sur le réseau.

6. Cliquez sur **Enregistrer**.

Définition de la stratégie « Connexion en tant que tâche par lots »

L'authentification Windows locale renvoie au compte utilisateur Active Directory sur le serveur Control Manager. Vérifiez les éléments suivants pour ce compte :

- Privilège de l'administrateur
- Définition de la stratégie « Connexion en tant que tâche par lots »

Procédure

1. Cliquez sur **Démarrer** > **Paramètres** > **Panneau de configuration**.

2. Cliquez sur **Outils d'administration**.

3. Ouvrez la **Stratégie de sécurité locale**. L'écran de configuration de la sécurité locale apparaît.

4. Cliquez sur **Stratégies locales** > **Attribution de droits utilisateurs**.
5. Double-cliquez sur **Connexion en tant que travail par lots**.

   La boîte de dialogue **Propriétés de Connexion en tant que travail par lots** apparaît.
6. Ajoutez l'utilisateur s'il n'est pas dans la liste.

Partie II

Surveillance du réseau Control Manager

Chapitre 6

Utilisation du tableau de bord et des widgets

Le tableau de bord remplace l'écran Résumé des versions antérieures de Control Manager.

Ce chapitre traite les rubriques suivantes :

Utilisation du tableau de bord

Le tableau de bord de Control Manager fournit des informations d'ensemble du réseau Control Manager. Il est constitué de deux composants :

- **Onglets :** Permettent aux administrateurs de créer un écran contenant un ou plusieurs widgets.
- **Widgets :** Fournissent des informations spécifiques sur divers événements liés à la sécurité.

Remarque

Pour que certains widgets fonctionnent, il est nécessaire d'activer Smart Feedback. Pour plus d'informations sur l'activation de Smart Feedback, consultez la section *Configuration des paramètres de Smart Protection Network à la page 6-25*.

Comptes utilisateurs et tableau de bord

Chaque compte utilisateur affiche son tableau de bord. Lorsqu'un utilisateur se connecte pour la première à Control Manager, les onglets par défaut et les widgets qu'ils contiennent s'affichent dans le tableau de bord.

Chaque compte utilisateur peut personnaliser le tableau de bord, les onglets et les widgets en fonction de ses besoins spécifiques. La personnalisation du tableau de bord, des onglets ou des widgets pour un compte utilisateur n'a aucun impact sur le tableau de bord, les onglets ou les widgets d'un autre compte utilisateur. Chaque compte utilisateur dispose d'un tableau de bord, d'onglets et de widgets totalement indépendants de tout autre compte utilisateur.

Définition des onglets

Le tableau de bord de Control Manager utilise des onglets pour offrir plus de souplesse aux administrateurs. Grâce au conteneur de widgets, ils peuvent créer leur tableau de bord personnalisé. Ce tableau de bord prend en charge jusqu'à 30 onglets par compte utilisateur.

Vous pouvez déplacer des widgets sur les onglets en les faisant glisser, puis en les déposant à différents emplacement de l'onglet. Le widget peut être déplacé en fonction de la disposition d'un onglet.

Remarque

La personnalisation du tableau de bord, des onglets ou des widgets pour un compte utilisateur n'a aucun impact sur le tableau de bord, les onglets ou les widgets d'un autre compte utilisateur. Chaque compte utilisateur dispose d'un tableau de bord, d'onglets et de widgets totalement indépendants de tout autre compte utilisateur.

Onglets par défaut

Le tableau de bord est composé des onglets suivants :

- Résumé
- Investigation sur les incidents de DLP
- Prévention contre la perte de données
- Conformité
- Détection des menaces
- Smart Protection Network

Remarque

Si un compte utilisateur supprime définitivement les onglets par défaut, il ne peut plus les voir. Il est impossible de récupérer un onglet supprimé. La suppression d'un onglet par défaut n'a aucun impact sur le tableau de bord des autres comptes utilisateur.

Onglet Résumé

L'onglet Résumé remplace l'écran d'accueil de Control Manager. Toutes les informations disponibles sur cet écran sont disponibles via les widgets de l'onglet Résumé.

TABLEAU 6-1. Widgets de l'onglet Résumé

WIDGET	DESCRIPTION
Lancement rapide	Affiche les raccourcis des fonctions principales.
État de la stratégie	Affiche l'état du déploiement de vos stratégies.
Événements de rappel C&C	Affiche le nombre de tentatives de rappels en fonction des hôtes compromis ou des adresses de rappel.
État de la connexion des points finaux	Affiche l'état de connexion entre le client OfficeScan et son serveur OfficeScan (en ligne, hors ligne, itinérant).
État de la connexion du produit	Affiche l'état de connexion du produit géré à Control Manager (en ligne, hors ligne, désactivé, anormal).

Onglet Investigation sur les incidents de DLP

L'onglet Investigation sur les incidents de DLP contient des widgets qui affichent des informations sur les incidents DLP en se basant sur le statut de l'incident, les niveaux de gravité et les utilisateurs gérés.

TABLEAU 6-2. Widgets de l'onglet Investigation sur les incidents de DLP

WIDGET	DESCRIPTION
Incidents de prévention contre la perte des données par gravité et par état	Affiche le nombre d'incidents DLP en fonction des niveaux de gravité et de l'état des incidents.
Tendances des incidents de prévention contre la perte des données par utilisateur	Affiche les tendances d'incident en fonction des utilisateurs gérés.
Incidents de prévention contre la perte des données par utilisateur	Affiche le nombre d'incidents en fonction des utilisateurs gérés et des niveaux de gravité.

Onglet Prévention contre la perte de données

L'onglet Prévention contre la perte de données contient des widgets qui fournissent des informations sur les incidents de prévention contre la perte de données, les correspondances de modèles et les sources des incidents.

TABLEAU 6-3. Widgets de l'onglet Prévention contre la perte de données

WIDGET	DESCRIPTION
Incidents de prévention contre la perte de données par canal	Affiche le nombre d'incidents de prévention contre la perte de données en fonctions des canaux.
Correspondances de modèles de prévention contre la perte de données	Affiche le nombre de correspondances des critères dans un modèle. Chaque incident de prévention contre la perte de données peut avoir une ou plusieurs correspondances de modèles.
Sources principales d'incidents de prévention contre la perte de données	Affiche les sources principales d'incidents de prévention contre la perte de données incluant des utilisateurs, adresses électroniques, noms d'hôtes et adresses IP.
Incidents de prévention contre la perte de données par canal	Affiche le nombre d'incidents de prévention contre la perte de données en fonctions des canaux.

Onglet Conformité

L'onglet Conformité contient des widgets qui affichent des informations relatives à la conformité du composant ou de la connexion pour les produits gérés ou les points finaux.

TABLEAU 6-4. Widgets de l'onglet Conformité

WIDGET	DESCRIPTION
Conformité des applications de produits	Affiche la version, la compilation et l'état de mise à jour du produit pour les produits gérés. Ce widget permet aux administrateurs de distinguer rapidement les applications des produits gérés qui sont à jour et ceux nécessitant une mise à jour.
État des composants du produit	Affiche la version du composant (fichier de signatures, modèle, moteur, règle) et l'état (à jour ou obsolète) pour les produits gérés ou les points finaux. Ce widget permet aux administrateurs de savoir rapidement quels produits ou points finaux sont à jour.
État de la connexion du produit	Affiche l'état de connexion du produit géré à Control Manager (en ligne, hors ligne, désactivé, anormal).
État de la connexion des points finaux	Affiche l'état de connexion entre le client OfficeScan et son serveur OfficeScan (en ligne, hors ligne, itinérant).

Onglet Détection des menaces

L'onglet Détection des menaces contient des widgets qui affichent les détections regroupées des menaces de sécurité.

Remarque

Sur les serveurs Control Manager parents, les widgets **Principales menaces de Control Manager** et **Principales menaces détectées par File Reputation** requièrent des transferts programmés des journaux provenant des serveurs Control Manager enfants pour afficher des données précises.

Pour permettre les mises à jour programmées des journaux depuis des serveurs Control Manager : **Produits** > **Sélectionner un serveur enfant dans le répertoire Produits** > **Configurer** > **Programmer les téléchargements de journaux de serveur Control Manager enfant**

TABLEAU 6-5. Widgets de Détection des menaces

WIDGET	DESCRIPTION
Principales menaces de Control Manager	Le widget affiche 10/25/50 principales menaces détectées : • Fichiers malveillants • URL malveillantes
Statistiques des menaces de Control Manager	Affiche le nombre de détections de menaces et le ratio de menaces par rapport au nombre total de détections. Ce widget affiche ces données par : • Catégorie du produit • Type de menace
Statistiques des menaces de Smart Protection Network	Affiche le nombre de détections de menaces de manière globale, au sein d'un secteur, et localement sur votre réseau. Ce widget affiche ces données par : • Catégorie du produit • Type de menace
Principales menaces détectées par File Reputation	Affiche les 10 principales menaces détectées par File Reputation. Les données constituent une comparaison entre les détections globales sur la menace et les détections réalisées sur votre réseau.
Événements de rappel C&C	Affiche le nombre de tentatives de rappels en fonction des hôtes compromis ou des adresses de rappel.

Onglet Smart Protection Network

Dans l'onglet Smart Protection Network, figurent des widgets qui contiennent des informations provenant exclusivement de Trend Micro Smart Protection Network (réputation des e-mails, File Reputation et réputation de sites Web), combinées à des informations provenant du réseau Control Manager.

TABLEAU 6-6. Widgets de l'onglet Smart Protection Network

WIDGET	DESCRIPTION
Principales menaces détectées par File Reputation	Affiche les 10 principales menaces détectées par File Reputation. Les données constituent une comparaison entre les détections globales sur la menace et les détections réalisées sur votre réseau.
Connexions Smart Protection Network	Affiche le nombre de points finaux sur votre réseau qui se connectent au serveur Trend Micro Smart Protection Network pour rechercher des mises à jour ou effectuer des vérifications de menaces de sécurité.
Statistiques des menaces de Smart Protection Network	Affiche le nombre de détections de menaces de manière globale, au sein d'un secteur, et localement sur votre réseau. Ce widget affiche ces données par : • Catégorie du produit • Type de menace
Carte des menaces de File Reputation	Affiche le nombre total de menaces de sécurité détectées par File Reputation. Les informations s'affichent dans une mappemonde, en fonction de leur situation géographique.

Ajout d'onglets

Ajoutez des onglets au tableau de bord afin de fournir une matrice d'informations personnalisées pour les besoins de votre réseau Control Manager.

Procédure

1. Accédez à l'écran **Tableau de bord**.
2. Cliquez sur **Nouvel onglet**.

   L'écran **Nouvel onglet** s'affiche.
3. Saisissez un titre pertinent pour l'onglet dans le champ **Titre**.
4. Sélectionnez une disposition pour l'onglet.

Remarque

Le nombre de widgets que vous pouvez ajouter à un onglet dépend de la disposition de cet onglet. Lorsque l'onglet comporte le nombre maximum de widgets, vous devez supprimer un widget à partir de l'onglet ou créer un nouvel onglet pour le widget.

5. Cliquez sur **Enregistrer**.

   L'onglet vide s'affiche sur le tableau de bord.

6. Cliquez sur **Ajouter un widget** pour ajouter des widgets à l'onglet.

Configuration des paramètres de l'onglet

Vous pouvez modifier le nom par défaut d'un onglet à l'aide de l'écran **Paramètres de l'onglet**.

Procédure

1. Accédez à l'écran **Tableau de bord**.
2. Cliquez sur **Paramètres de l'onglet**.

   L'écran **Paramètres de l'onglet** s'affiche.

3. Saisissez un titre pertinent pour l'onglet dans le champ **Titre**.
4. Cliquez sur **Enregistrer**.

Définition des widgets

Les widgets sont les principaux composants du tableau de bord. Les onglets fournissent la disposition du tableau de bord, et les widgets ses données réelles.

Remarque

La personnalisation du tableau de bord, des onglets ou des widgets pour un compte utilisateur n'a aucun impact sur le tableau de bord, les onglets ou les widgets d'un autre compte utilisateur. Chaque compte utilisateur dispose d'un tableau de bord, d'onglets et de widgets totalement indépendants de tout autre compte utilisateur.

Téléchargez régulièrement le pool de widgets de Control Manager (sous **Programmes du produit et pool de widgets** sur les écrans **Téléchargement manuel** et **Téléchargement programmé**) pour rechercher les widgets nouveaux ou mis à jour.

Les données affichées par un widget proviennent de l'un des emplacements suivants :

- Base de données de Control Manager
- Trend Micro Smart Protection Network
- Produits gérés ajoutés à la liste **Visibilité du serveur** du tableau de bord

Remarque

Smart Feedback doit être activé pour afficher les données de widgets incluant les données de Smart Protection Network.

Les données affichées par un widget sont contrôlées de deux manières :

TABLEAU 6-7. Données de widget

ÉLÉMENT	DÉTAILS
Compte utilisateur	Un compte utilisateur accorde ou restreint l'accès aux produits gérés enregistrés sur Control Manager.
Étendue	La portée des données sur de nombreux widgets peut être configurée individuellement. Cela signifie qu'un utilisateur peut ensuite spécifier l'emplacement de la source de données du widget. **Exemple :** Un administrateur OfficeScan, qui gère plusieurs serveurs OfficeScan, peut créer un onglet et ajouter des widgets qui affichent les données d'un seul serveur OfficeScan.

Paramètres du widget

L'utilisation de certains widgets requiert la configuration de paramètres très spécifiques. Ainsi, le widget de vérification de la protection des points finaux exige une connexion à votre serveur Active Directory, à vos serveurs OfficeScan et à vos serveurs Deep Security.

Configuration des paramètres du widget de vérification d'Active Directory et de Protection des points finaux

Le widget de vérification de la protection des points finaux exige une connexion à votre serveur Active Directory, à vos serveurs OfficeScan et à vos serveurs Deep Security pour fonctionner correctement.

AVERTISSEMENT!

Les arborescences des clients du serveur OfficeScan et d'Active Directory doivent être synchronisées pour que le widget de vérification de la protection des points finaux fonctionne correctement.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres de widget et Active Directory**.

   L'écran **Paramètres Active Directory et du widget de vérification de la protection des points finaux** s'affiche.

2. Sélectionnez **Activer les connexions spécifiées**.

3. Configurez les paramètres de connexion du serveur Active Directory :

   - **FQDN ou adresse IP du serveur** : nom de domaine complet (FQDN) ou adresse IP de votre serveur Active Directory
   - **Nom de domaine\nom d'utilisateur** : Les noms de domaine et d'utilisateur requis pour vous connecter à votre serveur Active Directory
   - **Mot de passe** : mot de passe requis pour vous connecter à votre serveur Active Directory

4. Configurez les paramètres de connexion au serveur OfficeScan :

   - **ID produit** : identifiant court pour le serveur OfficeScan utilisé par le widget
   - **FQDN ou adresse IP du serveur** : nom de domaine complet (FQDN) ou adresse IP de votre serveur OfficeScan
   - **Port** : numéro de port utilisé pour communiquer avec votre serveur OfficeScan
   - **Nom d'utilisateur** : Le nom de domaine et le nom d'utilisateur requis pour vous connecter à votre serveur OfficeScan
   - **Mot de passe** : mot de passe requis pour vous connecter à votre serveur OfficeScan

5. Configurez les paramètres de connexion du serveur Deep Security :

   - **ID produit** : identifiant court pour le serveur Deep Security utilisé par le widget
   - **FQDN ou adresse IP du serveur** : nom de domaine complet (FQDN) ou adresse IP de votre serveur Deep Security
   - **Port** : numéro de port utilisé pour communiquer avec votre serveur Deep Security
   - **Nom d'utilisateur** : Le nom de domaine et le nom d'utilisateur requis pour vous connecter à votre serveur Deep Security
   - **Mot de passe** : mot de passe requis pour vous connecter à votre serveur Deep Security

6. Pour ajouter plusieurs serveurs OfficeScan ou Deep Security, cliquez sur l'icône +. Vous pouvez ajouter jusqu'à cinq serveurs OfficeScan et cinq serveurs Deep Security.

7. Configurez les paramètres de synchronisation :

   - Spécifiez à quelle fréquence tous les serveurs configurés dans cet écran se synchroniseront avec le widget de vérification de la protection des points finaux.

- Cochez la case **Synchroniser après avoir cliqué sur « Enregistrer »** pour forcer tous les serveurs configurés sur cet écran à se synchroniser avec le widget de vérification de la protection des points finaux, une fois que vous aurez cliqué sur Enregistrer.

8. Cliquez sur **Enregistrer**.

Paramètres de connexion Endpoint Encryption

Les widgets qui obtiennent des informations à partir du serveur Endpoint Encryption doivent d'abord s'y connecter.

Procédure

1. Accédez à l'écran **Tableau de bord**.
2. Cliquez sur **Visibilité du serveur**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres de connexion :
   - **Nom du serveur** : nom de domaine complet (FQDN) ou adresse IP ainsi que numéro de port de votre serveur
   - **Type de serveur** : sélectionnez **Endpoint Encryption** dans la liste.
   - **Compte** : nom d'utilisateur requis pour la connexion au serveur
   - **Mot de passe** : mot de passe requis pour la connexion au serveur
   - **Entreprise** : entreprise correspondant aux points finaux associés.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur ( ) en regard des paramètres proxy et configurez les paramètres si votre réseau utilise un serveur proxy.
7. Cliquez sur **Appliquer**.

8. Pour ajouter plus d'un serveur de produits, cliquez sur **Ajouter**.

Utilisation des widgets

Chaque widget fournit des informations de sécurité ciblées. Les widgets peuvent afficher ces informations sous différentes formes :

- Graphique en barres
- Graphique circulaire
- Graphique en ligne
- Tableau

Cliquez sur l'icône d'aide d'un widget pour afficher les types d'informations suivantes :

TABLEAU 6-8. Aide sur le widget

RUBRIQUE DU WIDGET	DESCRIPTION
Présentation	Fournit une description du widget et indique comment l'utiliser
Données de widget	Informations détaillées sur les données affichées dans la table du widget
Configurer	Description des paramètres facilement visibles sur le widget
Modifier	Description des paramètres pour lesquels il est nécessaire de cliquer sur l'icône de modification pour apporter une modification

Informations détaillées sur le widget

L'affichage de données de widget dans une table apporte un avantage supplémentaire aux utilisateurs. Il est possible de cliquer sur les données de certaines colonnes pour afficher des informations détaillées.

Exemple : Dans le widget, **Principales menaces de Control Manager** de l'onglet **Statistiques sur les menaces**, en cliquant sur un lien de la colonne **Détections** une table contenant les informations suivantes s'ouvre :

TABLEAU 6-9. Exemple d'informations détaillées sur un widget

DONNÉES	DESCRIPTION
Point final	Nom d'hôte du point final touché par un virus
Produit	Nom du produit qui a détecté le virus
Virus	Nom du virus
Heure de début	Heure de la première détection du virus
Heure de fin	Heure de la dernière détection du virus
Détections	Nombre de détections de virus

Liste des widgets

La table suivante répertorie les widgets disponibles dans le tableau de bord.

Remarque

Sur les serveurs Control Manager parents, les widgets **Principales menaces de Control Manager** et **Principales menaces détectées par File Reputation** requièrent des transferts programmés des journaux provenant des serveurs Control Manager enfants pour afficher des données précises.

Pour permettre les mises à jour programmées des journaux depuis des serveurs Control Manager : **Produits** > **Sélectionner un serveur enfant dans le répertoire Produits** > **Configurer** > **Programmer les téléchargements de journaux de serveur Control Manager enfant**

TABLEAU 6-10. Liste des widgets

WIDGET	OBJECTIF
Utilisateurs actifs pour File Reputation	Ce widget permet de suivre le nombre d'utilisateurs envoyant des requêtes File Reputation aux serveurs Smart Protection Server.
Utilisateurs actifs pour la réputation de sites Web	Ce widget permet de suivre le nombre d'utilisateurs envoyant des requêtes de réputation de sites Web aux serveurs Smart Protection Server.
Événements de rappel C&C	Utilisez ce widget pour vérifier le nombre de tentatives de rappel. Affichez les données par hôte compromis ou adresse de rappel.
Hôtes compromis uniques au fil du temps	Utilisez ce widget pour afficher les hôtes compromis uniques enregistrés par les produits gérés au cours des 30 derniers jours.
Incidents de prévention contre la perte des données par gravité et par état	Utilisez ce widget pour vérifier le nombre d'incidents déclenchés par des utilisateurs gérés. Filtrez les données par niveau de gravité de l'incident.
Tendances des incidents de prévention contre la perte des données par utilisateur	Utilisez ce widget pour vérifier les tendances d'incidents des utilisateurs gérés. Filtrez les données par niveau de gravité de l'incident.
Correspondances de modèles de prévention contre la perte de données	Ce widget permet de vérifier le type d'incidents de prévention contre la perte de données déclenchées dans votre réseau. Les données peuvent être filtrées par modèle.
Incidents de prévention contre la perte de données par stratégie	Ce widget permet de vérifier le nombre total d'incidents de prévention contre la perte de données. Par défaut, les données sont triées par le nombre d'incidents. Pour trier les données par nom de stratégie, cliquez sur le titre de la colonne **Stratégie**. **Exemple** : Vous souhaitez connaître le nombre total d'incidents de prévention contre la perte de données en fonction des stratégies.

WIDGET	OBJECTIF
Sources principales d'incidents de prévention contre la perte de données	Ce widget permet de vérifier les sources des incidents de prévention contre la perte de données sur votre réseau. Les données peuvent être filtrées par source dans laquelle l'incident s'est déclenché. **Exemple 1 :** Vous souhaitez connaître les incidents principaux de prévention contre la perte de données par expéditeur dans votre réseau. **Exemple 2 :** Vous souhaitez connaître les incidents principaux de prévention contre la perte de données par adresse IP dans votre réseau.
Incidents de prévention contre la perte des données par utilisateur	Utilisez ce widget pour vérifier le nombre d'incidents déclenchés par des utilisateurs gérés. Filtrez les données par niveau de gravité de l'incident.
Incidents de prévention contre la perte de données par canal	Ce widget permet de vérifier le nombre total d'incidents de prévention contre la perte de données sur votre réseau. Les données peuvent être filtrées par canal dans lequel l'incident s'est déclenché. Exemple 1 : Vous souhaitez connaître le nombre total d'incidents de prévention contre la perte de données dans votre réseau. Exemple 2 : Vous souhaitez connaître le nombre total d'incidents de prévention contre la perte de données par e-mail et courrier Internet dans votre réseau.
État d'Endpoint Encryption	Ce widget permet de surveiller l'état des points finaux protégés par les serveurs Endpoint Encryption. **Exemple** : Vous souhaitez savoir quels points finaux sont protégés, lesquels ne le sont pas et lesquels sont en voie de l'être.
Gestion d'Endpoint Encryption	Utilisez ce widget pour accéder à la console d'administration pour Trend Micro Endpoint Encryption.
Rapport de trafic HTTP pour File Reputation	Ce widget permet de suivre le trafic HTTP envoyé au serveur Smart Protection Server.

WIDGET	OBJECTIF
Trafic HTTP pour la réputation de sites Web	Ce widget permet de suivre le trafic HTTP envoyé au serveur Smart Protection Server.
État de la stratégie	Utilisez ce widget pour vérifier l'état du déploiement de vos stratégies.
Lancement rapide	Utilisez ce widget pour accéder aux raccourcis des fonctions.
État en temps réel	Ce widget permet de surveiller en temps réel l'état du serveur Smart Protection Server.
Statistiques des menaces de Control Manager	Ce widget permet de vérifier le nombre total de détections de menaces de sécurité sur votre réseau. Les données peuvent être filtrées par type de menace de sécurité ou en fonction de l'emplacement de la détection de la menace sur votre réseau. **Exemple 1 :** Vous souhaitez connaître le nombre total de détections de virus sur votre réseau. **Exemple 2 :** Vous souhaitez connaître le nombre total de détections de menaces provenant de serveurs de fichiers sur votre réseau.
Top 10 des ordinateurs infectés pour File Reputation	Ce widget permet de suivre les ordinateurs les plus infectés de votre réseau. **Exemple** : Vous souhaitez connaître les ordinateurs les plus infectés de votre réseau.
Top 10 des ordinateurs bloqués pour la réputation de sites Web	Ce widget permet de suivre les ordinateurs comportant le plus grand nombre d'URL bloquées de votre réseau.
Résumé des composants Deep Security	Ce widget permet de suivre les numéros de versions des mises à jour de composants Deep Security actuellement disponibles et le pourcentage d'ordinateurs mis à jour vers ces dernières versions.
Résumé des fonctions Deep Security	Utilisez ce widget pour suivre l'activité récente de tous les modules Deep Security.

WIDGET	OBJECTIF
Résumé d'état Deep Security	Utilisez ce widget pour suivre le nombre d'alertes critiques et d'avertissement et l'état des ordinateurs dans votre réseau.
Vérification de la protection des points finaux	Utilisez ce widget pour vérifier que vos points finaux sont protégés par OfficeScan ou Deep Security.
Connexion Smart Protection Network	Ce widget permet de suivre le nombre de points finaux qui se connectent au serveur Global Smart Scan Server.
Conformité des applications de produits	Ce widget permet de suivre les applications des produits gérés qui ne sont pas à jour. **Exemple :** Vous souhaitez connaître les serveurs OfficeScan 10 qui ne figurent pas dans trois versions de compilation de la dernière version d'OfficeScan 10.
État de la connexion des points finaux	Ce widget permet de suivre les clients OfficeScan hors ligne ou itinérants.
État de la connexion du produit	Ce widget permet de suivre les produits gérés hors ligne, désactivés ou encore ceux présentant une connexion anormale à Control Manager.
État des composants du produit	Ce widget permet de suivre les produits gérés ou les points finaux contenant des composants obsolètes. **Exemple :** Vous souhaitez savoir quels points finaux avec des clients OfficeScan ne possèdent pas la dernière version du fichier de signatures de virus.
Carte des menaces de la réputation des e-mails	Utilisez ce widget comme référence pour les tendances globales au niveau des spams.
Carte des menaces de File Reputation	Utilisez ce widget comme référence pour les tendances globales au niveau des fichiers malveillants.
Principales menaces détectées par File Reputation	Utilisez ce widget comme référence entre les principales menaces de manière globale et les menaces sur votre réseau.

WIDGET	OBJECTIF
État de conformité de Smart Protection Network	Utilisez ce widget comme référence pour les points finaux et les produits gérés qui possèdent des composants obsolètes.
Statistiques des menaces de Smart Protection Network	Utilisez ce widget comme référence pour les détections de menaces de sécurité sur votre réseau, de manière globale, et globalement au sein d'un secteur.
Résultats de la détection des menaces	Ce widget permet de suivre les points finaux ou les produits gérés qui nécessitent une action supplémentaire de la part des administrateurs. **Exemple :** Vous souhaitez savoir quels points finaux ou produits gérés sont touchés par des virus qui n'ont pas pu être nettoyés, supprimés ou mis en quarantaine.
Principales menaces de fichiers de Control Manager	Utilisez ce widget pour suivre la répartition des principaux fichiers malveillants détectés sur les points finaux de votre réseau.
Principales menaces de Control Manager	Ce widget permet de suivre les principaux fichiers malveillants détectés ou les principales URL malveillantes auxquelles votre point final accède sur votre réseau. Exemple : Vous souhaitez connaître les principales URL malveillantes détectées par un segment spécifique de votre réseau.
Détections de violations de stratégies	Ce widget permet de suivre les violations de services Network VirusWall Enforcer.
Principales sources de menaces détectées par la réputation de sites Web	Utilisez ce widget comme référence pour les tendances globales au niveau des URL malveillantes.
Principaux utilisateurs menacés détectés par la réputation de sites Web	Utilisez ce widget comme référence pour les tendances globales au niveau des URL malveillantes.

Configuration des widgets

Configurer un widget revient à modifier les paramètres facilement visibles sur le widget. Le tableau suivant répertorie quelques exemples de paramètres de widgets que les administrateurs peuvent modifier.

TABLEAU 6-11. Configuration des widgets

PARAMÈTRE	DESCRIPTION
Plage	Modifier la plage de temps pour les données qui affichent : • Aujourd'hui • 1 semaine • 2 semaines • 1 mois
Regroupement des données	Modifier le regroupement pour les données : • URL malveillantes • Fichiers malveillants ou • Catégorie du produit • Type de menace
Affichage	Modifier la manière dont les données s'affichent : • Graphique en barres • Graphique en ligne • Graphique circulaire • Tableau

Modification des widgets

La modification d'un widget correspond à la définition de paramètres qui ne sont pas facilement visibles sur le widget. Cliquez sur l'icône de modification pour accéder à ces paramètres. Exemples :

TABLEAU 6-12. Modification des widgets

PARAMÈTRE	DESCRIPTION
Titre	Modifier le nom qui s'affiche pour le widget.
Étendue	Spécifie l'emplacement de la source des données pour le widget. Le widget affiche par défaut les données de tous les produits gérés auxquels son utilisateur a accès. **AVERTISSEMENT!** La source des données a un impact significatif sur ce que le widget affiche. Procédez avec précaution lorsque vous modifiez ce paramètre. Il se peut, par exemple, que quelqu'un spécifie que ce widget affiche des données pour une partie de votre réseau uniquement.
Autres	Certains widgets fournissent des paramètres permettant de modifier la quantité de données affichées (plages d'entrées) ou le type des données affichées (type de menace de sécurité ou type de composant avec le type de produit).

Procédure

1. Accédez à l'écran **Tableau de bord**.
2. Cliquez sur un onglet disposant d'un widget avec une icône de modification.
3. Cliquez sur l'icône **Modification** du widget. L'écran Modification s'affiche.

4. Spécifiez un titre pertinent pour le widget dans le champ **Titre**.
5. Cliquez sur le bouton Parcourir situé en regard du champ **Étendue**.

   Une version du répertoire Produits s'affiche.
6. Spécifiez la source des données pour le widget à partir du répertoire Produits.
7. Cliquez sur **OK**.
8. Définissez des valeurs pour les autres paramètres disponibles pour le widget.

   Remarque

   Pour plus d'informations concernant les « autres » paramètres, consultez l'aide relative à chaque widget.
9. Cliquez sur **Enregistrer**.

   Le widget est actualisé afin d'appliquer les nouveaux paramètres.

Ajout de widgets

Le nombre de widgets que vous pouvez ajouter à un onglet dépend de la disposition de cet onglet. Lorsque l'onglet comporte le nombre maximum de widgets, vous devez supprimer un widget à partir de l'onglet ou créer un nouvel onglet pour le widget.

Procédure

1. Accédez à l'un des onglets du tableau de bord.
2. Cliquez sur **Ajouter un widget**.

   L'écran **Ajouter un widget** apparaît.
3. Cliquez sur l'une des options suivantes pour filtrer les widgets qui s'affichent :

Catégorie	Description
Widgets les plus récents	Affiche uniquement les tout derniers widgets disponibles
Tous les widgets	Affiche tous les widgets disponibles
Conformité	Affiche uniquement les widgets contenant des informations sur la conformité (exemple : conformité des composants, conformité des applications de produits)
Prévention contre la perte de données	Affiche uniquement les widgets de prévention contre la perte de données.
Deep Security Manager	Affiche uniquement les widgets Deep Security Manager
Endpoint Encryption	Affiche uniquement les widgets Endpoint Encryption
Gestion des stratégies	Affiche uniquement les widgets Gestion des stratégies
Smart Protection Network	Affiche uniquement les widgets de Smart Protection Network
Statistiques sur les menaces	Affiche uniquement les widgets contenant des informations statistiques sur les menaces (exemple : principales menaces sur votre réseau, nombre total de menaces sur votre réseau)
Control Manager	Affiche uniquement les widgets de Control Manager
Smart Protection Server	Affiche uniquement les widgets du serveur Smart Protection Server

4. Sélectionnez un ou plusieurs widgets à ajouter à un onglet.

5. Cliquez sur **Ajouter**.

Configuration des paramètres de Smart Protection Network

Activez Trend Micro Smart Feedback pour partager des informations sur les menaces avec Trend Micro Smart Protection Network. Votre réseau est ainsi mieux protégé dans la mesure où Trend Micro est capable d'identifier et de traiter rapidement les nouvelles menaces.

Pour que certains widgets fonctionnent, il est également nécessaire d'activer les paramètres de Smart Protection Network. Cela s'explique par le fait que les widgets reçoivent leurs données directement à partir de Trend Micro Smart Protection Network.

Remarque

La réputation des e-mails, File Reputation et la réputation de sites Web font partie du réseau Smart Protection Network.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres Smart Protection Network**.

   L'écran **Paramètres Smart Protection Network** apparaît.

2. Sélectionnez **Activer les widgets Trend Micro Smart Feedback et Smart Protection Network**.

3. Spécifiez à quelle fréquence Control Manager enverra des informations entièrement anonymes sur les menaces à Smart Protection Network à partir de la liste déroulante **Intervalle de temps**.

4. Spécifiez le secteur d'activité auquel votre société appartient à partir de la liste déroulante **Votre secteur d'activité**.

5. Cliquez sur **Enregistrer**.

Configuration des paramètres de connexion au serveur de gestion Deep Security

Les widgets qui obtiennent des informations à partir de Deep Security doivent d'abord s'y connecter.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Gestion Deep Security**.

   L'écran **Gestion Deep Security** apparaît.

2. Configurez les paramètres de connexion du serveur de gestion Deep Security :

   - **Nom du serveur ou adresse IP** : Nom du serveur ou adresse IP de votre serveur Deep Security
   - **Port** : Numéro de port utilisé pour communiquer avec votre serveur Deep Security
   - **Nom d'utilisateur** : Le nom d'utilisateur requis pour vous connecter à votre serveur Deep Security
   - **Mot de passe** : Mot de passe requis pour vous connecter à votre serveur Deep Security

3. Pour ajouter plusieurs serveurs Deep Security, cliquez sur l'icône +. Vous pouvez ajouter jusqu'à cinq serveurs Deep Security.

4. Cliquez sur **Enregistrer**.

Chapitre 7

Utilisation du suivi des commandes

Utilisez le suivi des commandes pour afficher des enregistrements de toutes les commandes émises vers les produits gérés et les serveurs enfants.

Ce chapitre traite les rubriques suivantes :

Définition du suivi des commandes

Le serveur Control Manager tient à jour un enregistrement de toutes les commandes émises vers les produits gérés et les serveurs enfants. Les commandes sont des instructions transmises aux produits gérés ou au serveur enfant en vue de la réalisation de tâches spécifiques (par exemple, mise à jour de composant). L'écran Suivi des commandes vous permet de surveiller la progression de toutes les commandes.

Par exemple, après l'émission d'une tâche Démarrer le scan immédiat, dont la réalisation peut prendre quelques minutes, vous pouvez lancer d'autres tâches, puis revenir ultérieurement au suivi des commandes pour examiner les résultats.

L'écran **Suivi des commandes** présente les détails suivants sous forme de tableau :

TABLEAU 7-1. Détails de l'écran Suivi des commandes

INFORMATIONS	DESCRIPTION
Date/Heure émise	Date et heure auxquelles le serveur Control Manager a transmis la commande au produit géré ou au serveur enfant
Commande	Type de la commande émise
Réussite	Nombre de produits gérés ou de serveurs enfants qui ont mené à bien la commande
Échec	Nombre de produits gérés ou de serveurs enfants qui n'ont pas pu exécuter la commande
En cours	Nombre de produits gérés ou de serveurs enfants qui sont en train d'exécuter la commande.
Tout	Nombre total de produits gérés ou de serveurs enfants auxquels Control Manager a transmis la commande

Remarque

Cliquez sur les liens disponibles dans les colonnes **Réussite**, **Échec**, **En cours** ou **Tous** pour afficher l'écran **Détails sur la commande**.

Définition de l'écran Détails sur la commande

L'écran **Détails sur la commande** communique des informations détaillées sur le résultat d'une commande. Control Manager enregistre et regroupe tous les détails d'une commande en fonction des éléments suivants :

- Produits gérés ou services impliqués
- Détails concernant des produits ou des services individuels

L'écran **Détails sur la commande** se réactualise toutes les 30 secondes.

Produits gérés ou services impliqués

TABLEAU 7-2. Détails généraux sur la commande

INFORMATIONS	DESCRIPTION
Démarré	Indique la date et l'heure auxquelles le serveur Control Manager a transmis la commande au produit géré ou au serveur enfant, ainsi que des informations complémentaires sur la commande. Par exemple, lorsque vous exécutez un téléchargement manuel, le champ Émise contiendra le paramètre concernant le composant que Control Manager a réussi ou non à télécharger. L'écran Détails sur la commande se rapportant à un téléchargement manuel peut comporter un paramètre appelé « moteur ». Ce paramètre indique que Control Manager a téléchargé le composant de moteur de scan. Si, pour une commande, aucun détail supplémentaire n'est fourni, le paramètre est défini sur « N/A ».
Signalé en dernier	Indique la date et l'heure auxquelles le serveur Control Manager a reçu une réponse de la part d'un produit géré ou d'un serveur enfant.

Informations	Description
Utilisateur	Indique le compte utilisateur qui a envoyé la tâche au produit géré ou au serveur enfant.
Réussite	Indique le nombre de produits gérés ou de serveurs enfants qui ont exécuté la commande.
Échec	Indique le nombre de produits gérés ou de serveurs enfants qui n'ont pas pu exécuter la commande.
En cours	Indique le nombre de produits gérés ou de serveurs enfants qui exécutent actuellement la commande.

Détails concernant des produits ou des services individuels

Tableau 7-3. Détails sur la commande concernant des produits ou des services individuels

Informations	Description
Signalé en dernier	Indique la date et l'heure auxquelles le produit géré envoie une réponse au serveur Control Manager.
Serveur/entité	Indique le nom d'hôte du serveur enfant ou du serveur de produit géré.

<table>
<tr><th>INFORMATIONS</th><th>DESCRIPTION</th></tr>
<tr><td>État</td><td>Indique l'état de la commande émise.
<table>
<tr><td>Réussite</td><td>En cours</td><td>Échec</td></tr>
<tr><td>Ignorer</td><td>Envoyer</td><td>Expiration</td></tr>
<tr><td>Non pris en charge</td><td>Suivi</td><td>Annulé</td></tr>
<tr><td>Réussite</td><td>Accepté</td><td>Non disponible</td></tr>
<tr><td colspan="2"></td><td>Échec</td></tr>
</table></td></tr>
<tr><td>Description</td><td>Explique à quoi correspond l'état.</td></tr>
</table>

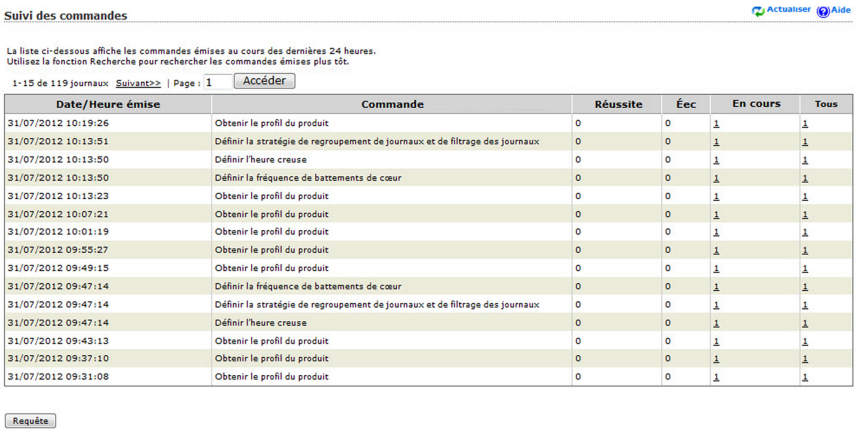
Recherche et affichage des commandes

Utilisez l'écran **Requête | Suivi des commandes** pour surveiller et visualiser les commandes précédemment émises.

Procédure

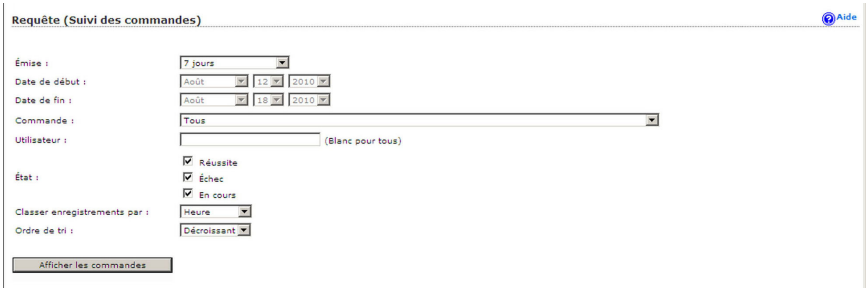
1. Accédez à **Administration** > **Suivi des commandes**.

   L'écran **Suivi des commandes** apparaît.



2. Dans la zone de travail, cliquez sur **Requête**.

   L'écran **Requête (Suivi des commandes)** apparaît.



3. Dans l'écran **Requête (Suivi des commandes)**, spécifiez les valeurs souhaitées pour les paramètres suivants :

   - **Émis** : précisez l'intervalle de temps de la requête.

     Choisissez parmi les plages prédéfinies ou définissez les plages de votre choix.

   - **Date de début**/**Date de fin**: personnalisez les plages en précisant le jour, le mois et l'année.

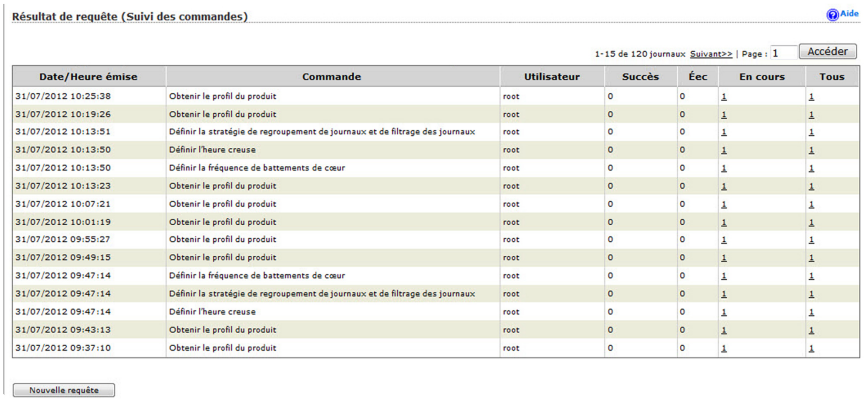
   - **Commande** : sélectionnez la commande à surveiller.

- **Utilisateur** : indiquez le nom du compte utilisateur à interroger. laissez ce champ vide pour rechercher les commandes indépendamment du nom de l'utilisateur
- **État** : sélectionnez l'état de la commande.
- **Classer par** : précisez la manière dont vous voulez afficher les résultats dans l'écran **Résultat de la requête**.

  Vous pouvez trier les résultats de la requête en fonction de l'heure, de la commande ou de l'utilisateur.
- **Ordre de tri** : précisez si les **résultats de la requête** s'affichent par ordre croissant ou décroissant.

4. Cliquez sur **Afficher les commandes**.

L'écran **Résultat de requête (Suivi des commandes)** affiche le nombre de produits concernés par la commande, ainsi que les résultats obtenus.


Résultat de requête (Suivi des commandes)

Aide

1-15 de 120 journaux Suivant>> | Page : 1 Accéder

Date/Heure émise	Commande	Utilisateur	Succès	Éec	En cours	Tous
31/07/2012 10:25:38	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 10:19:26	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 10:13:51	Définir la stratégie de regroupement de journaux et de filtrage des journaux	root	0	0	1	1
31/07/2012 10:13:50	Définir l'heure creuse	root	0	0	1	1
31/07/2012 10:13:50	Définir la fréquence de battements de cœur	root	0	0	1	1
31/07/2012 10:13:23	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 10:07:21	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 10:01:19	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 09:55:27	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 09:49:15	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 09:47:14	Définir la fréquence de battements de cœur	root	0	0	1	1
31/07/2012 09:47:14	Définir la stratégie de regroupement de journaux et de filtrage des journaux	root	0	0	1	1
31/07/2012 09:47:14	Définir l'heure creuse	root	0	0	1	1
31/07/2012 09:43:13	Obtenir le profil du produit	root	0	0	1	1
31/07/2012 09:37:10	Obtenir le profil du produit	root	0	0	1	1

Nouvelle requête

5. Cliquez sur le lien disponible dans la colonne **Réussite**, **Échec**, **En cours** ou **Tous** pour afficher les détails spécifiés de la commande.

Chapitre 8

Utilisation des notifications

Utilisez le Centre d'événements pour configurer Control Manager pour envoyer des notifications relatives à des événements qui se produisent sur le réseau Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition du Centre d'événements

Les événements sont des actions détectées par un produit géré et transmises au serveur Control Manager. Le Centre d'événements vous permet de définir diverses notifications selon les différents événements qui ont lieu.

Le Centre d'événements classe les événements selon les types suivants :

TABLEAU 8-1. Événements du Centre d'événements

TYPES D'ÉVÉNEMENT	DESCRIPTION
Alerte	Vous met en garde contre les virus/programmes espions/graywares détectés par les produits gérés antivirus. Pour plus d'informations, consultez la section *Événements d'alerte à la page 8-3*.
Outbreak Prevention Services	Fournit des informations sur l'application des stratégies et des informations de mise à jour sur Outbreak Prevention Services (OPS). Les notifications envoyées par Outbreak Prevention Services couvrent les événements suivants : • Stratégie de prévention des épidémies active reçue • Mode de prévention des épidémies démarré • Mode de prévention des épidémies arrêté • Échec de la mise à jour de la stratégie de prévention des épidémies • Mise à jour de la stratégie de prévention des épidémies réussie
Statistiques	Fournit des notifications d'événement « Statistiques de violation » pour les produits Network VirusWall.
Mise à jour	Fournit les résultats de la mise à jour des composants antivirus ou de sécurité de contenu (réussite ou échec). Pour plus d'informations, consultez la section *Événements d'alerte de mise à jour à la page 8-5*.

Types d'événement	Description
Inhabituel	Fournit des informations sur l'activation et la désactivation d'options de produits ou de services. Pour plus d'informations, consultez la section *Événements d'alerte inhabituels à la page 8-5*.
Violations de sécurité	Met en garde contre les violations de contenu de messages électroniques et les violations de sécurité Web de clients. Pour plus d'informations, consultez la section *Événements de violation de sécurité à la page 8-6*.
Prévention contre la perte de données	Fournit des informations sur la prévention contre la perte de données et les correspondances de modèles. Pour plus d'informations, consultez la section *Événements de prévention contre la perte de données à la page 8-6*.

Événements d'alerte

Tableau 8-2. Événements d'alerte

Alerte	Description
Alerte d'épidémie virale	Applicable à tous les produits antivirus gérés
Alerte de virus spécial	Applicable à tous les produits antivirus gérés
Alerte de programme espion/grayware spécial	Applicable aux produits gérés anti-spywares/graywares

ALERTE	DESCRIPTION
Virus détecté	Les options suivantes sont disponibles : • Échec de la première action et seconde action indisponible : applicable aux produits antivirus gérés • Échec des deux premières actions : applicable aux produits antivirus gérés • Réussite de la première action : applicable aux produits antivirus gérés • Réussite de la deuxième action : applicable aux produits antivirus gérés
Alerte de virus réseau	Applicable à tous les produits de scan par paquets (par exemple, Network VirusWall Enforcer 1500)
Attaque potentielle de faille de sécurité détectée	Applicable à tous les produits de scan par paquets (par exemple, Network VirusWall 1500)
Programme espion/grayware détecté	Les options suivantes sont disponibles : • Action réussie : applicable aux produits gérés anti-spywares/graywares • Action supplémentaire requise : applicable aux produits gérés anti-spywares/graywares
Alerte de rappel C&C	Applicable à tous les produits gérés de sécurité antivirus et de découverte de menaces
Alerte d'épidémie de rappel C&C	Applicable à tous les produits gérés de sécurité antivirus et de découverte de menaces

Événements d'alerte de mise à jour

Tableau 8-3. Événements d'alerte de mise à jour

Alerte	Description
Échec de la mise à jour du moteur de scan	Applicable à tous les produits antivirus gérés
Mise à jour du moteur de scan réussie	Applicable à tous les produits antivirus gérés
Échec de la mise à jour des fichiers de signatures/modèles Damage Cleanup	Applicable à tous les produits antivirus gérés
Mise à jour des fichiers de signatures/ modèles Damage Cleanup réussie	Applicable à tous les produits antivirus gérés
Échec de la mise à jour de la règle anti-spam	Applicable à tous les produits gérés chargés de la sécurité du contenu
Mise à jour de la règle anti-spam réussie	Applicable à tous les produits gérés chargés de la sécurité du contenu

Événements d'alerte inhabituels

Tableau 8-4. Événements d'alerte inhabituels

Alerte	Description
Scan en temps réel activé	Applicable à tous les produits antivirus gérés
Scan en temps réel désactivé	Applicable à tous les produits antivirus gérés
Service produit démarré	Applicable à tous les produits gérés de sécurité antivirale et de contenu
Service produit arrêté	Applicable à tous les produits gérés de sécurité antivirale et de contenu

Événements de violation de sécurité

TABLEAU 8-5. Événements de violation de sécurité

ALERTE	DESCRIPTION
Violation de sécurité du contenu	Applicable aux produits gérés chargés de la sécurité du contenu. Par exemple : InterScan Messaging Security Suite.
Violation de sécurité Web	Applicable aux produits gérés chargés de la sécurité Web. Par exemple : InterScan Web Security Suite.

Événements de prévention contre la perte de données

TABLEAU 8-6. Événements de prévention contre la perte de données

ALERTE	DESCRIPTION
Augmentation significative des incidents	Applicable à tous les produits antivirus gérés
Augmentation significative de correspondances de modèles	Applicable à tous les produits antivirus gérés
Augmentation significative des incidents par utilisateur	Applicable à tous les produits antivirus gérés
Augmentation significative des incidents par expéditeur	Applicable à tous les produits antivirus gérés
Augmentation significative des incidents par canal	Applicable à tous les produits antivirus gérés
Résumé d'incidents programmé	Applicable à tous les produits antivirus gérés
Informations détaillées des incidents mises à jour	Applicable à tous les produits antivirus gérés

Personnalisation des messages de notification

Utilisez des variables pour personnaliser les notifications d'événements. Insérez ces variables lors de la configuration des notifications de façon à fournir plus de détails aux destinataires des notifications.

Control Manager prend en charge les produits suivants :

TABLEAU 8-7. Variables courantes utilisées dans les messages de notification

VARIABLE	DESCRIPTION
Variables courantes utilisées dans toutes les notifications d'événements	
`%cmserver%`	Nom d'hôte de serveur Control Manager
`%computer%`	Nom réseau de l'ordinateur où a été détecté un événement
`%entity%`	Chemin d'accès au répertoire Produits du produit géré où a eu lieu un événement
`%event%`	Événement qui a déclenché la notification
`%pname%`	Nom du produit géré
`%pver%`	Version du produit géré
`%time%`	Heure (hh:mm) à laquelle un événement s'est produit
`%act%`	Action entreprise par le produit géré. Exemple : fichier nettoyé, fichier supprimé, fichier mis en quarantaine
`%actresult%`	Résultat de l'action entreprise par le produit géré. Exemple : réussite, action supplémentaire nécessaire

TABLEAU 8-8. Variables utilisées dans les messages de notification de virus

VARIABLE	DESCRIPTION
Variables de virus : utilisées par les notifications d'événements d'alertes ou Outbreak Prevention Services	
`%device_ip%`	Adresse IP d'un point final infecté.
`%engver%`	• Version du moteur de scan. • Utilisée dans les notifications d'événements de type alerte, ainsi que les notifications « Stratégie de prévention des épidémies active reçue » et « Mode de prévention des épidémies démarré ». Pour les notifications d'événements de type alerte, cette variable fait référence à la version du moteur de scan actuellement installée sur le serveur de produit géré. • Pour les notifications « Stratégie de prévention des épidémies active reçue » et « Mode de prévention des épidémies démarré », cette variable fait référence à la stratégie de prévention des épidémies requise.

VARIABLE	DESCRIPTION
`%ptnver%`	• Version du fichier de signatures. • Utilisée dans les notifications d'événements de type alerte, ainsi que les notifications « Stratégie de prévention des épidémies active reçue » et « Mode de prévention des épidémies démarré ». Pour les notifications d'événements de type alerte, cette variable fait référence à la version du fichier de signatures actuellement installée sur le serveur de produit géré. • Pour les notifications de la « Stratégie de prévention des épidémies active reçue » et du « Mode de prévention des épidémies démarré », cette variable fait référence à la stratégie de prévention des épidémies requise.
`%threat_info%`	• Informations relatives aux menaces de virus/programmes malveillants fournies par les stratégies de prévention des épidémies. • Utilisée dans les notifications « Stratégie de prévention des épidémies active reçue » et « Mode de prévention des épidémies démarré ».
`%vcnt%`	• Nombre de virus. • Utilisé dans les alertes d'épidémies virales.

VARIABLE	DESCRIPTION
`%vdest%`	• Destination du virus/programme malveillant. • Par exemple, le destinataire visé prend la valeur de %vdest% si un produit antivirus géré a détecté un virus/programme malveillant dans un message électronique. • Utilisée dans la catégorie des événements de type alerte.
`%vfile%`	Nom du fichier infecté. Utilisée dans la catégorie des événements de type alerte.
`%vfilepath%`	Répertoire du fichier infecté. Utilisée dans la catégorie des événements de type alerte.
`%vname%`	Nom du virus ou du programme malveillant. Utilisée dans la catégorie des événements de type alerte.
`%vsrc%`	• Origine du virus/programme malveillant ou source de l'infection. • Par exemple, l'expéditeur du message prend la valeur de %vsrc% si un produit antivirus géré a détecté un virus/programme malveillant dans un message électronique. • Utilisée dans les événements de type alerte ainsi que par les notifications d'alerte de virus réseau.

TABLEAU 8-9. Variables spéciales utilisées dans les messages de notification

VARIABLE	DESCRIPTION
Variables spéciales : Utilisées par les événements liés à la réalisation de tâches Network VirusWall Enforcer	

VARIABLE	DESCRIPTION
`%action%`	Action entreprise par Network VirusWall Enforcer (ignorer, supprimer ou mettre en quarantaine) à la suite d'un virus réseau.
`%description%`	Description d'erreur utilisée par les événements d'attaque potentielle de faille de sécurité détectée.

TABLEAU 8-10. Variables utilisées dans les messages de notification DLP

VARIABLE	DESCRIPTION
Variables DLP : Utilisées par les événements de résumé d'incidents programmé et d'informations détaillées des incidents mises à jour	
%DLP_INCIDENT_TOTAL_NUM%	Le nombre total d'incidents déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_HIGH_NUM%	Le nombre total d'incidents de gravité élevée déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_MED_NUM%	Le nombre total d'incidents de gravité moyenne déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_LOW_NUM%	Le nombre total d'incidents de gravité basse déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_INFO_NUM%	Le nombre total d'incidents informationnels déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_UNDEFINED_NUM%	Le nombre total d'incidents de gravité non définie déclenchés par des utilisateurs gérés directement
%DLP_INCIDENT_ALLTOTAL_NUM%	Le nombre total d'incidents déclenchés par tous les utilisateurs gérés

VARIABLE	DESCRIPTION
%DLP_INCIDENT_ALLHIGH_NUM%	Le nombre total d'incidents de gravité élevée déclenchés par des utilisateurs gérés
%DLP_INCIDENT_ALLMED_NUM%	Le nombre total d'incidents de gravité moyenne déclenchés par tous les utilisateurs gérés
%DLP_INCIDENT_ALLLOW_NUM%	Le nombre total d'incidents de gravité basse déclenchés par tous les utilisateurs gérés
%DLP_INCIDENT_ALLINFO_NUM%	Le nombre total d'incidents informationnels déclenchés par tous les utilisateurs gérés
%DLP_INCIDENT_ALLUNDEFINED_NUM%	Le nombre total d'incidents de gravité non définie déclenchés par tous les utilisateurs gérés
%DLP_START_TIME%	La date et l'heure de début de période du rapport
%DLP_END_TIME%	La date et l'heure de fin de période du rapport
%weblink%	Le lien pour voir les détails des informations de l'incident répertoriés dans le message de notification
%INCIDENTID%	Numéro d'identifiant d'incident
%SEVERITY%	Niveau de gravité de l'incident
%POLICY%	Nom de stratégie de Control Manager **Remarque** Pour les incidents déclenchant des stratégies DLP créées dans les produits gérés, ceci apparaît sous la forme **N/A**.
%ACCOUNT%	Nom d'utilisateur

VARIABLE	DESCRIPTION
%OLD_STATUS%	État de l'incident avant modification
%NEW_STATUS%	État de l'incident après modification
%LATEST_COMMENT%	Les derniers commentaires sur l'incident

TABLEAU 8-11. Variables de message de notification de rappel C&C

VARIABLE	DESCRIPTION
%CALLBACK_ADDR%	L'URL, l'adresse IP ou électronique à laquelle l'hôte compromis tente un rappel
%COMPR_HOST%	Adresse électronique ou hôte affectés
%CnC_LIST_SRC%	Nom de la liste contenant l'adresse de rappel
%CALLBACK_NUM%	Nombre de communications entre les adresses de rappel et les hôtes compromis
%COMPR_HOST_NUM%	Nombre d'hôtes compromis impliqués dans l'épidémie
%CALLBACK_ADDR_NUM%	Nombre d'adresses de rappel impliquées dans l'épidémie

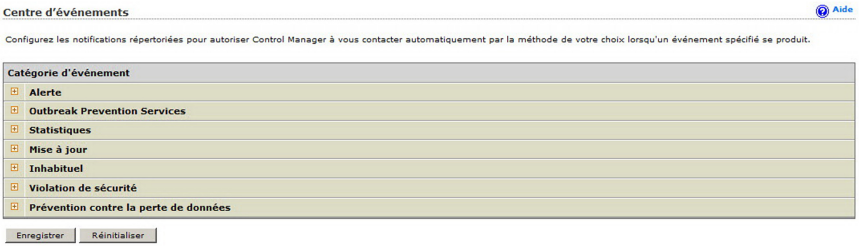
Activation ou désactivation des notifications

Activez ou désactivez les notifications à partir de l'écran **Centre d'événements**.

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.



2. Développez la catégorie d'événement contenant la notification d'événement à activer ou à désactiver.

3. Effectuez l'une des actions suivantes :

   - Activez ou désactivez les cases à cocher d'événements spécifiques.
   - Activez ou désactivez la case à cocher **Événement** pour sélectionner toutes les notifications d'une section entière.

4. Cliquez sur **Enregistrer**.

Description des méthodes de notification

Control Manager peut envoyer des notifications à des personnes ou à des groupes de destinataires pour les informer des événements qui se produisent sur le réseau Control Manager. Configurez le Centre d'événements de façon à envoyer les notifications par le biais le mieux adapté, à savoir :

TABLEAU 8-12. Méthodes de livraison de notifications

MÉTHODE D'ENVOI	DESCRIPTION
Message électronique	Les messages sont envoyés vers une boîte aux lettres appartenant au système de messagerie de l'entreprise ou vers un compte SMTP (par exemple Yahoo!™ ou Hotmail™).

MÉTHODE D'ENVOI	DESCRIPTION
Journal des événements Windows	Le journal de l'Observateur d'événements de Windows contient les événements consignés par Control Manager.
Déroutement SNMP	Un déroutement SNMP (Simple Network Management Protocol) permet d'envoyer des notifications aux administrateurs réseau utilisant des consoles Web compatibles avec ce protocole. Control Manager stocke les notifications dans des bases d'informations de gestion (Management Information Bases ou MIB). Utilisez le **navigateur MIB** pour afficher une notification par déroutement SNMP.
Pageur	Dispositif électronique qui reçoit les messages émis par un signal radio spécial.
Application de lancement	Application interne ou standard utilisée par votre entreprise pour envoyer une notification. Votre entreprise peut, par exemple, utiliser un fichier batch pour appeler la commande « net send ». Utilisez le champ **Paramètres** pour définir les commandes émises par l'application de lancement.
MSN Messenger	Service en ligne assuré par Microsoft qui permet d'établir une communication en temps réel entre deux utilisateurs. Control Manager envoie les notifications vers un compte MSN Messenger en ligne. Un compte MSN Messenger hors ligne ne peut pas recevoir de notifications de la part de Control Manager.

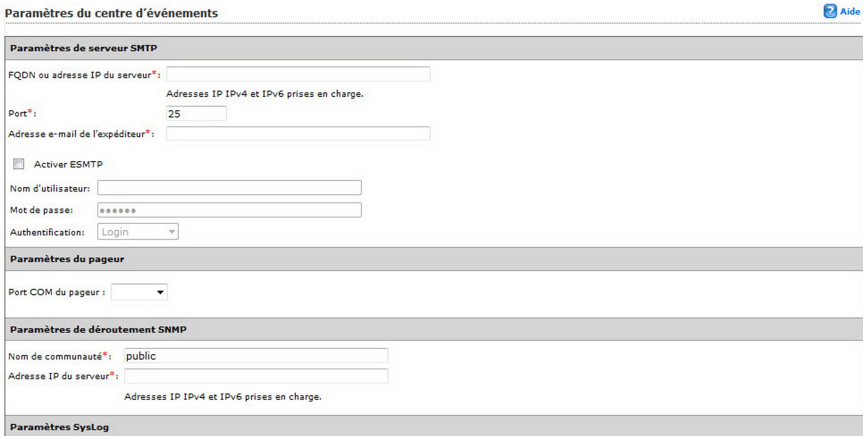
MÉTHODE D'ENVOI	DESCRIPTION
Syslog	Standard de transfert de messages de journaux dans un réseau IP. Control Manager peut diriger les journaux syslogs vers d'autres produits pris en charge. Par exemple, Cisco Security Monitoring, Analysis and Response System (MARS)

Configuration des paramètres des méthodes de notification

Procédure

- Accédez à **Administration** > **Centre d'événements** > **Paramètres d'événements généraux**.

