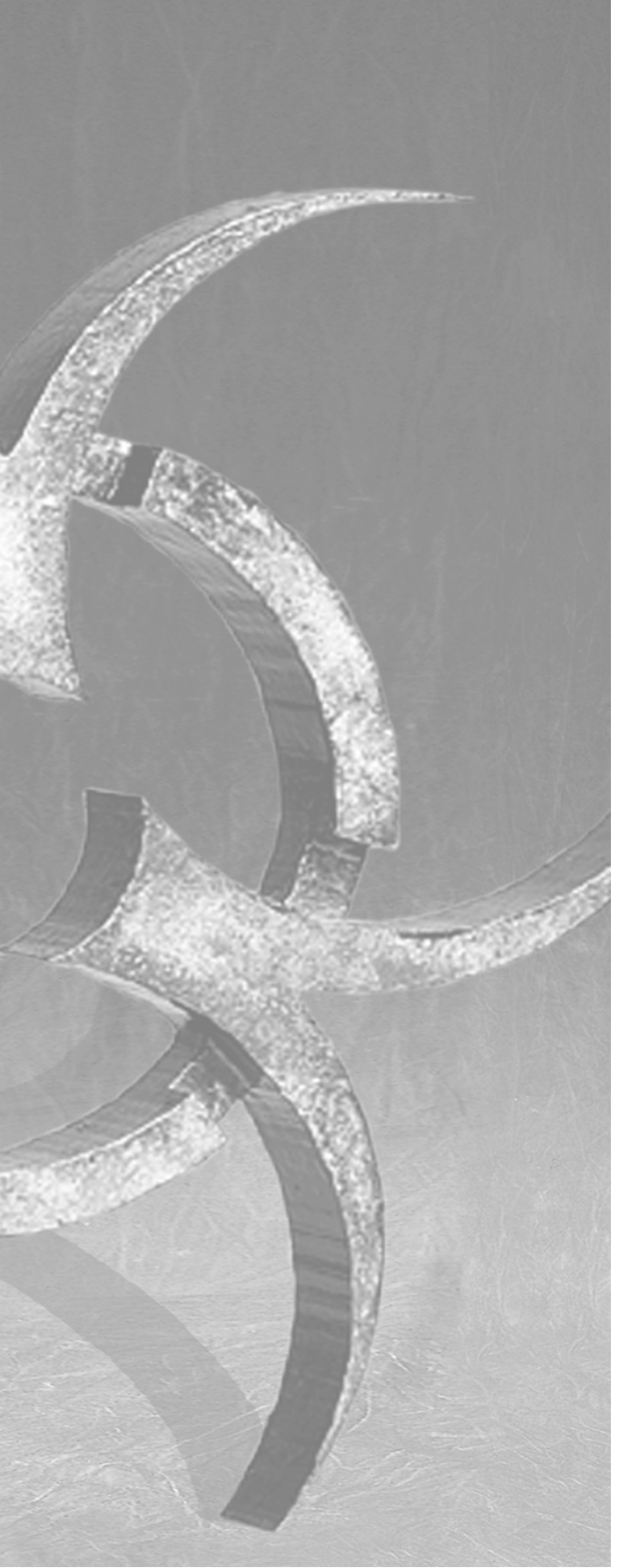


ePolicy Orchestrator

Guide du produit

Version 2.0

McAfee

A Network Associates Company

Sommaire

Préface

Objet

Ce guide du produit présente le logiciel McAfee ePolicy Orchestrator version 2.0 et fournit les informations suivantes : descriptions de toutes les fonctions du produit, instructions détaillées pour la configuration et le déploiement du logiciel, et procédures pour l'exécution de tâches. Il fournit également un guide permettant d'obtenir des informations ou de l'aide supplémentaires.

Assistance

Ce guide est conçu pour les administrateurs système et réseau qui sont responsables du programme anti-virus leur entreprise.

Obtention d'informations supplémentaires

AIDE

Vous pouvez trouver des informations supplémentaires sur le produit dans le système d'aide qui est inclus dans l'application. Pour accéder aux rubriques d'aide, utilisez le menu Aide de l'application.

- Le système d'aide fournit des informations de haut niveau et détaillées, auxquelles vous accédez à partir d'une option de menu ou d'un bouton de l'application.
- Aide contextuelle (*Qu'est-ce que c'est ?*) L'aide fournit de brèves descriptions des sélections effectuées dans l'application. Pour accéder à cette aide, cliquez avec le bouton droit de la souris sur une option, appuyez sur la touche Ctrl [F1] ou faites glisser l'icône représentant un point d'interrogation jusqu'à une option.

README.TXT

Des informations sur le produit information, les problèmes résolus, tous les problèmes connus et les ajouts ou modifications de dernière minute apportés au produit ou à ce guide.

CONTACT.TXT

Une liste de numéros de téléphone, d'adresses, d'adresses Web et de numéros de télécopies des bureaux Network Associates aux Etats-Unis et partout dans le monde. Il inclut également des informations relatives à des services et des ressources, notamment :

- Support technique
- Service clientèle
- Service de téléchargement
- Site de Recherche anti-virus AVERT
- Site bêta de McAfee
- Formation sur site
- Bureaux de Network Associates partout dans le monde
- Revendeurs

LICENSE.TXT	Les conditions d'utilisation du produit. Lisez attentivement ce fichier. Si vous installez le produit, vous acceptez les termes de la licence.
GUIDE D'INSTALLATION	Vous pouvez trouver des informations relatives à l'installation du produit dans ce guide : • Configuration système requise • Installation ou mise à niveau du logiciel • Désinstallation du logiciel • Dépannage • Où trouver des informations

Comment contacter McAfee et Network Associates

Support technique	http://knowledge.nai.com
Documentation technique	tvd_documentation@nai.com
Site bêta de McAfee	www.mcafeeb2b.com/beta/
Site de Recherche anti-virus AVERT	www.mcafeeb2b.com/avert
Site de téléchargement	www.mcafeeb2b.com/naicommon/download/
Mises à jour des fichiers .DAT	www.mcafeeb2b.com/naicommon/download/dats/find.asp
Mises à niveau du logiciel	www.mcafeeb2b.com/naicommon/download/upgrade/login.asp Numéro de licence valide requis. Contactez le service clientèle de Network Associates.
Formation sur site	www.mcafeeb2b.com/services/mcafee-training/default.asp
Recherche d'un revendeur	www.nai.com/asp_set/partners/tsp-seek/intro.asp

Service clientèle de Network Associates

Adresse électronique	services_corporate_division@nai.com
Site Web	www.nai.com www.mcafeeb2b.com

Appel gratuit depuis les Etats-Unis, le Canada et l'Amérique Latine :

Téléphone	+1-888-No VIRUS ou +1-888-847-8766 Du lundi au vendredi, de 8 heures à 20 heures (heure du centre des Etats-Unis)

Pour obtenir des informations supplémentaires sur la façon de contacter Network Associates et McAfee (y compris les numéros d'appel gratuits disponibles pour les autres zones géographiques), consultez le fichier CONTACT.TXT fourni avec cette version du produit.

Introduction au produit ePolicy Orchestrator 1

Introduction

Bienvenue dans ePolicy Orchestrator : Ce manuel fournit des informations essentielles sur la configuration et l'utilisation d'ePolicy Orchestrator.

Présentation d'ePolicy Orchestrator

Le produit ePolicy Orchestrator fournit une application et une gestion de la stratégie anti-virus multilingues centralisées, le déploiement de logiciels et des fonctionnalités de création de rapports pour garantir la protection contre les virus. Les administrateurs peuvent ainsi gérer des stratégies et déployer le produit McAfee VirusScan pour le bureau et le produit McAfee NetShield pour leurs serveurs de fichiers. L'outil de gestion ePolicy Orchestrator fournit un point de contrôle unique pour les produits McAfee. Il s'agit du premier outil de gestion anti-virus véritablement évolutif mis à la disposition des entreprises.

ePolicy Orchestrator est constitué de trois éléments distincts :

- **La console** fournit un point de contrôle unique pour le serveur et l'agent.
- **Le serveur** stocke le logiciel et la totalité des données du programme.
- **L'agent** applique la stratégie du logiciel anti-virus à la machine client.

Ces fonctions sont décrites en détail dans « Composants du produit » à la page 16.

Cela vous permet de gérer une stratégie de protection anti-virus où que vous soyez sur le réseau de votre société. La séparation de la console et du serveur vous permet de mettre en place plusieurs administrateurs si votre réseau s'étend à plusieurs domaines Windows NT. Dans l'environnement Microsoft de gestion de réseau avec des domaines à plusieurs maîtres, si vous placez le serveur ePolicy Orchestrator dans le domaine maître, le produit accède aux domaines ressources pour déployer l'agent et appliquer les stratégies anti-virus de votre société.