  L'écran **Paramètres du centre d'événements** apparaît.



  Consultez les sections suivantes pour obtenir des informations complémentaires sur la manière de configurer les différentes méthodes de notification.

Configuration des notifications par e-mail

Procédure

1. Dans Paramètres du serveur SMTP, saisissez le nom de domaine complet (FQDN) (par exemple, proxy.entreprise.com) ou l'adresse IP du serveur SMTP dans le champ approprié.
2. Spécifiez le numéro de port dans le champ **Port**.
3. Saisissez l'adresse e-mail de Control Manager expéditeur dans le champ approprié. Control Manager se sert de cette adresse comme adresse d'expédition (obligatoire pour certains serveurs SMTP).
4. Pour utiliser ESMTP, sélectionnez **Activer ESMPT**.
5. Saisissez le nom d'utilisateur et le mot de passe dans les champs appropriés pour l'authentification ESMTP.
6. Sélectionnez la méthode d'authentification dans la liste **Authentification** :
7. Cliquez sur **Enregistrer**.

Configuration des notifications par pageur

Procédure

1. Dans Port COM, sélectionnez le **Port COM de pageur** approprié dans la liste.
2. Cliquez sur **Enregistrer**.

Configuration des notifications SNMP

Procédure

1. Dans Paramètres de déroulement SNMP, spécifiez le **Nom de communauté**.
2. Précisez l'**adresse IP du serveur** du déroutement SNMP.

3. Cliquez sur **Enregistrer**.

Configuration des notifications Syslog

Procédure

1. Dans Paramètres Syslog, saisissez l'**adresse IP de serveur** et le **Port de serveur** du serveur syslog.
2. Sélectionnez l'**Équipement** pour syslogs dans la liste.
3. Cliquez sur **Enregistrer**.

Lancement d'une application spécifiée

Procédure

1. Dans Paramètres du lancement de l'application, sélectionnez **Utiliser un utilisateur spécifique pour lancer l'application**.
2. Saisissez le nom d'utilisateur et le mot de passe de l'utilisateur activant l'application spécifiée.
3. Cliquez sur **Enregistrer**.

Configuration des notifications MSN Messenger

Procédure

1. Dans Paramètres de notification par MSN Messenger, précisez l'**adresse électronique MSN Messenger**. Il s'agit du nom d'utilisateur utilisé dans MSN Messenger.
2. Saisissez le mot de passe de l'adresse électronique.

3. Si vous passez par un serveur proxy pour vous connecter à Internet, sélectionnez **Connexion avec un serveur proxy** pour vous connecter au serveur MSN.

   a. Précisez le **nom d'hôte** et le **port** du serveur proxy.

   b. Sélectionnez le protocole du serveur proxy : **SOCKS 4** ou **SOCKS 5**.

   c. Saisissez l'**identifiant** et le **mot de passe** utilisés pour l'authentification proxy.

4. Cliquez sur **Enregistrer**.

Configuration des destinataires de la notification et test de la diffusion des notifications

Utilisez l'écran **Modifier les destinataires** pour configurer les destinataires de la notification pour chaque événement.

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événement contenant la notification d'événement à configurer.

3. Cliquez sur le lien **Destinataires** de l'événement à configurer.

   L'écran **Modifier les destinataires** apparaît.

4. Sous Destinataires, ajoutez ou supprimez des utilisateurs dans la liste Utilisateurs et groupes sélectionnés en tant que destinataires de notifications :

   - Pour ajouter des destinataires à la liste :

   a. Cliquez sur l'utilisateur ou le groupe dans la liste Utilisateurs et groupes disponibles. Pour sélectionner plusieurs destinataires, maintenez la touche CTRL enfoncée.

   b. Cliquez sur (>) pour ajouter l'entrée dans la liste **Utilisateurs et groupes sélectionnés**.

   - Pour supprimer un destinataire de la liste :

   a. Cliquez sur l'utilisateur ou le groupe dans la liste Utilisateurs et groupes sélectionnés. Pour sélectionner plusieurs destinataires, maintenez la touche CTRL enfoncée.

   b. Cliquez sur (<) pour supprimer l'entrée de la liste Utilisateurs et groupes sélectionnés.

5. Sélectionnez une méthode de notification : Configurez la méthode de notification par le biais de l'écran Paramètres du centre d'événements. Consultez la section *Configuration des paramètres des méthodes de notification à la page 8-16*.

6. Étendez la méthode de notification et fournissez un **message de notification** dans les champs de message correspondants.

7. Cliquez sur **Enregistrer**.

Remarque

Vous pouvez également cliquer sur **Test** pour déterminer si votre système est en mesure de diffuser les notifications. Control Manager sauvegardera les paramètres après le test. Cependant, la fonction test n'est pas disponible pour certains événements.

Configuration des paramètres d'alerte

Les paramètres d'alerte permettent de spécifier à quel moment une notification est envoyée à un administrateur ou à d'autres destinataires.

Le tableau suivant répertorie les notifications prenant en charge la modification des activations de notification.

TABLEAU 8-13. Paramètres d'alerte

ALERTE	DESCRIPTION
Épidémie virale	Fournit une vue globale des épidémies virales/malveillantes.
Virus spéciaux	Propose un avertissement préalable sur une épidémie potentielle de virus/ programmes malveillants.
Programmes espions/graywares spéciaux	Propose un avertissement préalable sur une épidémie potentielle de programmes espions/graywares malveillants.
Virus réseau	Propose une perspective à l'échelle du système sur une épidémie potentielle de virus réseau

ALERTE	DESCRIPTION
Attaque potentielle de faille de sécurité détectée	Propose une perspective à l'échelle du système pour une attaque potentielle causée par des vulnérabilités du système
Rappel C&C et épidémie de rappel	Propose des perspectives à l'échelle du système d'alertes et d'épidémies de rappel C&C potentielles

Configuration des paramètres d'alerte d'épidémie virale

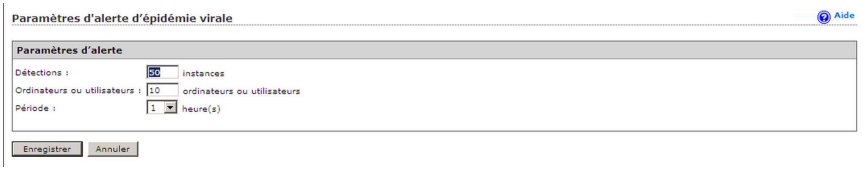
Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événement**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte d'épidémie virale**.

   L'écran **Paramètres d'alerte d'épidémie virale** apparaît.



3. Sous Paramètres d'alerte, saisissez les données suivantes :

   - **Détections** : nombre de virus qui déclenche une alerte d'épidémie
   - **Ordinateurs ou utilisateurs** : nombre d'ordinateurs ou d'utilisateurs infectés
   - **Période** : période prise en compte pour le paramètre du nombre de virus

4. Cliquez sur **Enregistrer**.

Configuration des paramètres d'alerte virale spéciale

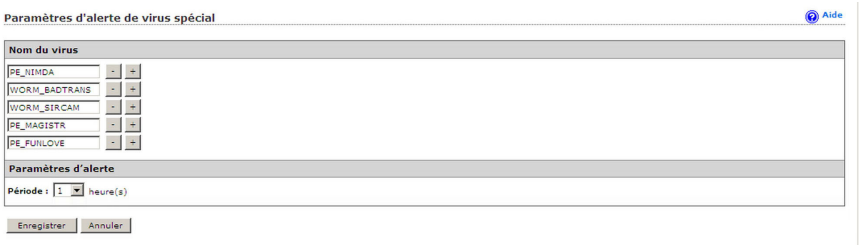
Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événement**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte de virus spécial**.

   L'écran **Paramètres d'alerte de virus spécial** apparaît.



3. Saisissez le nom des virus que vous souhaitez surveiller. Vous pouvez sélectionner jusqu'à 10 virus.

4. Sous Paramètres d'alerte, indiquez la **période** (en heures).

5. Cliquez sur **Enregistrer**.

Configuration des paramètres d'alerte spéciale de programme espion/grayware

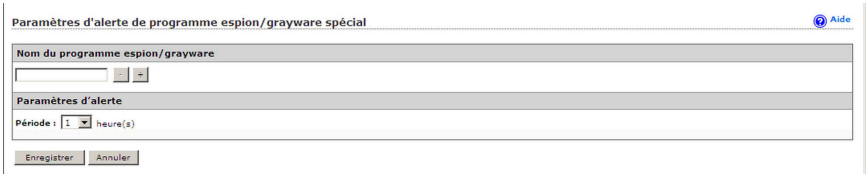
Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événement**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte de programme espion/grayware spécial**.

   L'écran **Paramètres d'alerte de programme espion/Grayware spécial** apparaît.



3. Saisissez le nom des programmes espions/graywares que vous souhaitez surveiller. Vous pouvez en répertorier jusqu'à 10.

4. Sous Paramètres d'alerte, indiquez la **période** (en heures).

5. Cliquez sur **Enregistrer**.

Configuration des paramètres d'alerte virale réseau

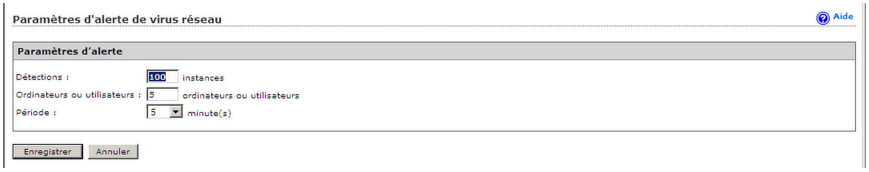
Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événement**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte de virus réseau**.

   L'écran **Paramètres d'alerte de virus réseau** apparaît.



3. Sous Paramètres d'alerte, saisissez les données suivantes :

- **Détections** : nombre de virus à partir duquel se déclenche une alerte d'épidémie
- **Ordinateurs ou utilisateurs** : nombre d'ordinateurs ou d'utilisateurs infectés
- **Période** : période prise en compte pour le paramètre du nombre de virus

4. Cliquez sur **Enregistrer**.

Configuration des paramètres d'alerte d'attaque potentielle de faille de sécurité

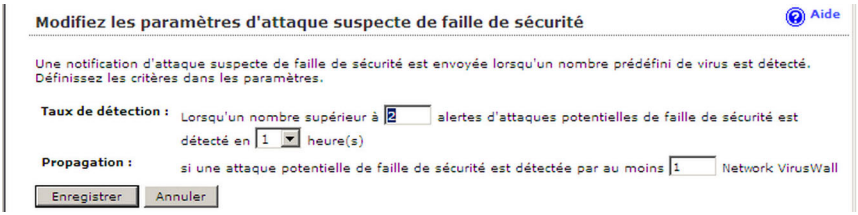
Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Attaque potentielle de faille de sécurité détectée**.

   L'écran **Modifier les paramètres d'attaque potentielle de faille de sécurité** apparaît.



3. Définissez des valeurs pour les paramètres suivants :

   - **Taux de détection :** nombre d'alertes déclenchées au cours du temps
   - **Propagation :** nombre de dispositifs Network VirusWall Enforcer qui détectent l'attaque

4. Cliquez sur **Enregistrer**.

Configuration des paramètres des alertes de rappel C&C

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte de rappel C&C**.

   L'écran **Paramètres d'alerte de rappel C&C** s'affiche.

3. Sélectionnez le type de source de liste C&C à inclure dans le message de notification.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres des alertes d'épidémie de rappel C&C

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Étendez la catégorie d'événements **Alerte** et cliquez sur le lien **Paramètres** pour **Alerte d'épidémie de rappel C&C**.

   L'écran **Paramètres d'alerte d'épidémie de rappel C&C** s'affiche.

3. Sélectionnez le type de source de liste C&C à inclure dans le message de notification.

4. Indiquez les informations suivantes :
   - **Tentatives de rappel** : Nombre de tentatives de rappel à partir duquel une alerte d'épidémie se déclenche
   - **Hôtes compromis** : Le nombre d'hôtes ou adresses électroniques affectés
   - **Période** : Période prise en compte pour le paramètre du nombre de rappels
5. Cliquez sur **Enregistrer**.

Configuration des paramètres de prévention contre la perte de données

Utilisez les écrans de configuration de la prévention contre la perte de données pour spécifier l'heure et le type d'informations à envoyer aux administrateurs ou autres destinataires.

Configuration des paramètres d'augmentation d'incident significative

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.
2. Développez la catégorie d'événement **Prévention contre la perte de données**, puis cliquez sur le lien **Paramètres** pour une des notifications d'augmentation significative des incidents.

   L'écran de configuration correspondant à la notification DLP sélectionnée s'affiche.
3. Spécifiez le nombre d'instances requises pour déclencher la notification dans les champs suivants :

- **Horaire**
- **Quotidien**

4. Cliquez sur **Enregistrer**.

Configuration des paramètres du résumé d'incidents programmé

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Développez la catégorie d'événement **Prévention contre la perte de données**, puis cliquez sur le lien **Paramètres** pour le résumé d'incidents programmé.

   L'écran **Paramètres de Paramètres du résumé d'incidents programmé** s'affiche.

3. Sous **Fréquence**, spécifiez la fréquence d'envoi de notifications :

   - **Quotidien**
   - **Hebdomadaire**

   Remarque

   Control Manager commence à générer des notifications à 3 h à la date spécifiée et met à jour l'état dans le champ **Dernière notification envoyée**.

4. Pour ajouter un fichier joint avec les détails de l'incident à la notification, sélectionnez **Joindre les détails de l'incident au format CSV** sous **Pièces jointes**.

Remarque

Rappelez aux réviseurs d'incidents de manipuler les contenus de la pièce jointe avec prudence, car la copie ou le transfert du contenu correspondant peut déclencher des incidents DLP supplémentaires. Les administrateurs peuvent également configurer des exceptions dans les règles DLP pour les actions prises sur le contenu correspondant.

5. Cliquez sur **Enregistrer**.

Configuration des paramètres des informations détaillées des incidents mises à jour

Procédure

1. Accédez à **Administration** > **Centre d'événements** > **Notifications d'événements**.

   L'écran **Centre d'événements** apparaît.

2. Développez la catégorie d'événement **Prévention contre la perte de données**, puis cliquez sur le lien **Paramètres** pour les Informations détaillées des incidents mises à jour.

   L'écran **Paramètres des informations détaillées des incidents mises à jour** s'affiche.

3. Spécifiez les informations mises à jour à recevoir :

   - **Fermé**

     Sélectionnez ceci pour recevoir des notifications quand un incident a été clos.

   - **Toute modification**

     Sélectionnez ceci pour recevoir des notifications sur les mises à jour, y compris les changements d'état et les modifications de commentaires.

4. Pour recevoir des notifications sur des niveaux de gravité particuliers, spécifiez les options de filtre :

- **Élevé**
- **Moyen**
- **Faible**
- **D'information**
- **Indéfini**

5. Cliquez sur **Enregistrer**.

Chapitre 9

Utilisation des journaux

Interrogez les journaux de tous les produits gérés enregistrés dans Control Manager à partir de l'écran de requête ad hoc.

Ce chapitre traite les rubriques suivantes :

Utilisation des journaux

Bien que Control Manager reçoive des données de divers types de journaux, il permet désormais aux utilisateurs d'effectuer des recherches de données de journal directement dans la base de données Control Manager. Les utilisateurs peuvent ainsi spécifier des critères de filtrage pour n'obtenir que les informations qui les intéressent.

Control Manager permet également désormais le regroupement de journaux. Le regroupement de journaux peut améliorer les performances des recherches et réduire la bande passante réseau utilisée par les produits gérés lors de l'envoi de journaux à Control Manager. Toutefois, de nombreuses données sont perdues en raison du regroupement. Control Manager ne peut pas rechercher des données si celles-ci ne sont pas dans la base de données Control Manager.

Description des journaux générés par Control Manager

Les journaux de Control Manager comportent deux catégories : Informations sur la licence et informations Control Manager.

TABLEAU 9-1. Journaux Control Manager

JOURNAL DES CATÉGORIES	DESCRIPTION
Informations sur la licence	Ces journaux enregistrent des informations pour Control Manager et les produits gérés enregistrés sur le serveur Control Manager. • État de la licence du produit • Résumé des informations sur la licence du produit • Informations détaillées sur la licence du produit

JOURNAL DES CATÉGORIES	DESCRIPTION
Informations Control Manager	Ces journaux enregistrent les actions des utilisateurs et les événements des produits. • Informations sur l'accès des utilisateurs • Informations sur les événements Control Manager • Informations de suivi des commandes • Informations détaillées de suivi des commandes

Description des journaux de produits gérés

Les journaux de produits gérés contiennent des informations sur les performances des produits gérés. Vous pouvez y trouver des informations sur des produits spécifiques ou des groupes de produits gérés par le serveur parent ou enfant. Grâce aux capacités de filtrage de données et de recherche de données sur les journaux de Control Manager, les administrateurs peuvent à présent se concentrer sur les informations dont ils ont besoin.

Remarque

Plus vous avez de journaux, plus vous disposez d'informations sur le réseau de Control Manager. Toutefois, ces journaux occupent de l'espace disque. Il vous appartient donc de trouver le juste équilibre entre le besoin d'informations et la disponibilité des ressources système.

Les produits gérés génèrent différents types de journaux selon leur fonction.

TABLEAU 9-2. Journaux de produits gérés

CATÉGORIE DE JOURNAL	DESCRIPTION
Informations sur le produit	Les journaux d'information sur les produits fournissent des renseignements sur des sujets allant de l'accès des utilisateurs et des événements sur les produits gérés jusqu'au déploiement des composants et de l'état des mises à jour. • Informations sur les produits gérés • Informations relatives aux composants
Informations sur les menaces de sécurité	Les journaux des menaces de sécurité fournissent des informations relatives aux menaces de sécurité connues et potentielles détectées sur votre réseau. • Informations sur les virus/programmes malveillants • Informations sur les programmes espions/graywares • Informations sur les violations de contenu • Informations sur les violations de spam • Informations sur les violations de stratégies/règles • Informations sur les violations de sécurité/de réputation Web • Informations sur les menaces suspectes • Informations sur l'ensemble des menaces
Informations sur la protection des données	Les journaux de protection des données fournissent des informations sur les incidents de prévention contre la perte de données, les correspondances de modèles et les sources des incidents. • Informations sur la prévention contre la perte de données

Définition du regroupement de journaux

Le regroupement de journaux de Control Manager permet aux administrateurs de diminuer l'impact des produits gérés sur la bande passante du réseau. En configurant le regroupement des journaux, les administrateurs peuvent choisir les informations des journaux que les produits gérés enverront à Control Manager.

Remarque

Le regroupement des journaux n'est pas sans risque. Les informations non envoyées par les produits gérés à Control Manager sont perdues. Control Manager ne peut pas créer des rapports ou des requêtes pour des informations dont le serveur ne dispose pas. Cela peut soulever des problèmes si les informations qui n'avaient pas l'air importantes et qui sont abandonnées par les produits gérés deviennent ensuite essentielles, et qu'il n'est pas possible de les récupérer.

Configuration des paramètres de regroupement de journaux

Procédure

1. Accédez à l'écran **Journaux** > **Paramètres de regroupement de journaux**.

   L'écran **Modifier la règle de regroupement de journaux** apparaît.

2. Sélectionnez **Activer le regroupement de journaux**.
3. Développez les catégories de journaux requises.
4. Décocher les cases des données que les produits gérés n'enverront pas à Control Manager.
5. Cliquez sur **Enregistrer**.

Requête de données de journaux

Les requêtes ad hoc offrent une méthode simple aux administrateurs pour retrouver directement des informations à partir de la base de données de Control Manager. La base de données regroupe toutes les informations recueillies à partir de tous les produits enregistrés auprès du serveur Control Manager (le regroupement des journaux peut modifier les données disponibles à la requête). Les requêtes ad hoc constituent un outil très performant pour les administrateurs.

En faisant une requête de données, les administrateurs peuvent filtrer les critères de requête pour obtenir uniquement les données dont ils ont besoin. Les administrateurs peuvent ensuite exporter ces données au format CSV ou XML pour faire une analyse détaillée, ou encore enregistrer la requête pour une recherche ultérieure. Control Manager prend également en charge le partage des requêtes enregistrées avec les autres utilisateurs pour que ces derniers puissent bénéficier des requêtes utiles.

Le processus d'une requête ad hoc comporte les étapes suivantes :

- Étape 1 : Sélectionnez le produit géré ou le serveur Control Manager actuel pour la requête
- Étape 2 : Sélectionnez l'affichage des données de la requête
- Étape 3 : Spécifiez les critères de filtrage et les informations spécifiques à afficher
- Étape 4 : Enregistrez et terminez la requête
- Étape 5 : Exportez les données au format CSV ou XML

Remarque

Control Manager prend en charge le partage des requêtes ad hoc enregistrées avec les autres utilisateurs. Les requêtes enregistrées et partagées apparaissent sur l'écran **Requêtes ad hoc enregistrées**.

Définition des affichages de données

Un affichage de données est un tableau regroupant des clusters de cellules de données liées. Les utilisateurs se basent sur les affichages de données pour effectuer les requêtes ad hoc de la base de données de Control Manager.

Control Manager permet d'exécuter des requêtes directes dans la base de données Control Manager. Les affichages de base de données sont disponibles pour les modèles de rapport Control Manager 5 et les requêtes ad hoc.

Les affichages de base de données sont des tables contenant des informations. Chaque en-tête d'une vue agit comme la colonne d'une table. Par exemple, l'affichage Résumé sur l'action/le résultat de virus/programmes malveillants possède les en-têtes suivants :

- Résultat de l'action
- Action entreprise
- Points finaux uniques
- Sources uniques
- Détections

À l'instar d'une table, un affichage de données prend la forme suivante, avec des sous-en-têtes potentiels sous chaque en-tête :

TABLEAU 9-3. Exemple d'affichage de données

RÉSULTAT DE L'ACTION	ACTION ENTREPRISE	POINTS FINAUX UNIQUES	SOURCES UNIQUES	DÉTECTIONS

Les informations suivantes sont particulièrement importantes lors de la spécification du mode d'affichage des données dans un modèle de rapport.

Control Manager divise les affichages de données en deux catégories principales : informations sur le produit et informations sur les menaces de sécurité. Pour plus d'informations sur les affichages de données, consultez l'annexe. Ces deux catégories se divisent ensuite en plusieurs sous-catégories, elles-mêmes séparées entre informations résumées et informations détaillées.

Informations sur le produit

Les affichages de données d'informations sur le produit fournissent des informations sur Control Manager, les produits gérés, les composants et les licences de produits.

TABLEAU 9-4. Affichages de données d'informations sur le produit

CATÉGORIE	DESCRIPTION
Informations Control Manager	Affiche des informations sur l'accès utilisateur à Control Manager, sur le suivi des commandes et les événements du serveur Control Manager.
Informations sur les produits gérés	Affiche l'état, les informations détaillées et les informations résumées des produits gérés ou des points finaux de produits gérés.
Informations relatives aux composants	Affiche l'état, les informations détaillées et les informations résumées sur l'état obsolète ou à jour et sur le déploiement des composants de produits gérés.
Informations sur la licence	Affiche l'état, les informations détaillées et les informations résumées sur Control Manager et les licences de produits gérés.

Informations sur les menaces de sécurité

Affiche des informations sur les menaces de sécurité détectées par les produits gérés : virus, programme espion/grayware, sites d'hameçonnage, etc.

TABLEAU 9-5. Affichages de données de menaces de sécurité

CATÉGORIE	DESCRIPTION
Informations sur l'ensemble des menaces	Affiche des données résumées et statistiques concernant le paysage global des menaces sur votre réseau.
Informations sur les virus/ programmes malveillants	Affiche des données résumées et détaillées sur les programmes malveillants/virus détectés par les produits gérés sur votre réseau.
Informations sur les programmes espions/ graywares	Affiche des données résumées et détaillées sur les programmes espions/graywares détectés par les produits gérés sur votre réseau.
Informations sur les violations de contenu	Affiche des données résumées et détaillées sur le contenu prohibé détecté par les produits gérés sur votre réseau.
Informations sur les violations de spam	Affiche des données résumées et détaillées sur les spams détectés par les produits gérés sur votre réseau.
Informations sur les violations de sécurité Web	Affiche des données résumées et détaillées sur les violations de sécurité Internet détectées par les produits gérés sur votre réseau.
Informations sur les violations de stratégies/règles	Affiche des données résumées et détaillées sur les violations de stratégies/règles détectées par les produits gérés sur votre réseau.
Informations sur les menaces suspectes	Affiche des données résumées et détaillées sur les activités suspectes détectées par les produits gérés sur votre réseau.

Remarque

Pour plus d'informations sur les affichages de données disponibles et pris en charge par Control Manager, consultez l'annexe.

Informations sur la protection des données

La catégorie Informations sur la prévention contre la perte de données affiche les informations sur les incidents DLP, les sources d'incidents et les correspondances de modèles collectés par les produits gérés sur votre réseau.

Terminologie de l'affichage des données

Control Manager utilise les termes suivants dans les affichages de données, les requêtes renvoyées et les rapports générés.

Remarque

Pour une liste complète de la terminologie de l'affichage des données, consultez *Affichages des données à la page B-1*.

TABLEAU 9-6. Terminologie de l'affichage des données

DONNÉES	DESCRIPTION
Point final	Affiche l'adresse IP ou le nom d'hôte d'un ordinateur.
IP	Affiche l'adresse IP d'un ordinateur.
Port	Affiche le numéro de port d'un ordinateur.
MAC	Affiche l'adresse MAC d'un ordinateur.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Hôte du produit	Affiche le nom d'hôte du serveur sur lequel le produit géré est installé.

Données	Description
Adresse IP du produit	Affiche l'adresse IP du serveur sur lequel le produit géré est installé.
Adresse MAC du produit	Affiche l'adresse MAC du serveur sur lequel le produit géré est installé.
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan 10.0, Control Manager 5.0
Hôte source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur dont proviennent les menaces de sécurité.
Adresse IP source	Affiche l'adresse IP de l'ordinateur dont proviennent les menaces de sécurité.
Port source	Affiche le numéro de port de l'ordinateur dont proviennent les menaces de sécurité.
Adresse MAC source	Affiche l'adresse MAC de l'ordinateur dont proviennent les menaces de sécurité.
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des menaces de sécurité. Exemple : OfficeScan détecte 10 instances du même virus sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources d'infection uniques dont proviennent les menaces de sécurité. Exemple : OfficeScan détecte 10 instances du même virus provenant de 2 sources d'infection. Sources uniques = 2

DONNÉES	DESCRIPTION
Expéditeurs/utilisateurs uniques	Affiche le nombre d'adresses électroniques ou d'utilisateurs uniques qui expédient du contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie provenant de 3 ordinateurs. Expéditeurs/utilisateurs uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messages électroniques uniques réceptrices de contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2
Détections uniques	Affiche le nombre de virus/programmes malveillants uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections uniques = 1
Détections	Affiche le nombre total de virus/ programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Définition des requêtes ad hoc

Une requête ad hoc est une demande directe d'informations à la base de données de Control Manager. La requête utilise les affichages de données pour réduire le champ de

cette dernière et améliorer les performances. Après avoir spécifié l'affichage des données, les utilisateurs peuvent réduire leur champ de recherche en spécifiant des critères de filtre pour la requête.

Remarque

Pour plus d'informations sur les affichages de données, consultez la section *Définition des affichages de données à la page 9-7*.

Prenons l'exemple suivant : Laure, administratrice OfficeScan, veut vérifier l'état des fichiers de signatures des serveurs OfficeScan dont elle a la charge. Laure sélectionne tout d'abord les **produits gérés**. Elle sélectionne ensuite l'affichage des données **État du fichier de signature du produit géré** sous **informations sur le produit** > **Informations relatives aux composants**. Dans l'étape suivante, elle spécifie les critères de recherche de la façon suivante : Type de produit : OfficeScan, État du fichier de signature : Obsolète. En cliquant sur **Modifier l'affichage de colonne**, Laure sélectionne également les champs que la requête affiche une fois qu'elle est terminée. Laure choisit d'afficher les informations suivantes : Version du fichier de signatures, nom d'hôte, adresse IP. Elle ne sélectionne pas Nom du produit ou État du fichier de signatures, parce qu'elle sait déjà que les résultats trouvés par Control Manager remplissent ce critère.

Remarque

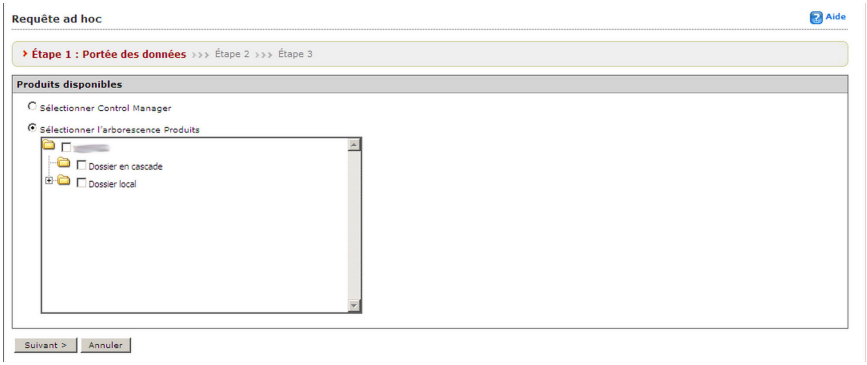
L'enregistrement d'une requête ad hoc entraîne uniquement l'enregistrement du critère spécifié pour cette requête. Les données renvoyées par une requête ad hoc ne sont pas enregistrées. Pour enregistrer les données, exportez les résultats de la requête ou créez un rapport à l'aide d'un tableau en grille.

Exécution d'une requête ad hoc

Procédure

1. Accédez à **Journaux** > **Nouvelle requête ad hoc**.

   L'écran **Requête ad hoc** apparaît.



2. Suivez les étapes ci-dessous pour exécuter une requête ad hoc.

Étape 1 : Spécifiez l'origine de l'information

Procédure

1. À partir de l'écran **Requête ad hoc**, sélectionnez l'origine de la requête d'information :

   - **Sélectionner Control Manager** : Spécifie que l'information provient du serveur Control Manager auquel l'utilisateur est actuellement connecté.

     En spécifiant cette option, l'arborescence produit est désactivée car les informations ne proviennent que du serveur Control Manager auquel l'utilisateur est connecté.

   - **Sélectionner l'arborescence Produits** : Spécifie que les informations proviennent des produits gérés de Control Manager. Cela peut comprendre les produits gérés des serveurs Control Manager enfants.

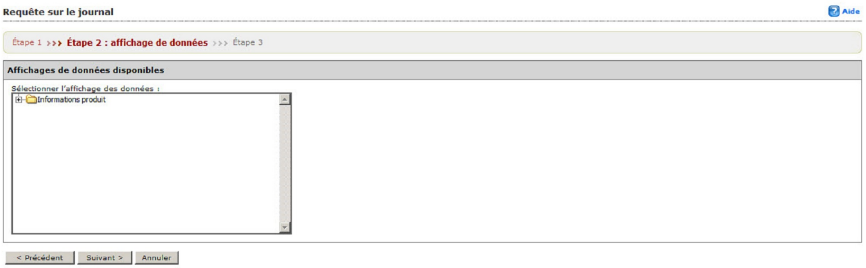
     En spécifiant cette option, l'utilisateur doit sélectionner les produits gérés ou le répertoire d'où proviennent les informations.

Remarque

La sélection du produit géré ou du répertoire sur cet écran affectera les affichages de données disponibles sur l'écran suivant. Par exemple, si vous sélectionnez OfficeScan dans le répertoire Produits, seuls s'affichent les affichages de données associés à OfficeScan dans la liste Affichages de données disponibles.

2. Cliquez sur **Suivant**.

   L'écran **Étape 2 : Affichage des données** apparaît.



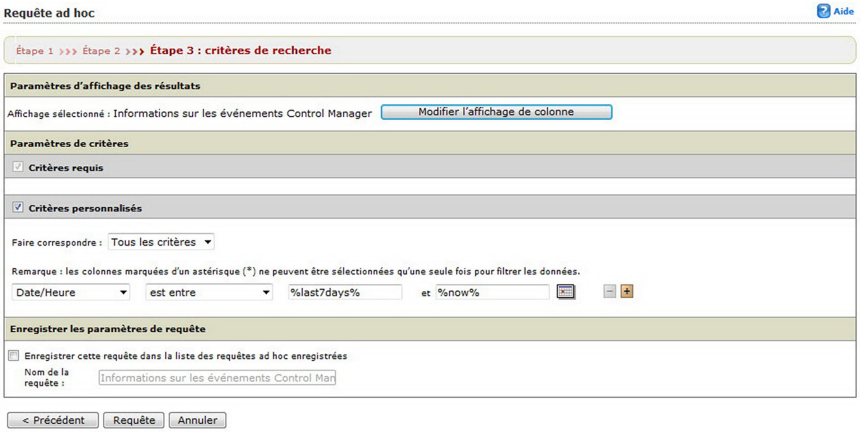
Étape 2 : Spécifiez un affichage de données pour la requête

Procédure

1. Sélectionnez un affichage de données dans la liste **Affichages de données disponibles**. Pour plus d'informations sur les affichages de données, consultez la section *Définition des affichages de données à la page 9-7*.

2. Cliquez sur **Suivant**.

   L'écran **Étape 3 : Critères de requête** apparaît.

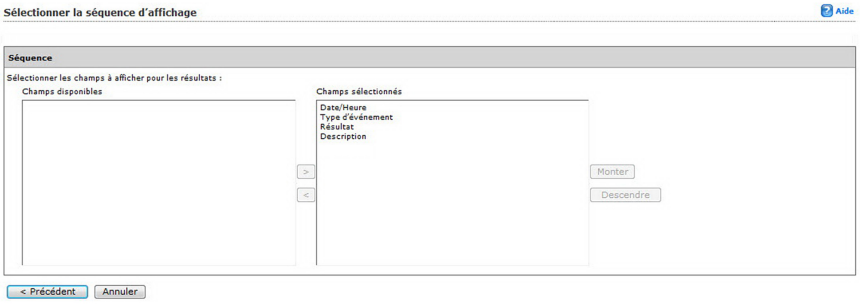


Étape 3 : Spécifiez la séquence d'affichage

Procédure

1. Cliquez sur **Modifier l'affichage de colonne**.

   L'écran **Sélectionner la séquence d'affichage** apparaît.



2. Dans la liste **Champs disponibles**, sélectionnez les colonnes d'affichage de données à afficher après le renvoi des informations par la requête.

   Les colonnes sélectionnées sont mises en surbrillance.

Remarque

Sélectionnez les colonnes une par une ou utilisez les touches **Maj** ou **Ctrl** pour sélectionner plusieurs colonnes.

La sélection et l'ajout d'une colonne à la fois sont une méthode permettant aux utilisateurs de spécifier la séquence d'affichage des informations.

3. Cliquez sur (>) pour inclure les champs dans la liste **Champs sélectionnés**.

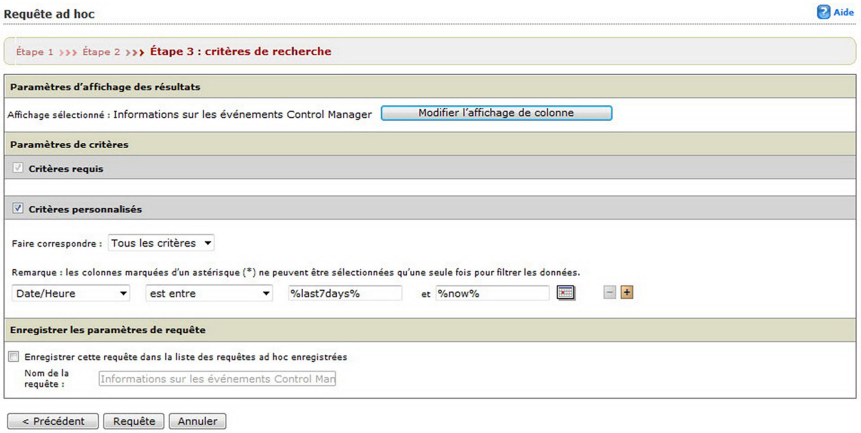
   Les colonnes sélectionnées apparaissent dans la liste Champs sélectionnés.

4. Continuez de sélectionner et d'ajouter les colonnes jusqu'à ce que vous disposiez de toutes les colonnes dont vous avez besoin.

5. Après avoir sélectionné une colonne dans la liste Champs sélectionnés, utilisez les boutons **Monter** et **Descendre** pour spécifier la séquence d'affichage des informations. La colonne située en haut de la liste apparaît comme étant la plus à gauche dans les résultats de la requête.

6. Cliquez sur **Précédent**.

   L'écran **Étape 3 : Critères de requête** apparaît.



Étape 4 : Spécifiez les critères de filtre

Procédure

1. Spécifiez les **Critères requis**.

   - Spécifiez une heure de résumé pour les données et, pour les affichages de données de programme espion/grayware, indiquez si vous voulez que les COOKIES apparaissent dans les résultats.

2. Spécifiez les **Critères personnalisés**.

   a. Sélectionnez **Critères personnalisés**.

      L'option des critères personnalisés apparaît.

   b. Spécifiez les règles de filtrage des critères pour les catégories de données du champ **Faire correspondre**.

      - **Tous les critères** : cette sélection est équivalente à une fonction logique AND. Les données apparaissant dans le rapport doivent correspondre à tous les critères de filtrage.
      - **L'un des critères** : cette sélection est équivalente à une fonction logique OR. Les données apparaissant dans le rapport doivent correspondre à l'un des critères de filtrage.

   c. Spécifiez les critères de filtrage pour les données : Control Manager prend en charge jusqu'à 20 critères pour le filtrage des données.

      Remarque

      Si vous ne spécifiez aucun critère de filtrage, la requête ad hoc renvoie tous les résultats pour les colonnes concernées. Trend Micro recommande de spécifier des critères de filtrage pour simplifier l'analyse des données après le renvoi des informations par la requête.

      i. À partir de la liste déroulante située la plus à gauche, sélectionnez la colonne à filtrer.

      ii. Dans la liste déroulante du milieu, sélectionnez la condition de correspondance du filtre.

iii. Dans le champ situé le plus à droite, entrez le critère de filtre. Une liste ou une zone de texte apparaît en fonction de la colonne sélectionnée pour le filtre.

iv. Clique sur l'icône **+** pour ajouter un nouveau critère de filtre à l'affichage de données.

Étape 5 : Enregistrez et terminez la requête

Procédure

1. Pour enregistrer la requête ad hoc, cliquez sur **Enregistrer cette requête dans la liste des requêtes ad hoc enregistrées** dans Enregistrer les paramètres de requête.
2. Spécifiez un nom de requête ad hoc dans le champ **Nom de la requête**.

Remarque

Control Manager prend en charge le partage des requêtes ad hoc enregistrées avec les autres utilisateurs. Les requêtes enregistrées apparaissent dans l'écran **Requêtes ad hoc enregistrées**.

3. Cliquez sur **Requête**.

   L'écran **Résultats de requête ad hoc** apparaît avec les résultats de la requête.

   Pour des informations détaillées sur un élément donné, cliquez sur son lien souligné.

Étape 6 : Exportez les résultats de la requête au format CSV ou XML

Procédure

1. Une boîte de dialogue **Téléchargement de fichier** apparaît si vous cliquez sur un des éléments suivants :

- **Exporter vers CSV** : Exporte les résultats de la requête au format CSV.
- **Exporter vers fichier XML** : Exporte les résultats de la requête au format XML.

2. Choisissez l'une des options suivantes :
   - Cliquez sur **Ouvrir** pour visualiser immédiatement les résultats de la requête au format CSV ou XML.
   - Cliquez sur **Enregistrer**. Une boîte de dialogue Enregistrer sous s'affiche. Spécifiez l'emplacement dans lequel enregistrer le fichier.
3. Pour enregistrer les paramètres de la requête :
   a. Cliquez sur **Enregistrer les paramètres de requête**.

      Une fenêtre de confirmation apparaît.

   b. Saisissez un nom pour la requête enregistrée dans le champ **Nom de la requête**.

   c. Cliquez sur **OK**.

      La requête enregistrée apparaît dans l'écran Requêtes ad hoc enregistrées.

Utilisation des requêtes ad hoc enregistrées et partagées

Control Manager prend en charge l'enregistrement d'une requête ad hoc créée par un utilisateur. Les requêtes ad hoc enregistrées apparaissent sur l'écran **Requêtes ad hoc enregistrées**. L'écran **Requêtes ad hoc enregistrées** contient deux onglets : Mes requêtes et Requêtes disponibles.

La section Mes requêtes de l'écran **Requêtes ad hoc enregistrées** affiche toutes les requêtes ad hoc créées par l'utilisateur connecté. Dans l'onglet Mes requêtes, l'utilisateur peut ajouter, modifier, afficher, supprimer, exporter et partager/arrêter le partage des requêtes. En partageant les requêtes enregistrées, ces dernières deviennent disponibles pour les autres utilisateurs.

Remarque

Le contrôle d'accès Control Manager, déterminé par le compte et le rôle d'utilisateur, limite les informations auxquelles un utilisateur a accès. Ainsi, bien que tous les utilisateurs puissent afficher les requêtes partagées, le contrôle d'accès limite l'efficacité de la requête.

Exemple : Chris, l'administrateur OfficeScan, crée et partage une requête ad hoc relative aux informations du serveur OfficeScan. Claire, administratrice de ScanMail for Exchange, a accès à la requête partagée, mais si elle tente de générer une requête ad hoc en utilisant la requête de Laure, elle n'obtiendra pas de résultats. Claire n'a en effet pas accès aux informations du serveur OfficeScan. Cet exemple montre que seule Laure a accès aux serveurs OfficeScan, et que seule Claire a accès aux serveurs ScanMail for Exchange.

Modification de requêtes ad hoc enregistrées

Control Manager prend en charge la modification de requêtes ad hoc enregistrées sous l'onglet Mes requêtes dans l'écran **Requêtes ad hoc enregistrées**. Pour modifier une requête ad hoc enregistrée, suivez les étapes suivantes :

Étape 1 : Sélectionnez le produit géré ou le serveur Control Manager actuel pour la requête

Étape 2 : Sélectionnez l'affichage des données de la requête

Étape 3 : Spécifiez les critères de filtrage et les informations spécifiques à afficher

Étape 4 : Enregistrez et terminez la requête

Étape 5 : Exportez les données au format CSV ou XML

Procédure

1. Accédez à **Journaux** > **Requêtes ad hoc enregistrées**.

   L'écran **Requêtes ad hoc enregistrées** apparaît.

2. Cliquez sur le nom de la requête ad hoc enregistrée à modifier.

   L'écran **Sélectionner l'arborescence Produits** apparaît.

Étape 1 : Spécifiez l'origine de l'information

Procédure

1. Dans l'écran **Requête ad hoc Query**, spécifiez la catégorie de protection du réseau (produit géré ou répertoire) à partir duquel le rapport est généré.

   - **Sélectionner Control Manager** : Spécifie que l'information provient du serveur Control Manager auquel l'utilisateur est actuellement connecté.

     En spécifiant cette option, l'arborescence produit est désactivée car les informations ne proviennent que du serveur Control Manager auquel l'utilisateur est connecté.

   - **Sélectionner l'arborescence Produits** : Spécifie que les informations proviennent des produits gérés de Control Manager.

     En spécifiant cette option, l'utilisateur doit sélectionner la catégorie de protection d'où proviennent les informations. L'utilisateur peut le faire en sélectionnant les produits gérés/répertoires à partir du répertoire Produits.

   Remarque

   La sélection du produit géré/répertoire sur cet écran affectera les affichages de données disponibles. Par exemple, en sélectionnant OfficeScan dans le répertoire produit, seuls les affichages de données associés à la protection des postes de travail s'afficheront dans la liste Affichages de données.

2. Cliquez sur **Suivant**.

   L'écran **Sélectionner l'affichage des données** apparaît.

Étape 2 : Spécifiez un affichage de données pour la requête

Procédure

1. Sélectionnez un affichage de données dans la liste **Affichages de données disponibles**. Pour plus d'informations sur les affichages de données, consultez la section *Définition des affichages de données à la page 9-7*.

2. Cliquez sur **Suivant**.

   L'écran **Critères de requête** apparaît.

Étape 3 : Spécifiez la séquence d'affichage

Spécifiez l'affichage et la séquence d'informations trouvées pour la requête.

Procédure

1. Cliquez sur **Modifier l'affichage de colonne**.

   L'écran **Sélectionner la séquence d'affichage** apparaît.

2. À partir de la liste **Champs disponibles**, sélectionnez les colonnes d'affichage des données qui s'affichent pour les informations trouvées de la requête.

   Les colonnes sélectionnées sont mises en surbrillance.

   Conseil

   Sélectionnez les colonnes une par une ou utilisez les touches **Maj** ou **Ctrl** pour sélectionner plusieurs colonnes.

   La sélection et l'ajout d'une colonne à la fois sont une méthode permettant aux utilisateurs de spécifier la séquence d'affichage des informations.

3. Cliquez sur () pour inclure les champs dans la liste **Champs sélectionnés**.

   Les colonnes sélectionnées apparaissent dans la liste Champs sélectionnés.

4. Continuez de sélectionner et d'ajouter les colonnes jusqu'à ce que vous disposiez de toutes les colonnes dont vous avez besoin.

5. Après avoir sélectionné une colonne dans la liste Champs sélectionnés, utilisez les boutons **Monter** et **Descendre** pour spécifier la séquence d'affichage des informations. La colonne située en haut de la liste apparaît comme étant la plus à gauche dans les résultats de la requête.

6. Cliquez sur **Précédent**.

L'écran **Étape 3 : Critères de requête** apparaît.

Étape 4 : Spécifiez les critères de filtre

En effectuant une recherche de données résumées (tous les affichages de données contenant le mot Résumé dans leur titre), vous devez spécifier les éléments sous Critères requis.

Procédure

1. Spécifiez les **Critères requis**.
   - Spécifiez une heure de résumé pour les données ou si vous souhaitez que les COOKIES apparaissent dans vos rapports.
2. Spécifiez les **Critères personnalisés**.
   a. Sélectionnez **Critères personnalisés**.

      L'option des critères personnalisés apparaît.

   b. Spécifiez les règles de filtrage des critères pour les catégories de données du champ **Faire correspondre**.
      - **Tous les critères** : cette sélection est équivalente à une fonction logique AND. Les données apparaissant dans le rapport doivent correspondre à tous les critères de filtrage.
      - **L'un des critères** : cette sélection est équivalente à une fonction logique OR. Les données apparaissant dans le rapport doivent correspondre à l'un des critères de filtrage.

   c. Spécifiez les critères de filtrage pour les données : Control Manager prend en charge jusqu'à 20 critères pour le filtrage des données.

Remarque

Si vous ne spécifiez aucun critère de filtrage, la requête ad hoc renvoie tous les résultats pour les colonnes concernées. Trend Micro recommande de spécifier des critères de filtrage pour simplifier l'analyse des données après le renvoi des informations par la requête.

i. À partir de la liste déroulante située la plus à gauche, sélectionnez la colonne à filtrer.

ii. Dans la liste déroulante du milieu, sélectionnez la condition de correspondance du filtre.

iii. Dans le champ situé le plus à droite, entrez le critère de filtre. Une liste ou une zone de texte apparaît en fonction de la colonne sélectionnée pour le filtre.

iv. Clique sur l'icône + pour ajouter un nouveau critère de filtre à l'affichage de données.

Étape 5 : Enregistrez et terminez la requête

Procédure

1. Pour enregistrer la requête ad hoc, cliquez sur **Enregistrer cette requête dans la liste des requêtes ad hoc enregistrées** dans Enregistrer les paramètres de requête.

2. Spécifiez un nom de requête ad hoc dans le champ **Nom de la requête**.

   Remarque

   Control Manager prend en charge le partage des requêtes ad hoc enregistrées avec les autres utilisateurs. Les requêtes enregistrées apparaissent dans l'écran **Requêtes ad hoc enregistrées**.

3. Cliquez sur **Requête**.

   L'écran **Résultats de requête ad hoc** apparaît avec les résultats de la requête.

Étape 6 : Exportez les résultats de la requête au format CSV ou XML

Procédure

1. Une boîte de dialogue **Téléchargement de fichier** apparaît si vous cliquez sur un des éléments suivants :
   - **Exporter vers CSV** : Exporte les résultats de la requête au format CSV.
   - **Exporter vers fichier XML** : Exporte les résultats de la requête au format XML.
2. Choisissez l'une des options suivantes :
   - Cliquez sur **Ouvrir** pour visualiser immédiatement les résultats de la requête au format CSV ou XML.
   - Cliquez sur **Enregistrer**. Une boîte de dialogue **Enregistrer sous** s'affiche. Spécifiez l'emplacement dans lequel enregistrer le fichier.

Partage de requêtes ad hoc enregistrées

Control Manager prend en charge le partage de requêtes ad hoc enregistrées sous l'onglet Mes requêtes dans l'écran **Requêtes ad hoc enregistrées**.

Procédure

1. Accédez à **Journaux** > **Requêtes ad hoc enregistrées**.

   L'écran **Requêtes ad hoc enregistrées** apparaît.
2. Cochez la case correspondant à la requête ad hoc que vous souhaitez partager.
3. Cliquez sur **Partager**.

   Une icône apparaît dans la colonne Partagée de la requête ad hoc enregistrée.

Utilisation des requêtes ad hoc partagées

Après avoir créé une requête ad hoc, un utilisateur peut la partager avec d'autres utilisateurs. Toutes les requêtes partagées de tous les utilisateurs apparaissent sous l'onglet Requêtes disponibles de l'écran **Requêtes ad hoc enregistrées**. Les utilisateurs peuvent afficher et exporter ces requêtes partagées.

Procédure

1. Accédez à **Journaux** > **Requêtes ad hoc enregistrées**.

   L'écran **Requêtes ad hoc enregistrées** apparaît.

2. Cliquez sur l'onglet **Requêtes disponibles**.

3. Utilisez les requêtes pour afficher des informations ou pour exporter des requêtes partagées.

Suppression de journaux

Utilisez l'écran **Maintenance des journaux** pour supprimer immédiatement des journaux ou configurer automatiquement la suppression de journaux pour les types suivants :

- Journaux de virus/programmes espions/graywares
- Journaux d'événements du produit
- Journaux de sécurité
- Journaux de sécurité Web
- journaux de virus réseau
- Journaux de point final
- Journaux de violation de sécurité
- Journaux de respect de sécurité
- Journaux de statistiques de sécurité

- Journaux des virus suspects
- Journaux de réputation de réseau
- Journaux de programmes espions/graywares sur le poste de travail
- Journaux de violation de pare-feu
- Journaux de surveillance des comportements
- Journaux d'accès
- Journaux des événements du serveur
- Journaux de migration des menaces
- Journaux de prévention contre la perte de données

Remarque

Trend Micro conseille de sauvegarder les journaux de Prévention contre la perte de données vers Informations de sécurité et Gestion d'événements (SIEM) et de les garder au moins 2 ans.

Procédure

1. Accédez à **Journaux** > **Maintenance des journaux**.

   L'écran **Maintenance des journaux** apparaît.

2. Cochez la case correspondant aux journaux que vous souhaitez supprimer.

3. Cliquez sur **Tout supprimer** dans la ligne correspondant aux journaux que vous souhaitez supprimer.

Configuration des paramètres de suppression automatique des journaux

L'écran **Maintenance des journaux** offre deux méthodes de suppression automatique des journaux :

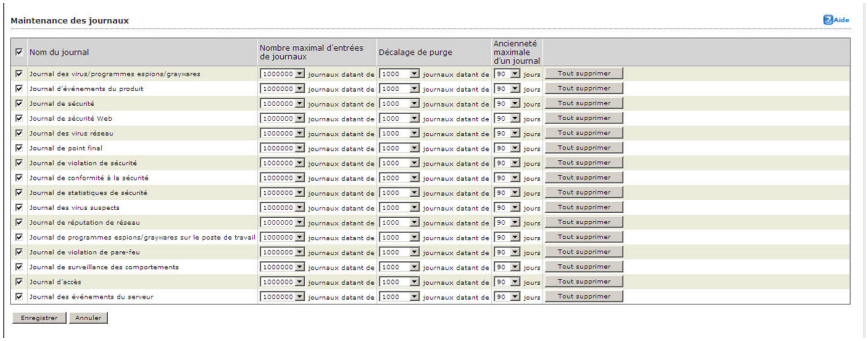
- Par nombre de journaux (minimum : 30 000, maximum : 1 000 000, par défaut : 1 000 000)
- Par ancienneté des journaux (minimum : 1 jour, maximum : 90 jours, par défaut : 90 jours)

Le décalage de purge spécifie le nombre de journaux supprimés par Control Manager lorsque le nombre de journaux d'un type donné atteint le seuil maximal. Les paramètres de purge par défaut sont de 1 000, tous types de journaux confondus.

Procédure

1. Accédez à **Journaux** > **Maintenance des journaux**.

   L'écran **Maintenance des journaux** apparaît.



2. Cochez la case correspondant aux journaux pour lesquels vous souhaitez configurer les paramètres.

3. Spécifiez le nombre maximum de journaux que Control Manager peut conserver dans la colonne **Nombre maximal d'entrées de journaux** .

4. Dans **Décalage de purge**, spécifiez le nombre de journaux supprimés par Control Manager lorsque le nombre de journaux atteint le nombre spécifié dans la colonne Nombre maximal d'entrées de journaux.

5. Dans **Ancienneté maximale d'un journal**, spécifiez l'ancienneté des journaux supprimés automatiquement par Control Manager.

6. Cliquez sur **Enregistrer**.

Chapitre 10

Utilisation des rapports

Générez des rapports avec les données de journal collectées à partir des produits gérés enregistrés dans Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition des rapports

Les rapports de Control Manager consistent en deux parties : les modèles de rapport et les profils de rapport. Tandis qu'un modèle de rapport détermine l'apparence et l'agencement du rapport, le profil de rapport spécifie la provenance des données du rapport, la période ou la programmation ainsi que les destinataires du rapport.

Control Manager 5.0 a mis en place des changements radicaux par rapport aux versions précédentes en introduisant les rapports personnalisés pour les administrateurs de Control Manager. Control Manager 6.0 prend toujours en charge les modèles de rapport des versions précédentes de Control Manager, mais Control Manager 6.0 permet aux administrateurs de personnaliser leurs propres modèles de rapport.

Définition des modèles de rapport de Control Manager

Un modèle de rapport définit l'aspect et la présentation des rapports de Control Manager. Control Manager classe les modèles de rapport selon les types suivants :

- Modèles de Control Manager 5 : Modèles de rapport personnalisé définis par l'utilisateur, qui utilisent les requêtes de bases de données directes (affichages de base de données) et les éléments des modèles de rapport (graphiques et tableaux). Les utilisateurs disposent d'une plus grande flexibilité pour spécifier les données apparaissant dans leurs rapports par rapport aux modèles de rapport des versions précédentes de Control Manager. Pour plus d'informations sur les modèles de Control Manager 5, consultez la section *Définition des modèles de Control Manager 5 à la page 10-2*.
- Modèles prédéfinis de Control Manager 3 : Contient des modèles prédéfinis Pour plus d'informations sur les modèles de Control Manager 3, consultez la section *Définition des modèles de Control Manager 3 à la page 10-10*.

Définition des modèles de Control Manager 5

Les modèles de rapport de Control Manager 5 basent leurs informations sur les affichages de base de données. Pour plus d'informations sur les affichages de données,

consultez la section *Définition des affichages de données à la page 9-7*. L'apparence et l'agencement des rapports générés se reportent sur les éléments du rapport. Le rapport comporte les éléments suivants.

TABLEAU 10-1. Éléments des modèles de rapport de Control Manager 5

ÉLÉMENT DU MODÈLE	DESCRIPTION
Saut de page	Insère un saut de page pour un rapport. Chaque page de rapport peut contenir jusqu'à trois éléments de modèle de rapport.
Texte statique	Donne une description définie par l'utilisateur ou une explication du rapport. Le texte statique peut contenir jusqu'à 4 096 caractères.
Graphique en barres	Insère un graphique en barre dans un modèle de rapport.
Graphique en ligne	Insère un graphique en ligne dans un modèle de rapport.
Graphique circulaire	Insère un graphique circulaire dans un modèle de rapport.
Tableau dynamique	Insère un tableau dynamique/tableau croisé dynamique dans un modèle de rapport.
Tableau en grille	Insère un tableau dans un modèle de rapport. Les informations d'un tableau en grille seront les mêmes que celles d'une requête ad hoc.

Chaque modèle de Control Manager 5 peut contenir jusqu'à 100 éléments de modèle de rapport. Chaque page du modèle de rapport peut contenir jusqu'à trois éléments de modèle de rapport. Utilisez le saut de page pour créer des pages de modèle de rapport.

Pour mieux comprendre les modèles de rapport de Control Manager 5, Trend Micro fournit les modèles de rapport prédéfinis suivants.

Remarque

Accédez à l'écran **Modèles de rapport** pour consulter les modèles prédéfinis de Trend Micro.

TABLEAU 10-2. Modèles prédéfinis de Control Manager 5

MODÈLE	DESCRIPTION
Résumé sur la détection de violation de contenu TM	Indique les informations suivantes : • Détections de violations de contenu classées par jour (graphique en ligne) • Stratégie en matière du décompte de violations classées par jour (graphique en ligne) • Décompte de violations expéditeur/utilisateurs classées par jour (graphique en ligne) • Décompte de destinataires classés par jour (graphique en ligne) • 25 principales violations de stratégies (graphique en barres) • Résumé sur la stratégie en matière de violation de contenu (tableau en grille) • 25 principaux expéditeurs/utilisateurs violés (graphique en barres) • Résumé sur les expéditeurs/utilisateurs de violation de contenu (tableau en grille) • Résumé sur le résultat de l'action (graphique circulaire)

Modèle	Description
État de connexion/ composant des produits gérés par TM	Indique les informations suivantes : • État de la connexion du serveur/de l'appliance (graphique circulaire) • État de la connexion client (graphique circulaire) • État de la mise à jour du fichier de signatures/de la règle de l'appliance/du serveur (graphique circulaire) • État de la mise à jour du fichier de signatures client/de la règle (graphique circulaire) • État de la mise à jour du moteur de scan de l'appliance/du serveur (graphique circulaire) • État de le mise à jour du moteur de scan client (graphique circulaire) • Fichier de signature/Résumé de la règle pour serveurs/ Appliances (tableau en grille) • Fichier de signature/Résumé de la règle pour les clients (tableau en grille) • Résumé du moteur de scan pour serveurs/appliances (tableau en grille) • Résumé du moteur de scan pour clients (tableau en grille)
Résumé sur l'ensemble des menaces TM	Indique les informations suivantes : • Résumé sur l'analyse des risques de sécurité de l'ensemble du réseau (tableau en grille) • Résumé sur les limites de protection du réseau (tableau en grille) • Informations sur l'analyse des points d'entrée des risques de sécurité (tableau en grille) • Informations sur l'analyse des destinations des risques de sécurité (tableau en grille) • Informations sur l'analyse des sources des risques de sécurité (tableau en grille)

MODÈLE	DESCRIPTION
Résumé sur la détection de pourriel TM	Indique les informations suivantes : • Détections de pourriels classées par jour (graphique en ligne) • Décompte de domaines destinataires classés par jour (graphique en ligne) • Décompte de destinataires classés par jour (graphique en ligne) • 25 principaux domaines destinataires (graphique en barres) • Résumé de l'ensemble des violations de pourriels (tableau en grille) • 25 principaux destinataires de pourriel (graphique en barres) • Résumé des destinataires de pourriels (tableau en grille)

Modèle	Description
Résumé sur la détection de programmes espions/ grayware TM	Indique les informations suivantes : • Détections de programmes espions/graywares classées par jour (graphique en ligne) • Décompte de programmes espions/graywares uniques classées par jour (graphique en ligne) • Décompte des sources de programmes espions/ graywares classées par jour (graphique en ligne) • Décompte des destinations de programmes espions/ graywares classées par jour (graphique en ligne) • 25 principaux programmes espions/graywares (graphique en barres) • Résumé de l'ensemble des violations de programmes espions/graywares (tableau en grille) • 25 principales sources de programmes espions/ graywares (graphique en barres) • Résumé des sources de programmes espions/ graywares (tableau en grille) • 25 principales destinations de programmes espions/ graywares (graphique en barres) • Résumé des destinations de programmes espions/ graywares (tableau en grille) • Résumé sur le résultat de l'action (graphique circulaire) • Résumé de l'action/du résultat des programmes espions/graywares (tableau en grille)

MODÈLE	DESCRIPTION
Résumé sur la détection des menaces suspectes TM	Indique les informations suivantes : • Détections de menaces suspectes classées par jour (graphique en ligne) • Décompte des règles violées classées par jour (graphique en ligne) • Décompte d'expéditeurs classés par jour (graphique en ligne) • Décompte de destinataires classés par jour (graphique en ligne) • Décompte d'adresses IP source classées par jour (graphique en ligne) • Décompte d'adresses IP de destination classées par jour (graphique en ligne) • 25 principaux expéditeurs (graphique en barres) • 25 principaux destinataires (graphique en barres) • Résumé des expéditeurs de menaces suspectes (tableau en grille) • Résumé sur le destinataire des menaces suspectes les plus dangereuses (tableau en grille) • 25 principales adresses IP sources (graphique en barres) • 25 principales adresses IP de destination (graphique en barres) • Résumé sur la source de menace suspecte (tableau en grille) • Résumé sur la destination la plus dangereuse de menace suspecte (tableau en grille) • 25 principaux noms de protocole (graphique en barres) • Résumé sur la détection de protocole de menace dangereuse (tableau en grille) • Résumé sur l'ensemble des menaces suspectes (tableau en grille)

Modèle	Description
Résumé sur la détection des virus/programmes malveillants TM	Indique les informations suivantes : • Détections de virus/programmes malveillants classées par jour (graphique en ligne) • Décompte de virus/programmes malveillants uniques classés par jour (graphique en ligne) • Décompte de destinations d'infections classées par jour (graphique en ligne) • 25 principaux programmes malveillants/virus (graphique en barres) • Résumé de l'ensemble des virus/programmes malveillants (tableau en grille) • 25 principales sources d'infection (graphique en barres) • Résumé sur les sources d'infections de virus/programmes malveillants (tableau en grille) • 25 principales destinations d'infection (graphique en barres) • Résumé sur les destinations d'infections de virus/programmes malveillants (tableau en grille) • Résumé sur le résultat de l'action (graphique circulaire) • Résumé de l'action/du résultat des virus/programmes malveillants (tableau en grille)

MODÈLE	DESCRIPTION
Résumé sur la détection de violation de sécurité Web TM	Indique les informations suivantes : • Détections de violations Web classées par jour (graphique en ligne) • Stratégie en matière du décompte de violations classées par jour (graphique en ligne) • Décompte de violations client classées par jour (graphique en ligne) • Décompte de violations d'URL classées par jour (graphique en ligne) • 25 principales violations de stratégies (graphique en barres) • Résumé de l'ensemble des violations Web (tableau en grille) • 25 principaux clients en situation de violation (graphique en barres) • Résumé sur l'adresse IP du client en situation de violation de sécurité Web (tableau en grille) • 25 principales URL en situation de violation (graphique en barres) • Résumé des URL en situation de violation de sécurité Web (tableau en grille) • Résumé sur le type de filtre/blocage (graphique circulaire)

Définition des modèles de Control Manager 3

Control Manager a ajouté 87 modèles de rapport prégénérés répartis en six catégories : Résumé exécutif, passerelle, serveur de messagerie, serveur, poste de travail, produits pour réseau, et prévention contre la perte de données.

Remarque

Dans Control Manager 3.5, les programmes espions/graywares ne sont plus considérés comme des virus. Cette modification influe sur le décompte des virus effectué dans tous les rapports d'origine relatifs aux virus.

La génération du rapport peut demander quelques secondes, selon le volume de son contenu. Dès que Control Manager a fini de créer un rapport, l'écran se réactualise et le lien **Afficher** correspondant au rapport devient disponible.

Utilisez la liste Catégorie de rapport de l'écran de Control Manager pour passer en revue les six catégories de rapport répertoriées ci-dessous :

TABLEAU 10-3. Rapports de la catégorie Résumé exécutif et types de rapports

RAPPORTS RÉSUMÉ EXÉCUTIF	TYPES DE RAPPORTS
Rapports de détection des programmes espions/graywares	• Programmes espions/graywares détectés • Programmes espions/graywares le plus souvent détectés (10, 25, 50, 100) • Liste des programmes espions/ graywares détectés pour toutes les entités
Rapports de détection de virus	• Virus détectés • Virus le plus souvent détectés (10, 25, 50, 100) • Liste des infections virales pour toutes les entités

Rapports Résumé exécutif	Types de rapports
Rapports comparatifs	• Programmes espions/graywares classés par (jour, semaine, mois) • Virus classés par (jour, semaine, mois) • Services Damage Cleanup classés par (jour, semaine, mois) • Pourriel classé par (jour, semaine, mois)
Rapports sur les failles	• Évaluation du niveau de risque pour l'ordinateur • Évaluation des failles • Infections le plus souvent nettoyées (10, 25, 50, 100) • Failles potentielles les plus dangereuses (10, 25, 50, 100) • Classement des failles selon le niveau de risque

Tableau 10-4. Rapports de la catégorie Produits pour passerelles et types de rapports

Rapports Produits pour passerelles	Types de rapports
Rapports de détection des programmes espions/graywares	• Programmes espions/graywares détectés • Programmes espions/graywares le plus souvent détectés (10, 25, 50, 100)
Rapports de détection de virus	• Virus détectés • Virus le plus souvent détectés (10, 25, 50, 100)

Rapports Produits pour passerelles	Types de rapports
Rapports comparatifs	• Programmes espions/graywares classés par (jour, semaine, mois) • Pourriel classé par (jour, semaine, mois) • Virus classés par (jour, semaine, mois)
Rapports sur le taux de déploiement	• Résumé détaillé • Résumé de base • Résumé détaillé sur le taux d'échec • Taux de déploiement OPS pour IMSS

Tableau 10-5. Rapports de la catégorie Produits pour serveurs de messagerie et types de rapports

Rapports Produits pour serveurs de messagerie	Types de rapports
Rapports de détection des programmes espions/graywares	• Programmes espions/graywares détectés • Programmes espions/graywares le plus souvent détectés (10, 25, 50, 100)
Rapports de détection de virus	• Virus détectés • Principaux expéditeurs de courrier électronique infecté (10, 25, 50, 100) • Virus le plus souvent détectés (10, 25, 50, 100)
Rapports comparatifs	• Programmes espions/graywares classés par (jour, semaine, mois) • Virus classés par (jour, semaine, mois)

Rapports Produits pour serveurs de messagerie	Types de rapports
Rapports sur le taux de déploiement	• Résumé détaillé • Résumé de base • Résumé détaillé sur le taux d'échec

Tableau 10-6. Rapports de la catégorie Produits pour réseaux et types de rapports

Rapports Produits basés sur serveur	Types de rapports
Rapports de détection des programmes espions/graywares	• Programmes espions/graywares détectés • Programmes espions/graywares le plus souvent détectés (10, 25, 50, 100)
Rapports de détection de virus	• Virus détectés • Virus le plus souvent détectés (10, 25, 50, 100)
Rapports comparatifs	• Programmes espions/graywares classés par (jour, semaine, mois) • Virus classés par (jour, semaine, mois)
Rapports sur le taux de déploiement	• Résumé détaillé • Résumé de base • Résumé détaillé sur le taux d'échec

TABLEAU 10-7. Rapports de la catégorie Produits pour postes de travail et types de rapports

RAPPORTS PRODUITS POUR POSTES DE TRAVAIL	TYPES DE RAPPORTS
Rapports de détection des programmes espions/graywares	• Programmes espions/graywares détectés • Programmes espions/graywares le plus souvent détectés (10,25,50,100)
Rapports de détection de virus	• Virus détectés • Virus le plus souvent détectés (10,25,50,100)
Rapports d'informations d'OfficeScan	• Résumé détaillé • Résumé de base
Rapport d'enregistrement du produit OfficeScan	État d'enregistrement
Rapports comparatifs	• Programmes espions/graywares classés par (jour, semaine, mois) • Virus classés par (jour, semaine, mois)
Rapports de déploiement d'OfficeScan	• Résumé détaillé • Résumé de base • Résumé détaillé sur les taux d'échec
Rapports d'OfficeScan Damage Cleanup Services	• Résumé détaillé • Infections le plus souvent nettoyées (10, 25, 50, 100)

TABLEAU 10-8. Rapports Produits pour réseaux et types de rapports

RAPPORTS PRODUITS POUR RÉSEAUX	TYPES DE RAPPORTS
Rapports de Network VirusWall	• Rapport de violations de stratégies classées par (jour, semaine, mois) • Clients victimes de violation le plus souvent détectés (10, 25, 50, 100) • Rapport de violations de service classées par (jour, semaine, mois)
Rapports de Trend Micro Total Discovery Appliance	• Rapport sur le résumé des incidents, classés par (jour, semaine, mois) • Clients exposés à des risques importants (10, 25, 50, 100) • Rapport de résumé des risques connus et inconnus

TABLEAU 10-9. Rapports de prévention contre la perte de données et types de rapport

RAPPORTS DE PRÉVENTION CONTRE LA PERTE DE DONNÉES	TYPES DE RAPPORTS
Sources principales d'incidents de prévention contre la perte de données	• Incidents par expéditeur (10, 20, 30, 40, 50) • Incidents par nom d'hôte (10, 20, 30, 40, 50) • Incidents par destinataire (10, 20, 30, 40, 50) • Incidents par adresse IP source (10, 20, 30, 40, 50) • Incidents par URL (10, 20, 30, 40, 50) • Incidents par utilisateur (10, 20, 30, 40, 50) • Principales correspondances de modèles (10, 20, 30, 40, 50) • Répartition des incidents par canal • Tendances des incidents, groupés par (jour, semaine, mois) • Incidents par canal, classés par (jour, semaine, mois)

RAPPORTS DE PRÉVENTION CONTRE LA PERTE DE DONNÉES	TYPES DE RAPPORTS
Augmentation significative des incidents	• Augmentation significative des incidents (%) par canal (10, 20, 30, 40, 50) • Augmentation significative des incidents par canal (10, 20, 30, 40, 50) • Augmentation significative des incidents (%) par expéditeur (10, 20, 30, 40, 50) • Augmentation significative des incidents par expéditeur (10, 20, 30, 40, 50) • Augmentation significative des incidents (%) par nom d'hôte (10, 20, 30, 40, 50) • Augmentation significative des incidents par nom d'hôte (10, 20, 30, 40, 50) • Augmentation significative des incidents (%) par utilisateur (10, 20, 30, 40, 50) • Augmentation significative des incidents par utilisateur (10, 20, 30, 40, 50) • Augmentation significative des incidents (%) par adresse IP source (10, 20, 30, 40, 50) • Augmentation significative des incidents par adresse IP source (10, 20, 30, 40, 50) • Augmentation significative des incidents (%) par modèle (10, 20, 30, 40, 50) • Augmentation significative des incidents par modèle (10, 20, 30, 40, 50)

Ajout des modèles de rapport de Control Manager 5

Les modèles de Control Manager 5 offrent une plus grande flexibilité pour la génération de rapports que les versions précédentes de modèles de Control Manager. Les modèles de Control Manager 5 accèdent directement à la base de données Control Manager, permettent aux utilisateurs de créer des rapports basés sur n'importe quelle information de la base de données de Control Manager.

Pour ajouter un modèle personnalisé de Control Manager 5, suivez les étapes suivantes :

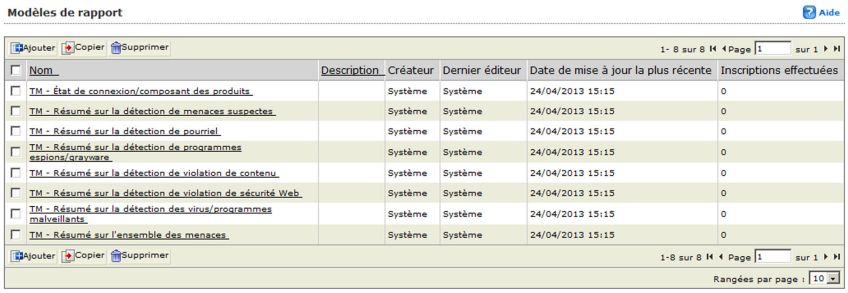
1. Accédez à l'écran Ajouter un modèle de rapport et nommez le modèle.
2. Spécifiez le composant du modèle à ajouter au modèle de rapport.
3. Spécifiez l'affichage des données pour le modèle.
4. Spécifiez les critères de requête pour le modèle.
5. Spécifiez les données devant apparaître dans le rapport et le dossier dans lequel les données doivent apparaître.
6. Terminez la création du modèle de rapport.

Étape 1 : Accédez à l'écran Ajouter un modèle de rapport et nommez le modèle.

Procédure

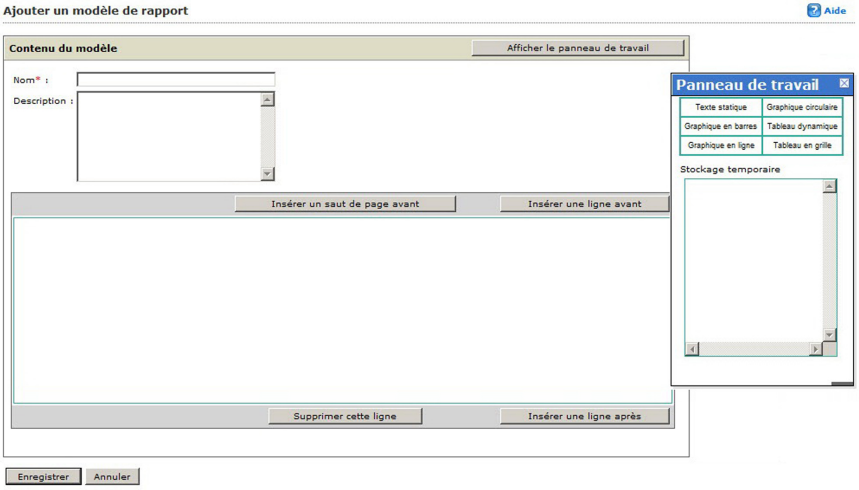
1. Accédez à **Rapports** > **Modèles de rapport**.

   L'écran **Modèles de rapport** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un modèle de rapport** apparaît.



3. Saisissez un nom pour le modèle de rapport dans le champ **Nom**.

4. Saisissez une description pour le modèle de rapport dans le champ **Description**.

Étape 2 : Spécifiez le composant du modèle à ajouter au modèle de rapport.

Procédure

1. Glissez un élément de modèle de rapport depuis le panneau de travail dans le modèle de rapport :
   - **Texte statique** : Texte que l'utilisateur insère dans le modèle. Il peut s'agir d'un résumé des informations contenues dans le rapport.
   - **Graphique circulaire** : les données du rapport s'affichent dans un graphique circulaire
   - **Graphique en barres** : les données du rapport s'affichent dans un graphique en barres
   - **Tableau dynamique** : les données du rapport s'affichent dans un tableau similaire à un tableau croisé dynamique
   - **Graphique en ligne** : les données du rapport s'affichent dans un graphique en ligne
   - **Tableau en grille** : les données du rapport s'affichent dans un tableau similaire à un tableau de requête ad hoc
2. Ajoutez des composants multiples pour que le rapport soit complet. Vous pouvez ajouter jusqu'à trois composants par page et 100 composants de rapport à un modèle de rapport.
3. Ajoutez des sauts de page et des lignes au modèle de rapport pour séparer les données ou les éléments du modèle de rapport.

Étape 3 : Spécifiez l'affichage des données pour le modèle

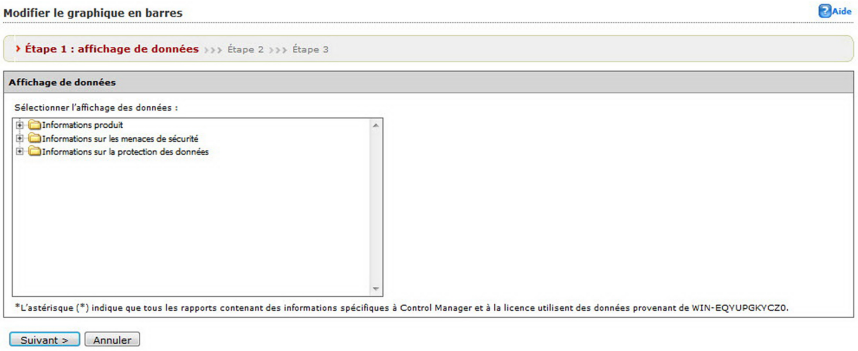
Procédure

1. Cliquez sur **Modifier** sur l'élément d'un modèle de rapport.

L'écran **Modifier <Élément d'un modèle de rapport> Étape 1 : Affichage des données** apparaît.

Remarque

Pour chaque composant autre que le texte statique, l'écran **Modifier <Élément d'un modèle de rapport> Étape 1 : Affichage des données** apparaît. Le lien **Modifier** dans le texte statique ouvre l'écran **Modifier le texte statique**.



2. Sélectionnez les données objets de la requête depuis la zone **Affichages de données**. Pour plus d'informations sur les affichages de données, consultez la section *Définition des affichages de données à la page 9-7*.

3. Cliquez sur **Suivant**.

   L'écran **Étape 2 : Définir le critère de requête** apparaît.

Étape 4 : Spécifiez les critères de requête pour le modèle

Remarque

Si vous ne spécifiez aucun critère de filtrage, le rapport renvoie tous les résultats pour les colonnes concernées. Trend Micro recommande de spécifier des critères de filtrage pour simplifier l'analyse des données après le renvoi des informations par le rapport.

Procédure

1. Sélectionnez **Critères personnalisés**.
2. Spécifiez les règles de filtrage des critères pour les catégories de données :
   - **Tous les critères** : cette sélection est équivalente à une fonction logique AND. Les données apparaissant dans le rapport doivent correspondre à tous les critères de filtrage.
   - **L'un des critères** : cette sélection est équivalente à une fonction logique OR. Les données apparaissant dans le rapport doivent correspondre à l'un des critères de filtrage.
3. Spécifiez les données, l'opérateur et les critères spécifiques à filtrer. Control Manager prend en charge jusqu'à 20 critères pour le filtrage des données.

Étape 5 : Spécifiez les données devant apparaître dans le rapport et l'ordre dans lequel les données doivent apparaître.

En fonction de la sélection pour l'élément du rapport, spécifiez les données à afficher dans les rapports :

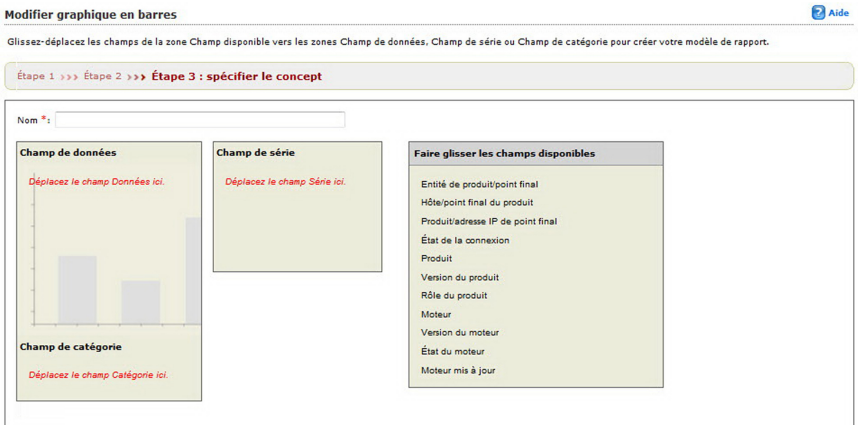
- Graphique en barres
- Graphique circulaire
- Tableau dynamique
- Tableau en grille
- Graphique en ligne

Configuration des paramètres des graphiques en barres

Procédure

1. Cliquez sur **Suivant**.

   L'écran **Étape 3 : Spécifier le concept** apparaît.



2. Saisissez un nom pour le graphique en barres dans le champ **Nom**.

3. Glissez les éléments de la liste **Faire glisser les champs disponibles** dans les zones suivantes :

   - **Champ de données** : spécifie les données apparaissant le long de l'axe vertical du graphique en barres
   - **Champ de série** : spécifie les données supplémentaires apparaissant le long de l'axe horizontal
   - **Champ de catégorie** : spécifie les données apparaissant le long de l'axe horizontal du graphique en barres

4. Spécifiez les propriétés des données du champ de données :

   a. Saisissez une étiquette pertinente pour le champ **Étiquette de la valeur**.

   b. Spécifiez la façon dont les données s'affichent pour le champ de données à partir de la liste **Regroupé par** :

      - **Nombre total d'instances** : Spécifie le décompte total du nombre d'incidents utilisé pour les résultats
      - **Nombre d'instances uniques** : Spécifie que seul le décompte des éléments distincts est utilisé pour les résultats
      - **Somme des valeurs**: Spécifie que la somme de toutes les valeurs du « décompte » de la colonne Affichage des données est utilisée pour les résultats

      Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Le **Nombre du décompte de lignes** est de 10, mais le Décompte distinct de lignes est de 1.

5. Spécifiez les propriétés de la catégorie du champ Catégorie :

   a. Saisissez un nom pertinent pour le champ **Nom de l'étiquette**.

   b. Spécifiez la façon dont les données doivent être classées dans le graphique à partir des listes de tri :

      - **Valeur de regroupement** : Trie les données en fonction des valeurs des données.

- **Nom de catégorie** : Trie les données par ordre alphabétique des noms de catégories.
- **Croissant** : Trie les données par ordre croissant.
- **Décroissant** : Trie les données par ordre décroissant.

c. Spécifiez le nom d'éléments affichés dans le champ de catégorie en sélectionnant **Filtrer le récapitulatif des résultats** et en spécifiant une valeur dans la zone de texte **Afficher le premier**. La valeur par défaut est 10.

d. Sélectionnez **Regrouper les éléments restants** pour placer tous les éléments restants dans le groupe « Autre » du graphique.

6. Spécifiez les propriétés de la série du champ Série :

a. Saisissez une étiquette pertinente pour le champ **Nom de l'étiquette**.

7. Cliquez sur **Enregistrer**.

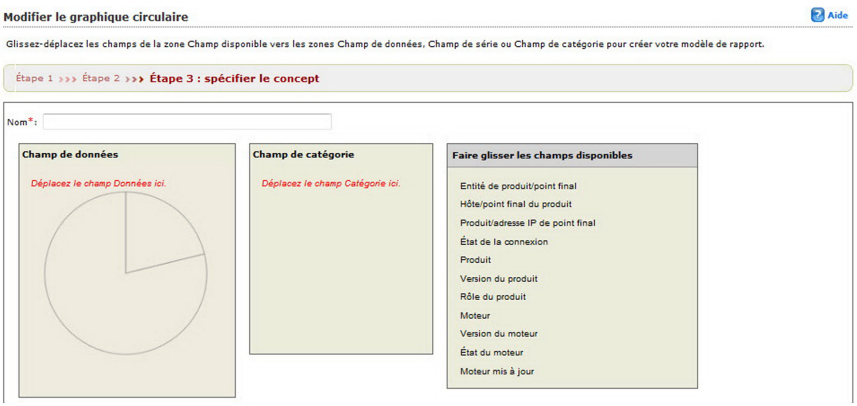
L'écran **Ajouter un modèle de rapport** apparaît.

Configuration des paramètres des graphiques circulaires

Procédure

1. Cliquez sur **Suivant**.

L'écran **Étape 3 : Spécifier le concept** apparaît.



2. Saisissez un nom pour le graphique circulaire dans le champ **Nom**.

3. Glissez les éléments de la liste **Faire glisser les champs disponibles** dans les zones suivantes :

   - **Champ de données** : Spécifie le décompte total de données apparaissant dans le graphique
   - **Champ Catégorie** : Spécifie la façon dont les données sont séparées dans le graphique

   Exemple : Pour obtenir un graphique affichant la répartition des virus à travers votre réseau, les champs de données représenteraient le nombre total de virus de votre réseau. Les champs de catégorie représenteraient la façon dont le nombre total de virus apparaît en pourcentage.

4. Spécifiez les propriétés des données du champ de données.

   a. Spécifiez la façon dont les données s'affichent pour le champ de données à partir de la liste Regroupé par :

      - **Nombre total d'instances** : Spécifie le décompte total du nombre d'incidents utilisé pour les résultats
      - **Nombre d'instances uniques** : Spécifie que seul le décompte des éléments distincts est utilisé pour les résultats

- **Somme des valeurs**: Spécifie que la somme de toutes les valeurs du « décompte » de la colonne Affichage des données est utilisée pour les résultats

Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Le Nombre du décompte de lignes est de 10, mais le Décompte distinct de lignes est de 1.

5. Spécifiez les propriétés de la catégorie du champ Catégorie :

   a. Saisissez une étiquette pertinente pour le champ **Nom de l'étiquette**.

   b. Spécifiez la façon dont les données doivent être classées dans le graphique à partir de la liste de tri :

      - **Valeur de regroupement** : Trie les données en fonction des valeurs des données.
      - **Nom de catégorie** : Trie les données par ordre alphabétique des noms de catégories.
      - **Croissant** : Trie les données par ordre croissant.
      - **Décroissant** : Trie les données par ordre décroissant.

   c. Spécifiez le nom d'éléments affichés dans le champ de catégorie en sélectionnant **Filtrer le récapitulatif des résultats** et en spécifiant une valeur dans la zone de texte **Afficher le premier**. La valeur par défaut est 10.

   d. Sélectionnez **Regrouper les éléments restants** pour placer tous les éléments restants dans le groupe « Autre » du graphique.

6. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un modèle de rapport** apparaît.

Configuration des paramètres des tableaux dynamiques

Procédure

1. Cliquez sur **Suivant**.

L'écran **Étape 3 : Spécifier le concept** apparaît.

2. Saisissez un nom pour le tableau dans le champ **Nom**.

3. Glissez les éléments de la liste Faire glisser les champs disponibles dans les zones suivantes :

   - **Champ de données** : Spécifie le décompte total de données apparaissant dans le tableau
   - **Champs de ligne** : Spécifie la façon dont les données sont séparées horizontalement dans le tableau
   - **Champs de colonne** : Spécifie la façon dont les données sont séparées verticalement dans le tableau

   Exemple : Olivia sélectionne l'affichage de données « Informations détaillées sur les virus/programmes malveillants ». Elle ne spécifie aucun critère de filtrage. Elle souhaite obtenir un tableau affichant les clients infectés, les virus infectant les clients et l'action entreprise par le produit géré contre les virus. Olivia glisse les champs suivants dans les champs Données, Ligne et Colonne :

   - Champ de données : Détections
   - Champs Ligne : Virus/programme malveillant et action
   - Champ Colonne : Hôte

4. Spécifiez les propriétés des données du champ de données :

   a. Saisissez un nom pour le **titre du champ Données**.

   b. Spécifiez la façon dont les données s'affichent pour le champ de données à partir de la liste Regroupé par :

      - **Nombre total d'instances** : Spécifie le décompte total du nombre d'incidents utilisé pour les résultats
      - **Nombre d'instances uniques** : Spécifie que seul le décompte des éléments distincts est utilisé pour les résultats
      - **Somme des valeurs**: Spécifie que la somme de toutes les valeurs du « décompte » de la colonne Affichage des données est utilisée pour les résultats

      Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Le Nombre du décompte de lignes est de 10, mais le Décompte distinct de lignes est de 1.

5. Spécifiez les propriétés de la ligne pour le champ Ligne.

   a. Saisissez un nom pour le **titre de la ligne**.

   b. Spécifiez la façon dont les données doivent être classées dans le tableau à partir de la liste de tri :

      - **Valeur de regroupement** : Trie les données en fonction des valeurs des données.
      - **Titre** : Trie les données par ordre alphabétique des noms des titres.
      - **Croissant** : Trie les données par ordre croissant.
      - **Décroissant** : Trie les données par ordre décroissant.

   c. Spécifiez le nombre d'éléments affichés dans les champs Ligne en sélectionnant **Filtrer le récapitulatif des résultats** et en spécifiant une valeur dans la zone de texte **Afficher le premier**. La valeur par défaut est 10.

   d. Sélectionnez **Regrouper les éléments restants** pour placer tous les éléments restants dans le groupe « Autre » du graphique.

6. Spécifiez les propriétés de la colonne du champ Colonne.

   a. Saisissez un nom pour le **titre de la colonne**.

   b. Spécifiez la façon dont les données doivent être classées dans le tableau à partir de la liste de tri :

      - **Valeur de regroupement** : Trie les données en fonction des valeurs des données.
      - **Titre** : Trie les données par ordre alphabétique des noms des titres.
      - **Croissant** : Trie les données par ordre croissant.
      - **Décroissant** : Trie les données par ordre décroissant.

   c. Spécifiez le nombre de colonnes affichées en sélectionnant **Filtrer la colonne** et en spécifiant une valeur dans la zone de texte **Afficher le premier**. La valeur par défaut est 10.

   d. Sélectionnez **Regrouper les éléments restants** pour placer tous les éléments restants dans le groupe « Autre » du graphique.

7. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un modèle de rapport** apparaît.

Configuration des paramètres des graphiques en ligne

Procédure

1. Cliquez sur **Suivant**.

   L'écran **Étape 3 : Spécifier le concept** apparaît.

2. Saisissez un nom pour le graphique en ligne dans le champ **Nom**.

3. Glissez les éléments de la liste Faire glisser les champs disponibles dans les zones suivantes :

   - **Champ de données** : Spécifie le décompte total de données apparaissant dans le tableau
   - **Champ de série** : Spécifie la façon dont les données sont séparées dans le graphique le long de l'axe vertical
   - **Champ de catégorie** : Spécifie la façon dont les données sont séparées dans le graphique le long de l'axe horizontal

   Exemple : Olivia sélectionne l'affichage de données « Informations détaillées sur les virus/programmes malveillants ». Elle ne spécifie aucun critère de filtrage. Elle souhaite obtenir un graphique affichant les infections de virus au cours du temps. Olivia glisse les champs suivants dans les champs Données, Série et Catégorie :

   - Champ de données : Détections
   - Champ Catégorie : Généré
   - Champ Série : Virus/programmes malveillants

4. Spécifiez les propriétés des données du champ de données.

   a. Saisissez une étiquette pertinente pour le champ **Étiquette de la valeur**.

b. Spécifiez la façon dont les données s'affichent pour le champ de données à partir de la liste Regroupé par :

- **Nombre total d'instances** : Spécifie le décompte total du nombre d'incidents utilisé pour les résultats
- **Nombre d'instances uniques** : Spécifie que seul le décompte des éléments distincts est utilisé pour les résultats
- **Somme des valeurs**: Spécifie que la somme de toutes les valeurs du « décompte » de la colonne Affichage des données est utilisée pour les résultats

Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Le Nombre du décompte de lignes est de 10, mais le Décompte distinct de lignes est de 1.

5. Spécifiez les propriétés de la catégorie du champ Catégorie :

a. Saisissez une étiquette pertinente pour le champ **Nom de l'étiquette**.

b. Spécifiez la façon dont les données doivent être classées dans le graphique à partir de la liste de tri :

- **Valeur de regroupement** : Trie les données en fonction des valeurs des données.
- **Nom de catégorie** : Trie les données par ordre alphabétique des noms de catégories.
- **Croissant** : Trie les données par ordre croissant.
- **Décroissant** : Trie les données par ordre décroissant.

c. Spécifiez le nom d'éléments affichés dans le champ de catégorie en sélectionnant **Filtrer le récapitulatif des résultats** et en spécifiant une valeur dans la zone de texte **Afficher le premier**. La valeur par défaut est 10.

d. Sélectionnez **Regrouper les éléments restants** pour placer tous les éléments restants dans le groupe « Autre » du graphique.

6. Spécifiez les propriétés de la série du champ Série :

a. Saisissez une étiquette pertinente pour le champ **Nom de l'étiquette**.

7. Cliquez sur **Enregistrer**.

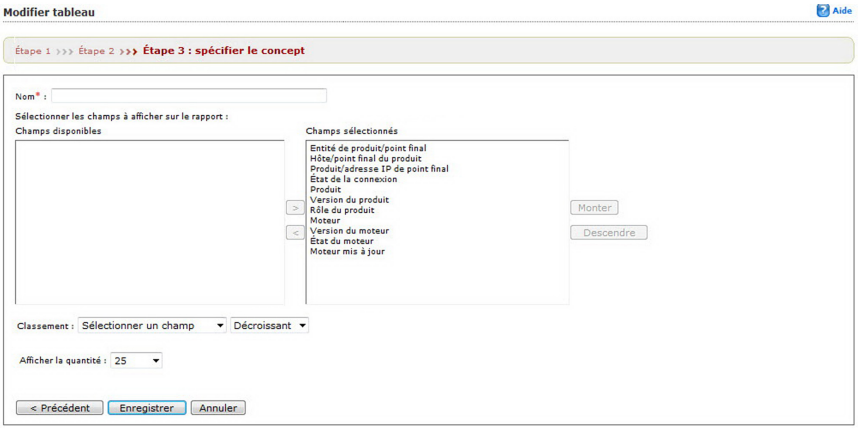
   L'écran **Ajouter un modèle de rapport** apparaît.

Configuration des paramètres des tableaux en grille

Procédure

1. Cliquez sur **Suivant**.

   L'écran **Étape 3 : Spécifier le concept** apparaît.



2. Saisissez un nom pour le tableau dans le champ **Nom**.
3. Spécifiez les colonnes devant apparaître dans les tableaux et leur ordre d'apparition.
4. Indiquez le mode de tri des colonnes.
5. Indiquez le nombre d'éléments à afficher dans le tableau.
6. Cliquez sur **Enregistrer**.

   L'écran **Ajouter un modèle de rapport** apparaît.

Étape 6 : Terminez la création du modèle de rapport

Procédure

1. Ajoutez ou supprimez les éléments de modèle de rapport selon vos besoins.
2. Cliquez sur **Enregistrer**.

Définition des rapports à usage unique

Les rapports à usage unique sont générés à la demande. La création de rapports à usage unique permet aux administrateurs de créer efficacement des rapports de type gestion pour leurs réseaux en cas d'épidémie.

Le tableau Rapport à usage unique comporte les éléments suivants :

TABLEAU 10-10. Liste des rapports à usage unique

ÉLÉMENT	DESCRIPTION
Nom	Indique le nom du rapport.
Description	Indique la description définie par l'utilisateur pour le rapport.
Période	Indique la plage de l'heure et de la date pour le rapport.
Heure de création	Indique à quel moment le rapport a été créé.
Heure de création	Indique à quel moment le rapport a été généré.
Format	Indique le format généré par le rapport (exemple : PDF, HTML, XML, CSV).
Taille	Indique la taille des rapports.
Affichage	Cliquez sur le lien Afficher correspondant au rapport pour l'afficher.

Ajout de rapports à usage unique

Control Manager prend en charge la génération de rapports à usage unique depuis les modèles de rapport de Control Manager 3 et 5. Les utilisateurs doivent créer des

modèles de rapport de Control manager 5 tandis que les modèles de rapport de Control Manager 3 ont été créés par Trend Micro. Le processus de création d'un rapport à usage unique est similaire pour tous les types de rapport et comprend les étapes suivantes :

1. Accédez à l'écran **Ajouter un rapport à usage unique** et sélectionnez le type de rapport.
2. Spécifiez le ou les produits à partir desquels les données du rapport seront générées.
3. Spécifiez la date à laquelle le ou les produits ont généré les données.
4. Spécifiez le destinataire du rapport.

Étape 1 : Accédez à l'écran Ajouter un rapport à usage unique et sélectionnez le type de rapport.

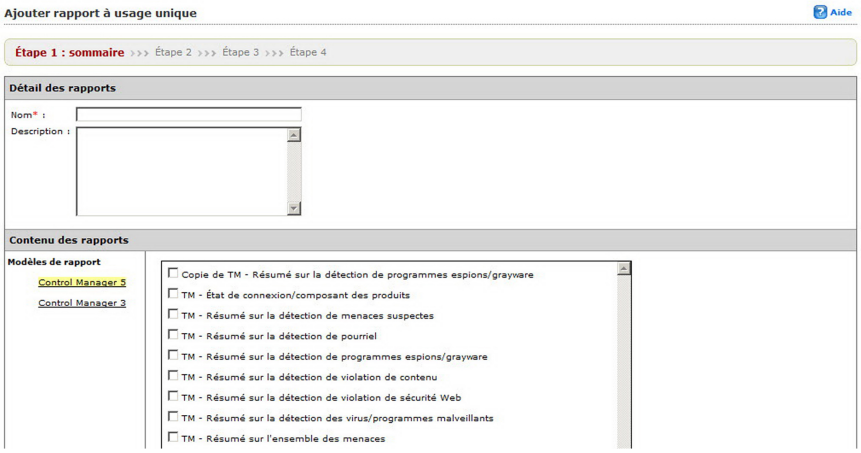
Procédure

1. Accédez à **Rapports** > **Rapports à usage unique**.

   L'écran **Rapports à usage unique** apparaît.

2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un rapport à usage unique > Étape 1 : Sommaire** apparaît.



3. Tapez un nom pour le rapport dans le champ **Nom**, sous Détails des rapports.

4. Tapez une description pour le rapport dans le champ **Description**, sous Détails des rapports.

5. Sélectionnez le modèle de Control Manager pour générer le rapport :

   - **Modèles de rapport de Control Manager 5** :

     a. Sélectionnez le modèle de Control Manager 5 pour générer le rapport. Si les rapports existants ne répondent pas à vos attentes, créez-en un nouveau à partir de l'écran **Modèles de rapport**. Consultez la rubrique *Ajout des modèles de rapport de Control Manager 5 à la page 10-19* pour obtenir plus d'informations.

   - **Modèles de rapport de Control Manager 3** :

     a. Cliquez sur **Control Manager 3** sous Contenu des rapports. Les modèles de Control Manager 3 apparaissent dans la zone de travail de droite, sous Contenu des rapports.

     b. Sélectionnez la catégorie de rapport sur laquelle baser le rapport.

     c. Sélectionnez les données du modèle de Control Manager 3 sur lesquelles baser le modèle.

6. Sélectionnez le format de génération du rapport.

   - **Formats de rapport de Control Manager 5** :
     - Format Adobe PDF (*.pdf)
     - Format HTML (*.html)
     - Format XML (*.xml)
     - Format CSV (*.csv)
   - **Formats de rapport de Control Manager 3** :
     - Format RTF (*.rtf)
     - Format Adobe PDF (*.pdf)
     - ActiveX
     - Format Crystal Report (*.rpt)

7. Cliquez sur **Suivant**.

   L'écran **Ajouter un rapport à usage unique > Étape 2 : Cibles** apparaît.

Étape 2 : Spécifiez le ou les produits à partir desquels les données du rapport sont générées.

Procédure

1. Sélectionnez le produit géré ou le répertoire à partir duquel Control Manager recueille les informations du rapport.
2. Si le rapport contient des données provenant d'un appareil Network VirusWall Enforcer, spécifiez les clients à partir desquels les rapports doivent être générés :
   - **Tous les clients** : rapports générés depuis tous les appareils Network VirusWall Enforcer
   - **Plage IP** : rapports générés à partir d'une plage d'adresses IP spécifique
   - **Segment** : rapports générés à partir d'un segment de réseau spécifique
3. Cliquez sur **Suivant**.

   L'écran **Ajouter un rapport à usage unique > Étape 3 : Période** apparaît.

Étape 3 : Spécifiez la date à laquelle le ou les produits ont généré les données :

Procédure

1. Spécifiez la date de génération des données :

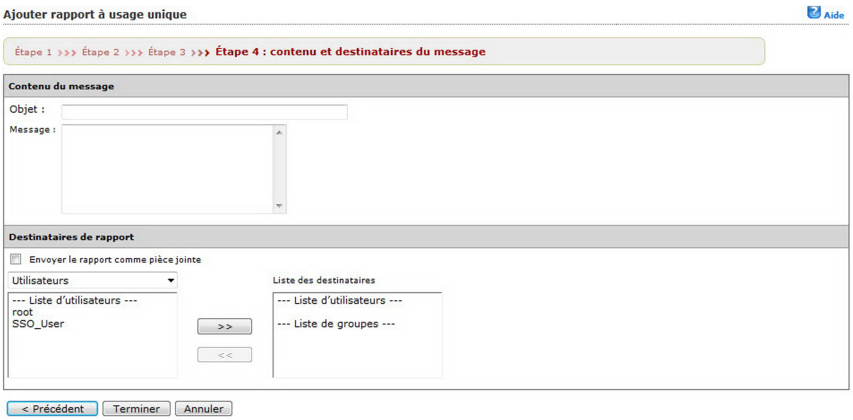
- À partir de la liste déroulante, sélectionnez l'un des éléments suivants :
  - Toutes les dates
  - Dernières 24 heures
  - Aujourd'hui
  - 7 derniers jours
  - 14 derniers jours
  - 30 derniers jours
- Spécifiez une plage de date :
  - Saisissez une date dans le champ **De**.
  - Spécifiez une heure dans les champs **hh** et **mm**.
  - Saisissez une date dans le champ **À**.
  - Spécifiez une heure dans les champs **hh** et **mm**.

Remarque

Cliquez sur l'icône du calendrier située près des champs **De** et **À** afin d'utiliser un calendrier dynamique pour spécifier la plage de date.

2. Cliquez sur **Suivant**.

   L'écran **Ajouter un rapport à usage unique > Étape 4 : Contenu et destinataires du message** apparaît.



Étape 4 : Spécifiez le destinataire du rapport :

Procédure

1. Tapez un titre pour le message électronique contenant le rapport dans le champ **Objet**.
2. Saisissez une description pour le rapport dans le champ **Message**.
3. Sélectionnez **Envoyer le rapport comme pièce jointe** pour envoyer le rapport à un destinataire particulier.
4. Spécifiez les utilisateurs ou les groupes dans la liste **Destinataires de rapport**.
5. Sélectionnez les utilisateurs/groupes qui recevront le rapport et cliquez sur le bouton **>>**.
6. Cliquez sur **Terminer** après avoir sélectionné tous les utilisateurs/groupes qui recevront le rapport.

Définition des téléchargements programmés

Les rapports programmés sont générés sur la base d'une programmation spécifiée par l'utilisateur. La création de rapports programmés permet aux administrateurs de créer efficacement des rapports de type gestion pour leurs réseaux lors d'un fonctionnement normal.

Le tableau Rapports programmés comporte les éléments suivants :

TABLEAU 10-11. Liste des rapports programmés

ÉLÉMENT	DESCRIPTION
Nom	Indique le nom du rapport.
Description	Indique la description définie par l'utilisateur pour le rapport.
Fréquence	Indique la fréquence à laquelle le rapport est généré.
Heure de création	Indique à quel moment le rapport a été créé.
Heure de création la plus récente	Indique à quel moment le rapport a été généré pour la dernière fois.
Prochaine programmation	Affiche le moment de la génération du rapport suivant
Historique	Cliquez sur le lien Afficher correspondant au rapport pour l'afficher.
Activer	Indique l'état du rapport (activé ou désactivé).

Ajout de rapports programmés

Control Manager prend en charge la génération de rapports programmés depuis les modèles de rapport de Control Manager 3 et 5. Les utilisateurs doivent créer des modèles de rapport de Control manager 5 tandis que les modèles de rapport de Control Manager 3 ont été créés par Trend Micro. Le processus de création d'un rapport programmé est le même pour tous les types de rapport :

1. Accédez à l'écran **Ajouter un rapport programmé** et sélectionnez le type de rapport.

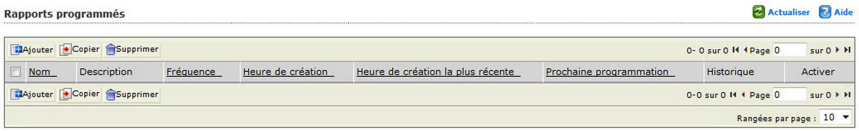
2. Spécifiez le ou les produits à partir desquels les données du rapport seront générées.
3. Spécifiez la date à laquelle le ou les produits ont généré les données.
4. Spécifiez le destinataire du rapport.

Étape 1 : Accédez à l'écran Ajouter un rapport programmé et sélectionnez le type de rapport

Procédure

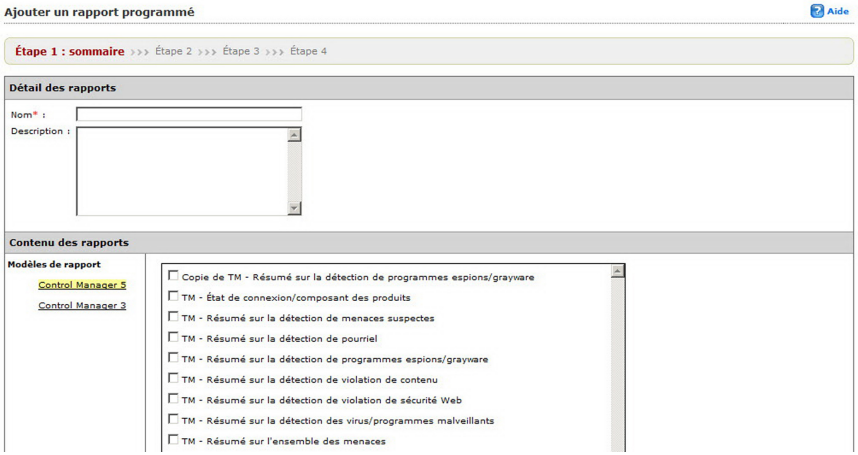
1. Accédez à **Rapports** > **Rapports programmés**.

   L'écran **Rapports programmés** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un rapport programmé > Étape 1 : Sommaire** apparaît.



3. Saisissez un nom pour le rapport dans le champ **Nom**.

4. Saisissez une description pertinente pour le rapport dans le champ **Description**.

5. Sélectionnez le modèle de Control Manager pour générer le rapport :

   - Modèles de rapport de Control Manager 5 :

     a. Sélectionnez le modèle de Control Manager 5 pour générer le rapport. Si les rapports existants ne répondent pas à vos attentes, créez-en un nouveau à partir de l'écran Modèles de rapport. Consultez la rubrique *Ajout des modèles de rapport de Control Manager 5 à la page 10-19* pour obtenir plus d'informations.

   - Modèles de rapport de Control Manager 3 :

     a. Cliquez sur **Control Manager 3** sous Contenu des rapports. Les modèles de Control Manager 3 apparaissent dans la zone de travail de droite, sous Contenu des rapports.

     b. Sélectionnez la catégorie de rapport sur laquelle baser le rapport.

     c. Sélectionnez les données du modèle de Control Manager 3 sur lesquelles baser le modèle.

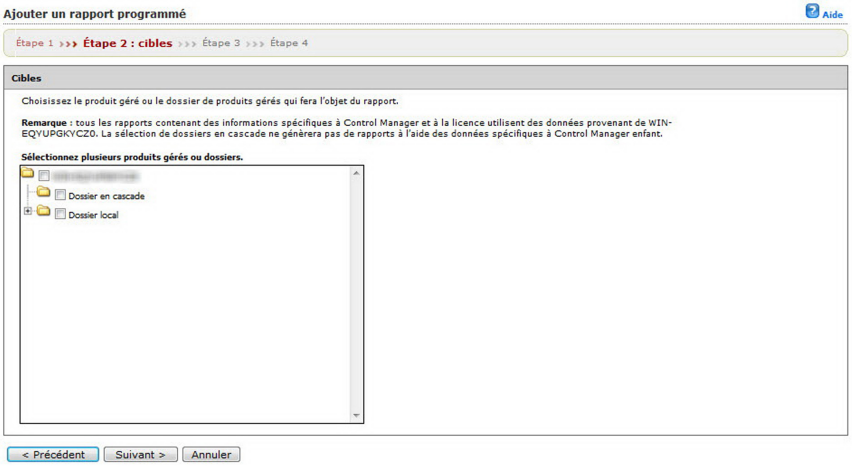
6. Sélectionnez le format de génération du rapport.

   - Formats de rapport de Control Manager 5 :
     - Format Adobe PDF (*.pdf)
     - Format HTML (*.html)
     - Format XML (*.xml)
     - Format CSV (*.csv)
   - Formats de rapport de Control Manager 3 :
     - Format RTF (*.rtf)
     - Format Adobe PDF (*.pdf)
     - ActiveX

- Format Crystal Report (*.rpt)

7. Cliquez sur **Suivant**.

   L'écran **Ajouter un rapport programmé > Étape 2 : Cibles** apparaît.



Étape 2 : Spécifiez le ou les produits à partir desquels les données du rapport sont générées

Procédure

1. Sélectionnez le produit géré ou le répertoire à partir duquel Control Manager recueille les informations du rapport.

2. Si le rapport contient des données provenant d'un appareil Network VirusWall Enforcer, spécifiez les clients à partir desquels les rapports doivent être générés :

   - **Tous les clients** : rapports générés depuis tous les appareils Network VirusWall Enforcer
   - **Plage IP** : rapports générés à partir d'une plage d'adresses IP spécifique
   - **Segment** : rapports générés à partir d'un segment de réseau spécifique

3. Cliquez sur **Suivant**.

   L'écran **Ajouter un rapport à usage unique > Étape 3 : Fréquence** s'affiche.

Étape 3 : Spécifiez la date à laquelle le ou les produits ont généré les données

Procédure

1. Spécifiez la fréquence de génération des rapports :

   - **Quotidien** : les rapports seront générés tous les jours.
   - **Hebdomadaire** : les rapports seront générés une fois par semaine au jour spécifié.
   - **Bihebdomadaire** : les rapports seront générés toutes les deux semaines au jour spécifié.
   - **Mensuel** : les rapports sont générés tous les mois : le 1er, le 15 ou le dernier jour du mois.

2. Spécifiez la plage de date :

   - **Les rapports incluent les données comprises jusqu'à l'heure Démarrer la programmation spécifiée ci-dessous** : Cela signifie qu'un rapport peut

avoir jusqu'à 23 heures de données supplémentaires contenues dans le rapport. Si les conséquences sont moindres pour des rapports hebdomadaires ou mensuels, il en est autrement pour un rapport quotidien qui peut contenir près de deux jours de données en fonction de l'heure Démarrer la programmation.

- **Les rapports incluent les données comprises jusqu'à 23 h 59 min 59 s du jour précédent** : Cela signifie que la collecte de données pour le rapport s'arrête juste avant minuit. Les rapports s'appuient sur une période exacte (par exemple : les rapports quotidiens sont de 24 heures), mais ne contiennent pas les données les plus récentes.

3. Spécifiez l'heure et la date de démarrage du rapport :

- **Immédiatement** : La programmation du rapport démarre immédiatement après avoir activé le rapport.
- **Heure de début** : la programmation du rapport démarre à la date et à l'heure spécifiées dans les champs correspondants.

a. Saisissez une date dans le champ **dd/mm/yyyy**.

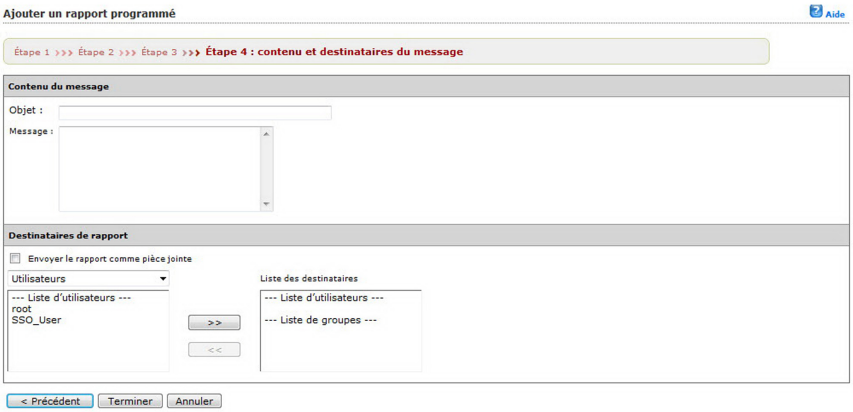
b. Spécifiez une heure dans les champs **hh** et **mm**.

Remarque

Cliquez sur l'icône du calendrier située près du champ **dd/mm/yyyy** afin d'utiliser un calendrier dynamique pour spécifier la plage de date.

4. Cliquez sur **Suivant**.

L'écran **Ajouter un rapport programmé > Étape 4 : Contenu et destinataires du message** apparaît.



Étape 4 : Spécifiez le destinataire du rapport

Procédure

1. Tapez un titre pour le message électronique contenant le rapport dans le champ **Objet**.
2. Saisissez une description pour le rapport dans le champ **Message**.
3. Sélectionnez **Envoyer le rapport comme pièce jointe** pour envoyer le rapport à un destinataire particulier.
4. Spécifiez les utilisateurs ou les groupes dans la liste **Destinataires de rapport**.
5. Sélectionnez les utilisateurs/groupes qui recevront le rapport et cliquez sur le bouton **>>**.
6. Cliquez sur **Terminer** après avoir sélectionné tous les utilisateurs/groupes qui recevront le rapport.

Activation/Désactivation des rapports programmés

Par défaut, Control Manager active les profils programmés dès la création. Si vous avez désactivé un profil (en cas de migration de la base de données ou d'un agent, par exemple), vous pouvez le réactiver en passant par l'écran **Rapports programmés**.

Procédure

1. Accédez à **Rapports** > **Rapports programmés**.

   L'écran **Rapports programmés** apparaît.

2. Cliquez sur l'icône activé ()/désactivé () dans la colonne Activer du tableau Rapports programmés.

   Une icône désactivé/activé apparaît dans la colonne.

Affichage des rapports générés

En plus d'envoyer des rapports en pièce jointe, vous pouvez afficher les rapports générés à partir de l'une de ces zones :

- Rapports à usage unique
- Rapports programmés

Affichage des rapports à usage unique

Procédure

1. Accédez à l'écran **Rapport** > **Rapport à usage unique**.

   L'écran **Rapports à usage unique** apparaît.

2. Cliquez sur le lien du rapport que vous souhaitez afficher dans la colonne Afficher.

Affichage des rapports programmés

Procédure

1. Accédez à **Rapports** > **Rapports programmés**.

   L'écran **Rapports programmés** apparaît.

2. Cliquez sur le lien du rapport que vous souhaitez afficher dans la colonne **Historique**.

   L'écran **Historique des rapports programmés** pour ce rapport s'affiche.

3. Sélectionnez le rapport à afficher à partir de l'écran **Historique des rapports programmés**.

Configuration de la maintenance des rapports

Configurez les paramètres de maintenance des rapports pour supprimer les rapports.

Procédure

1. Accédez à **Rapports** > **Maintenance des rapports**.

   L'écran **Maintenance des rapports** apparaît.

2. Spécifiez le nombre maximal de rapports à usage unique et de rapports programmés à conserver.

3. Cliquez sur **Enregistrer**.

Définition de Mes rapports

L'écran **Mes rapports** contient tous les rapports créés par un utilisateur particulier (et les groupes auxquels l'utilisateur appartient). Pour chaque utilisateur qui se connecte à Control Manager, l'écran affiche uniquement les rapports générés par l'utilisateur en question (ou le groupe auquel l'utilisateur appartient).

L'écran **Mes rapports** affiche les éléments suivants :

TABLEAU 10-12. Liste Mes rapports

ÉLÉMENT	DESCRIPTION
Nom	Nom du rapport généré.
Période	Heure et date de création du rapport.
Heure d'envoi	Heure à laquelle le rapport a été lancé.
Heure de création	Heure de création du rapport.
Format	Format utilisé pour la création du rapport (par exemple, pdf ou xml).
Taille	Taille du rapport créé.
Affichage	Cliquez sur le lien correspondant dans la ligne pour afficher le rapport.

Partie III

Administration de Control Manager

Chapitre 11

Agents MCP et Control Manager

Ce chapitre présente le matériel dont disposent les administrateurs pour comprendre les agents qui permettent à Control Manager de gérer le réseau.

Ce chapitre traite les rubriques suivantes :

Définition des agents

Control Manager 5.0/5.5 utilise les agents MCP et Control Manager 2.x pour gérer les produits sur le réseau Control Manager :

- Control Manager Agent (version 2.51 ou ultérieure) : les versions antérieures de produits Trend Micro requièrent cet agent, conçu selon l'architecture de Control Manager 2.5/3.0.
- Agent MCP (Trend Micro Management Communication Protocol) : Dernière génération d'agents Trend Micro prenant en charge les fonctions de sécurité avancée, le système SSO, les modes de communication unidirectionnelle et bidirectionnelle, ainsi que les nœuds de cluster.

Le tableau suivant répertorie les fonctions prises en charge par les agents Control Manager 2.x et MCP.

TABLEAU 11-1. Comparaison des agents

FONCTION	AGENTS MCP	AGENTS CONTROL MANAGER 2.X
Outbreak Prevention Services (OPS)	●	●
Système de signature unique (SSO)	●	
Communications en mode unidirectionnel et bidirectionnel	●	
Prise en charge du mode NAT	●	
Prise en charge de nœuds de cluster	●	
Interrogation de Control Manager par l'agent pour obtenir des mises à jour et des commandes	●	
Réenregistrement sur le serveur Control Manager en cas de corruption ou de suppression de la base de données de l'agent	N/A (ce problème ne survient pas avec les agents MCP)	Automatique au bout de 8 heures

Fonction	Agents MCP	Agents Control Manager 2.x
Sécurité des communications	HTTPS/HTTP	Chiffrement avec authentification facultative
Communicateurs		●
Prise en charge des états actif et inactif	●	●
Battement de cœur du communicateur/de l'agent	●	●
Notification : Expiration du fichier de signatures de virus	●	●
Notification : Agent non autorisé à mettre à jour les composants	●	●
Notification : Agent non autorisé à déployer les composants	●	●
Notification : Service produit arrêté	●	●

Chaque produit géré possède son propre agent, chargé des tâches suivantes :

Tableau 11-2. Comparaison des agents MCP et 2.x

Agents MCP	Agents 2.x
Commandes d'interrogation pour le produit géré émises par le serveur Control Manager	Réception des commandes du serveur Control Manager via le communicateur
Collecte de l'état et des journaux des produits gérés, et envoi de ces données au serveur Control Manager via HTTPS ou HTTP	Collecte de l'état et des journaux des produits gérés, et envoi de ces données au serveur Control Manager via le communicateur

Définition d’un communicateur

Le communicateur, ou infrastructure d’acheminement des messages, constitue la dorsale de communication pour les anciens produits gérés et Control Manager. Ce composant de l'infrastructure Trend Micro Management Infrastructure (TMI) gère l'ensemble des communications entre le serveur Control Manager et les produits gérés pour les anciens produits. Les communicateurs interagissent avec Control Manager pour communiquer avec les anciens produits gérés.

Si vous installez l'agent Control Manager 2.5 sur un serveur de produits gérés, vous pouvez utiliser cette application pour administrer les produits avec Control Manager. 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.

Le programme d’installation de Control Manager vérifie si le communicateur est déjà disponible sur le serveur de produits gérés. S’il l’est, aucune autre instance du communicateur n’est installée. En effet, les agents d’un serveur de produits partagent le même communicateur. Le communicateur est chargé de :

- sécuriser les messages, au moyen des fonctions de chiffrement et de protection contre la retransmission fournies par la bibliothèque OpenSSL, ainsi que de l’authentification de bout en bout développée par Trend Micro ;
- recevoir les commandes en provenance du serveur Control Manager et les transmettre au produit géré ;
- recevoir les informations d'état émanant des produits gérés et les transmettre au serveur Control Manager.

Les descriptions ci-dessus mettent en lumière les points suivants :

- Si TMI peut exister de manière autonome, les produits gérés, eux, ne peuvent fonctionner en l'absence d'un communicateur.
- Bien qu'il puisse exister autant d'agents que de produits gérés sur un serveur, un seul communicateur est requis par serveur.
- Plusieurs produits gérés peuvent partager les fonctions d’un communicateur.

Définition des icônes d'état de la connexion

Les produits gérés, les communicateurs et les serveurs enfants de Control Manager utilisent les icônes suivantes pour indiquer l'état de leur connexion :

TABLEAU 11-3. ICÔNES D'ÉTAT DES PRODUITS GÉRÉS

DESCRIPTION DE L'ÉTAT DE LA CONNEXION	PRODUIT GÉRÉ	
Le service produit est en cours d'exécution		
Le service produit n'est pas en cours d'exécution		
Le service TMI n'est pas en cours d'exécution		Dans la limite du temps de retard maximum de battement de cœur
		Au-delà de la limite du temps de retard maximum de battement de cœur
Le socket ou la connexion réseau entre le communicateur et le produit géré est interrompu(e)		
Impossible de résoudre le nom DNS entre le communicateur et le serveur Control Manager		Dans la limite du temps de retard maximum de battement de cœur
		Au-delà de la limite du temps de retard maximum de battement de cœur

TABLEAU 11-4. ICÔNES D'ÉTAT DES COMMUNICATEURS

DESCRIPTION DE L'ÉTAT DE LA CONNEXION	COMMUNICATEURS
Le service TMI est en cours d'exécution	

DESCRIPTION DE L'ÉTAT DE LA CONNEXION	COMMUNICATEURS	
Le service TMI n'est pas en cours d'exécution		Dans la limite du temps de retard maximum de battement de cœur
		Au-delà de la limite du temps de retard maximum de battement de cœur
Mode inactif après exécution du Programmateur d'agent/de communicateur		
Le socket ou la connexion réseau entre le communicateur et le produit géré est interrompu(e)		
Impossible de résoudre le nom DNS entre le communicateur et le serveur Control Manager		

TABLEAU 11-5. Icônes d'état des serveurs enfants

DESCRIPTION DE L'ÉTAT DE LA CONNEXION	ENFANT	
Le service TMI n'est pas en cours d'exécution	État non modifié	Dans la limite du temps de retard maximum de battement de cœur
		Au-delà de la limite du temps de retard maximum de battement de cœur
Le service du serveur enfant (Casprocessor.exe) est en cours d'exécution		
Casprocessor.exe ou le communicateur du serveur enfant n'est pas en cours d'exécution Soit le serveur enfant est arrêté, soit le service du communicateur est désactivé		

DESCRIPTION DE L'ÉTAT DE LA CONNEXION	ENFANT
Le serveur enfant a été désactivé depuis la console Web du serveur parent	

Définition des niveaux de sécurité de Control Manager

Control Manager propose trois niveaux de sécurité pour la communication entre le serveur, d'un côté, et les produits gérés et les serveurs enfants, de l'autre, aussi bien pour les anciens agents que pour les agents MCP. Pour les agents MCP, le niveau de sécurité s'applique aux dossiers virtuels d'IIS. Il existe trois différents niveaux : élevé, moyen et normal.