Une fois le serveur et la console installés avec succès, vous pouvez vous connecter à la console. A partir de cette dernière, vous pouvez installer les versions souhaitées des produits NetShield et VirusScan pour « pousser » l'agent sur les ordinateurs client dans votre domaine à partir d'un emplacement central.

Une fois l'agent installé sur les ordinateurs client, la console vous permet d'afficher les produits installés sur chaque machine agent et de mettre à jour ou d'installer des logiciels pour appliquer votre stratégie anti-virus.

Fonctionnement d'ePolicy Orchestrator

ePolicy Orchestrator utilise une technologie client/serveur pour distribuer et appliquer votre stratégie anti-virus à toute l'entreprise. Cette opération peut être effectuée simultanément pour plusieurs langues. L'administrateur d'ePolicy Orchestrator définit les stratégies au niveau d'une console unique et les applique à tous les ordinateurs client du réseau.

Ce produit assure quatre fonctions principales : le déploiement de logiciels, l'application de stratégies anti-virus, la planification de tâches et la création de rapports d'événements.

Ce produit comprend :

- un référentiel pour les logiciels anti-virus,
- une option d'installation du produit logiciel anti-virus à partir d'une console centralisée,
- une interface qui permet à l'administrateur d'afficher les propriétés et l'état anti-virus de tous les ordinateurs sur le réseau vers lequel l'agent est déployé, et de définir des stratégies à partir d'une console unique pour la totalité du réseau,
- la possibilité d'appliquer ces stratégies à tout le réseau,
- la possibilité de gérer la façon dont les logiciels anti-virus McAfee mettent à jour les fichiers de définition de virus (.DAT),
- une méthode pour le lancement des analyses à la demande à la disposition de tous les systèmes sur le réseau,
- une méthode permettant de planifier des tâches (mises à niveau ou analyses de logiciels par exemple) pour la totalité du réseau à partir d'une console centralisée,
- un moyen garantissant une protection anti-virus automatique aux utilisateurs itinérants,

- un moyen de déployer, gérer, mettre à jour et créer des rapports simultanément dans plusieurs langues,
- une prise en charge de plusieurs fournisseurs de services pour gérer la protection anti-virus au sein de toute l'entreprise,
- une capture des données de l'activité anti-virus sur tout le réseau pour toute machine exécutant l'agent,
- des rapports complets sur l'activité du logiciel anti-virus,
- une série de rapports par défaut qui peuvent être personnalisés par l'administrateur pour refléter l'activité du logiciel de protection anti-virus.

Nouveautés de cette version

La version 2.0 comporte plusieurs nouvelles fonctions :

- **Installation du serveur améliorée ; plus simple et au moins deux fois plus rapide.** La taille du programme d'installation du produit a été réduite ce qui permet une installation plus rapide. Si vous pré-installez Microsoft Data Engine (MSDE) ou la base de données Microsoft SQL Server 7, le temps d'installation est encore réduit.
- **Prise en charge de Windows 2000 par la console et le serveur.** La console et le serveur prennent désormais en charge Windows 2000 Server ou Advanced Server. La console prend désormais en charge Windows 2000 Professional.
- **Gérer plusieurs langues simultanément.** Les clients peuvent déployer, gérer, mettre à jour et créer des rapports simultanément dans plusieurs langues. Le référentiel peut être configuré pour gérer plusieurs langues. Voir « Configuration du référentiel » à la page 30.
- **Intégration avec WebShield e-500 pour la gestion anti-virus des passerelles.** Les clients peuvent configurer, mettre à jour et créer des rapports sur WebShield eppliance 500 pour la protection des passerelles au niveau des entreprises.
- **Création de rapports graphiques en temps réel.** Les clients peuvent configurer l'agent sur des bureaux gérés pour que leurs événements soient automatiquement transmis au serveur ePolicy Orchestrator en fonction de niveaux qui peuvent être définis. Les données sont désormais stockées dans une base de données unique, ce qui élimine ainsi le délai associé à la réplication des données de la machine de la base de données LDAP vers la base de données de rapport.