- Élevé : Indique que Control Manager communique uniquement à l'aide de HTTPS.
- Moyen : Control Manager utilise HTTPS pour communiquer, s'il est disponible ; si ce n'est pas le cas, il utilise HTTP.
- Normal : Control Manager utilise le protocole HTTP pour communiquer.

Les comportements correspondant aux différents niveaux de sécurité sont décrits ci-dessous :

FONCTIONS	NIVEAU DE SÉCURITÉ		
	ÉLEVÉ	MOYEN	NORMAL
Accès à l'interface graphique avec HTTPS uniquement	●	●	
Accès à l'interface graphique avec HTTPS et HTTP			●
Redirection vers l'interface graphique du produit avec HTTPS ou HTTP	●	●	●

FONCTIONS	NIVEAU DE SÉCURITÉ		
	ÉLEVÉ	MOYEN	NORMAL
Intégration aux produits compatibles HTTPS uniquement (MCP)	●		
Intégration aux produits compatibles HTTPS et HTTP		●	●
Téléchargement des mises à jour par les produits à partir de Control Manager avec HTTP ou HTTPS	●	●	●

Selon le niveau de sécurité des agents plus anciens, Control Manager fournit les fonctions de chiffrement et d'authentification suivantes :

- Chiffrement SSL au niveau paquet : Control Manager applique le chiffrement SSL (Secure Socket Layer) au niveau paquet, quel que soit le niveau de sécurité. Le chiffrement SSL au niveau paquet est un protocole développé par Netscape en vue de sécuriser les transactions via le Web. SSL a recours à une forme de chiffrement avec clé publique : le navigateur peut encoder les informations au moyen d'une clé publique disponible librement, mais seuls les utilisateurs connaissant la clé privée correspondante peuvent décoder ces données.

  Les agents Control Manager peuvent chiffrer leurs communications au moyen d'une clé publique. Le serveur Control Manager utilise alors une clé privée pour déchiffrer le message de l'agent.

- Authentification Trend Micro : Control Manager applique l'authentification Trend Micro au niveau de sécurité 5 (Élevé).

  Lorsque le niveau élevé est employé, Control Manager commence par appliquer le chiffrement SSL au niveau paquet, puis renforce le chiffrement à l'aide de l'authentification Trend Micro.

Remarque

Il est possible de modifier le niveau de sécurité de Control Manager par le biais du fichier TMI.cfg. Cela implique toutefois la modification de tous les fichiers TMI.cfg présents sur le réseau Control Manager. Cela comprend le fichier TMI.cfg du serveur Control Manager et celui de tous les produits gérés et serveurs enfants. Sinon, la communication entre le serveur et les agents ne fonctionnera pas.

TABLEAU 11-6. Comportement des niveaux de sécurité pour les anciens agents

NIVEAU DE SÉCURITÉ (FIGURANT DANS TMI.CFG)	SÉLECTION DU NIVEAU DE SÉCURITÉ (PENDANT L'INSTALLATION)	AUTHENTIFICATION DE BOUT EN BOUT	CHIFFREMENT AU NIVEAU MESSAGE
1	Faible	N/A	40 bits (RC4)
2	Moyen	N/A	128 bits (RC4)
5	Élevé	Authentification Trend Micro	128 bits (RC4 + 3DES)

Utilisation du Programmateur de communication des agents

La programmation de communication d'agent détermine les périodes pendant lesquelles l'agent envoie des informations au serveur Control Manager, ce qui vous permet de gérer le flux des informations.

Le programme d'installation de l'agent Control Manager attribue une programmation de communication par défaut, mais vous pouvez la modifier en fonction des besoins de votre réseau Control Manager. Le Programmateur de communication d'agent suit une configuration quotidienne, ce qui signifie qu'il applique la programmation à un agent quotidiennement. Il n'est pas possible de définir des heures d'activité hebdomadaires ou mensuelles.

Lorsque vous configurez une programmation, elle s'applique à tous les produits gérés enregistrés sur Control Manager.

Remarque

Lorsqu'un agent est inactif en mode de prévention des épidémies, les produits gérés correspondants continuent d'exécuter les commandes Outbreak Prevention Services sans en communiquer les résultats à Control Manager. Par conséquent, Control Manager ne connaît ni l'état ni les résultats. La fonction de suivi des commandes répertorie les résultats des commandes liées à la stratégie de prévention des épidémies sous la catégorie Échec.

Les programmations d'inactivité et d'activité de la communication d'agent ne s'appliquent qu'aux agents des produits gérés. Vous ne pouvez pas définir de programmation d'inactivité pour les serveurs enfants de Control Manager 3.5.

Remarque

La programmation de communication d'agent répertorie les agents des serveurs enfants.

Définition du battement de cœur du communicateur/de l'agent

Le battement de cœur fait référence au message que l'agent MCP ou Control Manager 2.x envoie au serveur Control Manager pour lui signaler qu'il est actif. L'agent fournit ce mécanisme afin de déterminer si les produits gérés restent actifs.

Remarque

Utilisez l'écran Programmateur de communication d'agent pour définir les heures d'activité et d'inactivité du battement de cœur.

L'agent interroge le serveur Control Manager à intervalles réguliers pour s'assurer que la console Control Manager affiche les dernières informations et pour vérifier le bon fonctionnement de la connexion entre les produits gérés et le serveur.

Voici les trois états possibles du battement de cœur :

- **Actif** : correspond à l'heure d'activité.
- **Inactif** : heure d'inactivité ou en dehors de l'heure d'activité.

- **Anormal** : déconnecté.

Pour plus de détails, consultez la section *Définition des icônes d'état de la connexion à la page 11-5*.

Remarque

Outre un battement de cœur périodique, l'agent envoie également au serveur Control Manager des informations en temps réel sur l'état des produits gérés.

Battement de cœur MCP

Pour surveiller l'état des produits gérés, les agents MCP interrogent Control Manager selon une programmation définie. L'interrogation permet d'indiquer l'état du produit géré et de vérifier si Control Manager a émis des commandes à destination du produit géré. La console Web de Control Manager présente ensuite l'état du produit. En d'autres termes, l'état du produit ne reflète pas l'état du réseau en temps réel. Control Manager vérifie l'état de chaque produit géré de façon séquentielle et en arrière-plan, et définit l'état sur «hors ligne» lorsqu'un délai fixé s'écoule sans qu'un battement de cœur ne soit reçu du produit géré.

Outre les battements de cœur, il existe d'autres moyens pour Control Manager de déterminer l'état des produits gérés, Les éléments suivants fournissent également à Control Manager l'état du produit géré :

- Control Manager reçoit les journaux des produits gérés. Le simple fait que Control Manager reçoive ces journaux indique que les produits gérés correspondants fonctionnent.
- En mode de communication bidirectionnel, Control Manager envoie un message de notification afin d'obliger le produit géré à récupérer la commande en attente. Si le serveur parvient à se connecter au produit géré, cela indique que ce dernier fonctionne correctement et l'événement est considéré comme un battement de cœur.
- En mode de communication unidirectionnel, l'agent MCP envoie régulièrement des commandes de requête à Control Manager. Ce comportement périodique fonctionne de la même manière qu'un battement de cœur et est considéré comme tel par Control Manager.

Les battements de cœur MCP sont envoyés de deux manières :

- **UDP** : si le produit parvient à contacter le serveur via le protocole UDP, cette solution est la plus légère et la plus rapide. Toutefois, elle ne fonctionne pas dans les environnements NAT ou dotés de pare-feu. De plus, le client émetteur ne peut vérifier que le serveur reçoit bien la requête.
- **HTTP/HTTPS** : dans un environnement NAT ou doté d'un pare-feu, une connexion HTTP plus lourde peut être utilisée pour transférer le battement de cœur.

Control Manager prend en charge les protocoles UDP et HTTP/HTTPS pour acheminer les battements de cœur. Le serveur Control Manager détecte le mode applicable au produit géré au cours du processus d'enregistrement. Un protocole de transfert distinct a lieu entre les deux parties en vue de déterminer le mode adéquat.

Outre les battements de cœur indiquant l'état du produit géré, celui-ci transmet d'autres données à Control Manager. Ces données contiennent généralement des informations concernant l'activité du produit géré à afficher sur la console.

Utilisation de la barre de programmation

La barre de programmation qui figure dans l'écran **Programmation de la communication des agents** permet d'afficher et de définir les programmations des communicateurs. Cette barre comporte 24 intervalles, représentant les heures de la journée.

Les intervalles comportant des icônes d'horloge indiquent un état actif ou les heures pendant lesquelles l'agent/le communicateur envoie des informations au serveur Control Manager. Les intervalles blancs indiquent les périodes inactives. Pour définir les heures d'activité et d'inactivité, il vous suffit de changer les intervalles appropriés en cliquant dessus.

Vous ne pouvez définir que trois périodes d'inactivité consécutives au maximum. La barre de programmation ci-dessous n'indique que deux heures d'inactivité :

FIGURE 11-1. Barre de programmation

Les périodes d'activité indiquées vont de minuit à 7:00, de 8:00 à 16:00:00 et de 18:00 à minuit.

Définition du battement de cœur approprié

Lorsque vous définissez la fréquence du battement de cœur, choisissez une valeur qui vous permette d'afficher l'état le plus récent du produit géré tout en gérant les ressources système dans les meilleurs délais. Les paramètres par défaut conviennent à la plupart des situations. Toutefois, si vous devez personnaliser cette configuration, tenez compte des points suivants :

TABLEAU 11-7. Battements de cœur recommandés

FRÉQUENCE DES BATTEMENTS DE CŒUR	RECOMMANDATION
Battements de cœur à intervalle long (supérieur à 60 minutes)	Plus l'intervalle est grand entre les battements de cœur, plus le nombre d'événements susceptibles de se produire avant que Control Manager reflète l'état du communicateur dans la console Web de Control Manager peut être important. Par exemple, si un problème de connexion avec un communicateur est résolu entre deux battements de cœur, les échanges de données avec ce communicateur redeviennent possibles même si la console indique que son état est « Inactif » ou « Anormal ».
Battements de cœur à intervalle court (inférieur à 60 minutes)	Les intervalles courts permettent d'obtenir un cliché plus d'actualité de l'état du réseau au niveau du serveur Control Manager. En revanche, cela demande une plus forte sollicitation de la bande passante.

Configuration des programmations de communication d'agent

Il est possible de définir jusqu'à trois programmations spécifiant à quel moment le produit géré doit interagir avec le serveur Control Manager.

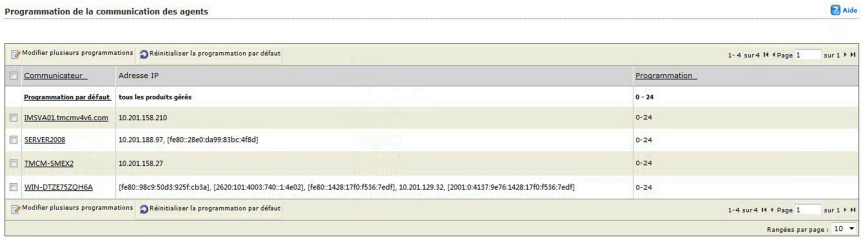
Un serveur Control Manager enfant doit établir une communication permanente avec le serveur Control Manager parent ; l'écran Programmation de la communication des agents ne permet pas de modifier la programmation de communication d'agent des serveurs enfants avec les produits gérés des serveurs enfants.

Définition d'une programmation de communication des agents pour un produit géré

Procédure

1. Accédez à **Administration** > **Paramètres** > **Programmation de communication des agents**.

   L'écran **Programmation de la communication des agents** apparaît.



2. Sélectionnez la programmation du produit géré à modifier.

   L'écran **Définir la programmation d'un communicateur** apparaît.

3. Définissez la programmation. Indiquez une nouvelle heure ou choisissez le paramètre par défaut :

   - Pour modifier ce paramètre, changez les intervalles appropriés dans la barre de programmation, puis cliquez sur **Enregistrer**.
   - Pour utiliser le paramètre par défaut, revenez sur l'écran **Programmation de la communication des agents**. Sélectionnez la programmation à appliquer et cliquez sur **Réinitialiser la programmation par défaut**

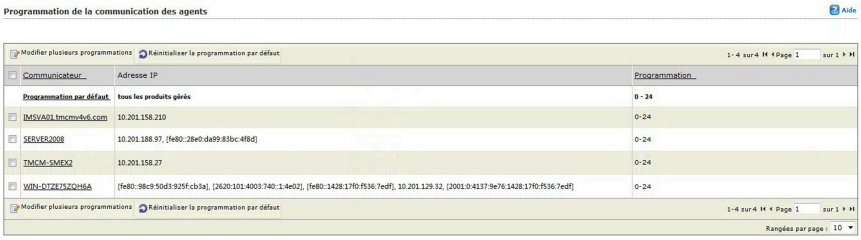
Modification de la programmation par défaut de l'agent de communication

La programmation par défaut vous permet de définir automatiquement la programmation de la communication de l'agent.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Programmation de la communication de l'agent**.

   L'écran **Programmation de la communication des agents** apparaît.



2. Dans la zone de travail, cliquez sur **Programmation par défaut**.

3. Dans l'écran **Programmation quotidienne**, modifiez les intervalles de temps appropriés.

4. Cliquez sur **Enregistrer**.

Configuration du battement de cœur du communicateur/de l'agent

L'écran **Délai d'attente de communication** permet de définir la fréquence et le temps de retard maximum (en minutes) des communications entre le serveur Control Manager et l'agent de communication.

Remarque

Ces paramètres ne s'appliquent qu'aux communicateurs des produits gérés directement contrôlés par le serveur Control Manager. Les communicateurs des serveurs Control Manager enfants utilisent des valeurs prédéfinies :

Fréquence : 3 minutes

Retard maximum : 5 minutes

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres du délai d'attente de communication**.

   L'écran **Paramètres du délai d'attente de communication** apparaît.

2. Dans la zone de travail, conservez les valeurs par défaut ou définissez-en de nouvelles pour les paramètres suivants :

   - **Notifier sur l'état du produit géré toutes les** : Définit la fréquence à laquelle le produit géré répond aux messages du serveur Control Manager. Les valeurs valides doivent être comprises entre 5 et 480 minutes.
   - **En l'absence de communication, définir l'état comme anormal après** : Indique la durée pendant laquelle Control Manager attend une réponse du produit géré avant que la console Web ne passe à l'état « Inactif ». Les valeurs valides doivent être comprises entre 15 et 1440 minutes.

   Remarque

   La valeur du champ **En l'absence de communication, définir l'état comme anormal après** doit faire au moins trois fois la valeur du champ **Notifier sur l'état du produit géré toutes les**.

3. Cliquez sur **Enregistrer**.

Arrêt et redémarrage des services Control Manager

L'écran **Services Windows** permet de redémarrer n'importe lequel des services Control Manager suivants :

- Trend Micro Management Infrastructure
- Trend Micro Common CGI

- Trend Micro Control Manager

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).

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**.
3. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Démarrer**.

Modification du port de communication externe de Control Manager

Le communicateur est chargé de la communication entre les agents et le serveur.

Par défaut, il utilise le port 10198 pour les communications entre les processus Control Manager (communication interne) et le port 10319 pour les communications entre les agents et le serveur Control Manager (communication externe).

Modification du port de communication externe sur le serveur Control Manager

Procédure

1. Ouvrez `<racine>\Program Files\Trend Micro\COMMON\ccgi \commoncgi\config\CCGI_Config.xml` dans un éditeur de texte tel que le Bloc-notes.

   AVERTISSEMENT!

   Soyez prudent lorsque vous modifiez les fichiers *.xml ou *.cfg de Control Manager. Pour être sûr de pouvoir rétablir les paramètres d'origine, sauvegardez le fichier CCGI_Config.xml.

2. Indiquez une nouvelle valeur pour le paramètre `OuterPort`. Cette valeur représente le port de communication externe. Par exemple, paramétrez OuterPort="2222" si vous souhaitez utiliser le port 2222.

3. Enregistrez et fermez `CCGI_Config.xml`.

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

   AVERTISSEMENT!

   Toute saisie incorrecte dans le fichier de configuration pourrait provoquer de graves erreurs système. Sauvegardez TMI.cfg afin d'être en mesure de rétablir les paramètres d'origine.

5. Remplacez la valeur du paramètre `OuterPort` par celle du fichier `CCGI_Config.xml`.

6. Enregistrez et fermez `TMI.cfg`.

7. Arrêtez et redémarrez tous les services Control Manager.

Modification du niveau de sécurité pour les agents TMI

Control Manager implémente le niveau de sécurité défini lors de l'installation de Control Manager. Vous pouvez néanmoins changer ce niveau dans le fichier `TMI.cfg` sans avoir à réinstaller le produit.

Procédure

1. Ouvrez `<racine>:\Program files\Trend Micro\COMMON\TMI\TMI.cfg` dans un éditeur de texte tel que le Bloc-notes.

   AVERTISSEMENT!

   Toute saisie incorrecte dans le fichier de configuration pourrait provoquer de graves erreurs système.

2. Sauvegardez `TMI.cfg` afin d'être en mesure de rétablir les paramètres d'origine.
3. Modifiez la valeur du paramètre `MaxSecurity`. Saisissez `1`, `2` ou `5` pour indiquer le niveau de sécurité souhaité.
4. Enregistrez et fermez `TMI.cfg`.
5. Ouvrez l'écran **Windows Services** afin d'arrêter puis de redémarrer les services Control Manager.
6. Répétez les étapes 1 à 3 de façon à modifier le fichier `TMI.cfg` de tous les agents présents sur le réseau Control Manager.

   AVERTISSEMENT!

   Dans tous les fichiers TMI.cfg du réseau Control Manager (serveur et agents), définissez le même niveau de sécurité (paramètre MaxSecurity). Sinon, la communication entre le serveur et les agents ne fonctionnera pas.

Modification du protocole du battement de cœur d'un communicateur

Par défaut, le protocole sans connexion UDP (User Datagram Protocol) est utilisé pour transférer le battement de cœur du communicateur entre le produit géré et le serveur Control Manager.

Procédure

1. Ouvrez `<racine>:\Program files\Trend Micro\COMMON\TMI\TMI.cfg` dans un éditeur de texte tel que le Bloc-notes.

   AVERTISSEMENT!

   Toute saisie incorrecte dans le fichier de configuration pourrait provoquer de graves erreurs système. Sauvegardez TMI.cfg afin d'être en mesure de rétablir les paramètres d'origine.

2. Attribuez au paramètre `AllowUDP` la valeur `0`.

3. Enregistrez et fermez `TMI.cfg`.

4. Ouvrez l'écran Windows Services afin d'arrêter puis de redémarrer les services Control Manager.

5. Répétez les étapes 1 à 3 de façon à modifier le fichier `TMI.cfg` de tous les agents présents sur le réseau Control Manager.

   AVERTISSEMENT!

   Dans tous les fichiers TMI.cfg du réseau Control Manager (serveur et agents), définissez le même niveau de sécurité (paramètre AllowUDP). Sinon, la communication entre le serveur et les agents ne fonctionnera pas.

Vérification de la méthode de communication entre MCP et Control Manager

Control Manager détecte automatiquement la méthode de connexion employée par les agents MCP pour communiquer avec Control Manager. En mode de communication bidirectionnel, Control Manager utilise les notifications CGI pour ses échanges avec les agents MCP.

Vérification de l'utilisation par Control Manager de la communication bidirectionnelle

Cette procédure tient compte des paramètres d'installation par défaut de Control Manager.

Procédure

1. Vous pouvez ouvrir l'application SQL Server Management Studio et rechercher une table de base de données de Control Manager.
2. Localisez **CDSM_Entity**.
3. Recherchez et vérifiez les éléments suivants dans CDSM_Entity :
   - Repérez la colonne **Jeton**. Les informations de cette colonne apparaissent au format suivant : `URLTOKEN:2; http;<Adress IP>;80; cgiCmdNotify;;!CRYPT!10…`

     `URLTOKEN:1` signifie que l'agent utilise une communication unidirectionnelle pour ses échanges avec Control Manager.

     `URLTOKEN:2` signifie que l'agent utilise une communication bidirectionnelle pour ses échanges avec Control Manager.

Vérification de l'utilisation par Control Manager de la communication bidirectionnelle depuis la console Web

Procédure

1. Cliquez sur **Produits**.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur le produit ou le répertoire dans le répertoire Produits.

3. Cliquez sur **Dossier**.

   Les informations de la zone de travail sont modifiées.

4. Sélectionnez **Affichage des informations de connexion** depuis la liste déroulante Dossier.

   La colonne **Mode** affiche le mode de communication que l'agent MCP du produit géré utilise.

Définition de l'installation à distance d'agents Control Manager

Control Manager peut prendre en charge les agents Control Manager 2.5x et MCP. Cependant, seuls les agents Control Manager 2.5x exigent une installation séparée. Utilisez l'écran **Paramètres d'agents de produits** pour obtenir les programmes d'installation à distance pour les agents Control Manager 2.x.

Remarque

L'installation à distance et la méthode d'installation prioritaire pour déployer des agents Control Manager 2.x sur un grand nombre de serveur de produit gérés plus anciens. Cette possibilité vous permet d'installer des agents Control Manager 2.x sans que vous ayez à être présent physiquement sur le serveur cible.

Il y a deux programmes d'installation à distance d'agents pour installer les agents Control Manager 2.x :

AGENT	DESCRIPTION
`CMAgentSetup.exe`	La base de ce programme d'installation d'agent est un programme semblable à celui utilisé dans Trend Virus Control System 1.x. Tous les agents requis pour les produits correspondants sont inclus dans ce fichier. Utilisez `CMAgentSetup.exe` pour installer l'agent Control Manager pour InterScan Messaging Security Suite 5.1 (InterScan Messaging Security Suite 5.15 et versions ultérieures utilise RemoteInstall.exe).
`RemoteInstall.exe`	Il s'agit d'un outil d'installation d'agent introduit dans Control Manager 2.5. Il a deux objectifs : • installer des agents sur des serveurs de produits pris en charge ; • télécharger des modules d'agents sur des serveurs Control Manager. Cet outil est différent du programme `CMAgentSetup.exe` d'origine, car il ne contient aucun agent. Il utilise des modules d'agent enregistrés sur les serveurs Control Manager. L'outil se contente d'identifier les serveurs cibles, puis les programmes d'installation des modules d'agent effectuent eux-mêmes l'installation. Après une nouvelle installation de Control Manager, les serveurs Control Manager ne contient pas de modules d'agent. Le produit antivirus ou de sécurité du contenu est téléchargé et enregistre ses agents sur le serveur, avant que vous ne puissiez les installer.

Chapitre 12

Administration des produits gérés

Ce chapitre présente les éléments nécessaires aux administrateurs pour gérer le réseau Control Manager.

Ce chapitre traite les rubriques suivantes :

Déploiement manuel des composants à l'aide du répertoire Produits

Les déploiements manuels permettent de mettre à jour les signatures de virus, les règles anti-pourriel et les moteurs de scan sur demande pour vos produits gérés. Utilisez cette méthode de mise à jour des composants lors des épidémies virales.

Téléchargez les nouveaux composants avant de déployer les mises à jour sur un produit géré précis ou sur des groupes de produits gérés.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez un produit géré ou un répertoire depuis le répertoire Produits.

   Le produit géré ou répertoire se met en surbrillance.

3. Déplacez le curseur sur **Tâches** dans le menu Répertoire produits.

4. Sélectionnez **Déployer <composant>** à partir du menu déroulant.

5. Cliquez sur **Déployer maintenant** pour lancer le déploiement manuel des nouveaux composants.
6. Surveillez la progression dans l'écran **Suivi des commandes**.
7. Cliquez sur le lien Détails sur la commande dans l'écran **Suivi des commandes** pour afficher des informations détaillées sur la tâche Déploiement maintenant.

Affichage des résumés d'état des produits gérés

L'écran État produit affiche les résumés d'antivirus, de sécurité de contenu et de sécurité Web pour tous les produits gérés présents dans l'arborescence du répertoire Produits.

Il existe deux façons d'afficher le résumé de l'état des produits gérés :

- Via le Tableau de bord en utilisant le widget Résultats de la détection de menaces (accessible dans l'onglet Résumé)
- Via le répertoire Produits

Accès au Tableau de bord

Procédure

- À l'ouverture de la console Web de Control Manager, l'onglet **Résumé** affiche le résumé de l'ensemble du réseau Control Manager. Ce résumé est identique à celui que fournit l'onglet État produit dans le dossier racine du répertoire Produits.

Accès via le répertoire Produits

Procédure

1. Cliquez sur **Produits** dans le menu principal.

L'écran **Répertoire Produits** apparaît.

2. Dans l'arborescence du répertoire Produits, sélectionnez le dossier ou le produit géré voulu.

   - Si vous cliquez sur un produit géré, l'onglet État produit affiche le résumé du produit en question.
   - Si vous cliquez sur le dossier racine, Nouvelle entité ou sur tout dossier défini par l'utilisateur, l'onglet État produit affiche les résumés Antivirus, Sécurité de contenu et Sécurité Web.

Remarque

Par défaut, l'onglet Résumé de l'état affiche les informations correspondant à une semaine, jusqu'à la date de votre requête. Vous pouvez néanmoins modifier cette étendue en choisissant **Aujourd'hui**, **La semaine dernière**, **Les deux dernières semaines** ou **Le dernier mois** dans la liste Afficher le résumé pour.

Configuration des produits gérés

En fonction de la version du produit et de l'agent, vous pouvez configurer le produit géré depuis la console Web du produit géré ou via une console générée par Control Manager.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez le produit géré souhaité depuis l'arborescence du répertoire Produits.

   L'état du produit apparaît dans la partie droite de l'écran.

3. Déplacez le curseur sur **Configurer** dans le menu Répertoire Produits.

4. Choisissez l'une des options suivantes :

- **Réplication de configuration** : L'écran **Paramètres de configuration** apparaît.

a. Sélectionnez le dossier vers lequel répliquer les paramètres du produit géré sélectionné depuis l'arborescence du répertoire Produits.

b. Cliquez sur **Répliquer**.

Les paramètres du produit géré sélectionné sont répliqués vers les produits gérés cibles.

- **<Nom Produit Géré> Signature unique** : La console Web du produit géré ou la console générée par Control Manager apparaît.

a. Configurez le produit géré depuis la console Web.

Remarque

Pour obtenir plus d'informations sur la configuration d'un produit géré, consultez la documentation du produit géré.

Exécution de tâches sur des produits gérés

L'élément de menu Tâches vous permet d'exécuter des actions sur un produit géré donné. Selon le produit géré, l'une ou plusieurs des tâches suivantes sont disponibles :

- Déployer les moteurs
- Déployer les fichiers de signatures/modèles Damage Cleanup
- Déployer les fichiers programme
- Activer ou désactiver le scan en temps réel
- Démarrer le scan immédiat

Déployez les règles anti-pourriel, les signatures ou le moteur de scan les plus récents sur les produits gérés contenant des composants obsolètes. Pour que cette opération réussisse, le serveur Control Manager doit posséder les derniers composants en date issus de Trend Micro ActiveUpdate Server. Procédez manuellement au téléchargement

de façon à vous assurer que les derniers composants en date figurent déjà sur le serveur Control Manager.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez le produit géré ou le répertoire pour exécuter une tâche.

3. Déplacez le curseur sur **Tâches**.

4. Cliquez sur une tâche dans la liste. Contrôlez la progression via le suivi des commandes. Cliquez sur le lien **Détails sur la commande** de l'écran de réponse pour afficher les informations relatives à la commande.

Interrogation et affichage des journaux des produits gérés

L'onglet Journaux vous permet d'interroger et d'afficher les journaux d'un groupe de produits gérés ou d'un produit précis.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

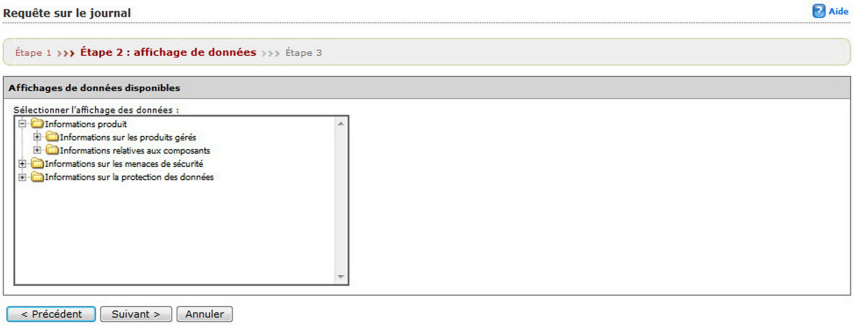
   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez le produit géré ou dossier souhaité depuis le répertoire Produits.

3. Déplacez le curseur sur **Journaux** dans le menu Répertoire Produits.

4. Cliquez sur **Journaux** depuis le menu déroulant.

   L'écran **Requête ad hoc > Étape 2 : Sélection de l'affichage de données** s'affiche.

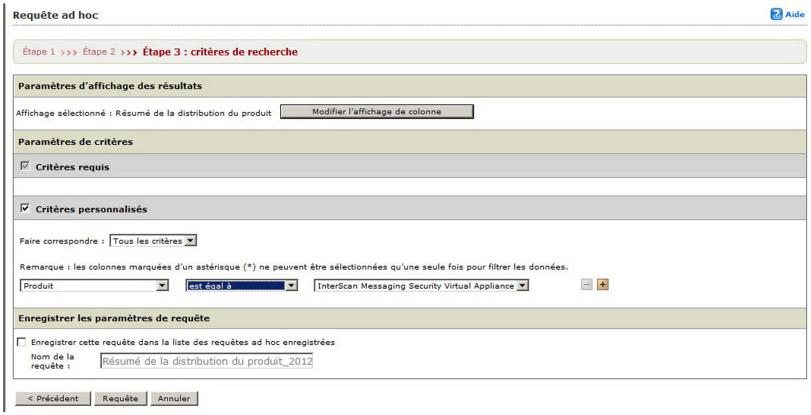


5. Spécifiez l'affichage des données pour le journal :

a. Sélectionnez les données objets de la requête depuis la zone Affichages de données disponibles.

b. Cliquez sur **Suivant**.

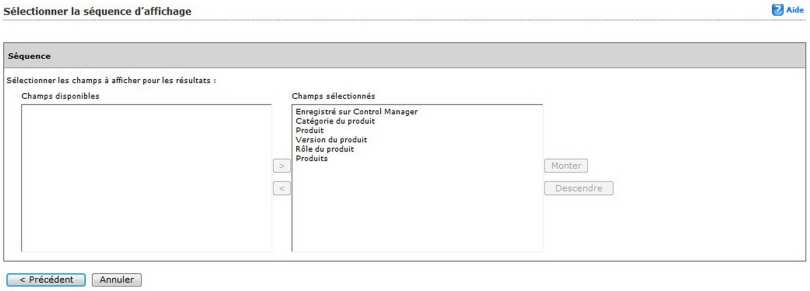
L'écran **Requête ad hoc > Étape 3 : Critères de recherche** apparaît.



6. Spécifiez les données devant apparaître dans le journal et l'ordre dans lequel les données doivent apparaître. Les éléments apparaissant en haut de la liste Champs sélectionnés apparaissent dans la colonne située à l'extrême gauche du tableau. Le fait de supprimer un champ de la liste Champs sélectionnés supprime la colonne correspondante du tableau renvoyé par la requête ad hoc.

a. Cliquez sur **Modifier l'affichage de colonne**.

L'écran **Sélectionner la séquence d'affichage** apparaît.



b. Sélectionnez une colonne de requête depuis la liste Champs disponibles. Sélectionnez plusieurs éléments à l'aide de la touche **Maj** ou **Ctrl**.

c. Cliquez sur **>** pour ajouter des éléments à la liste Champs sélectionnés.

d. Spécifiez l'ordre dans lequel les données doivent s'afficher en sélectionnant l'élément et en cliquant sur **Monter** ou **Descendre**.

e. Cliquez sur **Précédent** lorsque la séquence correspond à vos besoins.

7. Spécifiez les critères de filtrage pour les données :

Remarque

Lors d'une requête de données de résumé, les utilisateurs doivent spécifier les éléments dans Critères requis.

- Critères requis :
  - Spécifiez une heure de résumé pour les données ou si vous souhaitez que les COOKIES apparaissent dans vos rapports.
- Critères personnalisés :
  a. Spécifiez les règles de filtrage des critères pour les catégories de données :

- **Tous les critères** : cette sélection est équivalente à une fonction logique AND. Les données apparaissant dans le rapport doivent correspondre à tous les critères de filtrage.
- **L'un des critères** : cette sélection est équivalente à une fonction logique OR. Les données apparaissant dans le rapport doivent correspondre à l'un des critères de filtrage.

b. Spécifiez les critères de filtrage pour les données : Control Manager prend en charge jusqu'à 20 critères pour le filtrage des données.

Conseil

Si vous ne spécifiez aucun critère de filtrage, la requête ad hoc renvoie tous les résultats pour les colonnes concernées. Trend Micro recommande de spécifier des critères de filtrage pour simplifier l'analyse des données après le renvoi des informations par la requête.

8. Pour enregistrer la requête :

a. Cliquez sur **Enregistrer cette requête dans la liste des requêtes ad hoc enregistrées**.

b. Saisissez un nom pour la requête enregistrée dans le champ **Nom de la requête**.

9. Cliquez sur **Requête**.

L'écran **Résultats** apparaît.

10. Enregistrez le rapport dans un fichier CSV :

a. Cliquez sur **Exporter vers fichier CSV**.

b. Cliquez sur **Télécharger**.

c. Spécifiez l'emplacement dans lequel enregistrer le fichier.

d. Cliquez sur **Enregistrer**.

11. Enregistrez le rapport dans un fichier XML :

a. Cliquez sur **Exporter vers fichier XML**.

b. Cliquez sur **Télécharger**.

c. Spécifiez l'emplacement dans lequel enregistrer le fichier.

d. Cliquez sur **Enregistrer**.

Conseil

Pour afficher davantage de résultats sur un écran unique, sélectionnez une valeur différente dans Rangées par page. Un écran unique peut afficher 10, 15, 30 ou 50 résultats de requête par page.

12. Enregistrez les paramètres de la requête :

a. Cliquez sur **Enregistrer les paramètres de requête**.

b. Saisissez un nom pour la requête enregistrée dans le champ **Nom de la requête**.

c. Cliquez sur **OK**.

La requête enregistrée apparaît dans l'écran **Requêtes ad hoc enregistrées**.

À propos de la restauration de produits gérés supprimés du répertoire Produits

Les cas de figure suivants peuvent entraîner la suppression de certains produits gérés du répertoire Produits :

- Réinstallation du serveur Control Manager et sélection de l'option **Supprimer les enregistrements existants et créer une nouvelle base de données**

  Cette option entraîne la création d'une nouvelle base de données portant le nom de la base existante.

- Remplacement d'une base de données Control Manager endommagée par une autre base de données du même nom

- Suppression accidentelle du produit géré dans le Gestionnaire de répertoires

Lorsque les enregistrements des produits gérés d'un serveur Control Manager sont perdus, les agents TMI conservent ces informations et « savent » par conséquent où elles

sont enregistrées. L'agent Control Manager se réenregistre automatiquement au bout de 8 heures ou au redémarrage du service.

Les agents MCP ne se réenregistrent pas automatiquement. Les administrateurs doivent réenregistrer manuellement les produits utilisant des agents MCP.

Restauration de produits gérés supprimés du répertoire Produits

Procédure

- Redémarrez le service Trend Micro Control Manager sur le serveur des produits gérés. Pour plus d'informations, consultez la section *Arrêt et redémarrage des services Control Manager à la page 11-17*.
- Attendez que l'agent se réenregistre : Par défaut, les anciens agents Control Manager vérifient leur connexion au serveur toutes les huit (8) heures. S'il détecte que son enregistrement a été supprimé, il se réenregistre automatiquement. Consultez la section *Modification de la fréquence de vérification de connexion des agents Control Manager 2.x à la page 12-11* pour modifier l'heure de vérification d'un agent.
- Procédez à un réenregistrement manuel sur Control Manager : Les agents MCP ne se réenregistrent pas automatiquement et doivent être réenregistrés manuellement sur le serveur Control Manager.

Modification de la fréquence de vérification de connexion des agents Control Manager 2.x

Par défaut, les agents Control Manager 2.x vérifient leur connexion au serveur Control Manager toutes les huit heures. Pour changer cette fréquence, vous devez modifier un fichier de configuration sur l'ordinateur de l'agent.

Remarque

Les agents MCP ne peuvent pas se reconnecter à Control Manager si la connexion est perdue. Un utilisateur doit réenregistrer manuellement les produits gérés.

Procédure

1. Sur le serveur du produit géré, accédez au répertoire d'installation de l'agent Control Manager (par exemple, `C:\Program Files\Trend\IMSS\Agent`).
2. Sauvegardez le fichier `Entity.cfg`.
3. Ouvrez `Entity.cfg` dans un éditeur de texte tel que le Bloc-notes.
4. Recherchez le paramètre `ENTITY_retry_hour` et saisissez comme valeur un nombre entier pour modifier la fréquence de vérification par défaut. La valeur du paramètre `ENTITY_retry_hour` correspond au nombre d'heures. Les valeurs possibles sont comprises entre 1 et 24.
5. Enregistrez et fermez le fichier `Entity.cfg` afin d'appliquer la nouvelle fréquence de vérification.

Recherche de produits gérés, de dossiers du répertoire Produits ou d'ordinateurs

Utilisez le bouton **Rechercher** pour localiser rapidement un produit géré donné dans le répertoire Produits.

Recherche d'un dossier ou d'un produit géré

Procédure

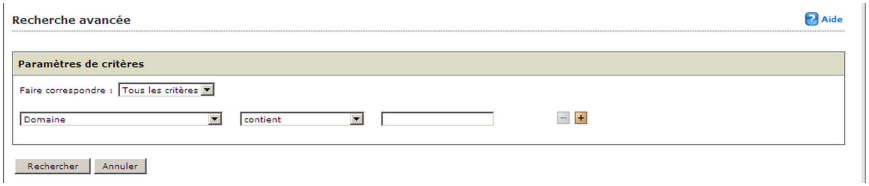
1. Accédez au répertoire Produits.
2. Saisissez le nom d'affichage du produit géré dans le champ **Chercher entité**.
3. Cliquez sur **Rechercher**.

Effectuer une recherche avancée

Procédure

1. Accédez au répertoire Produits.
2. Cliquez sur **Recherche avancée**.

   L'écran **Recherche avancée** apparaît.



3. Spécifiez vos critères de filtrage pour le produit. Control Manager prend en charge jusqu'à 20 critères de filtrage pour les recherches.
4. Cliquez sur **Rechercher** pour lancer la recherche.

   Les résultats de la recherche apparaissent dans le dossier **Résultat de la recherche** du répertoire Produits.

Actualisation du répertoire Produits

Procédure

- Dans l'écran **Répertoire Produits**, cliquez sur l'icône **Actualiser** dans le coin supérieur droit de l'écran.

Définition de l'écran Gestionnaire des répertoires

Une fois l'enregistrement sur Control Manager effectué, le produit géré apparaît dans le dossier par défaut du répertoire Produits.

Utilisez l'écran Gestionnaire de répertoires pour personnaliser la structure du répertoire Produits en fonction de vos besoins d'administration. Vous pouvez ainsi regrouper les produits par emplacement ou type de produit (sécurité de messagerie, sécurité Web, protection du stockage des fichiers).

Le gestionnaire de répertoires permet de créer, modifier ou supprimer des dossiers, et de déplacer des produits gérés d'un dossier vers un autre. Il est toutefois impossible de supprimer ou de renommer le dossier Nouvelle entité.

Organisez soigneusement les produits gérés appartenant à chaque dossier. Tenez compte des facteurs suivants lors de la planification et de l'implémentation de la structure des dossiers et des produits gérés :

- Répertoire Produits
- Comptes utilisateurs
- Plans de déploiement
- Requête ad hoc
- Rapports Control Manager

Regroupez des produits gérés selon des critères géographiques, administratifs ou spécifiques de ces produits. Le tableau suivant indique les types de regroupement recommandés avec leurs avantages et leurs inconvénients. Il présente également les différents droits d'accès aux produits gérés ou aux dossiers dans le répertoire.

TABLEAU 12-1. Comparaison des groupes de produits

TYPE DE REGROUPEMENT	AVANTAGES	INCONVÉNIENTS
Géographique ou administratif	Structure claire	Aucune configuration de groupe pour des produits identiques

TYPE DE REGROUPEMENT	AVANTAGES	INCONVÉNIENTS
Type de produit	Configuration de groupe et état disponible	Incompatibilité possible des droits d'accès
Combinaison des deux	Configuration de groupes et gestion des droits d'accès	Structure complexe, risque d'être difficile à gérer

Utilisation des options de l'écran Gestionnaire de répertoires

Ces options vous permettent de manipuler et d'organiser les produits gérés de votre réseau Control Manager.

L'écran **Gestionnaire de répertoires** propose plusieurs options :

- Ajouter des répertoires au répertoire Produits
- Renommer des répertoires dans le répertoire Produits
- Déplacer des produits gérés ou des répertoires dans le répertoire Produits
- Supprimer des produits gérés ou des répertoires du répertoire Produits

Remarque

La case à cocher de maintien des autorisations permet à un dossier de conserver son autorisation source lorsqu'il est déplacé.

Utilisation de l'écran Gestionnaire des répertoires

Procédure

- Sélectionnez un produit géré ou un répertoire et cliquez sur **Renommer** pour renommer un produit géré ou un répertoire.
- Cliquez sur le signe **+** ou sur un dossier pour afficher les produits gérés appartenant à ce dossier.

- Utilisez la fonction de glisser-déplacer pour déplacer les produits gérés ou les répertoires vers le répertoire Produits
- Cliquez sur **Ajouter dossier** pour ajouter un répertoire au répertoire Produits

Accès à l'écran Gestionnaire des répertoires

Utilisez l'écran **Gestion des répertoires** pour regrouper les produits gérés.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur **Gestionnaire des répertoires** depuis le menu Répertoire Produits.

   L'écran **Gestion des répertoires** apparaît.

Création de dossiers

Vous pouvez regrouper des produits gérés dans différents dossiers, en fonction des besoins du modèle d'administration du réseau Control Manager en vigueur dans votre organisation.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur **Gestionnaire des répertoires** depuis le menu Répertoire Produits.

   L'écran **Gestion des répertoires** apparaît.

3. Sélectionnez **Dossier local**.

4. Cliquez sur **Ajouter dossier**.

   L'écran **Ajouter répertoire** apparaît.

5. Saisissez un nom pour le nouveau répertoire dans le champ **Nom du répertoire**.

6. Cliquez sur **Enregistrer**.

Remarque

À l'exception du dossier **Nouvelle entité**, Control Manager répertorie tous les dossiers par ordre croissant, en commençant par les caractères spéciaux (!, #, $, %, (,), *, +, -, virgule, point, +, ?, @, [,], ^, _, {, |, }, et ~), suivis des nombres (0 à 9), puis des caractères alphabétiques (a/A à z/Z).

Changement du nom d'un dossier ou d'un produit géré

Vous pouvez renommer les répertoires et produits gérés depuis le **gestionnaire de répertoires**.

Remarque

Le fait de renommer un produit géré ne change que le nom stocké dans la base de données de Control Manager : cela n'a aucune incidence sur le produit géré.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur **Gestionnaire des répertoires** depuis le menu Répertoire Produits.

   L'écran **Gestion des répertoires** apparaît.

3. Sélectionnez le produit géré ou le répertoire à renommer.

4. Cliquez sur **Renommer**.

   L'écran **Renommer le répertoire** apparaît.

5. Saisissez un nom pour le produit géré ou le répertoire dans le champ **Nom du répertoire**.

6. Cliquez sur **Enregistrer**.

7. Cliquez sur **OK**.

   Le produit géré ou le répertoire s'affiche dans le répertoire Produits avec le nouveau nom.

Déplacement d'un dossier ou d'un produit géré

Lorsque vous déplacez des dossiers, portez une attention particulière à la case à cocher **Maintenez les permissions d'accès de l'utilisateur en cours pour déplacer les produits gérés/dossiers**. Si vous sélectionnez cette case à cocher et déplacez un produit géré ou un dossier, le produit géré ou le dossier conserve les permissions de son dossier source. Si vous désactivez la case à cocher de maintien des permissions, puis déplacez un produit géré ou un dossier, le produit géré ou le dossier récupère les permissions d'accès de son nouveau dossier parent.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur **Gestionnaire des répertoires** depuis le menu Répertoire Produits.

   L'écran **Gestion des répertoires** apparaît.

3. Dans la zone de travail, sélectionnez le dossier ou le produit géré à déplacer.

4. Glissez le dossier ou le produit géré dans le nouvel emplacement cible.

5. Cliquez sur **Enregistrer**.

Suppression d'un dossier défini par l'utilisateur

Faites preuve de prudence lors de la suppression de dossiers définis par l'utilisateur dans l'écran **Gestionnaire des répertoires**. Vous risquez de supprimer accidentellement un produit géré, ce qui entraîne l'annulation de son enregistrement sur le serveur Control Manager.

Remarque

Il n'est pas possible de supprimer le dossier **Nouvelle entité**.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur **Gestionnaire des répertoires** depuis le menu Répertoire Produits.

   L'écran **Gestion des répertoires** apparaît.

3. Sélectionnez le produit géré ou le répertoire à supprimer.

4. Cliquez sur **Supprimer**.

Une fenêtre de confirmation apparaît.

5. Cliquez sur **OK**.

6. Cliquez sur **Enregistrer**.

Chapitre 13

Activation de Control Manager et des produits gérés

Ce chapitre présente le matériel nécessaire aux administrateurs pour activer ou renouveler des licences pour Control Manager ou des produits gérés.

Ce chapitre traite les rubriques suivantes :

Activation et enregistrement des produits gérés

Pour utiliser les fonctionnalités de Control Manager 6.0, des produits gérés (OfficeScan, ScanMail for Microsoft Exchange) et des autres services (Outbreak Prevention Services), vous devez obtenir les codes d'activation correspondants pour activer ces logiciels ou services. Une clé d'enregistrement est fournie avec le logiciel. Utilisez cette clé pour enregistrer votre logiciel en ligne sur le site Web d'enregistrement en ligne de Trend Micro et obtenir un code d'activation.

Lors de l'enregistrement des produits gérés sur Control Manager, leur code d'activation est ajouté à la liste des codes d'activation des produits gérés dans l'écran **Gestion de la licence**. Les administrateurs peuvent ajouter de nouveaux codes d'activation à la liste et redéployer les codes d'activation renouvelés.

Tous les codes d'activation partagent les caractéristiques suivantes :

- Créés en temps réel lors de l'enregistrement
- Créés sur la base des informations de clé d'enregistrement
- Ont une date d'expiration
- Sont indépendants des versions de produit

Remarque

Dans les versions précédentes de Control Manager, un numéro de série était fourni avec le produit et les utilisateurs devaient s'enregistrer en ligne pour pouvoir utiliser toutes les fonctionnalités du logiciel.

Définition de la gestion de la licence

Dans l'écran **Gestion de la licence**, vous pouvez afficher, gérer et déployer les licences de tous les produits gérés.

Remarque

Choisissez le nombre de codes d'activation affiché dans l'écran **Gestion de la licence** à l'aide de la fonction **Rangées par page**. L'écran **Gestion de la licence** peut afficher 10 (paramètre par défaut), 15, 30 ou 50 codes d'activation en même temps.

Composant écran	Description
Code d'activation	Affiche le code d'activation du produit géré.
Remarque	Affiche des informations supplémentaires sur le code d'activation.
Produits	Affiche le nombre de produits pour lesquels le code d'activation est déployé.
État	Affiche l'état du code d'activation : • Activé • Expiré
Type	Affiche le type du code d'activation : • **Complète :** Permet l'utilisation complète du produit pour la période de maintenance (généralement, 1 an). • **Évaluation** : Permet l'utilisation complète du produit pour la période d'évaluation (généralement, 3 mois).
Date d'expiration	Affiche la date d'expiration du code d'activation.
Nombre de licences	Affiche le nombre de licences autorisées par le code d'activation.

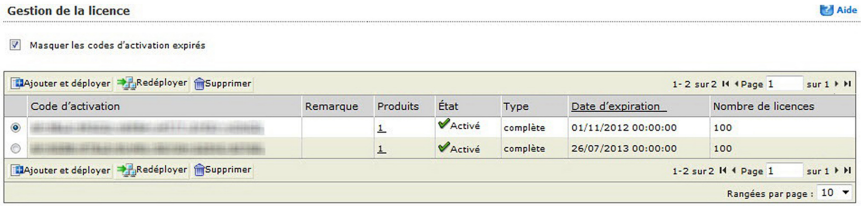
Activation des produits gérés

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

Procédure

1. Accédez à **Administration** > **Gestion de la licence** > **Produits gérés**.

   L'écran **Gestion de la licence** apparaît.



2. Cliquez sur **Ajouter et déployer**.

   L'écran **Ajouter et déployer une nouvelle licence > Étape 1 : Saisir le code d'activation** apparaît.

3. Saisissez un code d'activation pour le produit que vous souhaitez activer dans le champ Nouveau code d'activation.

4. Cliquez sur **Suivant**.

   L'écran **Ajouter et déployer une nouvelle licence > Étape 2 : Sélectionner les cibles** apparaît.

> **Remarque**
>
> Si aucun produit n'apparaît dans la liste, le code d'activation sélectionné ne prend en charge aucun des produits actuellement enregistrés auprès de Control Manager. Cela pourrait signifier que le produit géré ne prend pas en charge la réception de codes d'activation envoyés par les serveurs Control Manager.

5. Sélectionnez le produit géré vers lequel déployer le code d'activation.

6. Cliquez sur **Terminer**.

   L'écran **Gestion de la licence** apparaît avec le nouveau code d'activation figurant dans le tableau.

Renouvellement des licences des produits gérés

Control Manager peut déployer ou redéployer les codes d'activation vers les produits enregistrés depuis le répertoire Produits ou depuis l'écran **Gestion de la licence**.

Renouvellement des licences des produits gérés depuis l'écran Gestion de la licence

Procédure

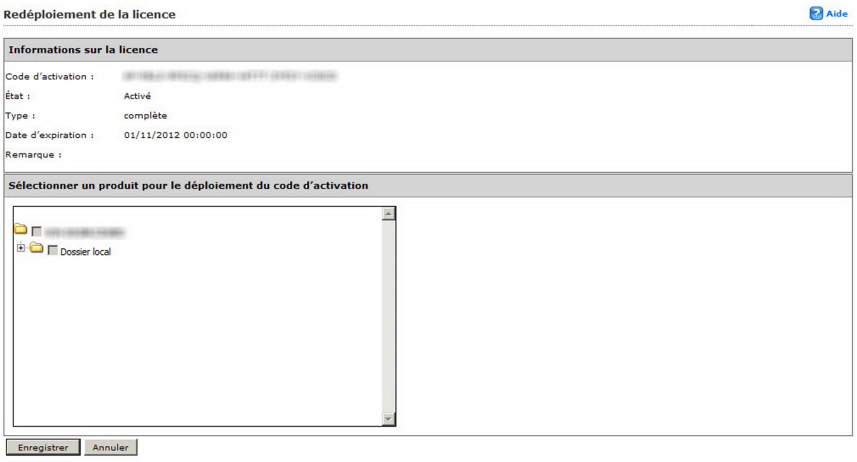
1. Accédez à **Administration** > **Gestion de la licence** > **Produits gérés**.

   L'écran **Gestion de la licence** apparaît.

2. Sélectionnez un code d'activation dans la liste.

3. Cliquez sur **Redéployer**.

   L'écran **Redéploiement de la licence** apparaît.



4. Cliquez sur **Enregistrer**.

Remarque

Si aucun produit n'apparaît dans la liste, le code d'activation sélectionné ne prend en charge aucun des produits actuellement enregistrés auprès de Control Manager.

Renouvellement des licences des produits gérés depuis le répertoire Produits

Procédure

1. Accédez au répertoire Produits.
2. Sélectionnez un produit géré depuis l'arborescence du répertoire Produits.
3. Cliquez sur **Tâches** depuis le menu Répertoire Produits.
4. Dans la liste des tâches, sélectionnez **Déployer les profils de licence**.
5. Dans l'écran **Profils de licence**, cliquez sur le lien **Déployer maintenant** pour que Control Manager charge les informations de licence mises à jour depuis le serveur de licences Trend Micro. Control Manager déploie ensuite les profils de licence automatiquement.
6. Cliquez sur le lien **Détails sur la commande** pour ouvrir l'écran **Détails sur la commande** dans lequel vous pouvez consulter les informations suivantes : date de déploiement des licences par Control Manager, heure du dernier rapport, ainsi qu'un décompte des déploiements en cours et des déploiements réussis ou avortés. Une liste des déploiements par serveur est également disponible.

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.

Remarque

Après avoir activé Control Manager, déconnectez-vous, puis reconnectez-vous à la console Web de Control Manager pour appliquer les modifications.

Définition des informations sur la licence

L'écran **Informations sur la licence** affiche les informations sur le produit pour Control Manager et les services gérés de Control Manager.

Chaque section comporte les informations suivantes :

TABLEAU 13-1. Écran Informations sur la licence

COMPOSANT ÉCRAN	DESCRIPTION
Produit	Affiche le nombre de produits pour lesquels le code d'activation est déployé.
Version	Affiche le type du code d'activation : • **Complète :** Permet l'utilisation complète du produit pour la période de maintenance (généralement, 1 an). • **Évaluation** : Permet l'utilisation complète du produit pour la période d'évaluation (généralement, 3 mois).
État	Affiche l'état du code d'activation : • Activé • Expiré
Code d'activation	Affiche le code d'activation du produit géré.
Date d'expiration	Affiche la date d'expiration du code d'activation.

Activation de Control Manager en cours

Procédure

1. Accédez à **Administration** > **Gestion de la licence** > **Control Manager**.

   L'écran **Informations sur la licence** apparaît.

2. Cliquez sur le lien **Spécifier un nouveau code d'activation**.

3. Dans le champ **Nouveau**, saisissez votre code d'activation. Si vous n'avez pas de code d'activation, cliquez sur le lien **Enregistrement en ligne** et suivez les instructions sur le site Web d'enregistrement en ligne pour en obtenir un.

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

Renouvellement du contrat de maintenance de Control Manager ou des services gérés

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.

Assurez-vous de disposer d'une clé d'enregistrement mise à jour pour acquérir un nouveau code d'activation afin de renouveler le contrat de maintenance de votre produit ou service.

Renouvellement du contrat de maintenance 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 le produit ou service à renouveler, cliquez sur **Vérifier l'état**.

3. Cliquez sur **OK**.

Remarque

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 le produit ou service à renouveler, cliquez sur le lien **Spécifier un nouveau code d'activation** (pour obtenir un code d'activation, cliquez sur le lien Enregistrement en ligne et suivez les instructions sur le site Web d'enregistrement en ligne).
3. Dans le champ **Nouveau**, saisissez votre code d'activation.
4. Cliquez sur **Activer**.
5. Cliquez sur **OK**.

Remarque

Déconnectez-vous et reconnectez-vous à la console Web pour que les modifications soient prises en compte.

Chapitre 14

Gestion des serveurs enfants

Ce chapitre présente les éléments nécessaires aux administrateurs pour gérer le réseau Control Manager. Pour plus d'informations sur la structure de gestion en cascade, consultez la section *Définition de la gestion en cascade à la page 4-10*.

Ce chapitre traite les rubriques suivantes :

Définition de la communication parent-enfant

Le répertoire Produits répertorie le serveur parent et tous les serveurs enfants du réseau Control Manager.

Le tableau ci-dessous décrit l'état des connexions dans une arborescence en cascade de Control Manager :

TABLEAU 14-1. Relation de serveur parent-enfant

ACTION	MAÎTRE  ENFANT 	MAÎTRE  ENFANT 	MAÎTRE  ENFANT 	MAÎTRE  ENFANT 	SERVEUR AUTONOME
Désenregistrement direct	●				
Enregistrement					●
Désinstallation de Control Manager (enregistrement de la base de données)	●	●	●	●	●
Désinstallation de Control Manager (suppression de la base de données)	●	●	●	●	●

Ce tableau met en lumière les points suivants :

- Le désenregistrement direct d'un serveur enfant désactivé n'est pas autorisé.
- En cas de désenregistrement direct ou forcé d'un serveur enfant actif, l'enregistrement du serveur est conservé dans la base de données du serveur parent mais supprimé de la base de données du serveur enfant.
- Si vous désinstallez l'application Control Manager d'un serveur enfant désactivé, enregistrez la base de données de Control Manager, réinstallez Control Manager, et réenregistrez-le sur le même serveur parent ; l'état du serveur enfant reste inchangé (désactivé).

- Si vous désinstallez l'application Control Manager d'un serveur enfant désactivé, supprimez la base de données de Control Manager, réinstallez Control Manager, puis réenregistrez-le sur le même serveur parent ; l'état du serveur enfant devient « actif ».

Ce tableau illustre par ailleurs la relation de serveur parent-enfant lorsque la relation en cascade est activée :

- Le serveur parent :
  - interroge chaque serveur enfant afin de mettre à jour l'écran Résumé de l'état en temps réel ;
  - met à jour l'état de la connexion des serveurs enfants toutes les 60 minutes.
- Le serveur enfant :
  - envoie des journaux au serveur parent ;
  - envoie des profils de rapports nouveaux ou mis à jour.

Le fait de désactiver un serveur enfant ne coupe pas la connexion de façon permanente entre les deux serveurs Control Manager. La connexion entre le serveur parent et le serveur enfant existe toujours. Le serveur parent émet une seule commande au serveur enfant — Activer Control Manager organisé en cascade. Lorsque le serveur enfant reçoit et accepte cette commande, le serveur parent reprend la gestion du serveur enfant.

Enregistrement et désenregistrement de serveurs enfants

L'enregistrement ou le désenregistrement d'un serveur enfant n'équivaut pas à l'activer ou à le désactiver. Si vous désenregistrez un serveur enfant, la liaison entre le serveur parent et le serveur enfant est définitivement rompue. La désactivation d'un serveur enfant suspend provisoirement la liaison et maintient la connexion de battement de cœur entre le serveur parent et les serveurs enfants.

Par exemple, si vous avez enregistré le serveur enfant XYZ sur le serveur parent A, puis désenregistré XYZ du serveur parent A et réenregistré celui-ci sur le serveur parent B, le

serveur parent B gère alors XYZ. L'arborescence du répertoire Produits du serveur A supprime XYZ de la liste.

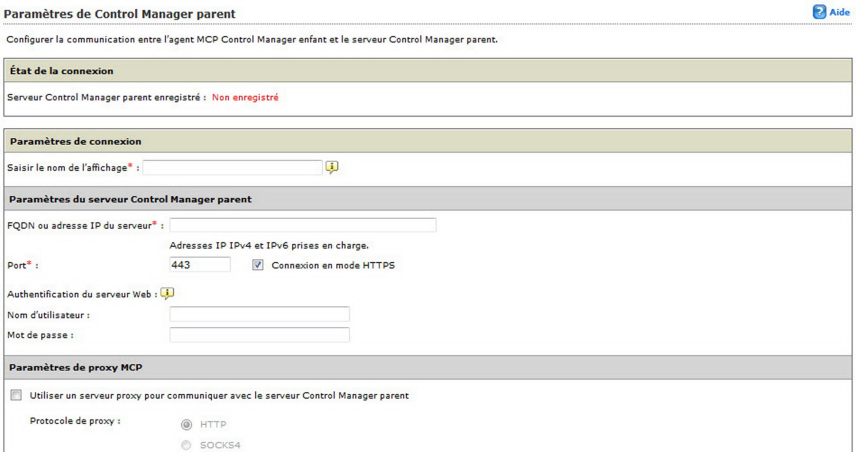
Utilisez l'écran **Paramètres de Control Manager parent** pour procéder à un enregistrement sur un serveur Control Manager parent ou à un désenregistrement d'un serveur Control Manager parent.

Enregistrement d'un serveur enfant

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres de Control Manager parent**.

   L'écran **Paramètres de Control Manager parent** apparaît.



2. Configurez les paramètres de connexion :

   - Saisissez le nom du serveur enfant qui s'affiche dans le serveur Control Manager parent dans le champ **Nom d'affichage de l'entité**.

3. Configurez les paramètres du serveur Control Manager parent :

a. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du serveur Control Manager parent dans le champ **FQDN ou adresse IP du serveur**.

b. Saisissez le numéro de port utilisé par le serveur Control Manager parent pour communiquer avec les agents MCP dans le champ **Port**.

Remarque

Pour une sécurité accrue, sélectionnez **Connexion en mode HTTPS**.

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

4. Configurez les paramètres proxy MCP :

a. Si vous utilisez un serveur proxy pour la connexion au serveur Control Manager, sélectionnez **Utiliser un serveur proxy pour communiquer avec le serveur Control Manager parent**.

b. Sélectionnez le protocole utilisé par le proxy :

- HTTP
- SOCKS 4
- SOCKS 5

c. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du serveur proxy dans le champ **Nom du serveur ou adresse IP**.

d. Saisissez le numéro de port du serveur proxy dans le champ **Port**.

e. Si le serveur proxy requiert une authentification de l'utilisateur, saisissez le nom d'utilisateur et le mot de passe.

5. Configurez le transfert du port de la communication à double-sens :

a. Si vous utilisez le transfert de port avec les agents MCP, sélectionnez **Autoriser la transmission du port de la communication à double sens** :

b. Saisissez l'adresse IP de transfert dans le champ **Adresse IP**.

c. Saisissez le numéro de port dans le champ **Port**.

6. Pour vérifier si le serveur enfant peut se connecter au serveur Control Manager parent, cliquez sur **Connexion test**.

7. Cliquez sur **Enregistrer** pour procéder à la connexion au serveur Control Manager parent.

Remarque

Si vous modifiez l'un des paramètres dans cet écran après l'enregistrement, cliquez sur **Paramètres de mise à jour** pour informer le serveur Control Manager des modifications. Si vous ne souhaitez plus que le serveur Control Manager gère le serveur, cliquez sur **Désenregistrer** à tout moment.

Vérification de l'état dans la console Web de Control Manager

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Vérifiez la présence de serveurs Control Manager enfants nouvellement enregistrés dans le **dossier en cascade**.

Désenregistrement d'un serveur enfant

L'enregistrement ou le désenregistrement d'un serveur enfant n'équivaut pas à l'activer ou à le désactiver. Si vous désenregistrez un serveur enfant, la liaison entre le serveur parent et le serveur enfant est définitivement rompue. La désactivation d'un serveur enfant suspend provisoirement la liaison et maintient la connexion de battement de cœur entre le serveur parent et les serveurs enfants.

Lorsque vous voulez équilibrer la charge entre les serveurs A et B, voici quelques scénarios courants :

- Le serveur parent A gère plus de serveurs enfants que le serveur parent B.

- La charge du serveur parent A augmente et vous voulez la réduire en transférant certains serveurs enfants vers le serveur B.

Utilisez l'écran **Paramètres de Control Manager parent** pour annuler l'enregistrement d'un serveur enfant auprès d'un serveur parent.

Procédure

1. Accédez à **Administration** > **Paramètres** > **Paramètres de Control Manager parent**.

   L'écran **Paramètres de Control Manager parent** apparaît.

2. Cliquez sur **Désenregistrer** en bas de l'écran.

Accès au dossier en cascade

Utilisez le répertoire Produits pour afficher les fonctions associées aux serveurs enfants et y accéder.

Remarque

Vous ne pouvez accéder au dossier en cascade que par l'intermédiaire de la console Web du serveur parent.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Développez le **dossier en cascade** dans le répertoire Produits.

Affichage des résumés d'état du serveur enfant

L'écran **Répertoire Produits** affiche les résumés d'antivirus, de programmes espions/graywares, de sécurité de contenu, de sécurité Web et de virus de réseau pour tous les produits gérés. Par défaut, les résumés s'affichent pour une semaine entière. Vous pouvez néanmoins modifier l'intervalle de temps en choisissant Aujourd'hui, La semaine dernière, Les deux dernières semaines ou Le dernier mois dans la liste **Afficher le résumé pour**.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez un serveur enfant.

   Tous les serveurs enfants envoient des résumés d'état au serveur parent. La fréquence de ces envois est déterminée par le paramètre d'intervalle défini dans le fichier `SystemConfiguration.xml`.

   L'intervalle par défaut est de 3 minutes et l'heure de début est 12 h. Configurez ces valeurs en fonction des besoins de votre mode d'administration. Tous les serveurs enfants envoient des résumés d'état au serveur parent. La fréquence de ces envois est déterminée par le paramètre d'intervalle défini dans le fichier `SystemConfiguration.xml`.

   Remarque

   Les serveurs enfants envoient les résumés d'état au serveur parent dès que le journal atteint 2500 enregistrements ou lorsque 3 minutes se sont écoulées. Pendant la période qui sépare chaque téléchargement de journal, il se peut par conséquent que les informations sur les produits gérés obsolètes, actuels et totaux ne soient pas à jour dans le tableau État du composant de l'écran État produit, sur le serveur enfant.

Configuration des paramètres de téléchargement des journaux

L'onglet Configuration, sur le serveur enfant, permet de définir la fréquence à laquelle ce dernier envoie les journaux au serveur parent.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez un serveur enfant dans le répertoire Produits.

   L'élément se met en surbrillance.

3. Déplacez le curseur sur **Configurer** dans le menu Répertoire Produits.

   Un menu déroulant apparaît.

4. Cliquez sur **Programmer les téléchargements de journaux de serveur Control Manager enfant**.

5. Sous Téléchargement des journaux, sélectionnez **Télécharger les journaux du serveur Control Manager enfant sur le serveur parent**.

6. Paramétrez la fréquence des téléchargements.

   - **Télécharger les journaux dès qu'ils sont disponibles**

     Sélectionnez cette option pour demander au serveur enfant d'envoyer les journaux directement au serveur parent.

     Remarque

     Si vous sélectionnez le **téléchargement immédiat des journaux**, le serveur enfant les enverra constamment au serveur parent, ce qui aura une incidence sur le trafic réseau.

   - **Programmer le téléchargement des journaux pour que ces derniers soient envoyés selon un planning défini**

a. Définissez la **Fréquence** : Quotidienne ou hebdomadaire.

b. Définissez **l'heure de début** en sélectionnant l'heure et les minutes dans la liste. Par défaut, l'heure de début est à 20:00.

7. Sélectionnez **Définir le temps maximum de téléchargement : heures** et définissez la durée à ne pas dépasser lors de l'envoi des journaux du serveur enfant au serveur parent. Le temps maximum de téléchargement par défaut est fixé à 8 heures.

8. Cliquez sur **Enregistrer**.

Remarque

Pour éviter un trafic réseau trop important pendant les heures de bureau, Trend Micro recommande les paramètres suivants : **Fréquence = Quotidienne** et **Heure de début = après les heures de bureau ou durant les heures creuses**. Toutefois, pendant la période qui sépare chaque téléchargement de journal, il se peut que le tableau État du composant de l'écran **État produit**, sur le serveur enfant, n'affiche pas les dernières informations en date concernant les produits gérés obsolètes, actuels et totaux.

Activation ou désactivation de la connexion du serveur enfant

Utilisez l'élément de menu Configuration pour activer ou désactiver la connexion du serveur enfant au serveur parent.

Procédure

1. Accédez à l'écran **Répertoire produits**.
2. Sélectionnez un serveur enfant dans le répertoire Produits.

   L'élément se met en surbrillance.
3. Déplacez le curseur sur **Configurer** dans le menu Répertoire Produits.

   Un menu déroulant apparaît.
4. Cliquez sur le lien **Activer ou désactiver une connexion à un serveur enfant**.

5. Dans la zone de travail, effectuez l'une des opérations suivantes :

   - Sélectionnez **Activer une connexion à ce serveur Control Manager enfant** pour activer un serveur enfant désactivé.
   - Sélectionnez **Désactiver la connexion à ce serveur Control Manager enfant** pour désactiver un serveur enfant activé.

AVERTISSEMENT!

Procédez avec précaution lorsque vous désactivez la connexion d'un serveur enfant. Les informations enregistrées sur les serveurs enfants concernant les produits gérés ne sont pas automatiquement transmises au serveur parent une fois la connexion du serveur enfant réactivée. Relancez le service Trend Micro Control Manager après avoir activé un serveur enfant, pour que les nouvelles informations sur les produits gérés soient téléchargées sur le serveur parent.

6. Cliquez sur **Appliquer**.

Exécution de tâches pour les serveurs enfants

Le menu Tâches permet d'effectuer les actions suivantes sur un serveur enfant précis ou sur tous les serveurs enfants :

- Déployer les règles anti-pourriel
- Déployer les moteurs
- Déployer les fichiers de signatures/modèles Damage Cleanup
- Déployer les fichiers programme

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Sélectionnez un serveur enfant dans le répertoire Produits.

3. Effectuez l'une des opérations suivantes :

   - Exécutez une tâche pour le serveur enfant

     a. Déplacez le curseur sur **Tâches** dans le menu Répertoire produits.

        Un menu déroulant apparaît.

     b. Cliquez sur l'une des tâches disponibles.

     c. Cliquez sur **Déployer maintenant**.

        Un écran de confirmation apparaît lorsque Control Manager a complété la tâche.

     d. Cliquez sur le lien **Détails sur la commande** de l'écran de réponse pour afficher les informations relatives à la commande ou cliquez sur **OK**.

   - Accédez à la console Web du serveur enfant

     a. Déplacez le curseur sur **Configurer** dans le menu Répertoire Produits.

        Un menu déroulant apparaît.

     b. Cliquez sur **Signature unique de Control Manager enfant**.

        La console Web du serveur enfant apparaît dans une nouvelle fenêtre.

     c. Connectez-vous au serveur enfant et effectuez les tâches requises.

Affichage des rapports de serveur enfant

Utilisez l'élément de menu **Tâches** > **Rapports** pour afficher les profils de rapport existants d'un serveur enfant pour les modèles de rapport Control Manager 3.

Pour afficher les rapports générés à l'aide des modèles de rapport Control Manager 5, utilisez la fonctionnalité SSO (Single Sign-On) pour vous connecter à la console Web du serveur Control Manager enfant.

Procédure

1. Accédez à l'écran **Répertoire produits**.
2. Sélectionnez un serveur enfant dans le répertoire Produits.

   L'élément se met en surbrillance.
3. Déplacez le curseur sur **Tâches** dans le menu Répertoire produits.

   Un menu déroulant apparaît.
4. Sélectionnez **Rapports** dans le menu déroulant.

   L'écran **Rapports** apparaît dans la zone de travail.

   Remarque

   Si l'écran **Rapports** contient plusieurs rapports, triez-les en fonction du nom du profil de rapport ou de la date de création.
5. Sous Rapports disponibles, cliquez sur le lien **Afficher** correspondant au profil de rapport à ouvrir.
6. Dans l'écran Rapports disponibles pour {nom du profil}, triez les rapports en fonction de l'**heure d'envoi** ou de l'**heure de réalisation de l'étape.**
7. Dans la colonne État, cliquez sur **Afficher le rapport de Control Manager enfant**.

   Une nouvelle fenêtre de navigateur s'ouvre et affiche le contenu du rapport.

Actualisation du répertoire Produits

Procédure

- Dans l'écran **Répertoire Produits**, cliquez sur l'icône **Actualiser** dans le coin supérieur droit de l'écran.

Remplacement du nom d'un serveur enfant

L'option Renommer permet de modifier le nom d'affichage d'entité d'un serveur enfant.

Procédure

1. Cliquez sur **Produits** dans le menu principal.

   L'écran **Répertoire Produits** apparaît.

2. Cliquez sur Gestion des répertoires.

   L'écran **Gestion des répertoires** apparaît.

3. Sélectionnez le serveur enfant à renommer.

4. Cliquez sur **Renommer**.

   L'écran **Renommer le répertoire** apparaît.

5. Saisissez un nom pour le serveur enfant dans le champ **Nom du répertoire**.

6. Cliquez sur **Enregistrer**.

   Un écran de confirmation apparaît.

7. Cliquez sur **OK**.

   Le serveur enfant s'affiche dans le répertoire Produits avec le nouveau nom.

Suppression de Serveur enfant supprimé accidentellement du Gestionnaire en cascade

Si vous supprimez accidentellement un serveur enfant du répertoire Produits, vous devrez désenregistrer puis réenregistrer le serveur enfant sur le serveur parent.

Chapitre 15

Gestion des stratégies

Ce chapitre contient des informations sur la manière d'exécuter la gestion des stratégies sur les produits gérés et les points finaux.

Ce chapitre contient les rubriques suivantes :

Description de la gestion des stratégies

La gestion des stratégies permet aux administrateurs d'appliquer les paramètres d'un produit dans les produits gérés et les points finaux à partir d'une seule console d'administration. Les administrateurs créent une stratégie en sélectionnant les cibles et en configurant une liste des paramètres du produit.

Une stratégie inclut les éléments suivants :

- Nom de la stratégie
- Cibles

  Les administrateurs peuvent sélectionner des cibles manuellement ou utiliser un filtre pour affecter automatiquement des cibles à leurs stratégies. La méthode de sélection de la cible détermine le type de stratégie et le fonctionnement de cette stratégie. Pour plus d'informations sur les types de stratégie, consultez la section *Description des types de stratégies à la page 15-4*.

  Pour définir un produit géré ou un point final comme une cible, assurez-vous que la version du produit géré ou du point final prend en charge la gestion des stratégies dans Control Manager. L'écran **Paramètres de modèle de stratégies** comprend des informations sur les versions de produits prises en charge.

- Paramètres

  Quand Control Manager déploie une stratégie dans les cibles, les paramètres définis dans la stratégie écrasent les paramètres existants dans les cibles. Control Manager applique les paramètres de la stratégie dans les cibles toutes les 24 heures. Bien que les administrateurs locaux puissent modifier les paramètres à partir de la console du produit géré, les modifications sont écrasées à chaque fois que Control Manager applique les paramètres de la stratégie.

Remarque

- Comme l'application de la stratégie n'a lieu que toutes les 24 heures, les paramètres du produit dans les cibles peuvent ne pas correspondre aux paramètres de la stratégie si les administrateurs locaux font des modifications via la console du produit géré entre deux périodes d'application.
- Les paramètres de la stratégie déployés vers les serveurs IMSVA ont la priorité sur les paramètres existants dans les serveurs cibles au lieu de les écraser. Les serveurs IMSVA sauvegardent ces paramètres de stratégie en haut de la liste.
- Si un client OfficeScan ayant une stratégie Control Manager qui lui est affectée a été déplacé dans un autre domaine OfficeScan, les paramètres du client seront temporairement remplacés par ceux définis par ce domaine OfficeScan. Quand Control Manager appliquera à nouveau la stratégie, les paramètres du client respecteront les paramètres de la stratégie.

Pour certains paramètres de produit, Control Manager doit obtenir des options de paramétrage spécifiques à partir des produits gérés. Si les administrateurs sélectionnent des cibles multiples pour une stratégie, Control Manager peut uniquement obtenir les options de paramétrage à partir de la première cible sélectionnée. Pour garantir un déploiement des stratégies réussi, assurez-vous que les paramètres du produit sont synchronisés dans les cibles.

Les administrateurs peuvent utiliser l'écran **Gestion des stratégies** pour effectuer les tâches suivantes :

- *Création d'une stratégie à la page 15-8*
- *Modification d'une stratégie à la page 15-15*
- *Suppression d'une stratégie à la page 15-16*
- *Copie des paramètres de stratégie à la page 15-14*
- *Réorganisation de la liste des stratégies à la page 15-17*

Remarque

Pour effectuer une gestion des stratégies sur un nouveau produit géré ou un point final, déplacez le produit géré depuis le dossier Nouvelle entité vers un autre dossier dans le répertoire Produits.

Description des types de stratégies

Control Manager fournit trois types de stratégies pouvant être créées par les administrateurs. Chaque type de stratégie diffère dans leur méthode de sélection de la cible, ce qui affecte le fonctionnement d'une stratégie. La liste des stratégies classe les types de stratégies dans l'ordre décrit dans le tableau suivant.

TABLEAU 15-1. Types de stratégies

TYPE DE STRATÉGIE	DESCRIPTION
Spécifié	• Utilise la fonction rechercher ou parcourir pour localiser des cibles spécifiques et les affecter manuellement à la stratégie • Utile quand les administrateurs planifient un déploiement de paramètres spécifiques uniquement dans certaines cibles • Reste statique au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées.
Filtré	• Utilise un filtre pour affecter automatiquement des cibles actuelles et futures à la stratégie • Utile pour le déploiement de paramètres standard dans un groupe de cibles • Les administrateurs peuvent modifier la priorité des stratégies filtrées dans la liste des stratégies • Pour plus d'informations sur la manière dont Control Manager affecte les cibles aux stratégies filtrées, consultez la section *Affectation de points finaux aux stratégies filtrées à la page 15-5* **Remarque** • Quand un administrateur réorganise la liste des stratégies, Control Manager affecte à nouveau les cibles aux différentes stratégies filtrées en fonction des critères de la cible et des rôles utilisateurs du créateur de chaque stratégie. • Le type de stratégie filtrée est uniquement disponible pour les paramètres de gestion d'OfficeScan.

TYPE DE STRATÉGIE	DESCRIPTION
Ébauche	Permet aux administrateurs de sauvegarder les paramètres de la stratégie en tant qu'ébauche sans choisir de cible. Control Manager enregistre les ébauches de stratégies avec la priorité la plus faible, en fin de liste.

Affectation de points finaux aux stratégies filtrées

Quand un nouveau point final s'enregistre auprès de Control Manager, il parcourt les stratégies filtrées de la liste par ordre décroissant. Control Manager affecte le nouveau point final à une stratégie filtrée quand les conditions suivantes sont toutes deux satisfaites :

- Le nouveau point final correspond aux critères de la cible dans la stratégie
- Le créateur de la stratégie a l'autorisation de gérer le nouveau point final

La même action s'applique à un point final déjà affecté à une stratégie, mais le créateur de la stratégie supprime la stratégie plus tard.

Remarque

Pour les points finaux qui viennent d'être enregistrés auprès de Control Manager et pour ceux qui viennent juste de sortir de stratégies supprimées, une période de grâce de trois minutes est appliquée durant laquelle aucune allocation de point final n'a lieu. Ces points finaux ne disposent temporairement pas de stratégie pendant cette période.

Si un point final ne correspond pas aux critères de la cible pour aucune des stratégies filtrées, le point final ne s'associe à aucune stratégie. Control Manager alloue ces points finaux à nouveau lorsque les actions suivantes se produisent :

- Créer une stratégie filtrée
- Modifier une stratégie filtrée
- Réorganiser les stratégies filtrées
- Programmer l'allocation journalière de points finaux

Control Manager utilise une programmation d'allocation journalière de points finaux pour garantir l'affectation des points finaux aux bonnes stratégies. Cette action se produit tous les jours à 15 h 15. Si les propriétés du point final changent, comme le système d'exploitation ou l'adresse IP, ces points finaux demandent à la programmation journalière de les réallouer aux bonnes stratégies.

Remarque

Si les points finaux sont hors ligne au moment de la programmation d'allocation des points finaux, l'état de la stratégie de ces points finaux restera en attente jusqu'à ce qu'ils soient connectés.

Quand les actions ci-dessus se produisent, Control Manager alloue les points finaux en fonction des conditions suivantes :

TABLEAU 15-2. Allocation de points finaux aux stratégies filtrées

	Nouveaux points finaux ou points finaux de stratégies supprimées	Points finaux sans stratégie	Points finaux avec stratégie
Créer une stratégie		●	
Modifier une stratégie	●	●	●
Réorganiser les stratégies filtrées	●	●	●
Programmer l'allocation journalière de points finaux	●	●	●

Description de la liste des stratégies

La liste des stratégies affiche les informations et l'état des stratégies créées par tous les utilisateurs. Quand un nouveau point final s'enregistre auprès de Control Manager, il parcourt les stratégies filtrées de la liste par ordre décroissant. Control Manager affecte le nouveau point final à une stratégie filtrée quand les conditions suivantes sont toutes deux satisfaites :

- Le nouveau point final correspond aux critères de la cible dans la stratégie
- Le créateur de la stratégie a l'autorisation de gérer le nouveau point final

Le tableau suivant décrit les éléments de la liste des stratégies.

TABLEAU 15-3. Liste des stratégies

ÉLÉMENT DE MENU	DESCRIPTION
Priorité	Affiche la priorité des stratégies. • Control Manager liste les stratégies en partant de la priorité la plus élevée à la priorité la plus basse. • Quand des administrateurs créent une stratégie filtrée, Control Manager enregistre la nouvelle stratégie en lui donnant la priorité la plus basse. • Une stratégie spécifiée a la priorité sur les stratégies filtrées et reste en début de liste. Les administrateurs ne peuvent pas réorganiser les stratégies spécifiées. • Control Manager place les ébauches de stratégies en fin de liste.
Stratégie	Indique le nom de la stratégie.
Cibles	Indique comment les administrateurs sélectionnent les cibles de la stratégie. • Spécifié : Utilise la fonction parcourir ou rechercher pour sélectionner les cibles spécifiques de la stratégie. Les stratégies spécifiées restent statiques au sommet de la liste des stratégies et a la priorité sur les stratégies filtrées. • Filtré : Utilise un filtre pour affecter automatiquement des points finaux actuels et futurs à la stratégie. Les administrateurs peuvent réorganiser la priorité des stratégies filtrées. • Aucune : Le créateur de la stratégie a sauvegardé la stratégie en tant qu'ébauche sans choisir de cible.
Déployé	Affiche le nombre de cibles qui ont appliqué les paramètres de la stratégie.

Élément de menu	Description
En attente	Affiche le nombre de cibles qui n'ont pas appliqué les paramètres de la stratégie. Cliquez sur le nombre en attente pour vérifier l'état de la stratégie.
Créateur	Affiche l'utilisateur ayant créé la stratégie.
Points finaux/produits sans stratégie	Affiche le nombre de produits gérés ou de points finaux auxquels Control Manager n'a affecté aucune stratégie.
Nombre de points finaux/ produits totaux	Affiche le nombre de produits gérés ou de points finaux disponibles pour une gestion des stratégies.

Remarque

Les nombres dans Déployé, En attente, Points finaux/Produits sans stratégie et les Points finaux totaux/produits ne reflètent que les points finaux

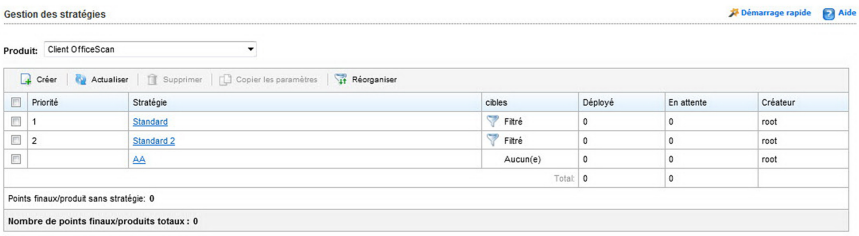
ou les produits gérés qu'un administrateur a le droit de gérer.

Création d'une stratégie

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

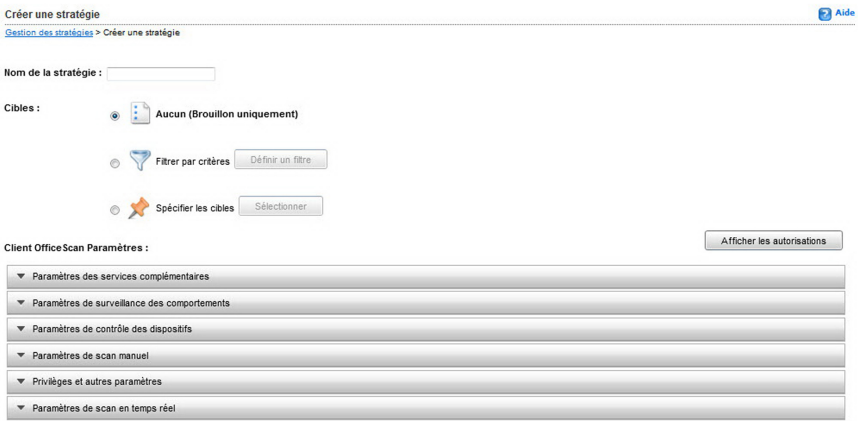


2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur **Créer**.

   L'écran **Créer une stratégie** apparaît.



4. Dans le champ **Nom de la stratégie**, saisissez un nom pour la stratégie.

5. Dans la section Cibles, sélectionnez une méthode d'affectation des cibles à la stratégie.

   - **Aucun (Brouillon uniquement)**

     Utilisez cette option pour sauvegarder la stratégie en tant qu'ébauche sans choisir de cible.

   - **Filtrer par critères**

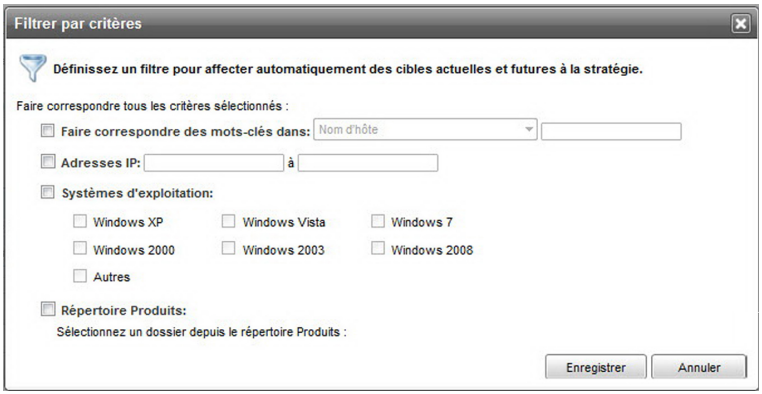
     Utilisez cette option pour allouer automatiquement des points finaux en fonction des critères de filtre.

     Remarque

     Cette option est uniquement disponible pour les paramètres OfficeScan.

     a. Cliquez sur **Définir un filtre**.

        L'écran **Filtrer par critères** apparaît.



b. Sélectionnez les options suivantes et définissez le critère. Control Manager affecte un point final à la stratégie si la stratégie correspond à tous les critères sélectionnés.

- **Faire correspondre des mots-clés dans**

  Définissez des mots-clés en fonction du nom de l'hôte ou du nom d'affichage de Control Manager.

- **Adresses IP**

  Remarque

  - La gestion des stratégies ne prend en charge que les adresses IPv4.
  - Quand un nouveau produit géré ou point final s'enregistre dans Control Manager, il faut environ une heure au produit géré ou au point final pour apparaître dans une recherche par adresse IP.

- **Systèmes d'exploitation**

- **Répertoire Produits**

  Sélectionnez un dossier depuis le répertoire Produits.

c. Cliquez sur **Enregistrer**.

Remarque

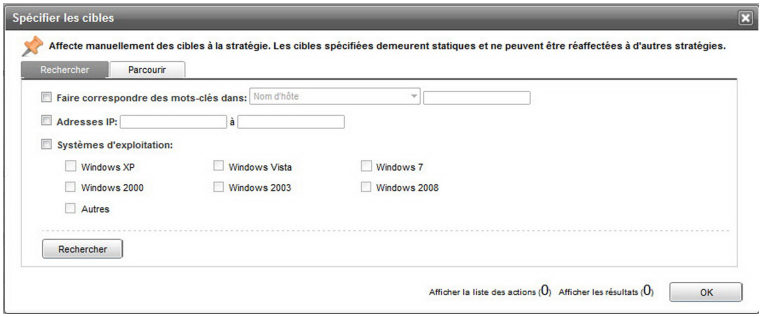
Control Manager peut seulement affecter des points finaux sans stratégies dans une nouvelle stratégie filtrée. Pour réallouer un point final déjà affecté à une stratégie filtrée, montez une autre stratégie filtrée avec les critères correspondants dans la liste de priorité.

- **Spécifier les cibles**

  Utilisez cette option pour sélectionner des points finaux ou des produits gérés spécifiques.

  a. Cliquez sur **Sélectionner**.

     L'écran **Spécifier les cibles** apparaît.



  b. Utilisez **Rechercher** ou **Parcourir** pour localiser les cibles.

     - **Rechercher** : Utilisez les critères de recherche suivants pour trouver les points finaux ou les produits gérés. Les résultats de la recherche affichent les points finaux ou les produits gérés qui correspondent à tous les critères sélectionnés.

       - **Faire correspondre des mots-clés dans**

         Définissez des mots-clés en fonction du nom de l'hôte ou du nom d'affichage de Control Manager.

       - **Adresses IP**

Remarque

- La gestion des stratégies ne prend en charge que les adresses IPv4.
- Quand un nouveau produit géré ou point final s'enregistre dans Control Manager, il faut environ une heure au produit géré ou au point final pour apparaître dans une recherche par adresse IP.

- **Systèmes d'exploitation**

- **Parcourir** : Parcourez le répertoire Produits ou Active Directory pour localiser les points finaux ou les produits gérés et les affecter à la stratégie.

Remarque

Pour des informations complémentaires sur le paramétrage d'Active Directory, consultez la section *Configuration des paramètres du widget de vérification d'Active Directory et de Protection des points finaux à la page 6-11*.

c. Sélectionnez les points finaux ou les produits gérés, puis cliquez sur **Ajouter les cibles sélectionnées**.

d. Attendez que les numéros changent dans **Afficher la liste des actions** et **Afficher les résultats**.

e. Cliquez sur **OK**.

6. Dans **Paramètres**, cliquez sur une fonctionnalité pour développer l'onglet et configurez ensuite les paramètres. Répétez l'étape pour configurer toutes les fonctionnalités.

   - Pour plus d'informations sur la configuration de chaque fonctionnalité, référez-vous à l'aide en ligne de Control Manager ou au manuel de l'administrateur du produit géré.
   - Pour plus d'informations sur le paramétrage des autorisations pour configurer les paramètres, consultez la section *Changement de la définition des autorisations à la page 15-13*.

7. Cliquez sur **Déployer**.

Control Manager démarre immédiatement pour déployer les paramètres dans les cibles. La stratégie apparaît dans la liste dans l'écran **Gestion des stratégies**.

Remarque

- Après avoir cliqué sur **Déployer**, veuillez attendre deux minutes pour que Control Manager puisse déployer la stratégie dans les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.
- Control Manager applique les paramètres de la stratégie dans les cibles toutes les 24 heures.

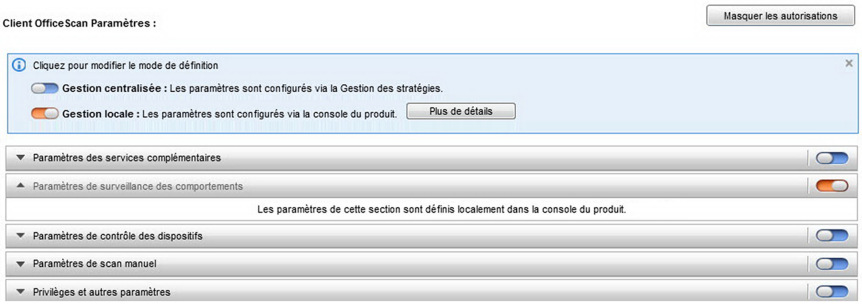
Changement de la définition des autorisations

En configurant les paramètres de la stratégie, les administrateurs peuvent attribuer aux administrateurs du produit géré les autorisations de définir les paramètres de certaines fonctionnalités. Suivez les étapes ci-dessous pour modifier les autorisations de configuration en créant ou en modifiant une stratégie :

Procédure

1. Dans la section Paramètres, cliquez sur **Afficher les autorisations**.

   Un commutateur apparaît sur le côté droit de chaque fonctionnalité.



2. Cliquez sur le commutateur pour modifier la définition de l'autorisation.

- **Gestion centralisée** (bleu) : Les cibles affectées suivront les paramètres définis dans la stratégie.
- **Gestion locale** (orange) : Control Manager ne déploie pas les paramètres de la fonction sélectionnée vers les cibles. Les administrateurs de produits gérés peuvent définir les paramètres à travers la console du produit.

Remarque

Quand les administrateurs déploient une stratégie ayant tous les paramètres des fonctionnalités passés sur géré localement, l'état de la stratégie des cibles sera en attente.

Copie des paramètres de stratégie

Les administrateurs peuvent copier les paramètres à partir d'une stratégie existante, créer une nouvelle stratégie avec les mêmes paramètres et déployer les paramètres dans différents points finaux ou produits gérés.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Sélectionnez une stratégie dans la liste.
4. Cliquez sur **Copier les paramètres**.

   L'écran **Copier et créer une stratégie** apparaît.

5. Dans le champ **Nom de la stratégie**, saisissez un nom pour la stratégie.
6. Affectez des **Cibles** à la stratégie.
7. Cliquez sur **Déployer**.

Remarque

- Après avoir cliqué sur **Déployer**, veuillez attendre deux minutes pour que Control Manager puisse déployer la stratégie dans les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.
- Control Manager applique les paramètres de la stratégie dans les cibles toutes les 24 heures.

Modification d'une stratégie

Les administrateurs peuvent modifier les informations d'une stratégie, incluant le nom de la stratégie, les cibles et les paramètres. Seul le créateur de la stratégie peut modifier la stratégie.

Control Manager prend en charge les modifications suivantes :

- modification d'une stratégie filtrée
- ajout de cibles à une stratégie spécifiée
- suppression de cibles d'une stratégie spécifiée

Remarque

Control Manager permet uniquement la modification des stratégies par leur créateur. Cependant, le compte racine peut modifier toutes les stratégies de la liste.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur le nom d'une stratégie dans la colonne **Stratégie**.

L'écran **Modifier une stratégie** apparaît.

4. Modifiez la stratégie.

Remarque

La modification des critères de filtre dans une stratégie filtrée peut affecter l'allocation de la cible. Control Manager peut réaffecter des cibles à d'autres stratégies filtrées ou ajouter des cibles supplémentaires à la stratégie en cours.

5. Cliquez sur **Déployer**.

Les modifications s'appliquent immédiatement.

Remarque

- Après avoir cliqué sur **Déployer**, veuillez attendre deux minutes pour que Control Manager puisse déployer la stratégie dans les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.
- Control Manager applique les paramètres de la stratégie dans les cibles toutes les 24 heures.

Suppression d'une stratégie

Les administrateurs peuvent supprimer une stratégie de la liste. Control Manager réalloue alors les cibles associées à la stratégie supprimée si les cibles correspondent aux critères de filtre d'une autre stratégie. Celles qui ne correspondent pas deviennent des points finaux sans stratégie et gardent alors les paramètres définis par la stratégie supprimée sauf si un administrateur de produit géré modifie ces paramètres.

Remarque

Control Manager permet uniquement la suppression des stratégies par leur créateur. Cependant, le compte racine peut supprimer toutes les polices de la liste.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Sélectionnez la stratégie à supprimer.

4. Cliquez sur **Supprimer**.

   Un écran de confirmation apparaît.

5. Cliquez sur **OK**.

Réorganisation de la liste des stratégies

Les administrateurs peuvent utiliser le bouton Réorganiser pour modifier l'ordre des stratégies filtrées. La réorganisation de la liste des stratégies peut affecter l'allocation de la cible. Control Manager peut réaffecter des cibles à des stratégies filtrées différentes.

Remarque

- Les stratégies spécifiées restent statiques et ont toujours la priorité sur les stratégies filtrées.
- Cette fonction n'est disponible que pour la gestion des paramètres OfficeScan.

Procédure

1. Accédez à **Stratégies** > **Gestion des stratégies**.

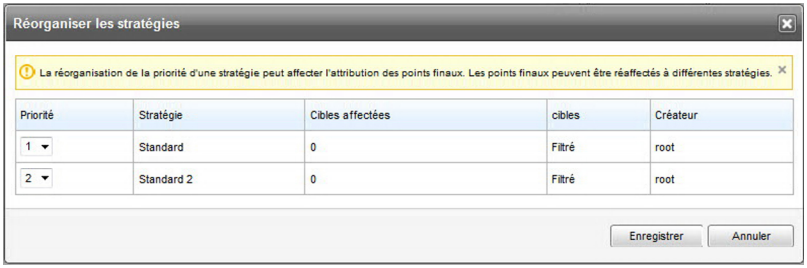
   L'écran **Gestion des stratégies** apparaît.

2. Sélectionnez les paramètres de type de produit dans la liste **Produits**.

   L'écran est actualisé pour afficher les stratégies créées du produit géré sélectionné.

3. Cliquez sur **Réorganiser**.

   L'écran **Réorganiser les stratégies** apparaît.



4. Réorganisez l'ordre de la colonne **Priorité**.

5. Cliquez sur **Enregistrer**.

Remarque

Après avoir cliqué sur **Enregistrer**, veuillez attendre deux minutes pour que Control Manager puisse réaffecter les cibles. Cliquez sur **Actualiser** dans l'écran **Gestion des stratégies** pour mettre à jour les informations d'état dans la liste des stratégies.

Description de la liste des serveurs gérés

L'écran **Serveurs gérés** affiche les serveurs pouvant être gérés par les administrateurs à l'aide de la gestion des stratégies. Utilisez l'écran pour ajouter et modifier les produits gérés qui n'ont pas d'agents MCP.

Remarque

Si le bouton **Ajouter** n'est pas actif, la gestion des stratégies ne prend en charge que les produits gérés à l'aide des agents MCP.

Pour les produits gérés à l'aide des agents MCP, Control Manager utilise la fonction d'authentification unique (SSO) par défaut pour accéder à ces produits. Les

administrateurs peuvent modifier les informations d'authentification pour les raisons suivantes :

- La fonction SSO ne fonctionne pas correctement
- Les administrateurs veulent accéder au produit géré en utilisant un autre compte

TABLEAU 15-4. Liste des serveurs gérés

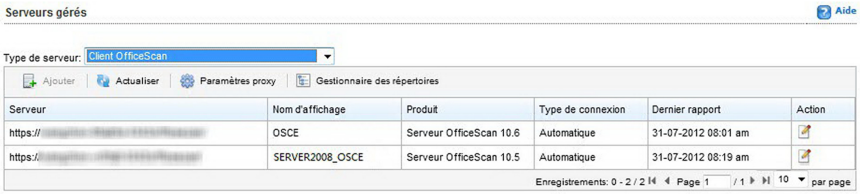
ÉLÉMENT DE MENU	DESCRIPTION
Serveur	Affiche le nom du serveur du produit géré.
Nom d'affichage	Affiche le nom d'affichage du serveur du produit géré.
Produit	Affiche le nom du produit géré.
Type de connexion	Affiche la manière pour le produit géré de s'enregistrer auprès de Control Manager. • Automatique : Le produit géré s'enregistre auprès de Control Manager via un agent MCP. • Manuel : Les administrateurs ajoutent manuellement le produit géré dans l'écran **Serveurs gérés**
Dernier rapport	Indique la date et l'heure auxquelles Control Manager a reçu une réponse du produit géré.
État	Indique l'état de la connexion entre Control Manager et le produit géré.
Actions	• Modifier : Cliquez sur cette icône pour mettre à jour les informations du serveur. • Supprimer : Cliquez sur cette icône pour supprimer un serveur ajouté manuellement. **Remarque** Control Manager ne peut pas supprimer des serveurs enregistrés à l'aide d'agents MCP.

Ajout d'un serveur

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Serveurs gérés**.

   L'écran **Serveurs gérés** apparaît.



2. Cliquez sur **Ajouter**.

   L'écran **Ajouter un serveur** apparaît.

3. Saisissez le nom du serveur dans le champ **Serveur**.

4. Spécifiez un nom d'affichage dans le champ fourni à cet effet.

5. Sélectionnez le produit géré dans la liste **Produits**.

6. Indiquez le nom d'utilisateur et le mot de passe du produit géré. Un compte avec les privilèges administrateur est requis pour permettre au Control Manager de déployer les paramètres de stratégies.

7. Sélectionnez **Utiliser un serveur proxy pour la connexion**. Pour des informations complémentaires sur le paramétrage de la connexion au serveur proxy, consultez la section *Configuration des paramètres proxy à la page 15-21*.

8. Cliquez sur **Enregistrer**.

Remarque

Pour effectuer une gestion des stratégies sur un nouveau produit géré, déplacez le produit géré depuis le dossier **Nouvelle entité** vers un autre dossier dans le répertoire Produits.

Modification d'un serveur

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Serveurs gérés**.

   L'écran **Serveurs gérés** apparaît.

2. Cliquez sur l'icône **Modifier** dans la colonne **Actions**.

3. Modifiez les informations du serveur.

4. Cliquez sur **Enregistrer**.

Configuration des paramètres proxy

Utilisez un serveur proxy pour vous connecter aux produits gérés.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Serveurs gérés**.

   L'écran **Serveurs gérés** apparaît.

2. Cliquez sur **Paramètres proxy**.

3. Sélectionnez le protocole :
   - **HTTP**
   - **SOCKS 5**
4. Saisissez le nom du serveur dans le champ **Serveur**.
5. Saisissez le numéro de port dans le champ **Port**.
6. Saisissez le nom d'utilisateur et le mot de passe pour accéder au serveur s'il requiert une authentification.
7. Cliquez sur **Enregistrer**.

Mise à jour des modèles de stratégie

L'écran **Paramètres de modèle de stratégie** liste les composants suivants disponibles pour l'activation ou la mise à niveau par les administrateurs :

- Structure de gestion des stratégies : La structure globale de la stratégie

- Assistance produit : Les modèles définis pour les produits gérés et les points finaux

Remarque

Pour vérifier les versions du produit qui prennent en charge la gestion des stratégies, déplacez le curseur de la souris sur l'icône d'information dans la colonne Version du modèle.

Procédure

1. Téléchargez la dernière version du composant **Pool de widgets de Control Manager et modèles de stratégie (Control Manager 6.0 et version ultérieure)**.

   Une notification en bleu apparaîtra en haut des écrans **Tableau de bord** et **Gestion des stratégies**.

2. Cliquez sur **Mettre à jour maintenant** dans la boîte de dialogue de notification sur chacun de ces écrans.

3. Cliquez sur **OK** quand la mise à jour est terminée.

   La fenêtre s'actualise et l'écran de connexion s'affiche.

4. Connectez-vous à la console Web.

5. Accédez à **Stratégies** > **Ressources de stratégies** > **Paramètres de modèle de stratégie**.

   L'écran **Paramètres de modèle de stratégie** apparaît.

6. Cliquez sur **Mise à jour <numéro de version>** dans la ligne de la structure de la stratégie.

7. Pour ajouter un nouveau modèle de stratégie, cliquez sur **Activer** dans la colonne Action.

   Les administrateurs peuvent alors sélectionner les nouveaux modèles définis dans la liste **Produits** de l'écran **Gestion des stratégies**.

8. Pour mettre à jour un modèle existant, cliquez sur **Mise à jour <numéro de version>** dans la colonne Action.

Remarque

Pour obtenir plus d'informations sur la mise à jour, cliquez sur **Détails** dans la colonne Action.

Une fois la mise à jour terminée, les administrateurs peuvent vérifier les fonctionnalités mises à jour en modifiant les stratégies existantes. Dans la section Paramètres, un message en rouge apparaît à côté du titre de la nouvelle fonctionnalité.

Description de la prévention contre la perte de données

La prévention contre la perte de données (DLP) protège les données sensibles et confidentielles d'une entreprise – appelées actifs numériques – contre les fuites de données délibérées ou accidentelles. DLP vous permet :

- d'identifier l'actif numérique à protéger ;
- de créer des stratégies qui limitent ou empêchent la transmission d'actifs numériques par les canaux de transmission classiques, tels que les e-mails et les dispositifs externes ;
- de renforcer la conformité à des normes de confidentialité établies.

DLP évalue les données par rapport à un ensemble de règles définies dans les stratégies. Les stratégies déterminent les données devant être protégées des transmissions non autorisées et l'action que DLP doit effectuer lorsqu'il détecte une transmission.

Types d'identificateurs de données

Les actifs numériques sont des fichiers et des données qu'une entreprise doit protéger contre les transmissions non autorisées. Vous pouvez définir les actifs numériques à l'aide des identificateurs de données suivants :

- **Expressions** : données ayant une certaine structure. Pour obtenir des informations détaillées, consultez la section *Expressions à la page 15-25*.

- **Attributs de fichier** : propriétés d'un fichier, tels le type de fichier ou la taille du fichier. Pour obtenir des informations détaillées, consultez la section *Attributs de fichier à la page 15-30*.
- **Mots-clés** : liste de mots ou phrases particuliers. Pour obtenir des informations détaillées, consultez la section *Mots-clés à la page 15-33*.

Remarque

Il n'est pas possible de supprimer un identificateur de données qui est utilisé dans un modèle DLP. Supprimez le modèle pour pouvoir supprimer l'identificateur de données.

Expressions

Une expression est constituée de données ayant une certaine structure. Par exemple, une carte de crédit possède généralement un numéro à 16 chiffres, présenté sous le format « nnnn-nnnn-nnnn-nnnn », pouvant être localisé lors d'une détection basée sur les expressions.

Vous pouvez utiliser des expressions prédéfinies et personnalisées. Pour obtenir des informations détaillées, consultez les sections *Expressions prédéfinies à la page 15-25* et *Expressions personnalisées à la page 15-26*.

Expressions prédéfinies

Un produit Trend Micro est fourni avec un jeu d'expressions prédéfinies. Ces expressions ne peuvent pas être modifiées ou supprimées.

Un produit Trend Micro vérifie ces expressions au moyen du processus de correspondance des signatures et d'équations mathématiques. Lorsqu'un produit Trend Micro fait correspondre des données potentiellement sensibles avec une expression, les données peuvent également être soumises à des vérifications supplémentaires.

Pour obtenir une liste complète d'expressions prédéfinies, accédez à http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Affichage des paramètres des expressions prédéfinies

Remarque

Les expressions prédéfinies ne peuvent pas être modifiées ou supprimées.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur le nom de l'expression.
4. Consultez les paramètres sur l'écran qui s'affiche.

Expressions personnalisées

Si aucune des expressions prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Les expressions constituent un outil puissant de correspondance de chaînes. Avant de procéder à la création d'expressions, vérifiez que vous maîtrisez la syntaxe des expressions. Les expressions mal formulées peuvent avoir un impact conséquent sur les performances.

Lors de la création d'expressions :

- Reportez-vous aux expressions prédéfinies pour savoir comment définir une expression valide. Par exemple, si vous créez une expression qui comprend une date, vous pouvez vous référer aux expressions précédées de « Date ».
- Notez qu'un produit Trend Micro respecte les formats d'expression définis dans la bibliothèque Perl Compatible Regular Expressions (PCRE). Pour plus d'informations sur la PCRE, consultez le site Web suivant :

  http://www.pcre.org/
- Commencez par des expressions simples. Modifiez les expressions si celles-ci déclenchent de fausses alertes ou ajustez-les pour améliorer les détections.

Lors de la création d'expressions, plusieurs critères sont à votre disposition. Une expression doit correspondre aux critères que vous avez choisis pour que le produit Trend Micro puisse la soumettre à une stratégie de prévention contre la perte de données. Pour plus de détails sur les différentes actions, reportez-vous à *Critères applicables aux expressions personnalisées à la page 15-27*.

Critères applicables aux expressions personnalisées

TABLEAU 15-5. Options de critères pour des expressions personnalisées

CRITÈRES	RÈGLE	EXEMPLE
Aucun	Aucun	Tous - Noms du Bureau du recensement des États-Unis Expression : [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
Caractères spécifiques	Une expression doit intégrer les caractères que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	US – Numéro de routage ABA Expression : [^\d]([0123678]\d{8})[^\d] Caractères : 0123456789 Caractères minimum : 9 Caractères maximums : 9

CRITÈRES	RÈGLE	EXEMPLE
Suffixe	Le suffixe correspond au dernier segment d'une expression. Un suffixe doit compter un certain nombre de caractères et inclure ceux que vous avez spécifiés. De plus, le nombre de caractères de l'expression doit être compris dans les limites minimale et maximale définies.	Tous - Adresse de domicile Expression : \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] Caractères pour le suffixe : 0123456789- Nombre de caractères : 5 Nombre minimum de caractères dans l'expression : 25 Nombre maximum de caractères dans l'expression : 80
Un seul caractère de séparation	Une expression doit comporter deux segments séparés par un caractère. Le caractère doit avoir une longueur d'un octet. De plus, le nombre de caractères situés à gauche du séparateur doit être compris dans les limites minimale et maximale définies. Le nombre de caractères situés à droite ne doit pas dépasser la limite maximale.	Tous - Adresse électronique Expression : [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] Séparateur : @ Nombre minimum de caractères à gauche : 3 Nombre maximum de caractères à gauche : 15 Nombre maximum de caractères à droite : 30

Création d'une expression personnalisée

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.

2. Cliquez sur l'onglet **expression**.

3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

4. Entrez un nom pour l'expression. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

5. Saisissez une description ne dépassant pas 256 octets en longueur.

6. Saisissez l'expression et indiquez si celle-ci respecte la casse.

7. Saisissez les données affichées.

   Par exemple, si vous créez une expression pour des numéros ID, saisissez un exemple de numéro ID. Ces données sont utilisées à des fins de référence uniquement et ne figureront pas sur le produit.

8. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère (voir *Critères applicables aux expressions personnalisées à la page 15-27*) :

   - Aucun
   - Caractères spécifiques
   - Suffixe
   - Un seul caractère de séparation

9. Testez l'expression avec une donnée actuelle.

   Par exemple, si l'expression s'applique à un ID national, entrez un numéro ID valide dans la zone de texte **Données de test**, cliquez sur **Tester**, puis vérifiez le résultat.

10. Cliquez sur **Enregistrer** si vous êtes satisfait du résultat.

Remarque

Enregistrez les paramètres uniquement si le test a réussi. Une expression qui ne détecte aucune donnée consomme les ressources du système inutilement et peut avoir une influence négative sur les performances.

Importation d'une expression personnalisée

Si le formatage du fichier `.dat` contenant les expressions est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les expressions à partir du serveur du produit Trend Micro actif ou à partir d'un autre serveur de produit Trend Micro.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.
2. Cliquez sur l'onglet **expression**.
3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les expressions.
4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une expression à importer existe déjà, elle sera ignorée.

Attributs de fichier

Les attributs de fichier sont des propriétés spécifiques à un fichier. Vous pouvez utiliser deux attributs de fichier lorsque vous définissez des identificateurs de données, à savoir le type de fichier et la taille de fichier. Par exemple, une entreprise de développement de logiciels souhaitera peut-être limiter le partage du programme d'installation du logiciel de l'entreprise aux membres du service de recherche et développement, lesquels sont chargés de développer et tester le logiciel. Dans ce cas, l'administrateur du produit Trend Micro peut créer une stratégie qui bloque la transmission des fichiers exécutables de 10 à 40 Mo vers l'ensemble des départements, à l'exception de celui de la R&D.

Les attributs de fichier ne permettent pas, en tant que tels, d'identifier les fichiers sensibles. Si nous reprenons l'exemple cité dans cette rubrique, les programmes d'installation de logiciels tiers partagés par d'autres départements risquent d'être bloqués. Par conséquent, Trend Micro recommande d'associer les attributs de fichier à d'autres identificateurs de données pour la prévention contre la perte de données, ce, pour permettre une détection plus ciblée des fichiers sensibles.

Pour obtenir une liste complète d'expressions prédéfinies, voir http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Création d'une liste d'attributs de fichier

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.
2. Cliquez sur l'onglet **attribut de fichier**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Saisissez un nom pour la liste d'attributs de fichier. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets en longueur.
6. Sélectionnez vos véritables types de fichiers favoris.
7. Si un type de fichier que vous souhaitez inclure n'est pas répertorié, sélectionnez **Extensions de fichiers** et entrez l'extension du type de fichier. Un produit Trend Micro vérifie les fichiers ayant l'extension spécifiée, mais pas leurs véritables types de fichier. Directives à suivre lorsque vous saisissez des extensions de fichiers :

   - Chaque extension doit commencer par un astérisque (*), suivi d'un point (.) et ensuite de l'extension. L'astérisque est un caractère générique qui représente un nom réel de fichier. Par exemple, `*.pol` correspond à `12345.pol` et `test.pol`.

- Vous pouvez inclure des caractères génériques dans les extensions. Utilisez un point d'interrogation (?) pour représenter un seul caractère et un astérisque (*) pour deux caractères ou plus. Voir les exemples suivants :

  - `*.*m` correspond aux fichiers suivants : `ABC.dem`, `ABC.prm`, `ABC.sdcm`

  - `*.m*r` correspond aux fichiers suivants : `ABC.mgdr`, `ABC.mtp2r`, `ABC.mdmr`

  - `*.fm?` correspond aux fichiers suivants : `ABC.fme`, `ABC.fml`, `ABC.fmp`

- Faites attention si vous utilisez un astérisque à la fin d'une extension car il peut correspondre à des parties de noms de fichiers et à une extension sans rapport. Par exemple : `*.do*` correspond à `abc.doctor_john.jpg` et `abc.donor12.pdf`.

- Utilisez les points-virgules (;) pour séparer les extensions de fichier. Il n'est pas nécessaire d'ajouter un espace après un point-virgule.

8. Entrez les tailles de fichier minimale et maximale en octets. Les valeurs doivent être des entiers non nuls.

9. Cliquez sur **Enregistrer**.

Importation d'une liste d'attributs de fichier

Si le formatage du fichier `.dat` contenant les listes d'attributs de fichier est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les listes d'attributs de fichier à partir du serveur du produit Trend Micro actif ou à partir d'un autre serveur de produit Trend Micro.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.

2. Cliquez sur l'onglet **attribut de fichier**.

3. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les listes d'attributs de fichier.

4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste d'attributs de fichier à importer existe déjà, elle sera ignorée.

Mots-clés

Les mots-clés sont des expressions ou des mots spéciaux. Vous pouvez ajouter des mots-clés de la même famille à une liste de mots-clés afin d'identifier un certain nombre de données spécifiques. Par exemple, « pronostic », « groupe sanguin », « vaccination » et « médecin » sont des mots-clés pouvant apparaître dans un certificat médical. Si vous souhaitez éviter la transmission de fichiers contenant des certificats médicaux, vous pouvez utiliser ces mots-clés dans une stratégie de prévention contre la perte de données, puis configurer un produit Trend Micro de manière à bloquer les fichiers contenant ces mots-clés.

Les mots habituellement utilisés peuvent être associés afin de former des mots-clés significatifs. Par exemple, « end », « read », « if » et « at » peuvent être associés pour former des mots-clés présents dans du code source, tels que « END-IF », « END-READ » et « AT END ».

Vous pouvez utiliser des listes de mots-clés prédéfinies et personnalisées. Pour obtenir des informations détaillées, voir *Listes de mots-clés prédéfinies à la page 15-33* et *Listes de mots-clés personnalisées à la page 15-35*.

Listes de mots-clés prédéfinies

Un produit Trend Micro est fourni avec un jeu de listes de mots-clés prédéfinies. Ces listes de mots-clés ne peuvent pas être modifiées ou supprimées. Chaque liste a ses propres conditions intégrées qui déterminent si le modèle doit déclencher une violation de stratégie.

Pour plus d'informations sur les listes de mots-clés prédéfinies dans un produit Trend Micro, consultez http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Fonctionnement des listes de mots-clés

Condition de nombre de mots-clés

Chaque liste de mots-clés contient une condition qui requiert qu'un certain nombre de mots-clés existe dans un document avant que la liste ne déclenche une violation.

La condition du nombre de mots-clés contient les valeurs suivantes :

- **Tous** : Tous les mots-clés de la liste doivent exister dans le document.
- **Tout** : N'importe quel mot-clé de la liste doit exister dans le document.
- **Nombre spécifique** : Le document doit comporter au moins le nombre spécifié de mots-clés. S'il y a plus de mots-clés dans le document que le nombre spécifié, une violation se déclenche.

Condition de distance

Certaines des listes contiennent une condition de « distance » pour savoir si une violation est présente. « Distance » se réfère au nombre de caractères existant entre le premier caractère d'un mot clé et le premier caractère d'un autre mot-clé. L'entrée suivante peut servir d'exemple :

F**irst Name:_John_ L**ast Name:_Smith_

La liste des **Formulaires - Prénom, nom** comporte une condition de « distance » de cinquante (50) et les champs de formulaire couramment utilisés de « Prénom » et « Nom ». Dans l'exemple ci-dessus, une violation se déclenchera car le nombre de caractères entre le « F » de « first name » et le « L » de « last name » est égal à dix-huit (18).

Voici un exemple d'entrée qui ne déclenchera pas de violation :

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

Dans cet exemple, le nombre de caractères entre le « f » de « first name » et le « l » de « last name » est soixante et un (61). Cela dépasse le seuil de distance et ne déclenche pas de violation.

Listes de mots-clés personnalisées

Si aucune des listes de mots-clés prédéfinies ne correspond à vos besoins, vous avez la possibilité d'en créer des personnalisées.

Lors de la configuration d'une liste de mots-clés, plusieurs critères sont à votre disposition. Une liste de mots-clés doit correspondre aux critères que vous avez choisis avant qu'un produit Trend Micro puisse la soumettre à une stratégie de prévention contre la perte des données. Pour chaque liste de mots-clés, choisissez l'un des critères suivants :

- **N'importe quel mot-clé**
- **Tous les mots-clés**
- **Tous les mots-clés de <x> caractères maximum**
- **Le score combiné des mots-clés dépasse le seuil**

Pour plus d'informations concernant les règles de critères, voir *Critères des listes personnalisées de mots-clés à la page 15-35*.

Critères des listes personnalisées de mots-clés

TABLEAU 15-6. Critères pour une liste de mots-clés

CRITÈRES	RÈGLE
N'importe quel mot-clé	Un fichier doit contenir au moins un mot-clé de la liste.
Tous les mots-clés	Le fichier doit contenir tous les mots-clés de la liste.

CRITÈRES	RÈGLE
Tous les mots-clés de <x> caractères maximum	Le fichier doit contenir tous les mots-clés de la liste. En plus, chaque paire de mots-clés doit se trouver à <x> caractères maximum l'un de l'autre. Par exemple, vos trois mots-clés sont WEB, DISK et USB. Le nombre spécifié de caractères est 20. Si un produit Trend Micro détecte tous les mots clés dans l'ordre DISK, WEB et USB, le nombre de caractères compris entre « D » (de DISK) et « W » (de WEB) et entre « W » et « U » (de USB) devra être de 20 au maximum. Les données suivantes correspondent au critère : DISK####WEB############USB Les données suivantes ne correspondent pas au critère : DISK******************WEB****USB(23 caractères entre « D » et « W ») Lors du choix du nombre de caractères, rappelez-vous qu'un faible nombre, comme 10, entraînera une exécution plus rapide du scan, mais couvrira uniquement une zone relativement réduite. Cela peut réduire les possibilités de détection de données sensibles, notamment dans les fichiers volumineux. Plus le nombre est grand, plus grande sera la zone couverte, mais le scan peut être plus lent.
Le score combiné des mots-clés dépasse le seuil	Un fichier doit contenir au moins un mot-clé de la liste de mots-clés. Si un seul mot-clé est détecté, son score doit être supérieur au seuil défini. Si plusieurs mots-clés sont détectés, leur score combiné doit être supérieur au seuil défini. Attribuez à chaque mot-clé un score de 1 à 10. Un terme ou une phrase à haute confidentialité, comme « augmentation des salaires » pour le département des ressources humaines, doit avoir un score relativement élevé. Les mots ou les expressions qui, en eux-mêmes, n'ont pas de poids significatif peuvent avoir des scores plus faibles. Tenez compte des scores attribués aux mots-clés lors de la configuration du seuil. Par exemple, si vous avez cinq mots-clés dont trois avec une priorité élevée, le seuil peut être égal ou inférieur au score combiné des trois mots-clés à priorité élevée. Cela signifie que la détection de ces trois mots-clés est suffisante pour traiter le fichier comme sensible.

Création d'une liste Mot-clé

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.
2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.
4. Entrez un nom pour la liste de mots-clés. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /
5. Saisissez une description ne dépassant pas 256 octets en longueur.
6. Choisissez l'un des critères suivants, puis configurez des paramètres complémentaires pour ce critère :

   - **N'importe quel mot-clé**
   - **Tous les mots-clés**
   - **Tous les mots-clés de <x> caractères maximum**
   - **Le score combiné des mots-clés dépasse le seuil**
7. Pour ajouter manuellement des mots-clés à la liste :

   a. Saisissez un mot-clé d'une longueur de 3 à 40 octets et indiquez s'il respecte la casse.

   b. Cliquez sur **Ajouter**.
8. Pour ajouter des mots-clés à l'aide de l'option d'« importation » :

Remarque

Si le formatage du fichier .csv contenant les mots-clés est approprié, utilisez cette fonction. Pour générer le fichier, vous pouvez exporter les mots-clés à partir du serveur d'un produit Trend Micro actif ou à partir d'un autre serveur de produit Trend Micro.

a. Cliquez sur **Importer** et identifiez le fichier `.csv` contenant les mots-clés.

b. Cliquez sur **Ouvrir**.

Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un mot-clé à importer existe déjà dans la liste, il sera ignoré.

9. Pour supprimer des mots-clés, sélectionnez-les puis cliquez sur **Supprimer**.

10. Pour exporter des mots-clés :

Remarque

Utilisez la fonctionnalité « exporter » pour sauvegarder les mots-clés ou les importer sur un autre serveur de produit Trend Micro. Tous les mots-clés de la liste seront exportés. Il n'est pas possible d'exporter un mot-clé individuel.

a. Cliquez sur **Exporter**.

b. Enregistrez le fichier `.csv` obtenu à l'emplacement de votre choix.

11. Cliquez sur **Enregistrer**.

Importation d'une liste Mot-clé

Utilisez cette option si vous avez un fichier `.dat` correctement formaté et contenant les listes de mots-clés. Pour générer le fichier, vous pouvez exporter les listes de mots-clés à partir du serveur du produit Trend Micro actif ou à partir de tout autre serveur d'un produit Trend Micro.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Indicateurs de données DLP**.

2. Cliquez sur l'onglet **Mot-clé**.
3. Cliquez sur **Importer** et identifiez le fichier `.dat` contenant les listes de mots-clés.
4. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si une liste de mots-clés à importer existe déjà, elle sera ignorée.

Modèles de prévention contre la perte de données

Un modèle DLP réunit les identificateurs de données et les opérateurs logiques (Et, Ou, Sauf) pour former des conditions. Seuls les fichiers ou les données qui satisfont à certaines conditions feront l'objet d'une stratégie de prévention contre la perte des données.