- **Gestion des stratégies plus puissante et plus rapide.** Les administrateurs peuvent utiliser des variables dans la gestion des stratégies et des tâches pour les valeurs qui peuvent changer d'une machine de l'agent à une autre.
- **Application de la stratégie en temps réel.** Les clients peuvent utiliser la nouvelle stratégie en mémoire cache locale pour appliquer la dernière stratégie téléchargée sans utiliser de bande passante supplémentaire.
- **Nouveaux rapports de couverture.** Les rapports de couverture sont plus faciles à lire et comprennent des informations pour les ordinateurs équipés d'une protection anti-virus et ceux n'ayant pas d'agent installé. Plusieurs nouveaux rapports ont été ajoutés : Le Rapport d'infection d'analyse d'apparition de virus, le Rapport d'infection du lecteur de disquette et le Rapport de couverture de la langue du produit. Deux nouveaux rapports de couverture du produit, le Résumé de l'absence de protection AV (No AV Protection Summary) et le Résumé de la protection du produit (Product Protection Summary), fournissent des informations relatives aux produits anti-virus non compatibles.
- **Déployer l'agent avec des droits configurables.** Les administrateurs peuvent facilement déployer des agents dans des environnements avec des scripts de connexion où l'utilisateur connecté n'a pas de droit d'administrateur.
- **L'agent se connecte au serveur en utilisant le nom d'ordinateur affecté à l'ordinateur serveur.** L'agent peut se connecter au serveur en utilisant le nom d'ordinateur affecté à l'ordinateur serveur (nom NetBIOS) lorsqu'il ne réussit pas à se connecter en utilisant l'adresse IP. Si l'adresse IP de votre ordinateur serveur change, l'agent peut rappeler le serveur sans problème.
- **Gestion des répertoires plus souple et plus rapide.** La fonction de recherche de répertoire avancée permet au client de rechercher n'importe quel critère de machine et d'effectuer des actions sur plusieurs ordinateurs en fonction de ce critère. Voir « Recherche d'ordinateurs dans le répertoire » à la page 56.

Choix du logiciel McAfee pour ePolicy Orchestrator

Le logiciel ePolicy Orchestrator prend en charge la gestion de stratégies et la création de rapports pour les produits et les composants logiciels enfichables suivants :

- VirusScan 4.03
- VirusScan 4.5.0
- VirusScan 4.5.1
- VirusScan TC 6.0.0
- NetShield 4.03a
- NetShield 4.50
- GroupShield Domino 5.0.0
- Alert Manager 4.5.0
- WebShield e-500

En outre, le logiciel ePolicy Orchestrator peut générer des rapports prédéfinis pour les produits suivants :

- GroupShield Exchange
- WebShield SMTP

ePolicy Orchestrator ne prend pas en charge les versions des produits McAfee antérieures à 4.03.

Composants du produit

Le produit ePolicy Orchestrator comprend trois composants distincts :

- Le **serveur**, qui héberge une base de données, un référentiel de logiciels, ainsi que d'autres fonctions de gestion.
- La **console**, interface qui permet à l'administrateur de déployer des agents et des logiciels et de gérer la protection anti-virus de votre société grâce aux produits McAfee.
- L'**agent**, composant déployé sur les ordinateurs client, qui assure une protection permanente contre les virus, exécute des tâches planifiées et signale au serveur les modifications intervenues sur la machine client.

Serveur

Le serveur ePolicy Orchestrator comporte trois fonctionnalités principales : une base de données qui stocke d'importantes quantités de données concernant les actions du produit McAfee sur les ordinateurs de votre réseau, un moteur de création de rapports qui vous permet de contrôler les performances de la protection anti-virus de votre société, ainsi qu'un référentiel de logiciels qui stocke les logiciels que vous déployez sur votre réseau.

Console

La console ePolicy Orchestrator fournit une interface utilisateur de type MMC (Microsoft Management Console) qui vous permet de gérer la protection anti-virus de l'intégralité de votre société et d'afficher les propriétés des machines qui hébergent chaque agent déployé. Elle permet de définir et d'appliquer des stratégies anti-virus à tous les ordinateurs déployés ou uniquement aux ordinateurs sélectionnés, et de planifier des tâches pour des ordinateurs particuliers ou des groupes d'ordinateurs particuliers selon diverses planifications. Enfin, la console permet d'afficher et de personnaliser des rapports pour contrôler votre déploiement.

Le serveur est toujours installé avec la console pour vous permettre d'interfacer avec lui-même lorsque le réseau est en panne. La console peut également être installée à distance de sorte que vous pouvez gérer le serveur ePolicy Orchestrator depuis une machine distante.