Par exemple, un fichier doit être un fichier Microsoft Word (attribut de fichier) ET doit contenir certains termes légaux (mots-clés) ET doit contenir des numéros d'identification (expressions) afin de devenir une stratégie de « Contrats de travail ». Cette stratégie autorise le personnel des Ressources humaines à imprimer le fichier afin que cette copie soit signée par un employé. La transmission par le biais de tous les autres canaux possibles, tels que le courrier électronique, est bloquée.

Vous pouvez créer vos propres modèles si vous avez configuré des identificateurs de données. Vous pouvez également utiliser des modèles prédéfinis. Pour obtenir des informations détaillées, voir *Modèles DLP personnalisés à la page 15-40* et *Modèles DLP prédéfinis à la page 15-39*.

Remarque

Il n'est pas possible de supprimer un modèle utilisé dans une stratégie de prévention contre la perte des données. Supprimez le modèle de la stratégie pour pouvoir la supprimer.

Modèles DLP prédéfinis

Un produit Trend Micro est fourni avec un jeu de modèles prédéfinis que vous pouvez utiliser afin de répondre à diverses normes de contrôle. Ces modèles ne peuvent pas être modifiés ou supprimés.

- **GLBA** : Loi Gramm-Leach-Billey Act
- **HIPAA** : Loi Health Insurance Portability and Accountability Act
- **PCI-DSS** : Norme de sécurité des données pour l'industrie des cartes de paiement
- **SB-1386** : US Senate Bill 1386 (Loi du Sénat américain)
- **US PII** : Données d'identification personnelles des États-Unis

Pour obtenir une liste plus détaillée sur tous les modèles prédéfinis, avec des exemples de données sous protection, voir http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Modèles DLP personnalisés

Créez vos propres modèles si vous avez configuré les identificateurs de données. Un modèle réunit des identificateurs de données et des opérateurs logiques (Et, Ou, Sauf) pour former des déclarations de condition.

Pour plus d'informations et d'exemples sur le fonctionnement des déclarations de condition et des opérateurs logiques, voir *Conditions et opérateurs logiques à la page 15-40*.

Conditions et opérateurs logiques

Un produit Trend Micro évalue les instructions conditionnelles de gauche à droite. Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus.

Reportez-vous aux exemples dans le tableau ci-dessous.

TABLEAU 15-7. Exemples de conditions

CONDITION	INTERPRÉTATION ET EXEMPLE
[Identificateur de données 1] **et** [Identificateur de données 2] **sauf** [Identificateur de données 3]	Un fichier doit satisfaire [Identificateur de données 1] et [Identificateur de données 2], mais pas [Identificateur de données 3]. Par exemple : Un fichier doit être [au format Adobe PDF] et doit contenir [une adresse e-mail], mais ne doit pas contenir [tous les mots-clés de la liste].
[Identificateur de données 1] **ou** [Identificateur de données 2]	Un fichier doit satisfaire [Identificateur de données 1] ou [Identificateur de données 2]. Par exemple : Un fichier doit être [un document Adobe PDF] ou [un document Microsoft Word].
Sauf [Identificateur de données 1]	Un fichier ne doit pas satisfaire [Identificateur de données 1]. Par exemple : Un fichier ne doit pas être [un fichier multimédia].

Comme illustré dans le dernier exemple du tableau, le premier identificateur de données de la déclaration de condition peut être associé à l'opérateur « sauf » si un fichier ne satisfait pas tous les identificateurs de données dans la déclaration. Cependant, dans la plupart des cas, le premier identificateur de données ne comporte pas d'opérateur.

Création d'un modèle

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Modèles DLP**.
2. Cliquez sur **Ajouter**.

   Un nouvel écran s'affiche.

3. Entrez un nom pour le modèle. La longueur du nom ne doit pas être supérieure à 100 octets. Le nom ne peut pas contenir les caractères suivants :

   - > < * ^ | & ? \ /

4. Saisissez une description ne dépassant pas 256 octets en longueur.

5. Sélectionnez des identificateurs de données puis cliquez sur l'icône « Ajouter ».

   Lorsque vous sélectionnez des définitions :

   - Sélectionnez plusieurs entrées en appuyant et en maintenant la touche **CTRL**, puis en sélectionnant les identificateurs de données.
   - Si vous recherchez une définition spécifique, utilisez la fonction de recherche. Vous pouvez saisir le nom complet ou partiel de l'identitificateur de données.
   - Chaque modèle peut contenir au maximum 30 identificateurs de données.

6. Pour créer une expression, cliquez sur **Expressions**, puis sur **Ajouter une nouvelle expression**. Dans l'écran qui s'affiche, configurez les paramètres de l'expression.

7. Pour créer une liste d'attributs, cliquez sur **Attributs de fichier**, puis sur **Ajouter un nouvel attribut de fichier**. Dans l'écran qui s'affiche, configurez les paramètres de la liste d'attributs de fichier.

8. Pour créer une liste de mots-clés, cliquez sur **Mots-clés**, puis sur **Ajouter un nouveau mot-clé**. Dans l'écran qui s'affiche, configurez les paramètres de la liste de mots-clés.

9. Si vous avez sélectionné une expression, saisissez le nombre d'occurrences, c'est-à-dire le nombre de fois qu'une expression doit se produire avant que le produit Trend Micro ne la soumette à une stratégie de prévention contre la perte des données.

10. Choisissez un opérateur logique pour chaque définition.

Remarque

Lorsque vous configurez des conditions, utilisez les opérateurs logiques avec précaution. Toute utilisation incorrecte génère des conditions erronées, susceptibles de produire des résultats inattendus. Pour des exemples d'utilisation correcte, voir *Conditions et opérateurs logiques à la page 15-40*.

11. Pour supprimer un identificateur de données de la liste d'identificateurs sélectionnés, cliquez sur l'icône « corbeille ».

12. Sous **Aperçu**, vérifiez la condition et effectuez des changements s'il ne s'agit pas de la condition souhaitée.

13. Cliquez sur **Enregistrer**.

Importation d'un modèle

Utilisez cette option si vous disposez d'un fichier `.dat`correctement formaté comprenant les modèles. Pour générer le fichier, vous pouvez exporter les modèles à partir du serveur du produit Trend Micro actif ou à partir de tout autre serveur de produit Trend Micro.

Procédure

1. Accédez à **Stratégies** > **Ressources de stratégies** > **Modèles DLP**.

2. Cliquez sur **Importer**, puis localisez le fichier `.dat` contenant les modèles.

3. Cliquez sur **Ouvrir**.

   Un message s'affiche et vous informe de la réussite ou de l'échec de l'importation. Si un modèle à importer existe déjà, il sera ignoré.

Chapitre 16

Investigation sur les incidents de prévention contre la perte de données

Control Manager propose aux responsables de conformité DLP et réviseurs d'incidents de réviser et de mettre à jour les informations d'incident.

Cette section de traite les rubriques suivantes :

Tâches de l'administrateur

Pour activer le processus de révision de l'incident, les administrateurs Control Manager doivent effectuer certaines tâches pré-requises. Le tableau suivant répertorie les tâches et références requises :

TABLEAU 16-1. Tâches de l'administrateur

TÂCHE	RÉFÉRENCES
Configurez les informations de responsable dans Active Directory.	*Configuration des informations de responsable pour les utilisateurs d'Active Directory à la page 16-3*
Configurez l'intégration Active Directory pour obtenir des informations sur les utilisateurs.	*Configuration des paramètres du widget de vérification d'Active Directory et de Protection des points finaux à la page 6-11*
Créez des comptes utilisateur spécifiques aux investigations sur les incidents DLP. Attribuez les rôles Responsable de conformité DLP ou Réviseur d'incidents DLP aux utilisateurs enquêtant sur les incidents DLP. **Remarque** Les rôles Responsable de conformité DLP et Réviseur d'incidents DLP sont disponibles pour les utilisateurs d'Active Directory uniquement.	• *Compréhension des rôles utilisateur DLP à la page 16-6* • *Définition des rôles utilisateurs à la page 3-4* • *À propos de l'ajout et l'importation de comptes utilisateur à la page 3-11*
Configurez les notifications **Résumé d'incidents programmé** et **Informations détaillées des incidents mises à jour**.	• *Configuration des paramètres du résumé d'incidents programmé à la page 8-28* • *Configuration des paramètres des informations détaillées des incidents mises à jour à la page 8-29*

TÂCHE	RÉFÉRENCES
Exportez les journaux DLP à des fins d'audit.	• *Création de journaux d'audit DLP à la page 16-8* • *Requête de données de journaux à la page 9-6*

Configuration des informations de responsable pour les utilisateurs d'Active Directory

Pour que les responsables puissent enquêter sur les incidents DLP, configurez les informations de responsable pour chaque utilisateur d'Active Directory.

Procédure

1. Ouvrez la console Utilisateurs et ordinateurs d'Active Directory. Cliquez sur **Démarrer** > **Outils d'administration** > **Utilisateurs et ordinateurs d'Active Directory**.

La console Utilisateurs et ordinateurs d'Active Directory s'affiche.

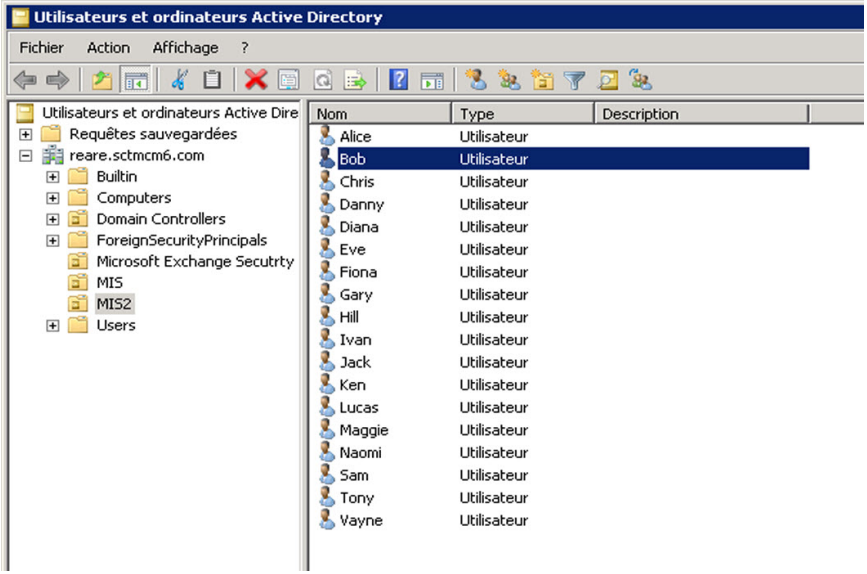


FIGURE 16-1. Console Utilisateurs et ordinateurs d'Active Directory

2. Double-cliquez sur un utilisateur.

L'écran **Propriétés de <utilisateur>** s'affiche.

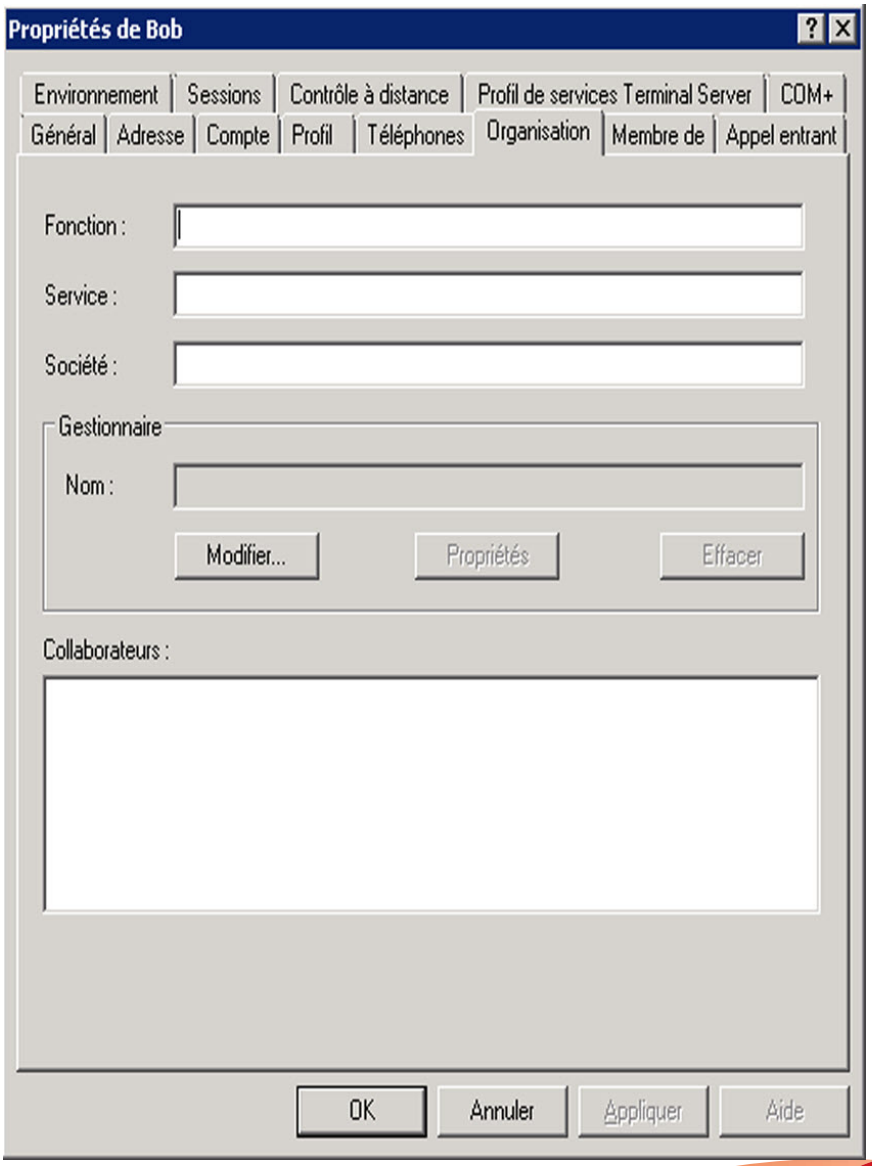


FIGURE 16-2. ÉCRAN DE PROPRIÉTÉS DE <UTILISATEUR>

3. Cliquez sur l'onglet **Organisation** puis cliquez sur **Modifier...**.

   L'écran **Sélectionner utilisateur ou contact** s'affiche.

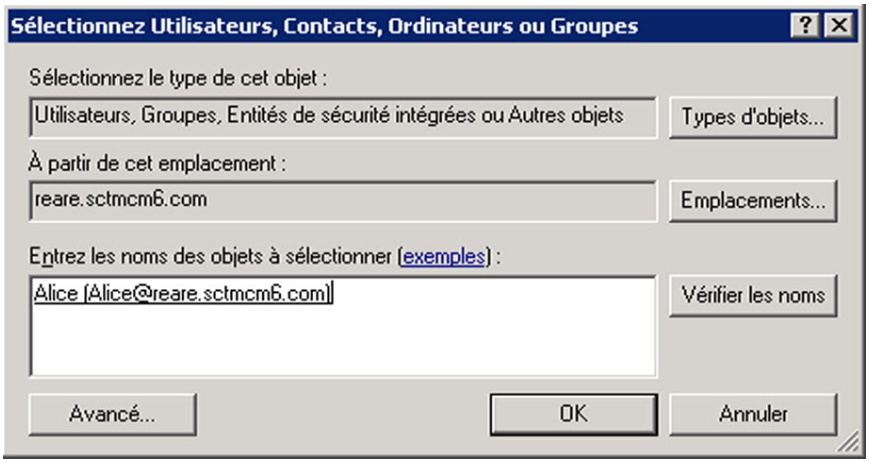


FIGURE 16-3. Écran Sélectionner utilisateur ou contact

4. Spécifiez les informations du responsable puis cliquez sur **OK**.

5. Pour vérifier la relation responsable-utilisateur, ouvrez l'écran **Propriétés de <utilisateur>**, cliquez sur l'onglet **Organisation** et vérifiez les informations utilisateur sous **Rapports directs**.

Compréhension des rôles utilisateur DLP

Responsable de conformité DLP et Réviseur d'incidents DLP sont les deux seuls rôles autorisés à réviser les incidents DLP.

Remarque

Les rôles Responsable de conformité DLP et Réviseur d'incidents DLP sont disponibles pour les utilisateurs d'Active Directory uniquement.

Le tableau suivant décrit les fonctions et caractéristiques liées à ces rôles utilisateur :

TABLEAU 16-2. Fonctions des rôles Responsable de conformité DLP et Réviseur d'incidents DLP

ÉLÉMENT	DESCRIPTION

Journaux DLP	L'accès aux journaux DLP est strictement limité aux rôles utilisateur suivants :
	• Responsable de conformité DLP :
	  • Accès complet
	  • Des widgets spécifiques affichent les informations d'incident DLP
	• Réviseur d'incidents DLP :
	  • Accès limité aux journaux DLP liés aux utilisateurs gérés directement
	  • Des widgets spécifiques affichent les informations d'incident DLP

Portée de l'incident	• Responsable de conformité DLP : Affichage des données de l'incident de l'ensemble des utilisateurs d'Active Directory • Réviseur d'incidents DLP : Affiche les données d'incident des utilisateurs gérés directement
Accès au menu	**Tableau de bord** et les widgets répertoriés dans l'onglet **Investigation sur les incidents de DLP** : • Incidents de prévention contre la perte des données par gravité et par état • Tendances des incidents de prévention contre la perte des données par utilisateur • Incidents de prévention contre la perte des données par utilisateur Consultez la rubrique *Onglet Investigation sur les incidents de DLP à la page 6-4* pour obtenir plus d'informations.

ÉLÉMENT	DESCRIPTION
Notification de résumé d'incidents programmé	• Notification par message électronique quotidienne ou hebdomadaire • Liste d'aperçu du nombre d'incidents par niveau de gravité • Lien vers la console Web Control Manager • Le Responsable de conformité DLP et le Réviseur d'incidents DLP reçoivent cette notification
Notification d'informations détaillées des incidents mises à jour	• Notification de modification de l'état de l'incident ou de commentaires • Seul le Responsable de conformité DLP reçoit cette notification

Création de journaux d'audit DLP

Les administrateurs peuvent utiliser des **Requêtes ad hoc** pour générer et exporter des journaux d'audit DLP. Effectuez une requête de journal tel que décrit dans *Requête de données de journaux à la page 9-6*et configurez ce qui suit :

- Portée des données : **Sélectionnez Control Manager**
- Affichage des données : Sélectionnez **Informations sur l'accès des utilisateurs**
- Critères de la requête : Ajoutez les activités suivantes aux **Critères personnalisés** :
  - Supprimer les journaux DLP
  - Supprimer les journaux d'accès
  - Télécharger le fichier d'incidents DLP
  - Activer la maintenance des journaux d'accès
  - Activer la maintenance des journaux DLP
  - Maintenance des journaux d'accès désactivée
  - Maintenance des journaux DLP désactivée

- Mettre à jour l'incident DLP
- Mettre à jour les paramètres de maintenance des journaux DLP
- Mettre à jour les paramètres de maintenance des journaux d'accès

Processus de révision d'incidents DLP

Une fois que les administrateurs de Control Manager ont effectué les tâches pré-requises, les réviseurs peuvent démarrer le processus de révision de l'incident. Le tableau suivant répertorie les tâches et références :

TABLEAU 16-3. Processus de révision d'incidents DLP

TÂCHE	DESCRIPTION
Réception du message de notification de résumé d'incidents programmé	Control Manager résume et envoie des notifications par message électronique aux réviseurs d'incidents tous les jours ou toutes les semaines.
Révisez les détails de l'incident en suivant l'une de ces méthodes : • Cliquez sur le lien fourni dans le message pour vous connecter à la console Web Control Manager • Ouvrez la pièce jointe (si disponible)	*Compréhension de la liste d'informations sur les incidents à la page 16-9*
Mettez à jour l'état d'incident et ajoutez des commentaires	*Révision des détails de l'incident à la page 16-11*

Compréhension de la liste d'informations sur les incidents

L'écran **Informations sur les incidents** affiche une liste d'incidents gérables par ce réviseur. Les réviseurs d'incidents peuvent utiliser cet écran pour faire ce qui suit :

- Voir le résumé de l'incident

- Prendre des mesures sur les incidents
- Informations détaillées des incidents d'exportation

TABLEAU 16-4. Liste d'informations sur les incidents

ÉLÉMENT	DESCRIPTION
ID	Identifiant d'incident unique
Reçu	Date et heure de réception des données de l'incident par Control Manager **Remarque** Après avoir reçu les journaux DLP des produits gérés, Control Manager a besoin de 30 minutes pour traiter les journaux avant que les réviseurs d'incidents ne puissent voir les données.
Gravité	Niveau de gravité de l'incident **Remarque** Une fois que Control Manager reçoit et traite un incident DLP, Control Manager ne met pas à jour le niveau de gravité si des changements surviennent sur le produit géré.
Stratégie	Nom de la stratégie Control Manager qui a déclenché l'incident **Remarque** Pour les incidents déclenchant des stratégies DLP créées dans les produits gérés, ceci apparaît sous la forme **N/A**.

Élément	Description
Utilisateur	Nom de l'utilisateur ayant déclenché l'incident
Responsable	Nom du responsable de l'utilisateur
État	État actuel de l'incident • Nouveau • En cours d'investigation • Référé • Fermé
Action	Action disponible pour gérer l'incident

Révision des détails de l'incident

En cliquant sur l'icône **Modifier** dans la colonne **Action** de l'écran **Informations sur les incidents**, l'écran **Détails de l'incident** s'affiche et présente les détails des informations de l'incident. Les réviseurs d'incidents DLP peuvent utiliser cet écran pour mettre à jour l'état de l'incident et proposer des commentaires à son sujet.

Tableau 16-5. Informations détaillées des incidents

Élément	Description
ID	Identifiant d'incident unique
État	Utilisez ceci pour mettre à jour l'état de révision de l'incident. Options disponibles : • **Nouveau** • **En cours d'investigation** • **Référé** • **Fermé**

ÉLÉMENT	DESCRIPTION
Gravité	Niveau de gravité de l'incident **Remarque** Une fois que Control Manager reçoit et traite un incident DLP, Control Manager ne met pas à jour le niveau de gravité si des changements surviennent sur le produit géré.
Stratégie	Nom de la stratégie Control Manager qui a déclenché l'incident **Remarque** Pour les incidents déclenchant des stratégies DLP créées dans les produits gérés, ceci apparaît sous la forme **N/A**.
Règle	Noms des règles ayant déclenché l'incident
Reçu	Date et heure de réception des données de l'incident par Control Manager **Remarque** Après avoir reçu les journaux DLP des produits gérés, Control Manager a besoin de 30 minutes pour traiter les journaux avant que les réviseurs d'incidents ne puissent voir les données.
Généré	Date et heure de l'incident dans le produit géré
Utilisateur	Nom de l'utilisateur ayant déclenché l'incident

Élément	Description
Responsable	Nom du responsable de l'utilisateur
Expéditeur	Adresse électronique source
Destinataire	Adresse électronique de destination
Point final	Nom d'hôte de la source
IP	Adresse IP source
Modèle	Noms des modèles ayant déclenché l'incident
Contenu correspondant	Actifs numériques ayant déclenché l'incident
Fichier	Nom ou lien vers le fichier ayant déclenché l'incident **Remarque** Le fichier est mis en quarantaine dans le produit géré.
Hachage du fichier	Informations de hachage du fichier
Objet du message	Objet du message électronique
Canal	Canal à travers lequel la transmission est survenue
Action	Actions prises pour l'incident
Commentaires	Remarques d'utilisateurs sur l'incident

Chapitre 17

Administration de la base de données

Ce chapitre présente le matériel nécessaire aux administrateurs pour gérer le réseau Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition de la base de données de Control Manager

Control Manager stocke dans la base de données Microsoft SQL Server (`db_ControlManager.mdf`) 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.

Le serveur Control Manager se connecte à la base de données à l'aide d'une connexion ODBC avec nom DSN système. Le programme d'installation de Control Manager génère cette connexion ainsi que l'ID et le mot de passe permettant d'accéder à `db_ControlManager.mdf`. L'ID par défaut est sa. Control Manager chiffre le mot de passe.

Pour garantir au maximum la sécurité du serveur SQL Server, configurez l'un des comptes SQL utilisés pour gérer db_ControlManager avec les autorisations minimales suivantes :

- dbcreator pour le rôle du serveur
- db_owner pour le rôle de db_ControlManager

Le produit géré eManager contribue à l'expansion de la base de données de façon notable. En effet, la taille moyenne des journaux d'eManager est d'environ 3000 octets. Par exemple :

Dans un environnement à faible trafic de courrier électronique (par exemple, 100 messages toutes les 10 h chaque jour), si eManager bloquait 1 250 messages par jour, le journal des violations de sécurité de contenu contiendrait 1 250 x 3 000, soit 3 750 000 octets par jour.

L'expansion de la base de données s'élèverait alors à 5 Mo par jour, ou 150 Mo par mois.

Les autres produits Trend Micro gérés par Control Manager n'entraînent généralement qu'une croissance de quelques kilo-octets par système et par jour.

Dans la mesure où la base de données Control Manager est exécutée sur une base de données capable de monter en charge (SQL Server), la limite théorique correspond à la capacité matérielle de la base de données. Trend Micro a testé jusqu'à 2 000 000 d'entrées. Si le serveur de base de données est surchargé ou s'il est sollicité au-delà de ses

limites de performances, la console Web risque de connaître des dépassements de délai de connexion.

Définition des tables de db_ControlManager

Pour accéder à l'ensemble des tables de la base de données de Control Manager, utilisez un projet Microsoft Access (*.adp /*.ade).

Remarque

N'employez pas les outils SQL pour ajouter, supprimer ou modifier des enregistrements, à moins de demander conseil au personnel de l'assistance technique de Trend Micro.

La base de données de Control Manager se compose des tables suivantes :

TABLEAU 17-1. Tables de gestion des répertoires

TABLES DE GESTION DES RÉPERTOIRES	DESCRIPTION
CDSM_Entity	Cette table stocke les informations relatives aux produits gérés
CDSM_Agent	Cette table stocke les informations relatives au communicateur
CDSM_Registry	Cette table stocke les informations relatives au registre
CDSM_UserLog	Cette table stocke des informations d'identification des utilisateurs qui se connectent à la console Web, ainsi que sur les options utilisées et l'heure de connexion ; ces données sont utiles lors de la vérification des accès à la console.
CDSM_SystemEventlog	Cette table stocke les journaux systèmes générés par les processus internes

TABLEAU 17-2. Tables du contrôleur de commandes du serveur

TABLES DU CONTRÔLEUR DE COMMANDES DU SERVEUR	DESCRIPTION
tb_TVCSCommandList	Cette table stocke les commandes des produits gérés
tb_TVCSCommandTaskQueue	Cette table stocke les commandes envoyées aux produits gérés
tb_CommandTracking	Cette table stocke l'état des commandes
tb_CommandItemTracking	Cette table stocke l'état détaillé des commandes
tb_ProcessInfo	Cette table stocke des informations sur MsgReceiver.exe, CmdProcessor.exe, LogReceiver.exe, LogRetriever.exe et UIProcessor.exe
tb_LoginUserSessionData	Cette table stocke des données de contrôle sur les sessions utilisateurs
tb_ManualDownload	Cette table stocke les informations relatives aux téléchargements manuels
tb_ScheduleDownload	Cette table stocke les informations relatives aux téléchargements programmés

TABLEAU 17-3. Tables des produits gérés

TABLES DES PRODUITS GÉRÉS	DESCRIPTION
tb_EntityInfo	Cette table stocke les informations relatives aux produits gérés
tb_VirtualEntity	Cette table stocke les informations concernant l'enregistrement des agents TVCS1.x

TABLEAU 17-4. Tables des journaux

TABLES DES JOURNAUX	DESCRIPTION
tb_TempLog	Cette table stocke les données brutes des journaux des produits
tb_AV*Log	Cette table stocke les journaux des produits * correspond à Virus, Event, Status, PEInfo, WebSecurity. Ces tables stockent le journal d'état des produits, les versions des signatures et du moteur, les heures de mise à jour et de déploiement, et le nombre de virus non traités.
tb_InValidLog	Cette table stocke les informations concernant les journaux non identifiés
• tb_TotalWebSecurityCount • tb_TotalVirusCount • tb_TotalSecurityCount • tb_TopTenSource • tb_TopTenDestination • tb_TopTenVirus	Ces tables stockent les résumés des virus pour le résumé d'état et les rapports
tb_LogPurgePolicy	Cette table stocke les paramètres de purge des journaux
tb_LogPurgeCounter	Cette table stocke le décompte des purges des journaux
• tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak	Ces tables stockent les instances de journaux utilisées dans les notifications d'alertes

TABLEAU 17-5. Tables de notification

TABLES DE NOTIFICATION	DESCRIPTION
• tb_Alert_NTF_JobList • tb_Event_NTF_JobList	Ces tables stockent les files d'attente de notifications
tb_EventNotificationFilter	Cette table stocke la configuration du Centre d'événements
• tb_SendEMailNotification • tb_SendPagerNotification • tb_SendSNMPTrapNotification • tb_SendWindowsNTEventLogNotification	Ces tables stockent les paramètres concernant les méthodes de notification
tb_VirusOutBreakPolicy	Cette table stocke les règles utilisées lors d'une épidémie virale
tb_SpecialVirusPolicy	Cette table stocke les noms de virus spécifiés par l'utilisateur
• tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate	Ces tables stockent les décomptes de virus
• tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation	Ces tables stockent les paramètres de notification des utilisateurs et des groupes

TABLEAU 17-6. Tables de rapports

TABLES DE RAPPORTS	DESCRIPTION
• tb_ReportScheduleTask • tb_ReportTaskQueue	Ces tables stockent et gèrent les tâches de génération de rapports
tb_ReportItemTracking	Cette table stocke le catalogue des modèles de rapport

TABLEAU 17-7. Tables de déploiement des signatures et du moteur

TABLES DE DÉPLOIEMENT DES SIGNATURES ET DU MOTEUR	DESCRIPTION
• tb_DeploymentPlans • tb_DeploymentPlansTF	Ces tables stockent les informations relatives aux plans de déploiement
tb_DeploymentPlanTasks	Cette table stocke la file d'attente des tâches de déploiement
tb_DeployNowJobList	Cette table stocke l'état du plan de déploiement en continu
tb_DeployCommandTracking	Cette table stocke les informations sur le suivi des commandes de déploiement
tb_DeploymentPlanTargets	Cette table stocke des informations sur le produit géré qui est à l'origine de la commande de déploiement

Sauvegarde de db_ControlManager à l'aide d'osql

Si la base de données Control Manager est corrompue ou ne fonctionne pas, utilisez une copie de sauvegarde pour restaurer vos paramètres. Si vous utilisez MSDE, servez-vous de son interface de ligne de commande, osql, pour générer une sauvegarde de la base de données.

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer** > **Exécuter**.
2. Tapez cmd, puis cliquez sur **OK**.
3. Sur l'invite de commande, exécutez les commandes suivantes :

```
osql -U {ID} -P {password} -n -Q "BACKUP DATABASE {Control Manager
database} TO DISK = '{path and backup name}'"
```

où :

{ID} : nom d'utilisateur du compte administrateur permettant d'accéder à la base de données de Control Manager. Ce nom est défini lors de la configuration de Control Manager.

{password} : mot de passe permettant d'accéder à la base de données de Control Manager. Ce nom est défini lors de la configuration de Control Manager.

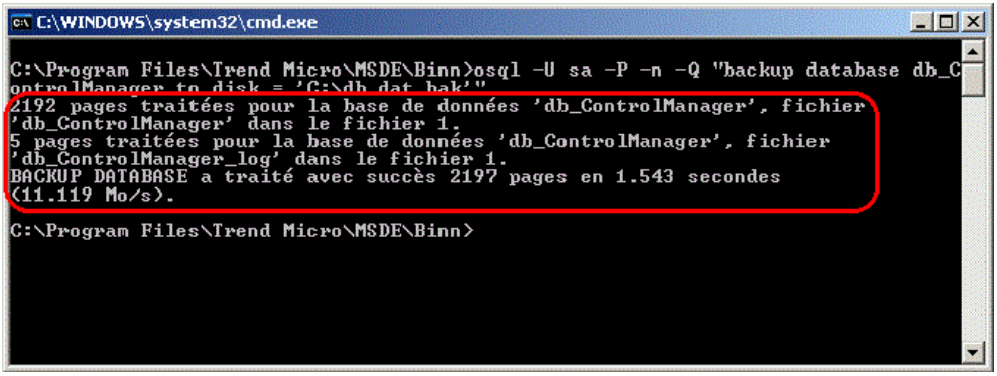
{Control Manager database} : nom de la base de données de Control Manager.

{path and backup name} : emplacement cible et nom du fichier de sauvegarde

Par exemple :

```
osql -U sa -P -n -Q "BACKUP DATABASE db_ControlManager TO DISK = 'f:
\db.dat_bak'"
```

Une sauvegarde réussie produit un résultat semblable à celui-ci :



Si le fichier de sauvegarde `db.dat_bak` existe déjà, la commande `osql` y insère de nouveaux enregistrements en vue de sauvegarder les nouvelles informations.

Remarque

Trend Micro recommande de sauvegarder la base de données de Control Manager régulièrement. Créez notamment une sauvegarde chaque fois que vous envisagez de la modifier (par exemple en installant un produit géré).

Restauration d'une sauvegarde de db_ControlManager à l'aide d'osql

Pour restaurer une sauvegarde de base de données, utilisez l'interface de ligne de commande qui accompagne votre version de MSDE, `<racine>:\Program Files \Trend Micro\MSDE\osql`.

Procédure

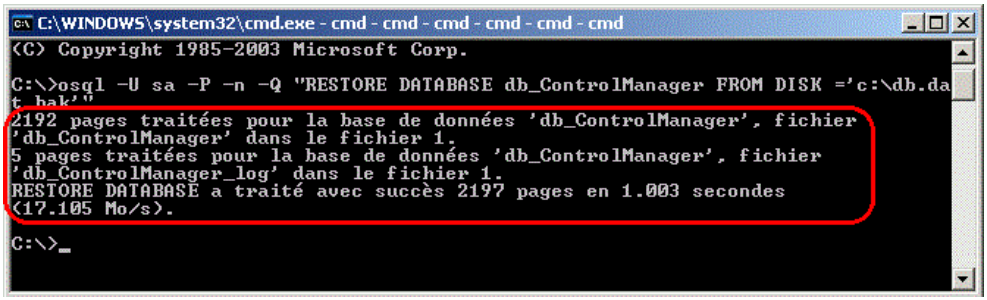
1. Arrêtez Control Manager.
2. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Services** pour ouvrir l'écran **Services**.
3. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Arrêter**.
4. Cliquez sur **Démarrer** > **Exécuter**.
5. Tapez `cmd`, puis cliquez sur **OK**.
6. Sur l'invite de commande, exécutez les commandes suivantes :

```
osql -U {ID} -P {password} -n -Q "RESTORE DATABASE {Control Manager
database} FROM DISK = '{path and backup name}'"
```

Par exemple :

```
osql -U sa -P -n -Q "RESTORE DATABASE db_ControlManager FROM DISK =
'f:\db.dat_bak'"
```

Une restauration de base de données réussie produit un résultat semblable à celui-ci :



7. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Services** pour ouvrir l'écran **Services**.

8. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Redémarrer**.

9. Lancez Control Manager. Pour obtenir plus d'informations sur l'utilisation d'osql, consultez la bibliothèque MSDN.

Sauvegarde de db_ControlManager au moyen de SQL Server Management Studio

Si vous utilisez SQL Server, servez-vous de SQL Server Management Studio pour sauvegarder la base de données de Control Manager.

Remarque

Trend Micro recommande d'effectuer des sauvegardes régulières de la base de données de Control Manager. Créez notamment une sauvegarde chaque fois que vous envisagez de modifier cette base de données (par exemple en ajoutant ou en installant un produit géré).

Procédure

1. Depuis le serveur Control Manager, cliquez sur **Démarrer** > **Programmes** > **Microsoft SQL Server 2005** > **Enterprise manager** pour accéder à SQL Server Management Studio.

2. Sur la console, cliquez sur **Serveurs Microsoft SQL Server** > **Groupe SQL Server** > **{SQL Server} (Windows NT)** > **Base de données**. {serveur SQL} est le nom d'hôte du serveur SQL.

3. Cliquez avec le bouton droit de la souris sur **db_ControlManager** et cliquez ensuite sur **Toutes les tâches** > **Sauvegarde de la base de données…**.

4. Dans l'écran **Sauvegarde SQL Server - db_ControlManager**, indiquez le nom de la base de données et entrez une description.

5. Sous Sauvegarde, sélectionnez **Base de données - complète**.

6. Sous Destination, cliquez sur **Ajouter** pour indiquer la destination du fichier de sauvegarde.

7. Dans **Sélectionner la destination de la sauvegarde**, indiquez le nom de la sauvegarde et le chemin dans lequel elle doit être enregistrée, puis cliquez sur **OK**.

8. Dans l'écran **Sauvegarde SQL Server - db_ControlManager**, cliquez sur **OK** pour lancer la sauvegarde de db_ControlManager.

9. Cliquez sur **OK** lorsque le message suivant s'affiche : « L'opération de sauvegarde s'est terminée avec succès. »

Restauration d'une sauvegarde de db_ControlManager au moyen de SQL Server Management Studio

Vous pouvez utiliser SQL Server Management Studio pour restaurer une copie de sauvegarde de la base de données de Control Manager.

Procédure

1. Arrêtez Control Manager.

2. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Services** pour ouvrir l'écran **Services**.

3. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Arrêter**.

4. Cliquez sur **Programmes** > **Microsoft SQL Server 2005** > **SQL Server Management Studio** pour accéder à SQL Server Management Studio.

5. Sur la console, cliquez sur **Microsoft SQL Server 2005** > **Groupe SQL server** > **{SQL server}** > **Bases de données**. {serveur SQL} est le nom d'hôte du serveur SQL.

6. Cliquez avec le bouton droit de la souris sur **db_ControlManager** > **Toutes les tâches** > **Restaurer la base de données…**.

7. Dans l'écran Restaurer la base de données, sélectionnez la base de données à restaurer.

8. Cliquez sur **OK** pour lancer le processus de restauration.

9. Cliquez sur **OK** lorsque le message suivant s'affiche : « Restauration de la base de données {base de données de Control Manager} terminée. »

10. Cliquez sur **Démarrer** > **Programmes** > **Outils d'administration** > **Services** pour ouvrir l'écran **Services**.

11. Cliquez avec le bouton droit de la souris sur **<Service Control Manager>**, puis cliquez sur **Redémarrer**.

12. Lancez Control Manager.

Réduction de db_ControlManager_log.ldf à l'aide de SQL Server Management Studio

Le fichier journal des transactions de la base de données de Control Manager est ... `\data\db_ControlManager_log.LDF`. SQL Server génère ce journal dans le cadre de son fonctionnement normal.

`db_ControlManager_log.LDF` contient toutes les transactions des produits gérés utilisant `db_ControlManager.mdf`.

Par défaut, la taille de ce fichier n'est pas limitée dans la configuration de SQL Server, ce qui à la longue peut entraîner la saturation de l'espace disque disponible.

Réduction de la taille du fichier db_ControlManager_log.ldf sous SQL Server 2008/2005 SP 3

Procédure

1. Sauvegardez la base de données de Control Manager à l'aide de SQL Server Management Studio.
2. Purgez le journal des transactions.
3. Sur le serveur SQL, cliquez sur **Programmes** > **Microsoft SQL Server 2008/2005** > **SQL Server Management Studio** pour ouvrir SQL Server Management Studio.
4. Sélectionnez le serveur SQL Server et choisissez l'authentification Windows si vous y êtes invité.
5. Cliquez avec le bouton droit de la souris sur **db_ControlManager** et sélectionnez **Propriétés**.

   La boîte de dialogue **Propriétés** s'affiche.
6. Cliquez sur **Options**.

   La zone de travail **Options** s'affiche.
7. Sélectionnez **Simple** dans la liste **Modèle de récupération :**
8. Cliquez sur **OK**.
9. Vérifiez la taille du fichier `db_ControlManager_log.ldf`. Elle doit être de 10 Mo.

Réduction de la taille du fichier db_ControlManager_log.ldf sous SQL Server 2005

Procédure

1. Sauvegardez la base de données de Control Manager à l'aide de SQL Server Management Studio.
2. Purgez le journal des transactions.
3. Sur le serveur SQL, cliquez sur **Programmes** > **Microsoft SQL Server 2005** > **SQL Server Management Studio** pour ouvrir SQL Server Management Studio.
4. Sélectionnez le serveur SQL Server et choisissez l'authentification Windows si vous y êtes invité.
5. Dans la liste, sélectionnez la base de données **db_ControlManager**.
6. Copiez et collez le script SQL suivant :

```
DBCC shrinkDatabase(db_ControlManager)

BACKUP LOG db_ControlManager WITH TRUNCATE_ONLY DBCC
SHRINKFILE(db_ControlManager_Log, 10)
```

Remarque

Le paramètre 10 de la fonction `SHRINKFILE(db_ControlManager_Log, 10)` correspond à la taille cible du fichier `db_ControlManager_Log.ldf`, en mégaoctets (Mo).

7. Cliquez sur **Exécuter** pour exécuter le script SQL.
8. Vérifiez la taille du fichier `db_ControlManager_log.ldf`. Elle doit être de 10 Mo.

Réduction de db_ControlManager.mdf et db_ControlManager.ldf à l'aide de commandes SQL

Procédure

- Exécutez les commandes SQL suivantes si vous utilisez MSDE ou si vous préférez avoir recours aux commandes SQL pour restreindre l'espace qu'occupent `db_ControlManager.mdf` et `db_ControlManager.ldf` sur le disque.

```
Alter Database db_ControlManager set recovery FULL

Backup log db_ControlManager with truncate_only

DBCC shrinkDatabase(db_ControlManager)
```

Remarque

La troisième commande risque de prendre plus de temps, selon la taille de la base de données.

```
EXEC sp_dboption 'db_ControlManager', 'trunc. log on
chkpt.', 'TRUE'

Alter Database db_ControlManager set recovery simple

Alter Database db_ControlManager set auto_shrink on
```

Partie IV

Services et outils

Chapitre 18

Utilisation des services Trend Micro

Ce chapitre vous renseigne sur les différents services Control Manager.

Ce chapitre traite les rubriques suivantes :

Définition des services Trend Micro

Trend Micro a toujours reconnu qu'il fallait aborder la gestion antivirus sous une nouvelle approche pour pouvoir minimiser les dommages et les coûts résultant d'une attaque virale. Après une phase intensive de recherche et de test, Trend Micro est arrivé à définir une nouvelle stratégie de protection antivirale. Il ne suffit plus de réagir aux menaces à l'aide de produits individuels, mais bel et bien de les combattre tout au long de leur cycle. Pour cela, il faut adopter un système de protection centralisé et proactif qui permet de contrecarrer, sans délai et méthodiquement, toute attaque éventuelle du système et ce, des passerelles Internet jusqu'aux ordinateurs, serveurs de fichiers et serveurs de messagerie.

Parfaitement intégrée, la stratégie de protection antivirale Trend Micro commence dès qu'un administrateur envoie un échantillon de virus aux TrendLabs. Dès cet instant, une stratégie de prévention ciblée (recommandations avant mise à disposition d'un fichier de signatures) est mise en œuvre pour contenir l'épidémie et en empêcher la propagation. Lorsque Control Manager récupère ces informations, les administrateurs peuvent faire appel au service Outbreak Prevention Services pour rapidement cerner le périmètre de l'attaque et prendre immédiatement les premières mesures qui s'imposent sans avoir à fermer un port ni compromettre la productivité de l'entreprise. Ils peuvent aussi diffuser très rapidement les stratégies de prévention des épidémies aux autres administrateurs de l'entreprise qui risquent de se trouver confrontés au même problème.

Seule une administration centralisée permet de gérer les épidémies de manière proactive puisqu'elle propose d'intégrer les connaissances et les compétences antivirales sur l'ensemble du réseau, et donne une visibilité en temps réel de toutes les attaques virales dès leur apparition. Les services d'identification rapide et les systèmes de diffusion accélèrent le confinement du virus et en limitent la propagation. Il est ainsi possible de minimiser l'impact du virus sur la productivité de l'entreprise, et de diminuer considérablement les coûts de nettoyage et de restauration.

Définition de la stratégie Enterprise Protection Strategy

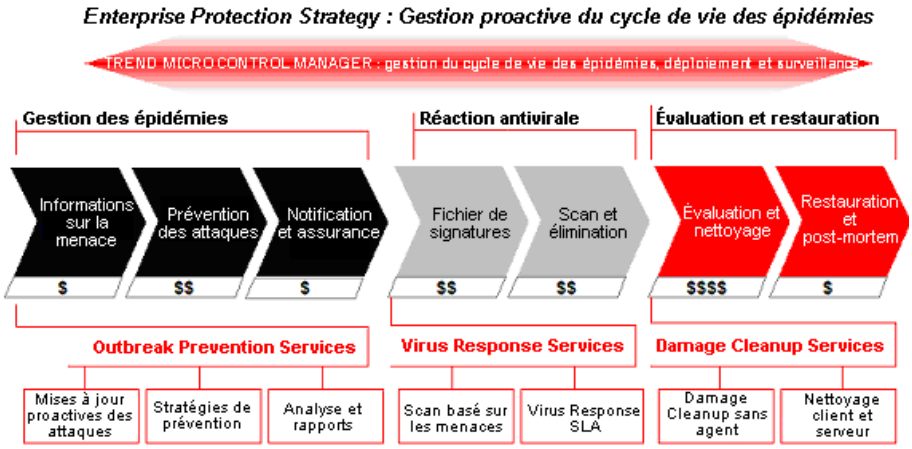


FIGURE 18-1. Enterprise Protection Strategy

Avec la stratégie Enterprise Protection Strategy (EPS), les entreprises bénéficient des services et du support nécessaires pour lutter, en toute confiance, contre les menaces combinées.

- Les services proactifs combattent les épidémies virales en empêchant l'infiltration du virus et en supprimant toute trace des attaquants potentiels, éventuellement dissimulés dans les systèmes
- Le Virus Response Service Level Agreement (accord de niveau de service de la réaction antivirale), premier accord de ce type dans le secteur, garantit la détection des virus
- L'architecture EPS tire parti des connaissances, des compétences et des services de Trend Micro pour protéger les points les plus vulnérables du réseau

Avec EPS, les entreprises peuvent mettre en place un véritable « poste de commande » pour identifier toutes les failles de sécurité et les protéger :

- Application cohérente de la stratégie et génération de rapports au sein de toute l'entreprise
- Prise en charge d'une plate-forme hétérogène

EPS fournit un plan de bataille en cas d'attaque virale afin de minimiser les pertes et les dommages. Ce plan consiste à :

- lutter contre les épidémies virales tout au long de leur cycle : approche unique dans ce secteur et basée sur le vécu des entreprises ;
- assurer la coordination au sein de l'entreprise pour identifier les vulnérabilités du réseau et contrecarrer de manière proactive les épidémies ;
- se concentrer sur les stades les plus critiques, avant et après le déploiement du fichier de signatures, pour mieux maîtriser les coûts et minimiser les dommages occasionnés au système.

Importance de la valeur d'EPS

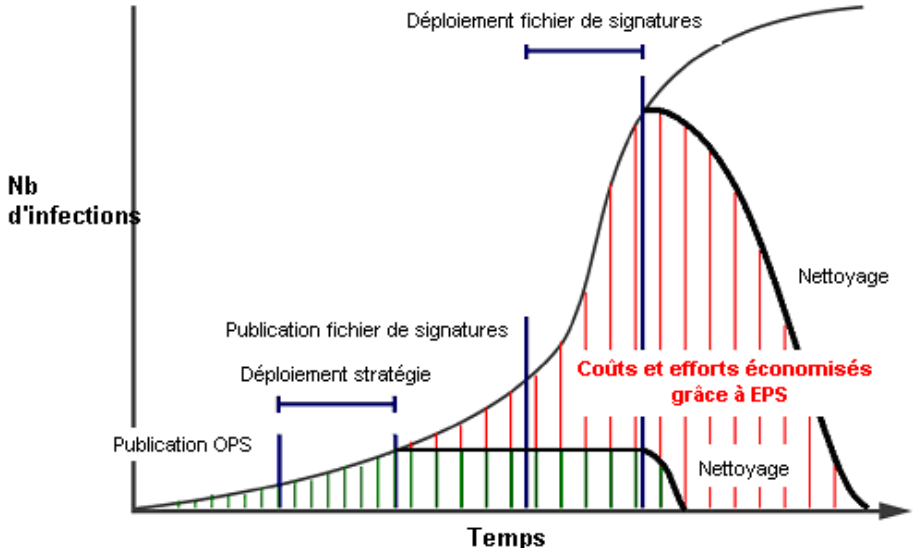


FIGURE 18-2. Comparaison des coûts et des efforts déployés

Le graphique explique comment il est possible de minimiser les effets dévastateurs des épidémies en mettant une protection en place, sans délai, et en supprimant toute trace de virus sur l'ensemble du réseau pour éviter les réinfections.

Grâce à EPS et à Outbreak Prevention Services, les entreprises sont en mesure d'atténuer les risques et de minimiser les coûts. En déployant les stratégies dès les premières phases du cycle de vie d'une attaque virale, et avant même la mise à disposition du fichier de signatures, une entreprise parvient à limiter les coûts et la perte de temps occasionnés lors de ces épidémies. De plus, elle renforce son niveau global de protection.

L'expertise, l'architecture et les services de Trend Micro offrent un solide retour sur investissement, renforcent la protection globale de l'entreprise et optimisent la productivité de ses réseaux.

Définition du service Outbreak Prevention Services

FIGURE 18-3. Outbreak Prevention Services

La phase Prévention des épidémies couvre la période critique où les produits gérés ont identifié une épidémie virale avant la mise à disposition d'un fichier de signatures. Au cours de cette période délicate, les administrateurs système passent un temps considérable à communiquer, de manière parfois chaotique, avec les différents groupes de leurs entreprises, souvent décentralisés et disséminés dans le monde.

Outbreak Prevention Services vous tient informé des nouvelles menaces et diffuse des mises à jour continuelles et complètes sur l'état du système au fur et à mesure de l'évolution d'une attaque. Il communique, au moment opportun, des informations détaillées sur les virus. Dès l'identification de nouvelles menaces, il préconise la stratégie de prévention et de scan à adopter pour chacune d'entre elles de façon à aider les entreprises à rapidement contenir les virus et à éviter toute contamination.

De plus, en déployant et en gérant les recommandations de manière centralisée, Outbreak Prevention Services réduit les efforts de coordination, contribue à l'application cohérente des stratégies et déploie les informations les plus vitales au fur et à mesure de l'évolution de l'épidémie.

Dans la mesure où Trend Micro Control Manager peut assurer le téléchargement, automatique ou manuel, et le déploiement des stratégies, le service Outbreak Prevention Services apporte aux points d'accès les plus essentiels du réseau les connaissances des experts des TrendLabs, ainsi que des centres de recherche et d'assistance internationaux de Trend Micro, véritables spécialistes de la sécurité.

Ce service, accessible par le biais d'un abonnement, ne demande qu'un investissement de départ minimal. En revanche, il vous aide à assurer une parfaite coordination au sein de l'entreprise et à maîtriser les épidémies à l'aide de produits Trend Micro, chargés de surveiller les points les plus vulnérables du réseau: passerelle Internet, serveur de messagerie, serveur de fichiers, serveur de cache, utilisateur client, distant et haut débit.

Avantages du service Outbreak Prevention Services

En plus d'accélérer la réactivité de l'entreprise, Outbreak Prevention Services renforce aussi la protection des opérations et contribue à la réduction des coûts.

TABLEAU 18-1. Avantages d'OPS

AVANTAGE	RAISONS
Protection proactive contre les menaces combinées	• Contient les épidémies sans nuire à la productivité de l'entreprise (autrement dit, sans fermer les ports) • Réduit les problèmes inhérents à la définition de la menace et de son comportement • Met automatiquement en place des stratégies pour assurer un système de défense, 24 heures sur 24 et 7 jours sur 7, sans intervention humaine

AVANTAGE	RAISONS
Expertise et connaissances	• Délivre les recommandations des experts et facilite la formulation de la stratégie. • Propose une base de connaissance des stratégies pour les virus antérieurs
Cohérence, réduction des efforts de coordination et diminution des coûts	• Contribue à l'application cohérente de la stratégie • Élimine les problèmes logistiques et facilite la notification des parties concernées
Mise en corrélation des stratégies et des attaques virales	• Assurance et rapports = Visibilité et coordination au sein de toute l'entreprise

Activation du service Outbreak Prevention Services

Une fois le service Outbreak Prevention Services activé, les administrateurs doivent démarrer le mode de prévention des épidémies pour protéger le réseau lors d'une attaque virale.

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 du service Outbreak Prevention Services, cliquez sur le lien **Activer le produit**.

3. Exécutez les opérations suivantes :

   - **Si vous n'avez pas de code d'activation :** cliquez sur le lien **Enregistrement en ligne** et suivez les instructions sur le site Web d'enregistrement en ligne pour en obtenir un
   - **Si vous avez un code d'activation :** dans la boîte de dialogue **Nouveau**, saisissez votre code d'activation

4. Cliquez sur **Activer**.

Affichage de l'état du service Outbreak Prevention Services

Affichez l'écran **Outbreak Prevention Services** pour connaître instantanément l'état des éléments suivants :

TABLEAU 18-2. État du service OPS

ÉLÉMENT	DESCRIPTION	ÉTAT
Téléchargement de stratégie programmé	Vous indique si Control Manager télécharge automatiquement les stratégies de prévention des épidémies selon un calendrier établi.	Actif/ Inactif
Mode de prévention automatique des épidémies pour alerte rouge	Vous indique si Control Manager déclenche automatiquement le mode de prévention des épidémies pour les virus de type alerte rouge.	Actif/ Inactif
Mode de prévention automatique des épidémies pour alerte jaune	Vous indique si Control Manager déclenche automatiquement le mode de prévention des épidémies pour les virus de type alerte jaune.	Actif/ Inactif

De plus, cet écran permet aisément d'afficher les composants de Control Manager, ainsi que la version qu'ils utilisent actuellement.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Stratégies**.

Remarque

Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

Prévention des épidémies virales et définition du mode de prévention des épidémies

Bien avant de recevoir le fichier de signatures de virus approprié de la part de Trend Micro, une entreprise peut détourner, isoler et contenir les attaques virales en s'appuyant sur les informations propres à chaque attaque et sur les stratégies de prévention délivrées par Trend Micro Outbreak Prevention Services. Avec Outbreak Prevention Services, vous pouvez déployer les recommandations stratégiques de manière centralisée pour réduire les efforts de coordination et contribuer à l'application cohérente de la stratégie sur l'ensemble du réseau. Les recommandations dispensées par Outbreak Prevention Services aident les administrateurs système à faire rapidement face à de nouveau virus et donc à contenir les épidémies, minimiser les dommages occasionnés au système et éviter des temps d'arrêt intempestifs.

Grâce aux plans de déploiement, vous pouvez restreindre l'application des paramètres d'OPS à des segments réseau spécifiques, sous réserve d'avoir divisé le réseau en segments et de leur appliquer des plans de déploiement différents. Cette approche s'avère très utile en cas de réseaux complexes composés de plusieurs sites. Les administrateurs ont alors la possibilité de n'appliquer les paramètres qu'aux zones réellement affectées par l'épidémie.

Lorsque le mode de prévention des épidémies est activé, il est possible d'assurer les opérations suivantes :

- Télécharger les stratégies de prévention des épidémies, c'est-à-dire un ensemble de paramètres logiciels recommandés pour la gestion de l'épidémie virale
- Afficher les paramètres des produits à configurer de façon à pouvoir les modifier en fonction des demandes de votre réseau

  Outbreak Prevention Services fournit des recommandations pour les produits gérés qu'il faut configurer.
- Bloquer/détourner le code malveillant pour l'empêcher de s'infiltrer ou de se propager sur l'ensemble du réseau.
- Personnaliser les fonctions de notification de Control Manager pour l'épidémie en question.
- Générer des rapports en temps réel sur le déploiement et l'état de la stratégie.

- Approuver et déployer la stratégie manuellement ou automatiquement.
- Définir un programme spécial abrégé de mise à jour/téléchargement pour la durée de cette stratégie.

  Vous pouvez ainsi mettre à jour automatiquement de nouvelles signatures de virus dès leur mise à disposition.
- Diffuser des informations détaillées sur les menaces dès qu'elles sont identifiées.

Définition des stratégies de prévention des épidémies

Appliquez les stratégies de prévention des épidémies (ensembles de paramètres de configuration des produits) à vos produits gérés à l'aide du service Outbreak Prevention Services. Trend Micro crée ces paramètres en réponse aux épidémies virales et les fournit aux utilisateurs de Trend Micro dans le cadre du service Outbreak Prevention Services.

Ces stratégies sont à la base même de la protection d'un réseau lors d'une épidémie virale. Elles protègent les points d'entrée importants du réseau : passerelle Internet, serveur de messagerie, serveur de fichiers, serveur de cache, utilisateur client, distant et haut débit. Par exemple, les virus qui se propagent uniquement par courrier électronique feront l'objet de stratégies où les paramètres seront uniquement destinés aux systèmes de messagerie.

Le schéma suivant illustre la méthode utilisée par Trend Micro pour déployer des stratégies à tous les niveaux pour protéger les points d'entrée vitaux lors d'une épidémie virale.

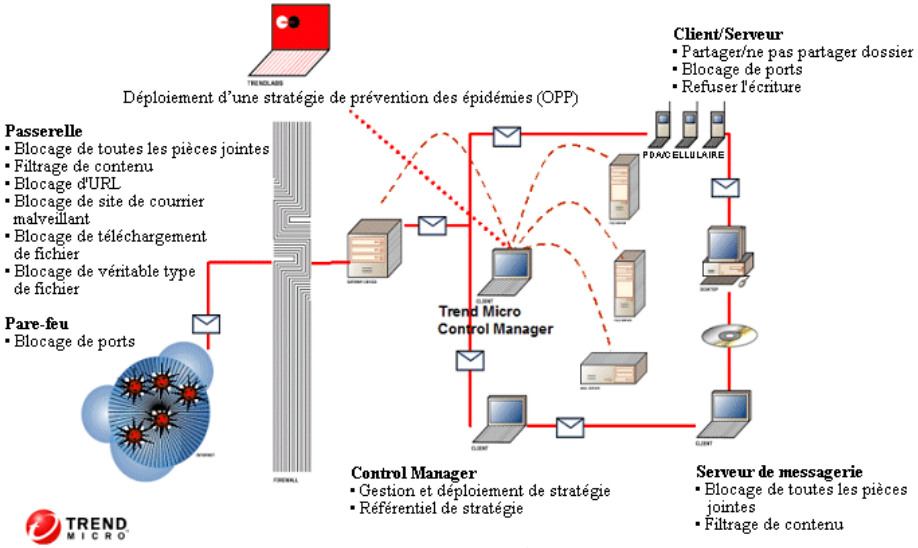


FIGURE 18-4. Déploiement des stratégies de prévention des épidémies

Accès à l'écran Paramètres relatifs au service Outbreak Prevention Services

- Accédez à **Administration** > **Outbreak Prevention Services** > **Paramètres**. L'écran **Paramètres relatifs à Outbreak Prevention Services** apparaît.

  Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

Mise à jour des stratégies de prévention des épidémies

Il est essentiel d'utiliser les toutes dernières stratégies de prévention des épidémies pour protéger votre réseau des attaques virales. Mettez à jour les stratégies de prévention manuellement ou programmez les mises à jour.

Remarque

En cas de première installation de Control Manager, Trend Micro vous recommande vivement de procéder immédiatement à la mise à jour de vos stratégies en suivant la procédure évoquée. Pour les mises à jour ultérieures, faites appel à la fonction Mise à jour programmée.

Mise à jour manuelle des stratégies de prévention des épidémies

Pour éviter des tâches de maintenance supplémentaires, programmez Control Manager de façon à ce qu'il recherche et télécharge automatiquement les dernières stratégies de prévention des épidémies.

Remarque

L'écran **Outbreak Prevention Services** s'actualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Stratégies**.
2. Dans la zone de travail, sous État du service, cliquez sur **Mise à jour immédiate** pour télécharger les dernières stratégies de prévention des épidémies.
3. Cliquez sur **OK** une fois le téléchargement des stratégies de prévention des épidémies terminé.

Configuration des mises à jour automatiques des stratégies de prévention des épidémies

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Paramètres**.
2. Sous Paramètres de téléchargement de stratégie programmé, sélectionnez **Activer la mise à jour programmée des stratégies**.
3. Dans la liste Fréquence de téléchargement, choisissez le nombre de minutes qui doit s'écouler avant que Control Manager recherche les mises à jour des stratégies de prévention des épidémies.
4. Sous Source de téléchargement, sélectionnez la source qui contient les dernières stratégies de prévention des épidémies. L'option par défaut est Trend Micro ActiveUpdate Server. Si vous choisissez une autre source Internet, saisissez l'emplacement dans **Autre source de mise à jour**.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **OK**.

Démarrage du mode de prévention des épidémies

Lors d'une épidémie virale, démarrez le mode de prévention des épidémies pour déployer les stratégies de prévention propres à l'attaque, et atténuer les risques d'infection de votre réseau. Démarrez le mode de prévention des épidémies pour contrecarrer une menace unique spécifique.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Stratégies**.

   L'écran **Outbreak Prevention Services** apparaît.

   Cet écran se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

2. Dans la zone de travail, sous État du service, cliquez sur **Mise à jour immédiate** pour télécharger les dernières stratégies de prévention. Cette action est facultative si vous avez activé la mise à jour programmée et que vous disposez déjà des dernières versions.

3. Cliquez sur **OK** une fois le téléchargement des stratégies de prévention des épidémies terminé.

4. Sous Principales menaces dans le monde, cliquez sur le nom du virus qui menace actuellement votre réseau. Par défaut, Control Manager commence la liste par les menaces les plus récentes, puis répertorie les autres menaces dans l'ordre alphabétique. Chaque stratégie de prévention est conçue pour contrecarrer une menace particulière.

5. Cliquez sur **Démarrer le mode de prévention des épidémies**.

6. Sous Stratégie de prévention des épidémies, dans la liste prévue à cet effet, choisissez le nombre de jours pendant lequel Control Manager fonctionne en mode de prévention des épidémies.

7. Dans la liste Plan de déploiement, choisissez le plan à utiliser pour déployer les stratégies de prévention des épidémies sur les produits gérés.

8. Dans Informations détaillées sur la stratégie de prévention des épidémies, sélectionnez **Ne pas bloquer les numéros de ports autorisés spécifiés dans les paramètres de prévention des épidémies** pour veiller à ne pas bloquer les ports définis en tant qu'exceptions.

9. Configurez les paramètres des produits gérés ou cliquez sur **Paramètres recommandés**.

10. Cliquez sur **Activer**.

11. Cliquez sur **OK**. Le mode de prévention des épidémies a démarré et l'icône  apparaît dans l'en-tête de la console d'administration.

Modification d'une stratégie de prévention des épidémies

Après avoir démarré le mode de prévention des épidémies, modifiez les stratégies de prévention des épidémies en fonction des besoins de votre réseau. Vous pouvez, par exemple :

- modifier la durée du mode de prévention des épidémies ;
- choisir un plan de déploiement différent ;
- autoriser des numéros de ports particuliers ;
- configurer les paramètres des produits gérés.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Stratégies**.

   L'écran **Outbreak Prevention Services** apparaît.

   Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

2. Dans la zone de travail, cliquez sur **Modifier la stratégie**.

3. Sous Stratégie de prévention des épidémies, dans la liste prévue à cet effet, choisissez le nombre de jours pendant lequel Control Manager fonctionne en mode de prévention des épidémies.

4. Dans la liste Plan de déploiement, choisissez le plan à utiliser pour déployer les stratégies de prévention des épidémies sur les produits gérés (pour afficher/modifier ou ajouter des plans de déploiement, placez le curseur de la souris sur **Mises à jour** et cliquez sur **Plan de déploiement**).

5. Dans Informations détaillées sur la stratégie de prévention des épidémies, sélectionnez **Ne pas bloquer les numéros de ports autorisés spécifiés dans les paramètres de prévention des épidémies** pour veiller à ne pas bloquer les ports définis en tant qu'exceptions.

6. Configurez les paramètres des produits gérés ou cliquez sur **Paramètres recommandés**.

Conseil

Lorsque vous cliquez sur Paramètres recommandés, les paramètres recommandés par les TrendLabs s'appliquent et les paramètres définis par l'utilisateur sont supprimés. Si nécessaire, en fonction des dernières informations, ces recommandations sont mises à jour lors de chaque nouvelle mise en circulation de stratégies de prévention. Trend Micro vous conseille d'appliquer les paramètres recommandés.

7. Cliquez sur **Activer**.

Activation du mode de prévention automatique des épidémies

Les épidémies peuvent survenir à tout moment. En cas de prévention automatique des épidémies, il est possible de déployer automatiquement des stratégies de prévention sur les produits gérés pour des virus de type alerte rouge ou jaune, et d'envoyer les notifications correspondantes.

TABLEAU 18-3. Critères d'alerte des virus

ALERTE VIRALE	DESCRIPTION
Critères pour les virus de type alerte rouge	Plusieurs rapports d'infection sont reçus de chacun des domaines d'activité. Cela dénote une propagation rapide des programmes malveillants qui nécessite la protection des passerelles et des serveurs de messagerie. Le processus de la solution d'alerte rouge de 45 minutes, premier dans le genre, est déclenché : une version de signatures officielle (OPR) est déployée et sa mise à disposition est annoncée. Toutes les autres notifications utiles sont envoyées. Les outils de correction, ainsi que les informations relatives aux failles de sécurité, sont accessibles à partir des pages de téléchargement.

ALERTE VIRALE	DESCRIPTION
Critères pour les virus de type alerte jaune	Des rapports d'infection sont reçus de plusieurs domaines d'activité, et des appels passés au support technique confirment la présence d'instances disséminées. Une version de signatures officielle (OPR) est automatiquement transmise sur les serveurs de développement et rendue disponible par téléchargement. Si un programme malveillant se propage par courrier électronique, des règles de filtrage de contenu, appelées stratégies de prévention des épidémies, sont diffusées de façon à bloquer automatiquement les pièces jointes correspondantes sur les serveurs équipés de la fonctionnalité du produit.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Paramètres**.

   L'écran **Paramètres relatifs à Outbreak Prevention Services** apparaît.

   Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

2. Cliquez sur l'onglet **Mode de prévention automatique des épidémies**.

3. Exécutez les opérations suivantes :

   - Pour activer le mode de prévention automatique des épidémies pour les virus de type alerte rouge, dans Virus de type alerte rouge, sélectionnez **Activer la prévention automatique des épidémies**.
   - Pour activer le mode de prévention automatique des épidémies pour les virus de type alerte jaune, dans Virus de type alerte jaune, sélectionnez **Activer la prévention automatique des épidémies**.

4. Dans la liste Durée de prévention, choisissez le nombre de jours pendant lequel le mode de prévention des épidémies reste actif.

5. Dans la liste Plan de déploiement, choisissez le plan à utiliser pour déployer les stratégies de prévention des épidémies sur les produits gérés.

6. Exécutez les opérations suivantes :

   - Sous Produits exclus, sélectionnez les produits gérés qui ne recevront pas les stratégies de prévention des épidémies.

     AVERTISSEMENT!

     Ces produits ne bénéficieront pas du service Outbreak Prevention Services et auront plus de risques d'être infectés lors des épidémies.

   - Sous Ports autorisés, précisez les ports que Control Manager conservera ouverts lors d'une épidémie.

   - Sélectionnez **Arrêter automatiquement la stratégie de prévention des épidémies (OPP) à l'expiration de la durée de prévention** pour arrêter automatiquement la stratégie de prévention des épidémies.

7. Cliquez sur **Enregistrer**.

Configuration des paramètres de téléchargement du mode de prévention des épidémies

Configurez la fréquence à laquelle Control Manager recherche les mises à jour des stratégies de prévention des épidémies lorsqu'il fonctionne en mode de prévention des épidémies. Vous pouvez en outre choisir le plan de déploiement à utiliser pour déployer les stratégies de prévention mises à jour.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Paramètres**.

   L'écran **Paramètres de prévention des épidémies** apparaît.

   Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

2. Sous Paramètres de téléchargement du mode de prévention des épidémies, effectuez les opérations suivantes :

   - Dans la liste Fréquence de téléchargement, choisissez la fréquence à laquelle Control Manager recherche les mises à jour des stratégies de prévention des épidémies.
   - Dans la liste Composants à déployer, choisissez le plan de déploiement à utiliser pour déployer les composants téléchargés. Pour plus d'informations sur les plans de déploiement, consultez la section *Définition des plans de déploiement à la page 5-25*.
   - Pour déployer uniquement le fichier de signatures de virus, sélectionnez **Exclure le déploiement du moteur de scan**.

3. Cliquez sur **Enregistrer**.

Arrêt du mode de prévention des épidémies

Arrêtez manuellement le mode de prévention des épidémies avant l'expiration de la durée de la stratégie.

Lorsque Control Manager fonctionne en mode de prévention des épidémies, l'icône  s'affiche sur la console Web.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Stratégies**.

   L'écran **Outbreak Prevention Services** apparaît.

   Cette page se réactualise automatiquement pour vous communiquer des informations à jour sur les principales menaces et leurs états.

2. Cliquez sur **Arrêter le mode de prévention des épidémies**.

3. Cliquez sur **OK**.

Affichage de l'historique du mode de prévention des épidémies

Cette fonction du service Outbreak Prevention Services vous permet d'afficher les stratégies de prévention des épidémies qui ont déjà été appliquées. L'écran **Historique** affiche les informations suivantes :

TABLEAU 18-4. Informations de l'historique

EN-TÊTE	DESCRIPTION
#	Indique l'ordre dans lequel les tâches ont été réalisées ; plus le numéro est faible, plus la tâche est récente.
Virus	Virus ou programme malveillant à l'origine de l'épidémie
Démarré par	Nom de l'utilisateur de Control Manager qui a appliqué la stratégie
Durée du mode de prévention des épidémies	Indique la période pendant laquelle le mode de prévention des épidémies a été en vigueur. L'heure de départ apparaît sur la gauche, l'heure de fin (ou d'annulation) sur la droite.
État	Indique les résultats de la tâche. Pour afficher le résultat ou l'état d'une tâche, cliquez sur le lien Afficher correspondant à la tâche qui vous intéresse.
Rapport	Le nombre de virus détectés par la stratégie de prévention des épidémies au cours de l'OPS. Si aucun virus n'est détecté, aucune donnée ne s'affiche sous Rapport.

Procédure

1. Accédez à **Administration** > **Outbreak Prevention Services** > **Historique**.

   L'écran **Historique** apparaît.

2. Pour afficher l'état d'une stratégie de prévention spécifique, cliquez sur le lien **Afficher** de la même ligne.

   L'écran d'état affiche le nombre de virus détectés par vos produits antivirus.

Utilisation du mode de prévention des épidémies

Ce didacticiel vous explique, pas à pas, comment démarrer le mode de prévention des épidémies, et aborde les points suivants :

Étape 1 : Identification de la source de l'épidémie

Trend Micro propose aux clients enregistrés des services qui les aident à identifier les menaces qui pèsent sur leurs systèmes. Les alertes suivantes vous mettent en garde contre de nouvelles ou d'éventuelles épidémies de virus et de programmes malveillants.

TABLEAU 18-5. Identification de la source de l'épidémie

MÉTHODES D'ALERTE	DESCRIPTION
Téléchargements programmés des stratégies de prévention des épidémies	Control Manager peut vous informer qu'il télécharge des stratégies de prévention correspondant à une épidémie virale déclarée. Pour recevoir la notification relative à cet événement, activez Stratégie de prévention des épidémies active reçue dans le Centre d'événements. Dès la réception de la notification, démarrez immédiatement le mode de prévention des épidémies.

MÉTHODES D'ALERTE	DESCRIPTION
Responsable technique de votre compte	Selon le contrat d'assistance souscrit auprès de Trend Micro, le responsable technique de votre compte vous informera des risques d'épidémie. Dès réception de la mise en garde, mettez à jour vos stratégies de prévention des épidémies.
Rapports viraux de Trend Micro	Vous pouvez vous abonner à ce service sur le site Web de Trend Micro.
Alerte de virus spécial	Cette fonction de Control Manager, configurée dans le Centre d'événements, vous avertit lorsqu'un produit Trend Micro détecte, sur votre réseau, un virus susceptible d'engendrer une épidémie. Vous pouvez ainsi prendre immédiatement les mesures préventives qui s'imposent et demander, par exemple, aux employés de votre entreprise de se méfier de certaines formes de messages électroniques.

Étape 2 : Évaluation des stratégies existantes

Dès la réception d'une alerte d'épidémie virale, évaluez votre système pour déterminer s'il est en mesure de contrecarrer la menace. Dans l'écran **Outbreak Prevention Services**, examinez les stratégies de prévention des épidémies en vigueur sur votre serveur Control Manager pour vérifier si les stratégies existantes vous protègent du virus à l'origine de l'épidémie.

Conseil

Pour simplifier ce processus d'évaluation, activez les fonctions de Control Manager qui vous informent de la mise à disposition des stratégies de prévention correspondant aux épidémies virales déclarées.

Pour obtenir plus d'informations sur les alertes du service Outbreak Prevention Services, consultez la section *Définition du Centre d'événements à la page 8-2*

Pour obtenir plus d'informations sur le téléchargement de stratégies programmé, consultez la section *Mise à jour des stratégies de prévention des épidémies à la page 18-12*

Quelle proposition décrit le mieux les aptitudes de votre serveur Control Manager ?

- Le virus est couvert par les stratégies de prévention des épidémies actuellement en vigueur sur Control Manager.
- Le virus n'est pas couvert par les stratégies de prévention des épidémies actuellement en vigueur sur Control Manager.

Virus couvert par les stratégies existantes

Control Manager peut juguler l'épidémie. Démarrez le mode de prévention des épidémies et appliquez la stratégie de prévention correspondant à l'épidémie virale.

Virus non couvert par les stratégies existantes

Si les stratégies de prévention des épidémies ne couvrent pas l'épidémie virale, vous devez vous procurer une nouvelle stratégie auprès de Trend Micro.

Trend Micro vous recommande de mettre à jour manuellement les stratégies de prévention des épidémies obsolètes.

Étape 3 : Démarrage du mode de prévention des épidémies

Démarrez le mode de prévention des épidémies et appliquez la stratégie de prévention correspondant à l'épidémie virale. Dès que Control Manager passe en mode de

prévention des épidémies, vous pouvez analyser les recommandations formulées par Trend Micro à l'égard de la configuration des produits, et les modifier en fonction des besoins de votre réseau. Les stratégies mettent en œuvre les paramètres qui bloquent les points d'entrée connus des virus.

Si les TrendLabs déploient une stratégie de prévention des épidémies, c'est qu'ils en sont encore à tester la signature de virus appropriée. Les paramètres des stratégies de prévention des épidémies vous permettent donc de protéger votre réseau pendant la phase critique qui précède la mise à disposition d'une nouvelle signature.

Avant de démarrer le mode de prévention des épidémies, définissez les destinataires visés et la méthode de notification dans le Centre d'événements.

Éléments à prendre en compte pour démarrer une prévention des épidémies

Pour démarrer la prévention des épidémies, répondez aux questions suivantes :

- Pendant combien de temps voulez-vous appliquer cette stratégie ?

  Définissez la période pendant laquelle la stratégie doit rester en vigueur en entrant une valeur dans la liste prévue à cet effet. La période commence à l'heure où vous démarrez le mode de prévention des épidémies. Par défaut, les stratégies de prévention des épidémies restent actives pendant deux jours.

  Remarque

  Si vous modifiez la stratégie, Control Manager réinitialise la période qui commence alors le jour où vous avez apporté vos modifications.

- Comment déployer la stratégie ?

  Sélectionnez le plan de déploiement de votre choix pour cette phase. Le plan détermine les segments du répertoire Produits qui bénéficieront des paramètres contenus dans la stratégie.

  Remarque

  Si aucun des plans de déploiement existants ne vous convient, créez-en un. Consultez la section *Définition des plans de déploiement à la page 5-25*.

- Quels sont les points d'entrée que doit bloquer cette stratégie ?

  Les produits impliqués à ce stade sont :

  - InterScan eManager
  - InterScan WebProtect for ICAP
  - InterScan Messaging Security Suite for Windows
  - InterScan Messaging Security Suite for UNIX/IMSA/Solaris
  - InterScan Web Security Suite for Windows/Solaris/Linux/Appliance
  - InterScan Gateway Security Appliance
  - InterScan VirusWall for Windows/Linux
  - Network VirusWall
  - PortalProtect
  - ScanMail for Microsoft Exchange
  - ScanMail for Lotus Notes/ScanMail for Domino
  - IM Security for Microsoft Live Communications Server
  - ServerProtect for Windows
  - ServerProtect for Linux
  - OfficeScan Corporate Edition
  - Firewall Management – NetScreen

  Si les paramètres destinés à un produit particulier sont présents dans la stratégie, Control Manager coche automatiquement la case correspondant au produit.

Remarque

Si un ou plusieurs des produits cités ci-dessus n'appartiennent pas à votre réseau Control Manager, Control Manager ignore tout simplement les paramètres définis pour ces produits.

Évaluation ou modification de n'importe quel paramètre du produit

1. Cliquez sur le lien du produit ou sur l'icône + pour afficher ses paramètres.
2. Pour afficher les paramètres de tous les produits confondus, cliquez sur **Développer tout**. Les recommandations de Trend Micro s'affichent en lecture seule dans la partie droite de l'écran.
3. Modifiez les paramètres en fonction de vos besoins.

Étape 4 : Opérations de suivi

Après avoir suivi les consignes du didacticiel de la prévention des épidémies, surveillez l'évolution de la stratégie à l'aide de l'historique du mode de prévention des épidémies.

Conseil

Arrêtez manuellement le mode de prévention des épidémies après l'expiration de la stratégie. Si vous ne le faites pas, la fonction Mise à jour programmée du mode de prévention des épidémies se trouve dans l'incapacité d'appliquer automatiquement de nouvelles stratégies de prévention.

Chapitre 19

Utilisation des outils de Control Manager

Control Manager met à votre disposition plusieurs outils pour vous aider à réaliser des tâches de configuration spécifiques. Control Manager regroupe la plupart de ces outils dans l'emplacement suivant :

```
<racine>:\Control Manager\WebUI\download\tools\
```

Control Manager 6.0 prend en charge les outils suivants :

- *Utilisation de l'outil de migration des agents (AgentMigrateTool.exe) à la page 19-2* : pour migrer des agents Control Manager vers un serveur Control Manager 6.0
- *Utilisation du fichier MIB de Control Manager à la page 19-2* : Utilisez le fichier MIB de Control Manager avec une application (par exemple, HP OpenView) qui prend en charge le protocole SNMP.
- *Utilisation du fichier MIB NVW Enforcer SNMPv2 à la page 19-3* : Utilisez le fichier MIB NVW Enforcer avec une application (par exemple, HP OpenView) qui prend en charge le protocole SNMP
- *Utilisation de l'outil DBConfig à la page 19-3* : Utilisez DBConfig pour modifier le compte utilisateur, le mot de passe et le nom de la base de données de Control Manager.

Utilisation de l'outil de migration des agents (AgentMigrateTool.exe)

L'outil de migration des agents fourni dans Control Manager 6.0 Standard ou Advanced Edition permet de migrer les agents administrés par un serveur Control Manager 5.5 ou 5.0.

Remarque

L'outil de migration des agents prend en charge la migration des agents Windows et Linux.

Procédure

1. Connectez-vous au serveur de destination.
2. Exécutez `AgentMigrateTool.exe` depuis l'emplacement suivant : `<racine>\Program Files\Trend Micro\Control Manager\`

Utilisation du fichier MIB de Control Manager

Téléchargez et utilisez le fichier MIB de Control Manager avec une application (par exemple : HP™OpenView) qui prend en charge le protocole SNMP.

Procédure

1. Accédez à **Administration** > **Outils**.

   L'écran **Outils** apparaît.

2. Dans la zone de travail, cliquez sur **Fichier MIB de Control Manager**.
3. Dans l'écran de **Téléchargement du fichier**, sélectionnez **Enregistrer**, spécifiez un emplacement du serveur, puis cliquez sur **OK**.
4. Sur le serveur, extrayez le fichier MIB de Control Manager `cm2.mib` (base d'informations de gestion ou MIB).

5. Importez `cm2.mib` à l'aide d'une application (HP OpenView, par exemple) qui prend en charge le protocole SNMP.

Utilisation du fichier MIB NVW Enforcer SNMPv2

Téléchargez et utilisez le fichier MIB NVW Enforcer SNMPv2 avec une application (HP OpenView, par exemple) qui prend en charge le protocole SNMP.

Procédure

1. Accédez à **Administration** > **Outils**.

   L'écran **Outils** apparaît.

2. Cliquez sur **fichier MIB NVW Enforcer SNMPv2**.

3. Dans l'écran de **Téléchargement du fichier**, sélectionnez **Enregistrer**, spécifiez un emplacement du serveur, puis cliquez sur **OK**.

4. Sur le serveur, extrayez le fichier MIB NVW Enforcer SNMPv2 `nvw2.mib2` (base d'informations de gestion ou MIB).

5. Importez `nvw2.mib2` à l'aide d'une application (HP OpenView, par exemple) qui prend en charge le protocole SNMP.

Utilisation de l'outil DBConfig

L'outil DBConfig permet aux utilisateurs de modifier le compte, le mot de passe et le nom de base de données de l'utilisateur pour la base de données Control Manager.

L'outil offre les options suivantes :

- **DBName :** nom de la base de données
- **DBAccount :** compte de la base de données

- **DBPassword :** mot de passe de la base de données
- **Mode :** mode d'authentification de la base de données (SQL ou authentification Windows)

Remarque

Le mode par défaut est le mode d'authentification SQL. Cependant, le mode d'authentification Windows est nécessaire pour la configuration de l'authentification Windows.

Procédure

1. Sur le serveur Control Manager, cliquez sur **Démarrer** > **Exécuter**.
2. Tapez `cmd`, puis cliquez sur **OK**.

   L'écran d'invite de commande apparaît.
3. Remplacez le répertoire par le répertoire racine de Control Manager (par exemple, `<racine>\Program Files\Trend Micro\Control Manager \DBConfig`).
4. Saisissez `dbconfig`.

   L'interface de l'outil DBConfig apparaît.
5. Spécifiez les paramètres que vous souhaitez modifier :
   - **Exemple 1 :** `DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - **Exemple 2 :** `DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
   - **Exemple 3** : `DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`

Partie V

Suppression de Control Manager et contact de l'assistance technique

Chapitre 20

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

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 deTrend 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 20-4*
2. *Suppression des paramètres IIS de Control Manager à la page 20-6*
3. *Suppression de Crystal Reports, PHP, FastCGI, TMI et CCGI à la page 20-7*
4. *Suppression des fichiers/répertoires et clés de registre de Control Manager à la page 20-8*
5. *Suppression des composants de base de données à la page 20-9*
6. *Suppression de Control Manager et des services NTP à la page 20-11*