Agent

L'agent ePolicy Orchestrator est le composant du produit que vous poussez vers les ordinateurs client (appelés *hôtes d'agents*) pour collecter et consigner des données, installer le logiciel et signaler n'importe quel événement au serveur. C'est un programme qui s'exécute en arrière-plan sur les ordinateurs client. Une fois installé, il recueille des données sur le logiciel de protection anti-virus résidant sur chaque machine client et renvoie ces données au serveur. L'agent rassemble toute nouvelle stratégie, toute tâche ou tout logiciel provenant du serveur qui s'applique à celui-ci. L'agent exécute la stratégie, installe tout logiciel téléchargé sur la machine client et effectue toute tâche programmée selon les instructions que vous avez définies pendant la session de configuration.

Quand une autre activité concernant les produits McAfee se produit sur la machine client, l'agent en informe le serveur. Un cas de figure serait l'apparition d'un virus sur l'ordinateur hôte de l'agent. L'agent accomplit toutes ses opérations sans que l'utilisateur ne s'en aperçoive. L'agent s'installe en arrière-plan en utilisant la technologie push et s'exécute en arrière-plan, sans que les utilisateurs ne le voient.

Ce produit permet une grande flexibilité de déploiement. Bien qu'il ait été conçu pour pousser l'agent vers des ordinateurs client équipés de Windows NT, Windows 98 et de Windows 2000, vous pouvez également copier le fichier d'installation de l'agent sur une disquette, dans un partage réseau ou sur tout autre support pour permettre une installation manuelle sur les ordinateurs client. Reportez-vous au paragraphe « L'agent » à la page 85 pour de plus amples informations.

Décisions et considérations 2

Choix de la méthode d'utilisation d'ePolicy Orchestrator

Utilisateurs du produit

Les administrateurs de réseaux locaux à grande envergure et de petites entreprises sont les mieux placés pour utiliser ePolicy Orchestrator. Ce logiciel simplifie une fonction essentielle de la gestion de réseau, à savoir l'application uniforme des stratégies de contrôle des virus. En installant un serveur unique et centralisé pour héberger vos produits logiciels McAfee préférés, tous configurés selon vos spécifications, vous pouvez assurer à tous vos ordinateurs client une protection uniforme, efficace et rapide. Grâce à la technologie « push », ces produits peuvent être déployés à partir d'une seule console sur tout votre réseau sans déranger les utilisateurs. Cette technologie garantit également que les utilisateurs ne changent pas vos paramètres une fois le produit installé.

Les fournisseurs de services gérés (MSP, Managed Service Providers), qui gèrent les ressources de différentes sociétés, trouveront plusieurs fonctions qui les aideront à garantir une protection anti-virus fiable et complète à leurs sociétés client à partir d'une seule console. Le produit ePolicy Orchestrator comporte des contrôles permettant de limiter l'accès au niveau des sites. Vous pouvez fournir des comptes avec accès en lecture seule, ainsi que des comptes administrateur de sites qui limitent l'écriture et n'exercent de contrôle que sur un site spécifique. Vous pouvez créer des comptes réviseur dotés d'un accès en lecture seule. Par ailleurs, le tri des adresses IP facilite la gestion des répertoires une fois que l'agent a été distribué.

Pourquoi utiliser ce produit ?

Le produit ePolicy Orchestrator présente plusieurs avantages pour les administrateurs :

Gestion de stratégie

Vous pouvez définir un groupe unique de stratégies de protection anti-virus pour tout votre réseau et les appliquer à l'ensemble de l'entreprise.

Création de rapports

Vous avez accès à un composant complet de création de rapports qui vous permet de demander plusieurs rapports spécialisés sur l'état de la protection totale contre les virus dans votre réseau. Toutes les données de ces rapports sont capturées dans la base de données du serveur relative à tous vos ordinateurs client.

Distribution de logiciels

Le produit offre un référentiel centralisé pour les produits McAfee que vous choisissez de déployer. Vous pouvez passer en revue la configuration de chacun de vos ordinateurs client une fois l'agent installé, déterminer le type de stratégies de protection anti-virus à appliquer sur chacun d'eux et y déployer les logiciels par l'intermédiaire de la console.