Arrêt des services Control Manager

L'écran Windows Services permet de redémarrer les services 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
```

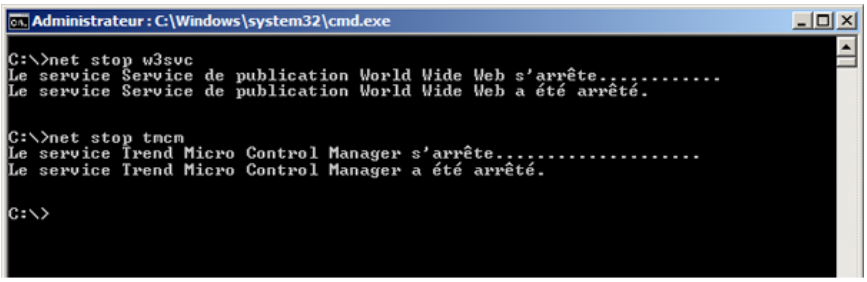


FIGURE 20-1. Vue de la ligne de commande avec les services nécessaires arrêtés

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. Exécutez l'outil de service Microsoft `Sc.exe`.
2. Entrez 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\OPPTrustPort
- 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 R2 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 R2**, puis cliquez sur **Supprimer** pour supprimer automatiquement les fichiers associés.

Conseil

Trend Micro vous recommande de consulter le site Web de Microsoft pour obtenir des instructions sur la suppression de SQL Server 2008 R2 Express si vous rencontrez des problèmes lors de la désinstallation :

http://support.microsoft.com/kb/955499

Suppression de Control Manager et des services NTP

Procédure

1. Exécutez l'outil de service Microsoft `Sc.exe`.
2. Entrez 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.

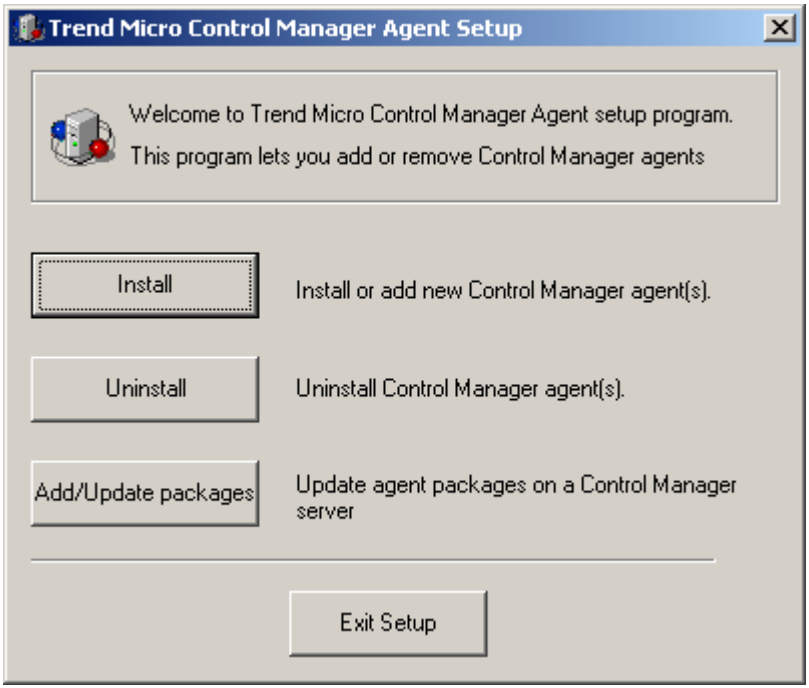


FIGURE 20-2. Programme d'installation des agents de Trend Micro Control Manager

5. Cliquez sur **Désinstaller**.

   L'écran de **Bienvenue** apparaît.

6. Cliquez sur **Suivant**.

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

FIGURE 20-3. 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.

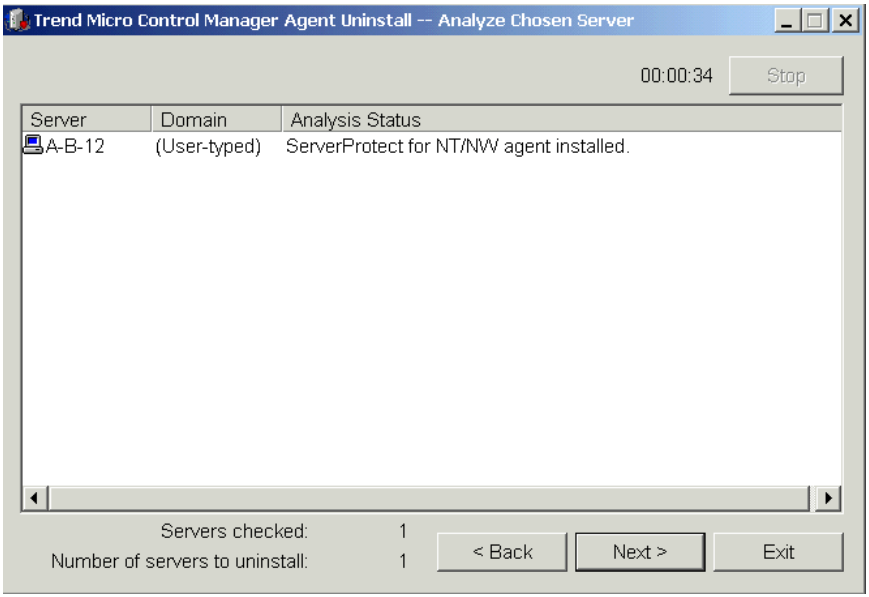


FIGURE 20-4. Analyse des serveurs Control Manager sélectionnés

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 21

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

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 TrendLabs℠ 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

Annexes

Annexes

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

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	
Nom (d'hôte) NetBIOS	proxyserver	

INFORMATIONS REQUISES	ÉCHANTILLON	VOTRE VALEUR
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	serveur de messagerie	
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	
Pare-feu, port de "transfert" (facultatif ; utilisé lors de l'installation d'agents Control Manager)	224	

PORT	ÉCHANTILLON	VOTRE VALEUR
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 \E2EPulic.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.

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.

TABLEAU 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 ProcessManager.exe
CmdProcessorEventHandler.xml	Utilisé par CmdProcessor.exe
UIProcessorEventHandler.xml	Utilisé par UIProcessor.exe
DMRegisterinfo.xml	Utilisé par CasProcessor.exe
DataSource.xml	Stocke les paramètres de connexion des processus Control Manager
SystemConfiguration.xml	Fichier de configuration système de Control Manager
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.
MsgReceiver.exe	Reçoit les messages provenant du serveur Control Manager, des produits gérés et des serveurs enfants.
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.

PROCESSUS	DESCRIPTION
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

Service	Port du service
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.

Tableau 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	●		●		●	

Fonctions	Version de Control Manager					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
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	●	●	●	●	●	●
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	●	●	●	●	●	●

Fonctions	Version de Control Manager					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
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	●	●	●	●	●	●
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	●	●	●	●	●	●

Fonctions	Version de Control Manager					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Microsoft SQL Express ou Microsoft SQL 2008			●	●	●	●
Microsoft SQL 2012					●	●
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) • 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	●	●	●	●	●	●
Gestion à distance	●	●	●	●	●	●
Création de rapports	●		●		●	
Communication sécurisée entre serveur et agents	●	●	●	●	●	●

Fonctions	Version de Control Manager					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
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			●	●	●	●
Intégration de Trend Micro InterScan for Cisco Content Security et Control Security Services Module (ISC CSC SSM)	●	●	●	●	●	●
Intégration de Trend Micro Network VirusWall 1200	●	●	●	●	●	●

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 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	●	●	●	●	●	●

Annexe B

Affichages des données

Les affichages de base de données sont disponibles pour les modèles de rapport Control Manager 5 et les requêtes ad hoc.

Cette annexe contient les sections suivantes :

Affichages des données : Informations sur le produit

Affiche des informations sur Control Manager, les produits gérés, les composants et les licences.

Informations sur la licence

Affiche l'état, les informations détaillées et les informations résumées sur Control Manager et les licences de produits gérés.

État de la licence du produit

Affiche des informations détaillées sur le produit géré ainsi que des informations sur le code d'activation utilisé par le produit géré. Exemples : des informations sur le produit géré, l'état actif ou non du code d'activation, le nombre de produits gérés activés par le code d'activation

TABLEAU B-1. Affichage des données État de la licence du produit

DONNÉES	DESCRIPTION
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Service	Affiche le nom du service de produit géré. Exemple : Outbreak Protection Services

Données	Description
État de la licence	Affiche l'état de la licence des produits gérés. Exemple : activé, expiré ou en période de grâce
Code d'activation	Affiche le code d'activation des produits gérés.
Codes d'activation	Affiche le nombre de codes d'activation utilisés par un produit géré.
Expiration de la licence	Affiche la date à laquelle la licence du produit géré expire.

Résumé des informations sur la licence du produit

Affiche des informations détaillées sur le code d'activation et des informations sur les produits gérés utilisant le code d'activation. Exemples : nombre de licences autorisées par le code d'activation, version d'évaluation ou complète du produit, description du code d'activation définie par l'utilisateur

Tableau B-2. Affichage des données Résumé des informations sur la licence du produit

Données	Description
Code d'activation	Affiche le code d'activation des produits gérés.
Description définie par l'utilisateur	Affiche la description du code d'activation telle que définie par l'utilisateur.
Produits/services	Affiche le nombre de services ou produits gérés utilisant le code d'activation.
État de la licence	Affiche l'état de la licence des produits gérés. Exemple : activé, expiré ou en période de grâce
Type de produit	Affiche le type de produit géré fourni par le code d'activation. Exemple : version d'évaluation, version complète

Données	Description
Expiration de la licence	Affiche la date à laquelle la licence du produit géré expire.
Sièges	Affiche le nombre de licences autorisées par le code d'activation.

Informations détaillées sur la licence du produit

Affiche des informations sur le code d'activation et sur les produits gérés utilisant ce code. Exemples : informations sur le produit géré, version d'évaluation ou complète du produit, date d'expiration de la licence

Tableau B-3. Affichage des données Informations détaillées sur la licence du produit

Données	Description
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Service	Affiche le nom du service géré. Exemple : Service de réputation de sites Web
État de la licence	Affiche l'état de la licence des produits gérés. Exemple : activé, expiré ou en période de grâce
Type de produit	Affiche le type de produit géré fourni par le code d'activation. Exemple : version d'évaluation, version complète

Données	Description
Code d'activation	Affiche le code d'activation des produits gérés.
Expiration de la licence	Affiche la date à laquelle la licence du produit géré expire.
Sièges	Affiche le nombre de licences autorisées par le code d'activation.
Description	Affiche la description du code d'activation.

Informations sur les produits gérés

Affiche l'état, les informations détaillées et les informations résumées des produits gérés ou des points finaux de produits gérés.

Résumé de la distribution du produit

Affiche des informations résumées sur les produits gérés enregistrés sur Control Manager. Exemples : nom de produit géré, numéro de version et nombre de produits gérés

Tableau B-4. Affichage des données Résumé de distribution des produits

Données	Description
Enregistré sur Control Manager	Affiche le serveur Control Manager sur lequel le produit géré est enregistré.
Catégorie du produit	Affiche la catégorie de protection contre les menaces pour un produit géré. Exemple : produits basés sur serveur, produits de poste de travail
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange

Données	Description
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Rôle du produit	Affiche le rôle du produit géré dans l'environnement réseau. Exemple : serveur, client
Produits	Affiche le nombre total d'unités d'un produit géré spécifique contenues dans un réseau.

Informations sur l'état du produit

Affiche des informations détaillées sur les produits gérés enregistrés sur Control Manager. Exemples : numéro de version et de compilation de produit géré, système d'exploitation

Tableau B-5. Affichage des données Informations sur l'état des produits

Données	Description
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

DONNÉES	DESCRIPTION
Hôte du produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'hôte du serveur sur lequel le produit géré est installé. • Nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse MAC de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse MAC du serveur sur lequel le produit géré est installé. • Adresse MAC d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Entité de gestion de Control Manager	Affiche le nom d'affichage d'entité du serveur Control Manager sur lequel le produit géré est enregistré.
Entité de serveur de gestion	Affiche le nom d'affichage d'entité d'un produit géré sur lequel un point final est enregistré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Domaine	Affiche le domaine auquel le produit géré appartient.

Données	Description
État de la connexion	Cette colonne de données affiche l'un des éléments suivants : • État de connexion du produit géré à Control Manager. Exemple : normal, anormal, hors ligne • État de connexion du client de point final au produit géré (OfficeScan). Exemple : normal, anormal, hors ligne
État du fichier de signatures	Affiche l'état des fichiers de signatures/des règles utilisés par le produit géré ou un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple). Exemple : à jour, obsolète
État du moteur	Affiche l'état des moteurs de scan utilisés par le produit géré ou un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple). Exemple : à jour, obsolète
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré ou de son client. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Compilation du produit	Affiche le numéro de compilation du produit géré. Ces informations apparaissent sur l'écran À propos des produits. Exemple : Version 5.0 (**Compilation 1219**)
Rôle du produit	Affiche le rôle du produit géré ou d'un ordinateur avec un client (par exemple un client OfficeScan) dans l'environnement de réseau. Exemple : serveur, client

Données	Description
Système d'exploitation	Affiche le système d'exploitation de l'ordinateur sur lequel le produit géré/ l'agent est installé.
Version du système d'exploitation	Affiche le numéro de version du système d'exploitation de l'ordinateur sur lequel le produit géré/l'agent est installé.
Service Pack du système d'exploitation	Affiche le numéro du service pack du système d'exploitation de l'ordinateur sur lequel le produit géré/l'agent est installé.

Résumé de l'état du serveur/domaine OfficeScan et ServerProtect

Affiche des informations résumées sur les produits gérés client/serveur. Exemples : fichier de signatures obsolète, moteur de scan obsolète,

Tableau B-6. Affichage des données Résumé de l'état du serveur/domaine OfficeScan et ServerProtect

Données	Description
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré.
Domaine	Affiche le domaine auquel le produit géré appartient.
Points finaux	Affiche le nombre de points finaux d'un domaine.
Fichiers de signatures obsolètes	Affiche le nombre de points finaux avec des fichiers de signatures obsolètes.
Taux de fichiers de signatures à jour (%)	Affiche le pourcentage de points finaux avec des fichiers de signatures à jour.
Moteurs obsolètes	Affiche le nombre de points finaux avec des moteurs de scan obsolètes.

Données	Description
Taux de moteurs à jour (%)	Affiche le pourcentage de points finaux avec des moteurs de scan à jour.

Informations sur les événements de produits

Affiche les informations relatives aux événements de produits gérés. Exemples : produits gérés enregistrés auprès de Control Manager, mises à jour de composants, déploiements de code d'activation

Tableau B-7. Affichage des données Informations sur les événements de produits

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données sur l'événement de produits gérés.
Généré	Affiche l'heure de création par le produit géré des données sur l'événement.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Gravité de l'événement	Affiche la gravité d'un événement. Exemple : informations, critique, avertissement
Type d'événement	Affiche le type de l'événement survenu. Exemple : virus de téléchargement détecté, blocage de fichier, rétrogradation

Données	Description
État de la commande	Affiche l'état de la commande. Exemple : réussite, échec, en cours
Description	Affiche la description fournie par un produit géré pour l'événement.

Informations relatives aux composants

Affiche l'état, les informations détaillées et les informations résumées sur l'état obsolète ou à jour et sur le déploiement des composants de produits gérés.

État du moteur

Affiche des informations détaillées sur les moteurs de scan utilisés par les produits gérés. Exemples : nom de moteur de scan, heure du dernier déploiement de moteur de scan et produits gérés utilisés par le moteur de scan

Tableau B-8. Affichage des données État du moteur

Données	Description
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

Données	Description
Hôte du produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'hôte du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
État de la connexion	Cette colonne de données affiche l'un des éléments suivants : • État de connexion du produit géré à Control Manager. Exemple : normal, anormal, hors ligne • État de connexion du client de point final au produit géré (OfficeScan). Exemple : normal, anormal, hors ligne
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré ou de son client. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Rôle du produit	Affiche le rôle du produit géré ou d'un ordinateur avec un client (par exemple un client OfficeScan) dans l'environnement de réseau. Exemple : serveur, client

Données	Description
Moteur	Affiche le nom du moteur de scan. Exemple : Moteur anti-pourriel (Windows), moteur de scan antivirus, moteur de scan IA 64 bits
Version du moteur	Affiche la version du moteur de scan. Exemple : Moteur anti-pourriel (Windows) : **3.000.1153**, moteur de scan antivirus, moteur de scan IA 64 bits : **8.000.1008**
État du moteur	Affiche l'état actuel du moteur de scan. Exemple : à jour, obsolète
Moteur mis à jour	Affiche l'heure du dernier déploiement du moteur de scan vers les produits gérés ou les points finaux.

État du fichier de signatures/de la règle

Affiche des informations détaillées sur les fichiers de signatures/règles utilisés par les produits gérés. Exemples : nom de fichier de signatures/règle, heure du dernier déploiement de fichier de signature/règle et produits gérés utilisant le fichier de signatures/la règle

Tableau B-9. Affichage des données État du fichier de signatures/de la règle

Données	Description
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

Données	Description
Hôte du produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'hôte du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
État de la connexion	Cette colonne de données affiche l'un des éléments suivants : • État de connexion du produit géré à Control Manager. Exemple : normal, anormal, hors ligne • État de connexion du client de point final au produit géré (OfficeScan). Exemple : normal, anormal, hors ligne
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré ou de son client. Exemple : OfficeScan **10.0**, Control Manager **5.0**
Rôle du produit	Affiche le rôle du produit géré ou d'un ordinateur avec un client (par exemple un client OfficeScan) dans l'environnement de réseau. Exemple : serveur, client

Données	Description
Fichier de signatures/règle	Affiche le nom du fichier de signature ou de la règle. Exemples : fichier de signatures de virus, signatures anti-pourriel
Version du fichier de signatures/de la règle	Affiche la version du fichier de signature ou de la règle. Exemples : fichier de signatures de virus : **3.203.00**, signatures anti-pourriel : **14256**
État du fichier de signatures/de la règle	Affiche l'état actuel du fichier de signatures/de la règle Exemple : à jour, obsolète
Fichier de signatures/règle mis à jour	Affiche l'heure du dernier déploiement de fichier de signatures/de règle vers les produits gérés ou les points finaux.

Déploiement des composants de produits

Affiche des informations détaillées sur les composants utilisés par les produits gérés. Exemples : nom de fichier de signatures/de règle, numéro de version de fichier de signatures/de règle et état de déploiement du moteur de scan

Tableau B-10. Affichage des données Déploiement de composants de produits

Données	Description
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Version du produit	Affiche le numéro de version du produit géré. Exemple : OfficeScan **10.0**, Control Manager **5.0**

Données	Description
État de la connexion	Affiche l'état de la connexion entre le produit géré et le serveur Control Manager ou les produits gérés et leurs points finaux.
État du fichier de signatures/de la règle	Affiche l'état actuel du fichier de signatures/de la règle Exemple : à jour, obsolète
État du déploiement du fichier de signatures/de la règle	Affiche l'état de déploiement de la dernière mise à jour de fichier de signatures/règle Exemple : réussite, échec, en cours
Déploiement du fichier de signatures/de la règle	Affiche l'heure du dernier déploiement de fichier de signatures/de règle vers les produits gérés ou les points finaux.
État du moteur	Affiche l'état actuel du moteur de scan. Exemple : à jour, obsolète
État du déploiement du moteur	Affiche l'état de déploiement de la dernière mise à jour du moteur de scan. Exemple : réussite, échec, en cours
Déploiement du moteur	Affiche l'heure du dernier déploiement du moteur de scan vers les produits gérés ou les points finaux.

Résumé de l'état du moteur

Affiche des informations résumées sur les moteurs de scan utilisés par les produits gérés. Exemples : nom de moteur de scan, taux de moteur de scan et nombre de moteurs de scan obsolètes

Tableau B-11. Affichage des données Résumé de l'état du moteur

Données	Description
Moteur	Affiche le nom du moteur de scan. Exemple : Moteur anti-pourriel (Windows), moteur de scan antivirus, moteur de scan IA 64 bits

Données	Description
Version	Affiche la version du moteur de scan. Exemple : Moteur anti-pourriel (Windows) : **3.000.1153**, moteur de scan antivirus, moteur de scan IA 64 bits : **8.000.1008**
À jour	Affiche le nombre de produits gérés avec des moteurs de scan à jour.
Obsolète	Affiche le nombre de produits gérés avec des moteurs de scan obsolètes.
Taux À jour (%)	Affiche le pourcentage de produits gérés avec des moteurs de scan à jour. Ce nombre inclut les moteurs de scan produisant une valeur N/A.

Résumé de l'état du fichier de signatures/de la règle

Affiche des informations résumées sur les fichiers de signatures/règles utilisés par les produits gérés. Exemples : nom de fichier de signatures/règle, taux de fichiers de signatures/règles à jour et nombre de fichiers de signatures/règles obsolètes.

Tableau B-12. Affichage des données Résumé de l'état de fichier de signatures/règle

Données	Description
Fichier de signatures/règle	Affiche le nom du fichier de signature ou de la règle. Exemples : fichier de signatures de virus, signatures anti-pourriel
Version	Affiche la version du fichier de signature ou de la règle. Exemples : fichier de signatures de virus : 3.203.00, signatures anti-pourriel : 14256
À jour	Affiche le nombre de produits gérés avec des fichiers de signatures ou règles à jour.
Obsolète	Affiche le nombre de produits gérés avec des fichiers de signatures ou règles obsolètes.

Données	Description
Taux À jour (%)	Affiche le pourcentage de produits gérés avec des fichiers de signatures/règles à jour. Ce taux inclut les fichiers de signatures/règles produisant une valeur N/A.

Informations Control Manager

Affiche des informations sur l'accès utilisateur à Control Manager, sur le suivi des commandes et les événements du serveur Control Manager.

Informations sur l'accès des utilisateurs

Affiche l'accès des utilisateurs à Control Manager et les activités effectuées par les utilisateurs lorsqu'ils sont connectés à Control Manager.

Tableau B-13. Affichage des données Informations sur l'accès des utilisateurs

Données	Description
Date/Heure	Affiche l'heure de début de l'activité.
Utilisateur	Affiche le nom de l'utilisateur débutant l'activité.
Type de compte	Affiche le type de compte attribué à un utilisateur par un administrateur Control Manager. Par exemple : Racine, Utilisateur expérimenté ou Opérateur.
Description du type de compte	Affiche la description du type de compte. Cette description est définie par Control Manager pour les types de comptes par défaut, tandis qu'elle est définie par l'utilisateur pour les types de comptes personnalisés.

Données	Description
Activité	Affiche l'activité effectuée par l'utilisateur sur Control Manager. Exemple : connexion, modification de compte utilisateur, ajout de plan de déploiement
Résultat	Affiche le résultat de l'activité.
Description	Affiche une description de l'activité, le cas échéant.

Informations sur les événements Control Manager

Affiche des informations relatives aux événements de Control Manager. Exemples : produits gérés enregistrés auprès de Control Manager, mises à jour de composants, déploiements de code d'activation

Tableau B-14. Affichage des données Informations sur les événements Control Manager

Données	Description
Date/Heure	Affiche l'heure à laquelle l'événement est survenu.
Type d'événement	Affiche le type de l'événement survenu. Exemple : notifier agent TMI, serveur notifie utilisateur, service de rapport notifie utilisateur
Résultat	Affiche le résultat de l'événement. Exemple : réussite, échec
Description	Affiche une description de l'activité, le cas échéant.

Informations de suivi des commandes

Affiche des informations relatives aux commandes que Control Manager envoie aux produits gérés. Exemples : produits gérés enregistrés auprès de Control Manager, mises à jour de composants, déploiements de code d'activation

TABLEAU B-15. Affichage des données Informations de suivi des commandes

DONNÉES	DESCRIPTION
Date/Heure	Affiche l'heure à laquelle la commande est envoyée par son émetteur.
Type de commande	Affiche le type de la commande émise. Exemple : mise à jour programmée, déploiement de code d'activation
Paramètre de la commande	Affiche des informations spécifiques relatives à la commande. Exemple : nom de fichier de signatures spécifique, code d'activation spécifique
Utilisateur	Affiche le nom de l'utilisateur ayant émis la commande.
Mis à jour	Affiche l'heure de la dernière vérification d'état de toutes les commandes pour le serveur Control Manager sélectionné.
Réussite	Affiche le nombre de commandes réussies.
Échec	Affiche le nombre de commandes non réussies.
En cours	Affiche le nombre de commandes en cours de traitement.
Tout	Affiche le nombre total de commandes (Réussite + Échec + En cours).

Informations détaillées de suivi des commandes

Affiche des informations détaillées sur les commandes. Exemples : produits gérés enregistrés auprès de Control Manager, mises à jour de composants, déploiements de code d'activation

TABLEAU B-16. Affichage des données Informations détaillées de suivi des commandes

DONNÉES	DESCRIPTION
Date/Heure	Affiche l'heure à laquelle la commande a été émise.
Type de commande	Affiche le type de la commande émise. Exemple : mise à jour programmée, déploiement de code d'activation
Paramètre de la commande	Affiche des informations spécifiques relatives à la commande. Exemple : nom de fichier de signatures spécifique, code d'activation spécifique
Entité du produit	Affiche le produit géré auquel la commande a été envoyée.
Utilisateur	Affiche le nom de l'utilisateur ayant émis la commande.
État de la commande	Affiche l'état de la commande : réussite, échec, en cours
Mis à jour	Affiche l'heure de la dernière vérification d'état de toutes les commandes pour le serveur Control Manager sélectionné.
Description détaillée du résultat	Affiche la description des événements fournie par Control Manager.

Affichage des données : Informations sur les menaces de sécurité

Affiche des informations sur les menaces de sécurité détectées par les produits gérés : virus, programme espion/grayware, sites d'hameçonnage, etc.

Informations sur les virus/programmes malveillants

Affiche des données résumées et détaillées sur les programmes malveillants/virus détectés par les produits gérés sur votre réseau.

Résumé sur l'ensemble des virus/programmes malveillants

Fournit un résumé spécifique général des détections de virus/programmes malveillants. Exemple : nom de virus/programme malveillant, nombre de points finaux touchés par le virus, nombre total d'instances du virus sur le réseau

TABLEAU B-17. Affichage des données Résumé de l'ensemble des virus/programmes malveillants

DONNÉES	DESCRIPTION
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources d'infections uniques dont proviennent des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus provenant de 2 sources d'infection. Sources uniques = 2

Données	Description
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Résumé des types généraux de virus/programmes malveillants

Fournit un résumé général des détections de virus/programmes malveillants. Exemple : type de virus/programme malveillant (chevaux de Troie, outils de piratage), nombre de virus/programmes malveillants uniques sur votre réseau, nombre total d'instances de virus/programmes malveillants sur le réseau

Tableau B-18. Affichage des données Résumé des types généraux de virus/programmes malveillants

Données	Description
Détections uniques	Affiche le nombre de virus/programmes malveillants uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections uniques = 1
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus sur 3 ordinateurs différents. Points finaux uniques = 3

Données	Description
Sources uniques	Affiche le nombre de sources d'infections uniques dont proviennent des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus provenant de 2 sources d'infection. Sources uniques = 2
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Résumé sur les sources de virus/programmes malveillants

Fournit un résumé des détections de virus/programmes malveillants issus de la source de l'épidémie. Exemple : nom de l'ordinateur source, nombre d'instances spécifiques de virus/programmes malveillants issus de l'ordinateur source, nombre total d'instances de virus/programmes malveillants sur le réseau

Tableau B-19. Affichage de données Résumé sur les sources de virus/programmes malveillants

Données	Description
Hôte source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur dont proviennent les virus/programmes malveillants.

DONNÉES	DESCRIPTION
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus sur 3 ordinateurs différents. Détections uniques = 3
Détections uniques	Affiche le nombre de virus/programmes malveillants uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Résumé sur les points finaux de virus/programmes malveillants

Fournit un résumé des détections de virus/programmes malveillants provenant de points finaux spécifiques. Exemple : nom du point final, nombre d'instances spécifiques de virus/programmes malveillants sur le point final, nombre total d'instances de virus/programmes malveillants sur le réseau

TABLEAU B-20. Affichage de données Résumé sur les points finaux de virus/programmes malveillants

DONNÉES	DESCRIPTION
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par les virus/programmes malveillants.
Sources uniques	Affiche le nombre de sources d'infections uniques dont proviennent des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus provenant de 2 sources d'infection. Sources uniques = 2
Détections uniques	Affiche le nombre de virus/programmes malveillants uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections uniques = 1
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Résumé chronologique des détections de violations de sécurité Web

Fournit un résumé des détections de violations de sécurité Web sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, nombre de points finaux en situation de violation, nombre total de violations de sécurité Web sur le réseau

TABLEAU B-21. Affichage des données Résumé chronologique des détections de violations de sécurité Web

DONNÉES	DESCRIPTION
Date/Heure	Affiche l'heure à laquelle le résumé des données a lieu.
Stratégies uniques	Affiche le nombre de stratégies violées. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies uniques = 1
Points finaux uniques	Affiche le nombre de points finaux uniques violés de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 4 ordinateurs. URL uniques = 1
URL uniques	Affiche le nombre d'URL uniques en situation de violation de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. URL uniques = 1
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Résumé sur l'action/le résultat de virus/programmes malveillants

Fournit un résumé des actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : actions spécifiques entreprises contre les virus/programmes malveillants, résultat de l'action entreprise, nombre total d'instances de virus/programmes malveillants sur le réseau

TABLEAU B-22. Affichage des données Résumé sur l'action/le résultat de virus/programme malveillant

DONNÉES	DESCRIPTION
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources d'infections uniques dont proviennent des virus/programmes malveillants. Exemple : OfficeScan détecte 10 instances du même virus provenant de 2 sources d'infection. Sources uniques = 2

Données	Description
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations détaillées sur les virus/programmes malveillants

Fournit des informations spécifiques sur les instances de virus/programmes malveillants sur votre réseau Exemple : produit géré détectant les virus/programmes malveillants, nom du virus/programme malveillant, nom du point final touché par le virus/programme malveillant

Tableau B-23. Affichage des données Informations détaillées sur les virus/programmes malveillants

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

Données	Description
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse MAC de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse MAC du serveur sur lequel le produit géré est installé. • Adresse MAC d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Entité de serveur de gestion	Affiche le nom d'affichage d'entité du serveur de produit géré sur lequel un point final est enregistré.
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par les virus/programmes malveillants.
Source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur dont proviennent les virus/programmes malveillants.

DONNÉES	DESCRIPTION
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des virus/programmes malveillants.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10
Type d'entité	Affiche le point d'entrée de virus/programmes malveillants détectés par les produits gérés. Exemple : virus détecté dans un fichier, HTTP, Windows Live Messenger (MSN)

Données	Description
Informations détaillées	Utilisé uniquement pour les requêtes ad hoc. Affiche des informations détaillées sur la sélection. Dans les requêtes ad hoc, cette colonne affiche la sélection soulignée. En cliquant sur la sélection soulignée, des informations supplémentaires sur celle-ci sont affichées. Exemple : Détails de l'hôte, Détails du réseau, Détails HTTP/FTP

Informations détaillées sur les virus/programmes malveillants des points finaux

Fournit des informations spécifiques sur les instances de virus/programmes malveillants détectées sur les points finaux. Exemple : produit géré détectant les virus/programmes malveillants, type de scan détectant les virus/programmes malveillants, chemin du fichier contenant les virus/programmes malveillants détectés sur le point final

Tableau B-24. Affichage des données Informations sur les virus/programmes malveillants des points finaux

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.

DONNÉES	DESCRIPTION
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Entité de serveur de gestion	Affiche le nom d'affichage d'entité du serveur de produit géré sur lequel un point final est enregistré.
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE
Point final	Affiche le nom de l'ordinateur touché par les virus/programmes malveillants.

Données	Description
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des virus/programmes malveillants.
Type de scan	Affiche le type de scan utilisé par le produit géré pour détecter les virus/programmes malveillants. Exemple : en temps réel, programmé, manuel
Fichier	Affiche le nom du fichier touché par les virus/programmes malveillants et détecté par les produits gérés.
Chemin d'accès du fichier	Affiche le chemin du fichier sur l'ordinateur de point final sur lequel les produits gérés ont détecté le virus/programme malveillant.
Fichier dans un fichier compressé	Affiche le nom du fichier infecté/virus/programme malveillant contenu dans un fichier compressé.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur les virus/programmes malveillants Web

Fournit des informations spécifiques sur les instances de virus/programmes malveillants détectées dans le trafic HTTP/FTP. Exemple : produit géré détectant les virus/programmes malveillants, direction du trafic contenant les virus/programmes malveillants, navigateur Internet ou point final FTP téléchargeant les virus/programmes malveillants.

TABLEAU B-25. Affichage des données Informations sur les virus/programmes malveillants Web

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE

Données	Description
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur sur lequel les produits gérés détectent les virus/programmes malveillants.
URL source	Affiche l'URL du site Web/FTP dont provient le virus/programme malveillant.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des virus/programmes malveillants.
Trafic/connexion	Affiche la direction de l'entrée du virus/programme malveillant.
Navigateur/client FTP	Affiche le navigateur Internet ou point final FTP dont proviennent les virus/programmes malveillants.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur les virus/programmes malveillants de courrier électronique

Fournit des informations spécifiques sur les instances de virus/programmes malveillants détectées dans les messages électroniques. Exemple : produit géré détectant les virus/programmes malveillants, contenu de la ligne d'objet du message électronique, expéditeur du message électronique contenant les virus/programmes malveillants

TABLEAU B-26. Affichage des données Informations sur les virus/programmes malveillants de courrier électronique

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE
Destinataire	Affiche le destinataire du message électronique contenant les virus/programmes malveillants.
Expéditeur	Affiche l'expéditeur du message électronique contenant les virus/programmes malveillants.

Données	Description
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des virus/programmes malveillants.
Objet	Affiche le contenu de la ligne d'objet du message électronique contenant les virus/programmes malveillants.
Fichier	Affiche le nom du fichier touché par les virus/programmes malveillants et détecté par les produits gérés.
Fichier dans un fichier compressé	Affiche le nom du fichier infecté/virus/programme malveillant contenu dans un fichier compressé.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur les virus/programmes malveillants de réseau

Fournit des informations spécifiques sur les instances de virus/programmes malveillants détectées dans le trafic réseau. Exemple : produit géré détectant les virus/programmes malveillants, protocole utilisé par le virus/programme malveillant pour pénétrer dans votre réseau, informations spécifiques sur la source et la destination du virus/programme malveillant

TABLEAU B-27. Affichage des données Informations sur les virus/programmes malveillants de réseau

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Virus/programme malveillant	Affiche le nom des virus/programmes malveillants détectés par les produits gérés. Exemple : NIMDA, BLASTER, I_LOVE_YOU.EXE

Données	Description
Point final	Affiche l'adresse IP/le nom d'hôte de l'ordinateur touché par les virus/ programmes malveillants.
Hôte source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur dont proviennent les virus/ programmes malveillants.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des virus/programmes malveillants.
Trafic/connexion	Affiche la direction de l'entrée du virus/ programme malveillant.
Protocole	Affiche le protocole utilisé par le virus/ programme malveillant pour pénétrer dans le réseau. Exemple : HTTP, SMTP, FTP
Ordinateur de point final	Affiche le nom de l'ordinateur touché par les virus/programmes malveillants.
Port de point final	Affiche le numéro de port de l'ordinateur touché par les virus/programmes malveillants.
Adresse MAC de point final	Affiche l'adresse MAC de l'ordinateur touché par les virus/programmes malveillants.
Ordinateur source	Affiche le nom de l'ordinateur dont proviennent les virus/programmes malveillants.
Port source	Affiche le numéro de port de l'ordinateur dont proviennent les virus/programmes malveillants.

DONNÉES	DESCRIPTION
Adresse MAC source	Affiche l'adresse MAC de l'ordinateur dont proviennent les virus/programmes malveillants.
Fichier	Affiche le nom du fichier touché par les virus/programmes malveillants et détecté par les produits gérés.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les virus/programmes malveillants. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les virus/programmes malveillants. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de virus/programmes malveillants détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur les programmes espions/graywares

Affiche des données résumées et détaillées sur les programmes espions/graywares détectés par les produits gérés sur votre réseau.

Résumé de l'ensemble des programmes espions/graywares

Fournit un résumé spécifique général des détections de programmes espions/graywares. Exemple : nom du programme espion/grayware, nombre de points finaux touchés par le programme espion/grayware, nombre total d'instances du programme espion/grayware sur le réseau

TABLEAU B-28. Affichage des données Résumé de l'ensemble des programmes espions/graywares

DONNÉES	DESCRIPTION
Programmes espions/graywares	Affiche le nom des programmes espions/ graywares détectés par les produits gérés.
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des programmes espions/ graywares. OfficeScan détecte 10 instances du même programme espion/grayware sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources uniques dont proviennent les programmes espions/ graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware provenant de 2 sources d'infection différentes. Sources uniques = 2
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés.

Résumé des sources de programmes espions/graywares

Fournit un résumé des détections de programmes espions/graywares issus de la source de l'épidémie. Exemple : nom de l'ordinateur source, nombre d'instances spécifiques de programmes espions/graywares issus de l'ordinateur source, nombre total d'instances de programmes espions/graywares sur le réseau

TABLEAU B-29. Affichage des données Résumé des sources de programmes espions/graywares

DONNÉES	DESCRIPTION
Hôte source	Affiche le nom de l'ordinateur dont proviennent les programmes espions/graywares.
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des programmes espions/graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur 3 ordinateurs différents. Points finaux uniques = 3
Détections uniques	Affiche le nombre de programmes espions/graywares uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections uniques = 1
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Résumé des programmes espions/graywares de point final

Fournit un résumé des détections de programmes espions/graywares provenant de points finaux spécifiques. Exemple : nom du point final, nombre d'instances spécifiques de programmes espions/graywares sur le point final, nombre total d'instances de programmes espions/graywares sur le réseau

TABLEAU B-30. Affichage des données Résumé des programmes espions/graywares de point final

DONNÉES	DESCRIPTION
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par les programmes espions/graywares.
Sources uniques	Affiche le nombre de sources uniques dont proviennent les programmes espions/ graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware provenant de 2 sources d'infection différentes. Sources uniques = 2
Détections uniques	Affiche le nombre de programmes espions/ graywares uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections uniques = 1
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Résumé chronologique des détections de programmes espions/graywares

Fournit un résumé des détections de programmes espions/graywares sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la

collecte des données de résumé, nombre de points finaux touchés par le programme espion/grayware, nombre total d'instances de programmes espions/graywares sur le réseau

TABLEAU B-31. Affichage des données Résumé chronologique sur les détections de programmes espions/graywares

DONNÉES	DESCRIPTION
Date/Heure	Affiche l'heure à laquelle le résumé des données a lieu.
Détections uniques	Affiche le nombre de programmes espions/graywares uniques détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections uniques = 1
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des programmes espions/graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources uniques dont proviennent les programmes espions/graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware provenant de 2 sources d'infection différentes. Sources uniques = 2

Données	Description
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Résumé de l'action/du résultat sur les programmes espions/graywares

Fournit un résumé des actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : actions spécifiques entreprises contre les programmes espions/graywares, résultat de l'action entreprise, nombre total d'instances de programmes espions/graywares sur le réseau

Tableau B-32. Affichage des données Résumé de l'action/du résultat sur les programmes espions/graywares

Données	Description
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé

DONNÉES	DESCRIPTION
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des programmes espions/ graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur 3 ordinateurs différents. Points finaux uniques = 3
Sources uniques	Affiche le nombre de sources uniques dont proviennent les programmes espions/ graywares. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware provenant de 2 sources d'infection différentes. Sources uniques = 2
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Informations détaillées sur les programmes espions/ graywares

Fournit des informations spécifiques sur les instances de programmes espions/ graywares sur votre réseau Exemple : produit géré détectant les programmes espions/ graywares, nom du programme espion/grayware, nom du point final touché par le programme espion/grayware

TABLEAU B-33. Affichage des données Informations détaillées sur les programmes espions/graywares

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.

DONNÉES	DESCRIPTION
Produit/adresse MAC de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse MAC du serveur sur lequel le produit géré est installé. • Adresse MAC d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Entité de serveur de gestion	Affiche le nom d'affichage d'entité du serveur de produit géré sur lequel un point final est enregistré.
Programmes espions/graywares	Affiche le nom des programmes espions/graywares détectés par les produits gérés.
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par le programme espion/grayware.
Hôte source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur d'où proviennent les programmes espions/graywares.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des programmes espions/graywares.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé

Données	Description
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10
Type d'entité	Affiche le point d'entrée de programmes espions/graywares détectés par les produits gérés. Exemple : virus détecté dans un fichier, HTTP, Windows Live Messenger (MSN)
Informations détaillées	Utilisé uniquement pour les requêtes ad hoc. Affiche des informations détaillées sur la sélection. Dans les requêtes ad hoc, cette colonne affiche la sélection soulignée. En cliquant sur la sélection soulignée, des informations supplémentaires sur celle-ci sont affichées. Exemple : Détails de l'hôte, Détails du réseau, Détails HTTP/FTP

Programmes espions/graywares de points finaux détaillés

Fournit des informations spécifiques sur les instances de programmes espions/graywares détectées sur les points finaux. Exemple : produit géré détectant les programmes espions/graywares, type de scan détectant les programmes espions/graywares, chemin du fichier contenant les programmes espions/graywares détectés sur le point final

TABLEAU B-34. Affichage des données Programmes espions/graywares de point final

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Entité de serveur de gestion	Affiche le nom d'affichage d'entité du serveur de produit géré sur lequel un point final est enregistré.

Données	Description
Programmes espions/graywares	Affiche le nom des programmes espions/ graywares détectés par les produits gérés.
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par le programme espion/grayware.
Hôte source	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur d'où proviennent les programmes espions/graywares.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des programmes espions/ graywares.
Type de scan	Affiche le type de scan utilisé par le produit géré pour détecter les programmes espions/graywares. Exemple : en temps réel, programmé, manuel
Ressource	Affiche les ressources spécifiques affectées. Exemple : application.exe, H Key Local Machine\SOFTWARE\ACME
Type de ressource	Affiche le type de ressources affectées par les programmes espions/graywares. Exemple : registre, ressource mémoire
Type de menace de sécurité	Affiche le type spécifique de programmes espions/graywares détectés par les produits gérés. Exemple : programmes publicitaires, COOKIE, application pair-à-pair

DONNÉES	DESCRIPTION
Niveau de risque	Affiche le niveau défini par Trend Micro du risque que représente le programme espion/grayware pour votre réseau. Exemple : Niveau élevé, Niveau moyen, Niveau faible
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé

Programmes espions/graywares Web

Fournit des informations spécifiques sur les instances de programmes espions/graywares détectées dans le trafic HTTP ou FTP. Exemple : produit géré détectant les programmes espions/graywares, direction du trafic contenant les programmes espions/graywares, navigateur Internet ou point final FTP téléchargeant les programmes espions/graywares.

TABLEAU B-35. Affichage des données Programmes espions/graywares Web

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.

Données	Description
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Programmes espions/graywares	Affiche le nom des programmes espions/graywares détectés par les produits gérés.
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur sur lequel les produits gérés détectent les programmes espions/graywares.
URL source	Affiche l'URL du site Web/FTP dont provient le programme espion/grayware.
Trafic/connexion	Affiche la direction de l'entrée du programme espion/grayware.
Navigateur/client FTP	Affiche le navigateur Internet ou point final FTP dont proviennent les programmes espions/graywares.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des programmes espions/graywares.

Données	Description
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Programmes espions/graywares de messages électroniques

Fournit des informations spécifiques sur les instances de programmes espions/graywares détectées dans les messages électroniques. Exemple : produit géré détectant les programmes espions/graywares, contenu de la ligne d'objet du message électronique, expéditeur du message électronique contenant les programmes espions/graywares

Tableau B-36. Affichage des données Programmes espions/graywares de courrier électronique

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.

Données	Description
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Programmes espions/graywares	Affiche le nom des programmes espions/graywares détectés par les produits gérés.
Destinataire	Affiche le destinataire du message électronique contenant les programmes espions/graywares.
Expéditeur	Affiche l'expéditeur du message électronique contenant les programmes espions/graywares.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des programmes espions/graywares.
Objet	Affiche le contenu de la ligne d'objet du message électronique contenant les programmes espions/graywares.
Fichier	Affiche le nom du fichier touché par les programmes espions/graywares et détecté par les produits gérés.
Fichier dans un fichier compressé	Affiche le nom du fichier infecté par un programme espion/grayware situé dans un fichier compressé.

Données	Description
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Programmes espions/graywares de réseau

Fournit des informations spécifiques sur les instances de programmes espions/graywares détectées dans le trafic réseau. Exemple : produit géré détectant les programmes espions/graywares, protocole utilisé par les programmes espions/graywares pour pénétrer dans votre réseau, informations spécifiques sur la source et la destination des programmes espions/graywares

Tableau B-37. Affichage des données Programmes espions/graywares de réseau

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.

Données	Description
Généré	Affiche l'heure de création par le produit géré des données.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est touché par le programme espion/grayware.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Programmes espions/graywares	Affiche le nom des programmes espions/graywares détectés par les produits gérés.
Trafic/connexion	Affiche la direction de l'entrée du programme espion/grayware.
Protocole	Affiche le protocole utilisé par les programmes espions/graywares pour pénétrer dans le réseau. Exemple : HTTP, SMTP, FTP
Adresse IP de point final	Affiche l'adresse IP de l'ordinateur touché par les programmes espions/graywares.
Point final	Affiche l'adresse IP ou le nom d'hôte de l'ordinateur touché par les programmes espions/graywares.
Port de point final	Affiche le numéro de port de l'ordinateur touché par les programmes espions/graywares.

DONNÉES	DESCRIPTION
Adresse MAC de point final	Affiche l'adresse MAC de l'ordinateur touché par les programmes espions/ graywares.
Adresse IP source	Affiche l'adresse IP de l'ordinateur dont proviennent les programmes espions/ graywares.
Hôte source	Affiche le nom d'hôte de l'ordinateur dont proviennent les programmes espions/ graywares.
Port source	Affiche le numéro de port de l'ordinateur dont proviennent les programmes espions/ graywares.
Adresse MAC source	Affiche l'adresse MAC de l'ordinateur dont proviennent les programmes espions/ graywares.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur de point final lorsqu'un produit géré détecte des programmes espions/ graywares.
Fichier	Affiche le nom du fichier touché par les programmes espions/graywares et détecté par les produits gérés.
Résultat	Affiche les résultats de l'action entreprise par les produits gérés contre les programmes espions/graywares. Exemple : réussite, action supplémentaire nécessaire
Action	Affiche le type d'actions entreprises par les produits gérés contre les programmes espions/graywares. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier supprimé

Données	Description
Détections	Affiche le nombre total de programmes espions/graywares détectés par les produits gérés. Exemple : OfficeScan détecte 10 instances du même programme espion/grayware sur un ordinateur. Détections = 10

Informations sur les violations de contenu

Affiche des données résumées et détaillées sur le contenu prohibé détecté par les produits gérés sur votre réseau.

Résumé sur la stratégie en matière de violation de contenu

Fournit un résumé des détections de violations de contenu en fonction de stratégies spécifiques. Exemple : nom de la stratégie violée, type de filtre détectant la violation de contenu, nombre total de violations de contenu sur le réseau

Tableau B-38. Affichage des données Résumé sur la stratégie en matière de violation de contenu

Données	Description
Stratégie	Affiche le nom de la stratégie violée par les points finaux.
Type de fichier	Affiche le type de filtre activant la violation. Exemple : filtre de contenu, filtre d'hameçonnage, filtre de réputation d'URL

DONNÉES	DESCRIPTION
Expéditeurs/utilisateurs uniques	Affiche le nombre d'adresses électroniques ou d'utilisateurs uniques qui expédient du contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie provenant de 3 ordinateurs. Expéditeurs/utilisateurs uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messages électroniques uniques réceptrices de contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2
Détections	Affiche le nombre total de violations de stratégie détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur un ordinateur. Détections = 10

Résumé sur l'expéditeur de violation de contenu

Fournit un résumé des détections de violations de contenu en fonction d'expéditeurs spécifiques. Exemple : nom de l'expéditeur du contenu, nombre de violations de contenu uniques, nombre total de violations de contenu sur le réseau

TABLEAU B-39. Affichage des données Résumé sur l'expéditeur de violation de contenu

DONNÉES	DESCRIPTION
Expéditeur/utilisateur	Affiche l'adresse électronique ou les utilisateurs qui expédient du contenu violant des stratégies de produit géré.
Détections	Affiche le nombre total de violations de stratégie détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur un ordinateur. Détections = 10
Destinataires uniques	Affiche le nombre d'adresses de messages électroniques uniques réceptrices de contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2
Stratégies uniques	Affiche le nombre de stratégies violées uniques détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur un ordinateur. Détections = 10

Résumé chronologique des détections de violations de contenu

Fournit un résumé des détections de violations de contenu sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, nombre de points finaux touchés par la violation de contenu,

nombre total de violations de contenu uniques et nombre total de violations de contenu sur le réseau

TABLEAU B-40. Affichage des données Résumé chronologique des détections de violations de contenu

DONNÉES	DESCRIPTION
Date/Heure	Affiche l'heure à laquelle le résumé des données a lieu.
Stratégies uniques	Affiche le nombre de stratégies violées uniques détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur un ordinateur. Détections = 10
Expéditeurs/utilisateurs uniques	Affiche le nombre d'adresses électroniques ou d'utilisateurs uniques qui expédient du contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie provenant de 3 ordinateurs. Expéditeurs/utilisateurs uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messages électroniques uniques réceptrices de contenu violant des stratégies de produit géré. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2

Données	Description
Détections	Affiche le nombre total de violations de stratégie détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur un ordinateur. Détections = 10

Résumé de l'action/du résultat sur la violation de contenu

Fournit un résumé des actions entreprises par les produits gérés contre les violations de contenu. Exemple : action entreprise par les produits gérés contre la violation de contenu, nombre de messages électroniques concernés par l'action entreprise

Tableau B-41. Affichage des données Résumé de l'action/du résultat sur la violation de contenu

Données	Description
Action	Affiche le type d'action entreprise par les produits gérés contre les messages électroniques en situation de violation des stratégies de contenu. Exemple : transmis, pièces jointes éliminées, supprimé
Détections	Affiche le nombre de violations concernées par l'action spécifique entreprise par les produits gérés.

Informations détaillées sur les violations de contenu

Fournit des informations spécifiques sur les violations de contenu sur votre réseau. Exemple : produit géré détectant la violation de contenu, nom de la stratégie spécifique violée, nombre total de violations de contenu sur le réseau

TABLEAU B-42. Affichage des données Informations détaillées sur les violations de contenu

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Destinataire	Affiche le destinataire de messages électroniques recevant du contenu violant les stratégies de produit géré.
Expéditeur/utilisateur	Affiche l'adresse électronique ou l'utilisateur qui expédie du contenu violant des stratégies de produit géré.
Objet	Affiche le contenu de la ligne d'objet du message électronique violant une stratégie.
Stratégie	Affiche le nom de la stratégie violée par un message électronique.
Paramètres de stratégie	Affiche les paramètres de la stratégie violée par un message électronique.
Emplacement du fichier	Affiche l'emplacement du fichier violant une stratégie.
Fichier	Affiche le nom du fichier violant une stratégie.

Données	Description
URL	Affiche l'URL violée de la stratégie spécifiée.
Niveau de risque	Affiche l'évaluation par Trend Micro du risque pour votre réseau. Exemple : niveau élevé, niveau faible, niveau moyen
Type de fichier	Affiche le type de filtre détectant le message électronique en situation de violation. Exemple : filtre de contenu, filtre de taille, filtre de pièces jointes
Action de filtre	Affiche l'action entreprise par le filtre de détection contre le message électronique violant une stratégie. Exemple : nettoyer, mettre en quarantaine, éliminer
Action	Affiche le type d'action entreprise par les produits gérés contre les messages électroniques en situation de violation des stratégies de contenu. Exemple : livrer, éliminer, transmettre
Détections	Affiche le nombre total de violations de stratégie détectées par les produits gérés.

Informations sur les violations de spam

Affiche des données résumées et détaillées sur les spams détectés par les produits gérés sur votre réseau.

Résumé sur les destinataires de spam

Fournit un résumé des violations de spam sur des points finaux spécifiques. Exemple : nom du point final, nombre total d'instances de virus/programmes malveillants sur le point final

TABLEAU B-43. Affichage des données Résumé sur le destinataire de pourriel

DONNÉES	DESCRIPTION
Destinataire	Affiche le nom du destinataire recevant le pourriel.
Détections	Affiche le nombre total de violations de pourriel détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même spam sur un ordinateur. Détections = 10

Résumé chronologique des détections de spam

Fournit un résumé des détections de pourriel sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, nombre de points finaux touchés par le spam, nombre total de violations de spam sur le réseau

TABLEAU B-44. Affichage des données Résumé chronologique des détections de pourriel

DONNÉES	DESCRIPTION
Heure du résumé	Affiche l'heure à laquelle le résumé des données a lieu.

Données	Description
Domaines destinataires uniques	Affiche le nombre total de domaines destinataires uniques touchés par le pourriel. Exemple : un produit géré détecte 10 instances de violation du même pourriel provenant de 2 domaines sur 1 domaine destinataire. Domaines destinataires uniques = 1
Destinataires uniques	Affiche le nombre de destinataires uniques recevant du pourriel provenant du domaine spécifique. Exemple : un produit géré détecte 10 instances de violation de pourriel provenant d'un même domaine sur 3 ordinateurs. Destinataires uniques = 3
Détections	Affiche le nombre total de violations de pourriel détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même spam sur un ordinateur. Détections = 10

Informations détaillées sur les spams

Fournit des informations spécifiques sur les violations de pourriel sur votre réseau. Exemple : produit géré détectant la violation de contenu, nom de la stratégie spécifique violée, nombre total de violations de spam sur le réseau

TABLEAU B-45. Affichage des données Informations détaillées sur les spams

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Destinataire	Affiche les destinataires de pourriel.
Expéditeur	Affiche les expéditeurs de pourriel.
Objet	Affiche le contenu de la ligne d'objet du pourriel.
Stratégie	Affiche le nom de la stratégie violée par le message électronique.
Action	Affiche le type d'actions entreprises par les produits gérés contre le pourriel. Exemple : livrer, transmettre, éliminer
Détections	Affiche le nombre total de violations de pourriel détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même spam sur un ordinateur. Détections = 10

Informations de connexion de spam

Fournit des informations spécifiques sur la source de spam sur votre réseau. Exemple : produit géré détectant la violation de pourriel, action spécifique entreprise par les produits gérés contre les violations de pourriel, nombre total de violations de pourriel sur le réseau

TABLEAU B-46. Affichage des données Informations de connexion de pourriel

DONNÉES	DESCRIPTION
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Adresse IP source	Affiche l'adresse IP du serveur de messagerie électronique dont provient le pourriel.
Type de fichier	Affiche le type de filtre détectant le message électronique en situation de violation. Exemple : Real-time Blackhole List (RBL+), Quick IP List (QIL)
Action	Affiche le type d'actions entreprises par les produits gérés contre le pourriel pour l'empêcher de pénétrer dans le réseau. Exemple : interrompre connexion, contourner connexion

Données	Description
Détections	Affiche le nombre total de violations de pourriel détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même spam sur un ordinateur. Détections = 10

Informations sur les violations de stratégies/règles

Affiche des données résumées et détaillées sur les violations de stratégies/règles détectées par les produits gérés sur votre réseau.

Informations détaillées sur les violations de pare-feu

Fournit des informations spécifiques sur les violations de règles de pare-feu sur votre réseau. Exemple : produit géré détectant la violation de règle de pare-feu, informations spécifiques sur la source et la destination, nombre total de violations de règles de pare-feu sur le réseau

Tableau B-47. Affichage de données Informations détaillées sur les violations de pare-feu

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.

DONNÉES	DESCRIPTION
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple) et qui est attaqué.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Type d'événement	Affiche le type d'événement activant la violation. Exemple : intrusion, violation de stratégie
Niveau de risque	Affiche l'évaluation par Trend Micro du risque pour votre réseau. Exemple : niveau élevé, niveau faible, niveau moyen
Trafic/connexion	Affiche la direction de l'entrée de la violation.
Protocole	Affiche le protocole utilisé par l'intrusion. Exemple : HTTP, SMTP, FTP
Adresse IP source	Affiche l'adresse IP de l'ordinateur effectuant une tentative d'intrusion sur votre réseau.
Port de point final	Affiche le numéro de port de l'ordinateur attaqué.
Adresse IP de point final	Affiche l'adresse IP de l'ordinateur attaqué.
Application cible	Affiche l'application ciblée par l'intrusion.

Données	Description
Description	Description détaillée par Trend Micro de l'incident.
Action	Affiche le type d'actions entreprises par les produits gérés contre les violations de stratégie. Exemple : fichier nettoyé, fichier mis en quarantaine, fichier ignoré
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Informations sur l'analyse des points finaux liés aux menaces de sécurité

Affiche des informations concernant principalement les points finaux touchés. Exemples : nom du point final, procédé général utilisé par la menace de sécurité pour pénétrer dans votre réseau, nombre de points finaux touchés

Tableau B-48. Affichage de données Informations sur l'analyse des points finaux liés aux menaces de sécurité

Données	Description
Point final	Affiche le nom de l'ordinateur touché par la menace de sécurité/violation.
Catégorie de menace de sécurité	Affiche la catégorie générale de la menace de sécurité détectée par les produits gérés. Exemple : antivirus, anti-programmes espions, anti-hameçonnage

Données	Description
Nom de la menace de sécurité	Affiche le nom de la menace de sécurité détectée par les produits gérés.
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10
Détecté	Affiche l'heure et la date de la dernière détection de menace de sécurité/violation sur l'ordinateur touché par celle-ci.

Informations détaillées sur la conformité à la sécurité des points finaux

Fournit des informations spécifiques sur les instances de conformité de la sécurité des points finaux sur votre réseau. Exemple : produit géré détectant la violation de la conformité de sécurité, nom de la stratégie spécifique conforme et nombre total d'instances conformes sur le réseau

Tableau B-49. Affichage des données Informations détaillées sur la conformité de la sécurité des points finaux

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.

DONNÉES	DESCRIPTION
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Point final	Affiche le nom d'hôte de l'ordinateur conforme à la stratégie/règle.
Adresse IP de point final	Affiche l'adresse IP de l'ordinateur conforme à la stratégie/règle.
Adresse MAC de point final	Affiche l'adresse MAC de l'ordinateur conforme à la stratégie/règle.
Stratégie/règle	Affiche le nom de la stratégie/règle respectée.
Service	Affiche le nom du service/programme conforme à la stratégie/règle.
Utilisateur	Affiche le nom de l'utilisateur connecté au point final lorsqu'un produit géré détecte une conformité de stratégie/règle.
Description	Description détaillée par Trend Micro de l'incident.
Détections	Affiche le nombre total d'instances de conformité de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de conformité du même type sur un ordinateur. Détections = 10

Activité détaillée de l'application

Affiche l'ensemble des informations relatives à l'activité de l'application sur votre réseau. Exemple : produit géré détectant l'instance de conformité de sécurité, nom de la stratégie spécifique conforme et nombre total d'instances de conformité sur le réseau

TABLEAU B-50. Affichage de données Activité détaillée de l'application

DONNÉES	DESCRIPTION
Reçu	Heure de réception par Control Manager des données provenant du produit géré.
Généré	Heure de création des données par le produit géré.
Entité du produit	Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Affiche l'ID de VLAN (VID) de la source dont provient la menace suspecte.
Détecté par	Affiche le filtre, le moteur de scan ou le produit géré détectant la menace suspecte.
Trafic/connexion	Affiche la direction du trafic réseau ou le point du réseau dont provient la menace suspecte.
Groupe de protocoles	Affiche le groupe général de protocoles à partir desquels un produit géré détecte la menace suspecte. Exemple : FTP, HTTP, P2P
Protocole	Affiche le protocole à partir duquel un produit géré détecte la menace suspecte. Exemple : ARP, Bearshare, BitTorrent
Description	Description détaillée par Trend Micro de l'incident.
Point final	Affiche le nom d'hôte de l'ordinateur conforme à la stratégie/règle.

Données	Description
Adresse IP source	Affiche l'adresse IP de la source dont provient la menace suspecte.
Adresse MAC source	Affiche l'adresse MAC de la source dont provient la menace suspecte.
Port source	Affiche le numéro de port de la source dont provient la menace suspecte.
Groupe d'adresses IP source	Affiche le groupe d'adresses IP de la source dont provient la violation.
Zone de réseau source	Affiche la zone de réseau de la source dont provient la violation.
Adresse IP de point final	Affiche l'adresse IP du point final touché par la menace suspecte.
Port de point final	Affiche le numéro de port du point final touché par la menace suspecte.
Adresse MAC de point final	Affiche l'adresse MAC du point final touché par la menace suspecte.
Groupe de points finaux	Affiche le groupe d'adresses IP du point final touché par la menace suspecte.
Zone de réseau de point final	Affiche la zone de réseau du point final touché par la menace suspecte.
Stratégie/règle	Affiche la stratégie/règle violée par la menace suspecte.
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Informations sur les violations de sécurité/de réputation Web

Affiche des données résumées et détaillées sur les violations de sécurité Internet détectées par les produits gérés sur votre réseau.

Résumé sur l'ensemble des violations de sécurité Web

Fournit un résumé des violations de sécurité Web de stratégies spécifiques. Exemple : nom de la stratégie violée, type de filtre/blocage empêchant l'accès à l'URL, nombre total de violations de sécurité Web sur le réseau

TABLEAU B-51. Affichage des données Résumé sur l'ensemble des violations de sécurité Web

DONNÉES	DESCRIPTION
Stratégie	Affiche le nom de la stratégie violée par l'URL.
Type de filtre/blocage	Affiche le type de filtre/blocage empêchant l'accès à l'URL en situation de violation. Exemple : blocage d'URL, filtrage d'URL, blocage Web
Points finaux uniques	Affiche le nombre de points finaux uniques violés de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 4 ordinateurs. Points finaux uniques = 4

Données	Description
URL uniques	Affiche le nombre d'URL uniques en situation de violation de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. URL uniques = 1
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 1 ordinateur. Détections = 10

Résumé sur les points finaux en situation de violation de sécurité Web

Fournit un résumé des détections de violation de sécurité Web provenant d'un point final spécifique. Exemple : adresse IP du point final violé, nombre de stratégies violées, nombre total de violations de sécurité Web sur le réseau

Tableau B-52. Affichage des données Résumé sur les points finaux en situation de violation de sécurité Web

Données	Description
Point final	Affiche l'adresse IP ou le nom d'hôte des points finaux qui violent les stratégies Web.
Stratégies uniques	Affiche le nombre de stratégies violées. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies uniques = 1

Données	Description
URL uniques	Affiche le nombre d'URL uniques en situation de violation de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. URL uniques = 1
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Résumé sur les URL de violation de sécurité Web

Fournit un résumé des détections de violation de sécurité Web provenant d'URL spécifiques. Exemple : nom de l'URL à l'origine de la violation de sécurité Web, type de filtre/blocage empêchant l'accès à l'URL, nombre total de violations de sécurité Web sur le réseau

Tableau B-53. Affichage des données Résumé sur les URL de violation de sécurité Web

Données	Description
URL	Affiche l'URL violant une stratégie de sécurité Web.
Type de filtre/blocage	Affiche le type de filtre/blocage empêchant l'accès à l'URL en situation de violation. Exemple : blocage d'URL, filtrage d'URL, blocage Web

DONNÉES	DESCRIPTION
Points finaux uniques	Affiche le nombre de points finaux uniques violés de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 4 ordinateurs. Points finaux uniques = 4
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Résumé sur le type de filtre/blocage de violation de sécurité Web

Fournit un résumé des actions entreprises par les produits gérés contre les violations de sécurité Web. Exemple : type de filtre/blocage empêchant l'accès à l'URL, nombre total de violations de sécurité Web sur le réseau

TABLEAU B-54. Affichage des données Résumé sur le type de filtre/blocage de violation de sécurité Web

DONNÉES	DESCRIPTION
Catégorie de blocage	Affiche le type général de filtre/blocage empêchant l'accès à l'URL en situation de violation. Exemple : blocage d'URL, filtrage d'URL, anti-spywares

Données	Description
Type de filtre/blocage	Affiche le type spécifique de filtre/blocage empêchant l'accès à l'URL en situation de violation. Exemple : blocage d'URL, filtrage d'URL, virus/programmes malveillants
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Résumé chronologique des détections de violations de sécurité Web

Fournit un résumé des détections de violations de sécurité Web sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, nombre de points finaux en situation de violation, nombre total de violations de sécurité Web sur le réseau

Tableau B-55. Affichage des données Résumé chronologique des détections de violations de sécurité Web

Données	Description
Date/Heure	Affiche l'heure à laquelle le résumé des données a lieu.
Stratégies uniques	Affiche le nombre de stratégies violées. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies uniques = 1

DONNÉES	DESCRIPTION
Points finaux uniques	Affiche le nombre de points finaux uniques violés de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 4 ordinateurs. URL uniques = 1
URL uniques	Affiche le nombre d'URL uniques en situation de violation de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. URL uniques = 1
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Résumé des détections de violations de sécurité Web

Fournit un résumé des détections de violations de sécurité Web sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, nombre de points finaux en situation de violation, nombre total de violations de sécurité Web sur le réseau

TABLEAU B-56. Affichage des données Résumé des détections de violations de sécurité Web

DONNÉES	DESCRIPTION
Stratégies uniques	Affiche le nombre de stratégies violées. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies uniques = 1
Points finaux uniques	Affiche le nombre de points finaux uniques violés de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur 4 ordinateurs. Points finaux uniques = 4
URL uniques	Affiche le nombre d'URL uniques en situation de violation de la stratégie spécifiée. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. URL uniques = 1
Utilisateurs/adresses IP uniques	Affiche le nombre d'utilisateurs uniques ou d'adresses IP de points finaux violés de la stratégie spécifiée. Exemple : Un produit géré détecte 10 instances de violation de la même URL provenant d'un utilisateur. Utilisateurs/adresses IP uniques = 1

Données	Description
Groupes d'utiisateurs uniques	Affiche le nombre de groupes d'utilisateurs uniques pour les utilisateurs en situation de violation de la stratégie spécifiée. Exemple : Un produit géré détecte 10 instances de violation de la même URL provenant d'un groupe d'utilisateur. Groupes d'utiisateurs uniques = 1
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Informations détaillées sur les violations de sécurité Web

Fournit des informations spécifiques sur les violations de sécurité Web sur votre réseau. Exemple : produit géré détectant la violation de sécurité Web, nom de la stratégie spécifique violée et nombre total de violations de sécurité Web sur le réseau

Tableau B-57. Affichage des données Informations détaillées sur les violations de sécurité Web

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.

Données	Description
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Trafic/connexion	Affiche la direction de l'entrée de la violation.
Protocole	Affiche le protocole à travers lequel la violation a lieu. Exemple : HTTP, FTP, SMTP
URL	Affiche le nom de l'URL violant une stratégie de sécurité Web.
Utilisateur/adresse IP	Affiche l'utilisateur ou l'adresse IP du point final violant une stratégie.
Groupe d'utilisateurs	Affiche le groupe d'utilisateurs de l'utilisateur violant une stratégie.
Point final	Affiche l'adresse IP ou le nom d'hôte du point final violant une stratégie.
Hôte du produit	Affiche l'adresse IP ou le nom d'hôte du produit géré détectant la violation.
Type de filtre/blocage	Affiche le type de filtre/blocage empêchant l'accès à l'URL en situation de violation. Exemple : blocage d'URL, filtrage d'URL, blocage Web
Règle de blocage	Affiche la règle de blocage empêchant l'accès à l'URL violée. Exemple : Blocage d'URL
Stratégie	Affiche le nom de la stratégie violée par l'URL.
Fichier	Affiche le nom du fichier violant la stratégie.

Données	Description
Évaluation de réputation de sites Web	Affiche la sécurité relative d'un site Web, en pourcentage, selon l'évaluation de Trend Micro.
Action	Affiche le type d'actions entreprises par les produits gérés contre les violations de stratégie. Exemple : ignorer, bloquer
Détections	Affiche le nombre total de violations de sécurité Web détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation de la même URL sur un ordinateur. Détections = 10

Informations détaillées sur la réputation de sites Web

Affiche l'ensemble des informations relatives à l'activité de l'application sur votre réseau. Exemple : produit géré détectant la violation de la conformité de sécurité, nom de la stratégie spécifique conforme et nombre total d'instances conformes sur le réseau

Tableau B-58. Affichage des données Informations détaillées sur la réputation de sites Web

Données	Description
Reçu	Heure de réception par Control Manager des données provenant du produit géré.
Généré	Heure de création des données par le produit géré.
Entité du produit	Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.

Données	Description
Produit	Nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
VLAN ID	Affiche l'ID de VLAN (VID) de la source dont provient la menace suspecte.
Détecté par	Affiche le filtre, le moteur de scan ou le produit géré détectant la menace suspecte.
Trafic/connexion	Affiche la direction du trafic réseau ou le point du réseau dont provient la menace suspecte.
Groupe de protocoles	Affiche le groupe général de protocoles à partir desquels un produit géré détecte la menace suspecte. Exemple : FTP, HTTP, P2P
Protocole	Affiche le protocole à partir duquel un produit géré détecte la menace suspecte. Exemple : ARP, Bearshare, BitTorrent
Description	Description détaillée par Trend Micro de l'incident.
Point final	Affiche le nom d'hôte de l'ordinateur conforme à la stratégie/règle.
Adresse IP source	Affiche l'adresse IP de la source dont provient la menace suspecte.
Adresse MAC source	Affiche l'adresse MAC de la source dont provient la menace suspecte.
Port source	Affiche le numéro de port de la source dont provient la menace suspecte.
Groupe d'adresses IP source	Affiche le groupe d'adresses IP de la source dont provient la menace suspecte.

DONNÉES	DESCRIPTION
Zone de réseau source	Affiche la zone de réseau de la source dont provient la menace suspecte.
Adresse IP de point final	Affiche l'adresse IP du point final touché par la menace suspecte.
Port de point final	Affiche le numéro de port du point final touché par la menace suspecte.
Adresse MAC de point final	Affiche l'adresse MAC du point final touché par la menace suspecte.
Groupe de points finaux	Affiche le groupe d'adresses IP du point final touché par la menace suspecte.
Zone de réseau de point final	Affiche la zone de réseau du point final touché par la menace suspecte.
Stratégie/règle	Affiche la stratégie/règle violée par la menace suspecte.
URL	Affiche l'URL considéré comme étant une menace suspecte.
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Informations sur les menaces suspectes

Affiche des données résumées et détaillées sur les activités suspectes détectées par les produits gérés sur votre réseau.

Résumé sur l'ensemble des menaces suspectes

Fournit des informations spécifiques relatives aux menaces suspectes sur votre réseau. Exemple : stratégie/règle violée, informations résumées sur la source et la destination, nombre total de menaces suspectes sur le réseau

TABLEAU B-59. Affichage de données Résumé sur l'ensemble des menaces suspectes

DONNÉES	DESCRIPTION
Stratégie/règle	Affiche le nom de la stratégie/règle violée.
Protocole	Affiche le protocole à travers lequel la violation a lieu. Exemple : HTTP, FTP, SMTP
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre de sources uniques dont proviennent les menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type provenant de 3 ordinateurs. Sources uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messagerie électronique uniques réceptrices de contenu violant des stratégies de produit géré relatives aux menaces suspectes. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2

DONNÉES	DESCRIPTION
Expéditeurs uniques	Affiche le nombre d'expéditeurs de messages électroniques uniques envoyant du contenu violant des stratégies de menaces suspectes de produits gérés. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie provenant de 3 ordinateurs. Expéditeurs uniques = 3
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Décompte de détections égal à 10.
Mitigations	Affiche le nombre de points finaux contre lesquels les dispositifs Network VirusWall Enforcer ou Total Discovery Mitigation Server entreprennent une action.
Points finaux nettoyés	Affiche le nombre total de points finaux nettoyés par Total Discovery Mitigation Server.
Taux de points finaux nettoyés (%)	Affiche le taux de points finaux nettoyés par Total Discovery Mitigation Server par rapport au nombre total de détections.

Résumé sur les sources suspectes

Fournit un résumé des détections de menaces suspectes provenant d'une source spécifique. Exemple : nom de la source, informations résumées concernant du destinataire et les règles/violations, nombre total de menaces suspectes sur le réseau

TABLEAU B-60. Affichage des données Résumé sur les sources suspectes

DONNÉES	DESCRIPTION
Adresse IP source	Affiche les adresses IP des sources dont proviennent les menaces suspectes.
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type sur 2 ordinateurs. Points finaux uniques = 2
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Résumé sur les points finaux suspects les plus dangereux

Fournit un résumé des points finaux présentant les détections de menaces les plus suspectes. Exemple : nom de la destination, informations résumées concernant la source et les règles/violations, nombre total de menaces suspectes sur le réseau

TABLEAU B-61. Affichage de données Résumé sur les points finaux suspects les plus dangereux

DONNÉES	DESCRIPTION
Adresse IP de point final	Affiche les adresses IP d'ordinateurs touchés par des menaces suspectes.
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Sources uniques	Affiche le nombre de sources uniques dont proviennent les menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type provenant de 3 ordinateurs. Sources uniques = 3
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Résumé sur les destinataires suspects les plus dangereux

Fournit un résumé des destinataires présentant les détections de menaces les plus suspectes. Exemple : nom du destinataire, informations résumées concernant les expéditeurs et les règles/violations, nombre total de menaces suspectes sur le réseau

TABLEAU B-62. Affichage des données Résumé sur les destinataires suspects les plus dangereux

DONNÉES	DESCRIPTION
Destinataire	Affiche l'adresse électronique du destinataire touché par la menace suspecte.
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Expéditeurs uniques	Affiche le nombre d'expéditeurs de messages électroniques uniques envoyant du contenu violant des stratégies de menaces suspectes de produits gérés. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie provenant de 3 ordinateurs. Expéditeurs uniques = 3
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Résumé sur les expéditeurs suspects

Fournit un résumé des détections de menaces suspectes provenant d'un expéditeur spécifique. Exemple : nom de l'expéditeur, informations résumées concernant le destinataire et les règles/violations, nombre total de menaces suspectes sur le réseau

TABLEAU B-63. Affichage de données Résumé sur les expéditeurs suspects

DONNÉES	DESCRIPTION
Expéditeur	Affiche l'adresse électronique de la source de violations de stratégie/règle.
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Destinataires uniques	Affiche le nombre d'adresses de messagerie électronique uniques réceptrices de contenu violant des stratégies de produit géré relatives aux menaces suspectes. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Résumé sur la détection des protocoles de menaces suspectes

Fournit un résumé des détections de menaces suspectes à travers un protocole spécifique. Exemple : nom du protocole, informations résumées concernant la source et la destination, nombre total de menaces suspectes sur le réseau

TABLEAU B-64. Affichage des données Résumé sur la détection des protocoles de menaces suspectes

DONNÉES	DESCRIPTION
Protocole	Affiche le nom du protocole à travers lequel la menace suspecte a lieu. Exemple : HTTP, FTP, SMTP
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre de sources uniques dont proviennent les menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type provenant de 3 ordinateurs. Sources uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messagerie électronique uniques réceptrices de contenu violant des stratégies de produit géré relatives aux menaces suspectes. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2

Données	Description
Expéditeurs uniques	Affiche le nombre d'expéditeurs de messages électroniques uniques envoyant du contenu violant des stratégies de menaces suspectes de produits gérés. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie provenant de 3 ordinateurs. Expéditeurs uniques = 3
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Résumé chronologique des détections de menaces suspectes

Fournit un résumé des détections de menaces suspectes sur une certaine période (quotidienne, hebdomadaire ou mensuelle). Exemple : heure et date de la collecte des données de résumé, informations résumées sur la source et la destination, nombre total de menaces suspectes sur le réseau

Tableau B-65. Affichage des données Résumé chronologique des détections de menaces suspectes

Données	Description
Date/Heure	Affiche l'heure à laquelle le résumé des données a lieu.

Données	Description
Stratégies/règles uniques	Affiche le nombre de stratégies/règles uniques violées par l'ordinateur source. Exemple : un produit géré détecte 10 instances de violation de la même stratégie sur 2 ordinateurs. Stratégies/règles uniques = 1
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par des menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre de sources uniques dont proviennent les menaces suspectes. Exemple : un produit géré détecte 10 instances de menace suspecte du même type provenant de 3 ordinateurs. Sources uniques = 3
Destinataires uniques	Affiche le nombre d'adresses de messagerie électronique uniques réceptrices de contenu violant des stratégies de produit géré relatives aux menaces suspectes. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie sur 2 ordinateurs. Destinataires uniques = 2

Données	Description
Expéditeurs uniques	Affiche le nombre d'expéditeurs de messages électroniques uniques envoyant du contenu violant des stratégies de menaces suspectes de produits gérés. Exemple : un produit géré détecte 10 instances de violation de menace suspecte de la même stratégie provenant de 3 ordinateurs. Expéditeurs uniques = 3
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Informations détaillées sur les menaces suspectes

Fournit des informations spécifiques relatives aux menaces suspectes sur votre réseau. Exemple : produit géré détectant la menace suspecte, informations spécifiques sur la source et la destination, nombre total de menaces suspectes sur le réseau

Tableau B-66. Affichage des données Informations détaillées sur les menaces suspectes

Données	Description
Reçu	Affiche l'heure de réception par Control Manager des données provenant du produit géré.
Généré	Affiche l'heure de création par le produit géré des données.

Données	Description
Entité du produit	Affiche le nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Hôte de migration	Affiche le nom d'hôte du serveur de mitigation.
Trafic/connexion	Affiche la direction du trafic réseau ou le point du réseau dont provient la menace suspecte.
Groupe de protocoles	Affiche le groupe général de protocoles à partir desquels un produit géré détecte la menace suspecte. Exemple : FTP, HTTP, P2P
Protocole	Affiche le protocole à partir duquel un produit géré détecte la menace suspecte. Exemple : ARP, Bearshare, BitTorrent
Adresse IP de point final	Affiche l'adresse IP du point final touché par la menace suspecte.
Port de point final	Affiche le numéro de port du point final touché par la menace suspecte.
Adresse MAC de point final	Affiche l'adresse MAC du point final touché par la menace suspecte.
Adresse IP source	Affiche l'adresse IP de la source dont provient la menace suspecte.
Hôte source	Affiche le nom d'hôte de la source dont provient la menace suspecte.
Port source	Affiche le numéro de port de la source dont provient la menace suspecte.

DONNÉES	DESCRIPTION
Adresse MAC source	Affiche l'adresse MAC de la source dont provient la menace suspecte.
Domaine source	Affiche le domaine de la source dont provient la menace suspecte.
VLAN ID	Affiche l'ID de VLAN de la source dont provient la menace suspecte.
Type de menace de sécurité	Affiche le type spécifique de menace de sécurité détecté par les produits gérés. Exemple : virus, programmes espions/ grayware, fraude
Niveau de confiance des menaces	Affiche la probabilité estimée par Trend Micro que la menace suspecte représente un danger pour votre réseau.
Détecté par	Affiche le filtre, le moteur de scan ou le produit géré détectant la menace suspecte.
Stratégie/règle	Affiche la stratégie/règle violée par la menace suspecte.
Destinataire	Affiche le destinataire de la menace suspecte.
Expéditeur	Affiche l'expéditeur de la menace suspecte.
Objet	Affiche le contenu de la ligne d'objet du message électronique contenant les programmes espions/graywares.
URL	Affiche l'URL considéré comme étant une menace suspecte.
Utilisateur	Affiche le nom de l'utilisateur connecté à l'ordinateur cible lorsqu'un produit géré détecte une menace suspecte.

Données	Description
Utilisateur de messagerie instantanée/IRC	Affiche le nom de l'utilisateur de messagerie instantanée ou d'IRC connecté lorsque Total Discovery Appliance détecte une violation.
Navigateur/client FTP	Affiche le navigateur Internet ou point final FTP dont provient la menace suspecte.
Nom de canal	Affiche le protocole utilisé par le logiciel de messagerie instantanée ou d'IRC pour la communication.
Fichier	Affiche le nom du fichier suspect.
Fichier dans un fichier compressé	Indique si la menace suspecte provient ou non d'un fichier compressé.
Taille du fichier	Affiche la taille du fichier suspect.
Extension de fichier	Affiche l'extension du fichier suspect. Exemple : .wmf, .exe, .zip
Véritable type de fichier	Affiche le « véritable » type de fichier détecté à l'aide de l'en-tête du fichier et non de l'extension de celui-ci.
Répertoire partagé	Indique si la menace suspecte provient ou non d'un dossier partagé.
Authentification	Indique l'utilisation ou non d'une authentification.
Commande BOT	Affiche la commande envoyée par les robogiciels au canal de commande ou par le canal de commande aux robogiciels.
URL de robogiciel	Affiche l'URL duquel les robogiciels reçoivent leurs commandes.
Type de contrainte	Affiche la raison pour laquelle un fichier ne peut pas être scanné correctement.

Données	Description
Résultat de mitigation	Affiche le résultat de l'action entreprise par le serveur de mitigation contre les menaces suspectes.
Action de mitigation	Affiche l'action entreprise par le serveur de mitigation contre les menaces suspectes. Exemple : fichier nettoyé, fichier effacé, fichier supprimé
Groupe d'adresses IP source	Affiche le groupe d'adresses IP de la source dont provient la menace suspecte.
Zone de réseau source	Affiche la zone de réseau de la source dont provient la menace suspecte.
Groupe de points finaux	Affiche le groupe d'adresses IP du point final touché par la menace suspecte.
Zone de réseau de point final	Affiche la zone de réseau du point final touché par la menace suspecte.
Détections	Affiche le nombre total de violations de stratégie/règle détectées par les produits gérés. Exemple : un produit géré détecte 10 instances de violation du même type sur un ordinateur. Détections = 10

Informations sur l'ensemble des menaces

Affiche des données résumées et statistiques concernant le paysage global des menaces sur votre réseau.

Informations sur l'analyse des menaces de sécurité

Affiche des informations sur l'ensemble des menaces de sécurité touchant vos postes de travail. Exemples : nom de la menace de sécurité, nombre total de détections de menaces de sécurité, nombre de points finaux touchés

TABLEAU B-67. Affichage de données Informations sur l'analyse des menaces de sécurité réseau

DONNÉES	DESCRIPTION
Catégorie de menace de sécurité	Affiche la catégorie générale de la menace de sécurité détectée par les produits gérés. Exemple : antivirus, anti-programmes espions, anti-hameçonnage
Menace de sécurité	Affiche le nom de la menace de sécurité détectée par les produits gérés.
Type d'entité	Affiche le point d'entrée de la menace de sécurité détectée par les produits gérés. Exemple : virus détecté dans un fichier, HTTP, Windows Live Messenger (MSN)
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par la menace de sécurité/ violation. Exemple : OfficeScan détecte 10 instances du même virus sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre d'ordinateurs uniques dont proviennent les menaces de sécurité/ violations. Exemple : OfficeScan détecte 10 instances du même virus, provenant de 3 sources, sur 2 ordinateurs. Sources uniques = 3

Données	Description
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur les limites de protection du réseau

Affiche des informations générales permettant une vue d'ensemble des menaces de sécurité touchant votre réseau complet. Exemples : type de protection de réseau du produit géré (passerelle, messagerie), type de menace de sécurité, nombre de points finaux touchés

Tableau B-68. Affichage des données Informations sur les limites de protection du réseau

Données	Description
Catégorie du produit	Affiche la catégorie à laquelle appartient le produit géré. Exemple : produits de poste de travail, produits de serveur de messagerie, produits de réseau
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Catégorie de menace de sécurité	Affiche la catégorie générale de la menace de sécurité détectée par les produits gérés. Exemple : antivirus, anti-programmes espions, anti-hameçonnage

Données	Description
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par la menace de sécurité/violation. Exemple : OfficeScan détecte 10 instances du même virus sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre d'ordinateurs uniques dont proviennent les menaces de sécurité/violations. Exemple : OfficeScan détecte 10 instances du même virus, provenant de 3 sources, sur 2 ordinateurs. Sources uniques = 3
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur l'analyse de l'entrée des menaces de sécurité

Affiche des informations concernant principalement le point d'entrée des menaces de sécurité. Exemples : type de protection de réseau du produit géré (passerelle, messagerie, poste de travail), nom de la menace de sécurité, heure de la dernière détection de menaces de sécurité

TABLEAU B-69. Affichage des données Informations sur l'analyse de l'entrée des menaces de sécurité

DONNÉES	DESCRIPTION
Type d'entité	Affiche le point d'entrée des menaces de sécurité détectées par les produits gérés. Exemple : Virus détecté dans un fichier, FTP, transfert de fichier
Produit	Affiche le nom du produit géré détectant la menace de sécurité. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Catégorie de menace de sécurité	Affiche la catégorie spécifique des menaces de sécurité détectées par les produits gérés. Exemple : antivirus, anti-programmes espions, filtrage de contenu
Points finaux uniques	Affiche le nombre d'ordinateurs uniques touchés par la menace de sécurité/ violation. Exemple : OfficeScan détecte 10 instances du même virus sur 2 ordinateurs. Points finaux uniques = 2
Sources uniques	Affiche le nombre d'ordinateurs uniques dont proviennent les menaces de sécurité/ violations. Exemple : OfficeScan détecte 10 instances du même virus, provenant de 3 sources, sur 2 ordinateurs. Sources uniques = 3

Données	Description
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Informations sur l'analyse de la source des menaces de sécurité

Affiche des informations concernant principalement la source de la menace de sécurité. Exemple : nom de la source de la menace de sécurité, procédé général utilisé par la menace de sécurité pour pénétrer dans votre réseau, nombre de points finaux touchés

Tableau B-70. Affichage des données Informations sur l'analyse de la source des menaces de sécurité

Données	Description
Hôte source	Affiche le nom de l'ordinateur à l'origine de la menace de sécurité/violation.
Catégorie de menace de sécurité	Affiche la catégorie générale de la menace de sécurité détectée par les produits gérés. Exemple : antivirus, anti-programmes espions, anti-hameçonnage
Menace de sécurité	Affiche le nom de la menace de sécurité détectée par les produits gérés.
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10

Données	Description
Détecté	Affiche l'heure et la date de la dernière détection de menace de sécurité/violation sur l'ordinateur touché par celle-ci.

Informations sur l'analyse des points finaux liés aux menaces de sécurité

Affiche des informations concernant principalement les points finaux touchés. Exemples : nom du point final, procédé général utilisé par la menace de sécurité pour pénétrer dans votre réseau, nombre de points finaux touchés

Tableau B-71. Affichage de données Informations sur l'analyse des points finaux liés aux menaces de sécurité

Données	Description
Point final	Affiche le nom de l'ordinateur touché par la menace de sécurité/violation.
Catégorie de menace de sécurité	Affiche la catégorie générale de la menace de sécurité détectée par les produits gérés. Exemple : antivirus, anti-programmes espions, anti-hameçonnage
Nom de la menace de sécurité	Affiche le nom de la menace de sécurité détectée par les produits gérés.
Détections	Affiche le nombre total de menaces de sécurité/violations détectées par les produits gérés. Exemple : OfficeScan détecte 10 instances du même virus sur un ordinateur. Détections = 10
Détecté	Affiche l'heure et la date de la dernière détection de menace de sécurité/violation sur l'ordinateur touché par celle-ci.

Informations de rappel C&C

Affiche des informations sur les détails de rappel C&C. Exemples : Nom de l'hôte affecté ou adresse électronique, saisissez la source de listes C&C.

TABLEAU B-72. Affichage des données des informations de rappel C&C

DONNÉES	DESCRIPTION
Reçu	Date et heure de réception par Control Manager des données provenant du produit géré.
Généré	Date et heure de génération des données par le produit géré
Hôte compromis	Adresse électronique ou hôte affectés
Adresse de rappel	L'URL, l'adresse IP ou électronique à laquelle l'hôte compromis tente un rappel
Source des listes C&C	Nom de la liste contenant l'adresse de rappel • Informations globales • Analyseur virtuel • Défini par l'utilisateur
Groupes d'attaquants	Noms des groupes d'attaquants surveillés par Trend Micro
Niveau de risque C&C	Niveau de gravité du rappel
Emplacement du serveur C&C	Région et pays de l'emplacement du serveur C&C
Premier contrôle	Date et l'heure du premier enregistrement de l'adresse de rappel par le produit géré
Dernière activité	Date et l'heure du dernier enregistrement de l'adresse de rappel par le produit géré

Données	Description
Familles de programmes malveillants	Les catégories de programmes malveillants associées à l'adresse de rappel
Entité du produit	Nom d'affichage pour un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage du produit géré.
Produit	Nom du produit géré Exemples : OfficeScan, ScanMail for Microsoft Exchange

Affichages des données : Informations sur la protection des données

Affiche les informations sur la Prévention contre la perte de données (DLP), y compris les incidents DLP et les correspondances de modèles DLP.

Informations sur la prévention contre la perte de données

Affiche les informations sur les incidents DLP, les correspondances de modèles et les sources d'incident collectés à partir des produits gérés.

Informations sur les incidents de prévention contre la perte de données

Tableau B-73. Informations sur les incidents de prévention contre la perte de données

Données	Description
Reçu	Affiche l'heure à laquelle Control Manager a reçu le journal.

Données	Description
Généré	Affiche l'heure à laquelle les données de journaux ont été générées dans le produit géré.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit/adresse MAC de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse MAC du serveur sur lequel le produit géré est installé. • Adresse MAC d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

Données	Description
Serveur de gestion	Affiche le nom d'affichage d'entité d'un produit géré sur lequel un point final est enregistré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Point final	Affiche l'adresse IP ou le nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Sources d'incidents (Utilisateur)	Affiche le nom de l'utilisateur connecté.
Sources d'incidents (Expéditeur)	Affiche l'adresse électronique source.
Destinataire	Affiche l'adresse électronique du destinataire.
Objet	Affiche le sujet du message électronique.
Emplacement du fichier	Affiche l'emplacement et le nom du fichier.
Fichier	Affiche le nom du fichier qui a déclenché l'incident.
Stratégie	Affiche le nom de la stratégie déclenchée par l'incident.
Modèle	Affiche le nom du modèle dans laquelle la correspondance de modèles a été déclenchée.
Canal	Affiche l'entité par l'intermédiaire de laquelle un actif numérique a été transmis.
Groupe de canaux	Affiche le type de canal.
Action	Affiche l'action prise sur l'incident.
Incidents	Affiche le nombre d'incidents.

Informations sur les correspondances de modèles de prévention contre la perte de données

TABLEAU B-74. Informations sur les correspondances de modèles de prévention contre la perte de données

DONNÉES	DESCRIPTION
ID	Entrez l'ID unique pour le journal.
Reçu	Affiche l'heure à laquelle le produit géré a reçu des informations sur l'incident.
Généré	Affiche l'heure à laquelle l'incident a été déclenché.
Entité de produit/point final	Cette colonne de données affiche l'un des éléments suivants : • Nom d'affichage d'entité d'un produit géré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré. • Adresse IP ou nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Produit	Affiche le nom du produit géré. Exemple : OfficeScan, ScanMail for Microsoft Exchange
Produit/adresse IP de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse IP du serveur sur lequel le produit géré est installé. • Adresse IP d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).

Données	Description
Produit/adresse MAC de point final	Cette colonne de données affiche l'un des éléments suivants : • Adresse MAC du serveur sur lequel le produit géré est installé. • Adresse MAC d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Serveur de gestion	Affiche le nom d'affichage d'entité d'un produit géré sur lequel un point final est enregistré. Control Manager identifie les produits gérés à l'aide du nom d'affichage d'entité du produit géré.
Point final	Affiche l'adresse IP ou le nom d'hôte d'un ordinateur sur lequel un client est installé (le client OfficeScan, par exemple).
Sources d'incidents (Utilisateur)	Affiche le nom de l'utilisateur connecté.
Destinataire	Affiche l'adresse électronique du destinataire.
Objet	Affiche le sujet du message électronique.
Emplacement du fichier	Affiche l'emplacement et le nom du fichier.
Fichier	Affiche le nom du fichier qui a déclenché l'incident.
Stratégie	Affiche le nom de la stratégie déclenchée par l'incident.
Modèle	Affiche le nom du modèle dans laquelle la correspondance de modèles a été déclenchée.
Canal	Affiche l'entité par l'intermédiaire de laquelle un actif numérique a été transmis.
Groupe de canaux	Affiche le type de canal.

Annexe C

Prise en charge d'IPv6 dans Control Manager

Cette section doit être lue par les utilisateurs qui prévoient de déployer Control Manager dans un environnement prenant en charge l'adressage IPv6. Cette annexe contient des informations sur le degré de prise en charge d'IPv6 dans Control Manager.

Trend Micro suppose que le lecteur est familiarisé avec les concepts d'IPv6 et les tâches qu'implique la configuration d'un réseau prenant en charge l'adressage IPv6.

Cette version 6.0 est la première à prendre en charge l'adressage IPv6 dans Control Manager. Les versions précédentes de Control Manager ne prennent pas en charge l'adressage IPv6. La prise en charge de l'adressage IPv6 est automatiquement activée après l'installation ou la mise à niveau du serveur Control Manager remplissant les exigences de l'adressage IPv6.

Configuration requise du serveur Control Manager

Les exigences IPv6 pour le serveur Control Manager sont les suivantes :

- Le serveur doit être installé sur Windows Server 2008. Il ne peut être installé sur Windows Server 2003, car ce système d'exploitation ne prend que partiellement en charge l'adressage IPv6.
- Installez les piles IPv4 et IPv6 et activez la pile IPv6.

Limitations des serveurs IPv6

Le tableau suivant répertorie les limitations de prise en charge d'IPv6 :

TABLEAU C-1. Limitations de prise en charge du protocole IPv6

ÉLÉMENT	RESTRICTION
Doubles piles IP	Control Manager ne prend en charge que les piles IP doubles. La prise en charge d'IPv6 peut ne pas fonctionner correctement si la pile IPv4 est supprimée.
Interface de bouclage IPv4	L'interface de bouclage IPv4 est requise. Pour vérifier que le logiciel TCP/IP fonctionne correctement, faites un ping de l'adresse `127.0.0.1`.
Windows Server 2008	Windows Server 2008 est requis pour la prise en charge du protocole IPv6.
Agent MCP	La prise en charge IPv6 ne fonctionne qu'avec les agents MCP. Elle ne fonctionne pas avec les agents Control Manager 2.x.
Format d'adresse IPv6	Le caractère **%** n'est pas pris en charge pour les adresses IPv6.
Rapports Control Manager	Les adresses IPv6 peuvent ne pas s'afficher correctement dans les rapports prédéfinis.

Configuration des adresses IPv6

La console Web vous permet de configurer une adresse IPv6. Voici quelques instructions de configuration.

- Control Manager accepte les présentations d'adresse IPv6 standard.

  Par exemple :

  `2001:0db7:85a3:0000:0000:8a2e:0370:7334`

  `2001:db7:85a3:0:0:8a2e:370:7334`

  `2001:db7:85a3::8a2e:370:7334`

  `::ffff:192.0.2.128`

- Control Manager accepte également les adresses IPv6 de type lien-local, telles que :

  fe80::210:5aff:feaa:20a2

  AVERTISSEMENT!

  Faites attention lors de la spécification d'une adresse IPv6 de type lien-local, car, même si Control Manager accepte cette adresse, il se peut qu'il ne fonctionne pas comme attendu dans certaines circonstances. Par exemple, Control Manager ne peut pas effectuer de mise à jour à partir d'une source de mise à jour si celle-ci se trouve sur un segment différent du réseau et est identifiée par son adresse IPv6 de type lien-local.

- Lorsque l'adresse IPv6 fait partie d'une URL, placez-la entre crochets ([]).

Écrans affichant les adresses IP

Les adresses IP sont affichées sur les écrans suivants :

- **Répertoire Produits**
- **Résultats de requête ad hoc**

- **Serveurs gérés**

Annexe D

Vérification de l'état de la stratégie

L'état des stratégies permet aux administrateurs de vérifier si Control Manager a déployer une stratégie avec succès dans ses cibles.

Pour vérifier l'état de déploiement de la stratégie, utilisez une des méthodes suivantes :

- Dans l'écran **Gestion des stratégies**, cliquez sur un nombre dans la liste des stratégies. L'écran **Résultats de requête ad hoc** apparaît.
- Dans le tableau de bord, cliquez sur un nombre dans le widget de l'état de la stratégie. L'écran **Résultats de requête ad hoc** apparaît.
- Exécutez une requête ad hoc

État de la stratégie

Le tableau suivant fournit des descriptions et des suggestions sur chaque état de stratégie :

TABLEAU D-1. État de la stratégie

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
En attente	La stratégie est en cours de traitement par Control Manager.	Attendez quelques minutes, puis vérifiez à nouveau l'état.
Sans stratégie	Control Manager n'a pas affecté de stratégie à ce point final ou à ce produit géré.	Affectez une stratégie au point final ou au produit géré.
Déployé	Control Manager a déployé la stratégie avec succès.	N/A
Le point final n'arrive pas à se connecter au serveur	• Le point final n'a pas reçu les paramètres de la stratégie. • Le serveur est actuellement occupé.	• Vérifiez l'état de la connexion du point final • Connectez le point final au réseau de l'entreprise • Attendez que l'état de la stratégie se mette à jour

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
Paramètres produit inapplicables	Le produit géré ne peut pas traiter certains des paramètres de la stratégie.	• Vérifiez les paramètres de la stratégie • Mettez à jour dans la dernière version du modèle de stratégie • Vérifiez les paramètres du produit géré • Vérifiez l'adresse IP du produit géré sur l'écran **Serveurs gérés** Si l'adresse IP est incorrecte, annulez l'enregistrement puis enregistrez à nouveau le produit géré dans Control Manager. • Consultez le manuel de l'administrateur du produit géré
Point final non pris en charge	Le point final ne prend pas en charge certaines fonctionnalités spécifiées dans les paramètres de la stratégie.	Mettez à niveau le client dans une version prise en charge.
Paramètres modifiés localement	Certains paramètres du point final ou du produit géré ne correspondent pas aux paramètres spécifiés dans la stratégie, car l'administrateur du produit géré a fait des modifications via la console du produit géré.	Vérifiez les paramètres dans la console du produit géré.

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
Services des produits inactivés	Le produit géré n'a pas activé certains des services spécifiés dans les paramètres de la stratégie.	Activez les services en question dans le produit géré.
Services des produits désactivés	Le produit géré a désactivé certains des services spécifiés dans les paramètres de la stratégie.	Activez les services en question dans le produit géré.
Partiellement déployé	Control Manager a appliqué une partie des paramètres de la stratégie.	Attendez quelques minutes, puis vérifiez à nouveau l'état.
Géré par [nom du serveur Control Manager]	Un autre Control Manager gère actuellement le produit géré.	Supprimez le produit géré de la liste du serveur géré et ajoutez à nouveau le produit géré à la liste.
Nom d'utilisateur ou mot de passe non valide.	Le nom d'utilisateur ou le mot de passe d'authentification est incorrect.	Vérifiez le nom d'utilisateur et le mot de passe.
Serveur de produit ou informations d'authentification non valide	Le nom du serveur ou les informations d'authentification sont incorrectes.	Vérifiez le nom du serveur et les informations d'authentification.
Connexion automatique au produit impossible	Control Manager ne peut pas utiliser la fonction d'authentification unique pour accéder au produit géré.	• Cliquez sur la fonction d'authentification unique dans le répertoire Produits • Vérifiez l'état de la connexion de l'agent MCP • Passez le type de connexion au serveur de **Automatique** à **Manuel** dans la liste **Serveurs gérés**.

ÉTAT DE LA STRATÉGIE	DESCRIPTION	SUGGESTIONS
Erreur de configuration du serveur Web	Une erreur de service Web est survenue.	Vérifiez la configuration IIS.
Erreur de communication du produit	Impossible d'accéder à la console du produit.	• Vérifiez si vous pouvez accéder à la console Web du produit géré. • Vérifiez les paramètres du produit géré.
Connexion au produit impossible	Control Manager n'arrive pas à établir une connexion avec le produit géré.	• Vérifiez l'état de la connexion du produit géré. • Vérifiez la connexion réseau
Version du produit non prise en charge	La version du produit géré n'est pas prise en charge.	Mettez à niveau le produit géré dans une version prise en charge.
Erreur de configuration du réseau	Une erreur de connexion réseau est survenue.	Vérifiez la connexion réseau.
Erreur système. ID erreur : [numéro ID de l'erreur].	Une erreur système est survenue.	Contactez votre représentant d'assistance Trend Micro.

Index

F

G

I

P

R

S

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: CMEM65910/130321