Mises à jour pour utilisateurs itinérants

Le produit ePolicy Orchestrator peut être configuré de façon à ce que les utilisateurs itinérants soient mis à jour à chaque fois qu'ils se connectent. A chaque fois qu'une machine se reconnecte au serveur après une période d'absence, l'agent contacte le serveur ePolicy Orchestrator afin de prendre connaissance des événements ou des propriétés et de recueillir les stratégies de protection ou les tâches. Grâce à cette fonction, vous êtes sûr que tous les utilisateurs disposent de la protection anti-virus la plus récente.

Prise en charge des fournisseurs de services gérés

Plusieurs fonctions d'ePolicy Orchestrator prennent en charge les besoins spécifiques des fournisseurs de services gérés. Vous pouvez créer des groupes au niveau du site qui incluent des masques de sous-réseau IP ou des plages d'adresses IP pour couvrir l'intégralité du réseau de votre société. Ensuite, grâce aux divers types de comptes, un administrateur de services gérés peut créer des comptes dotés d'un accès en lecture sur le système, ainsi que des comptes permettant uniquement de consulter ou de gérer des sites particuliers. Cela vous permet de n'accorder aux clients qu'un accès à leur site, tout en conservant la possibilité des fournisseurs de services gérés d'administrer l'intégralité de l'installation à partir d'une seule console. Les comptes réviseur peuvent réviser les statistiques des arborescences de répertoires, ainsi que les rapports.

Gestion des apparitions de virus

Le produit comporte maintenant une fonction d'appel de réveil de l'agent qui vous permet de programmer une mise à jour des fichiers .DAT à l'aide du planificateur, puis d'appeler vos agents afin qu'ils consultent le serveur et recueillent le nouveau fichier .DAT. Vos moyens de contrôle sont ainsi renforcés face aux apparitions de virus.

Installation et configuration du produit 3

Présentation

La console représente votre interface pour ce produit et ses fonctions. Cette interface est également celle où vous installez, configurez et déployez tous les produits anti-virus virus McAfee qui sont gérés via le logiciel ePolicy Orchestrator.

Ce chapitre présente la console et ses fonctions et décrit les tâches qui sont requises pour la configuration d'ePolicy Orchestrator :

Démarrage d'ePolicy Orchestrator

Si vous ouvrez la console pour la première fois après une nouvelle installation, vous êtes invité à modifier votre mot de passe. Cette invite n'apparaît pas si vous ouvrez la console après une mise à niveau.

Pour démarrer le produit ePolicy Orchestrator :

1. Cliquez sur **Démarrer** dans la barre des tâches Windows, pointez sur **Programmes**, choisissez **McAfee**, puis sélectionnez **Console ePolicy Orchestrator 2.0**.

   La console s'ouvre (Figure 3-1).

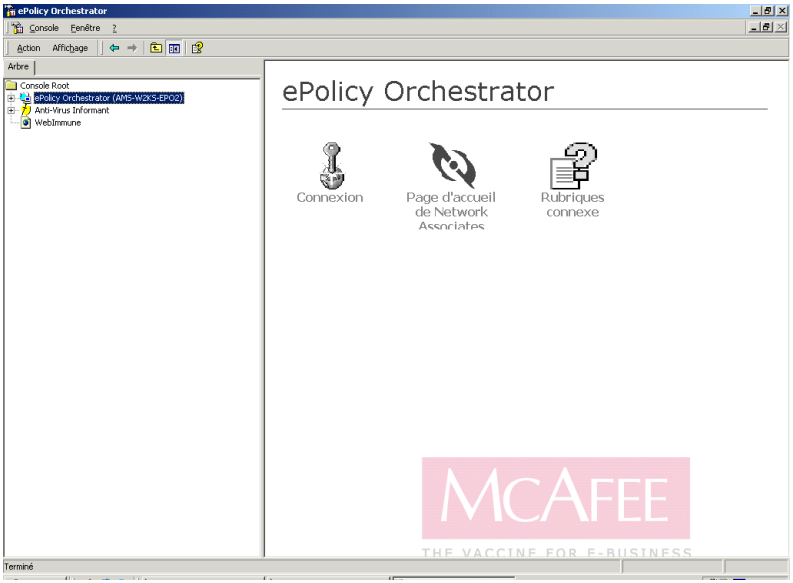


Figure 3-1. Volet de connexion d'ePolicy Orchestrator

2. Cliquez sur **Connexion** pour ouvrir ePolicy Orchestrator. La fenêtre Connexion s'affiche

   - Pour une première connexion après une nouvelle installation :

     a. Pour le **nom d'utilisateur**, saisissez `admin`.

     b. Pour le **mot de passe**, saisissez `admin`.

     c. Cliquez sur **OK**. Vous êtes invité à changer le mot de passe. Cliquez à nouveau sur **OK**.

     d. Saisissez un nouveau mot de passe, confirmez-le et cliquez sur **OK**. La console ePolicy Orchestrator s'affiche à l'écran.

   - Pour une première connexion après une mise à niveau :

     a. Spécifiez un **nom de serveur** et un **nom d'utilisateur** ou acceptez les valeurs par défaut fournies par le logiciel.

     b. Saisissez un **mot de passe** valide pour le compte d'utilisateur spécifié.

     c. Cliquez sur **OK** pour ouvrir la console ePolicy Orchestrator.

Présentation de la console

Lorsque vous vous connectez pour la première fois au serveur, la console apparaît, la racine de la console étant mise en surbrillance dans l'arborescence de la console. L'apparence de la console se modifie pour refléter les éléments que vous avez sélectionnés dans l'arborescence de la console et/ou le volet Détails.

La console utilise les fonctionnalités standard Microsoft Management Console (MMC). Deux rangées de menu en haut de la fenêtre affichent les fonctionnalités du menu standard et du menu personnalisé. Pour obtenir une description des commandes du menu personnalisé, reportez-vous à « Options de menu » à la page 25.

La console se divise en deux parties ou *volets* sous les menus. Ces volets comportent les éléments suivants :

- **L'arborescence de la console** est le volet gauche de la console. Reportez-vous à la section « Arborescence de la console » à la page 26 pour obtenir une description complète.
- **Le volet Détails** est le volet droit de la console. En fonction de l'élément sélectionné dans l'arborescence de la console, le volet Détails peut être divisé en un **volet supérieur Détails** et un **volet inférieur Détails**. Reportez-vous à la section « Volet Détails » à la page 29 pour obtenir une description complète.

Cette vue de la console affiche quatre options sur le volet Détails.

Gérer les administrateurs	Interface pour l'ajout, la suppression et la configuration des comptes administratifs. Voir « Création et gestion de comptes » à la page 80.
Paramètres du serveur	Interface pour le contrôle et l'affichage des paramètres généraux du serveur. Voir « Paramètres du serveur » à la page 202.
Page d'accueil Network Associates	Accès en un clic au site Web de Network Associates.
Rubriques d'aide	Accès en un clic à l'aide en ligne d'ePolicy Orchestrator.

Options de menu

Les menus suivants sont disponibles dans l'interface :

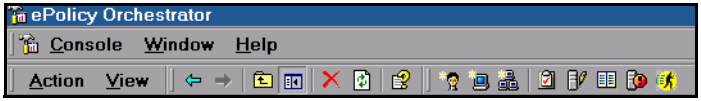


Figure 3-2. Options de menu de la console

La ligne supérieure du menu offre trois options de menu :

- **Console**
- **Fenêtre**
- **Aide**

Ces trois menus représentent les options du menu MMC standard qui apparaissent lors de chaque installation MMC. Pour de plus amples informations sur ces options, consultez **Rubriques d'aide** dans le menu Aide.

La deuxième ligne du menu offre un mélange de menus MMC et de menus qui sont spécifiques à ePolicy Orchestrator :

- **Action**
- **Affichage**

Ces deux menus constituent des commandes MMC courantes, mais ils affichent différentes options qui reflètent le type d'élément choisi dans l'arborescence de la console.

Au-delà des menus Action et Affichage se trouve une série d'icônes qui répètent les tâches et les commandes décrites dans le menu Action et dans les sous-menus qui apparaissent lorsque vous cliquez avec le bouton droit de la souris sur un objet dans l'arborescence de la console. Les icônes qui apparaissent peuvent varier en fonction de l'objet que vous sélectionnez dans l'arborescence de la console.

Arborescence de la console

L'*arborescence de la console* est le volet gauche de la console (Figure 3-3). Le logiciel ePolicy Orchestrator offre trois noeuds principaux sur l'arborescence de la console : le noeud **ePolicy Orchestrator**, le noeud **Anti-Virus Informant** et le noeud **WebImmune**. Le noeud ePolicy Orchestrator se divise encore en **Répertoire** et **Référentiel**.

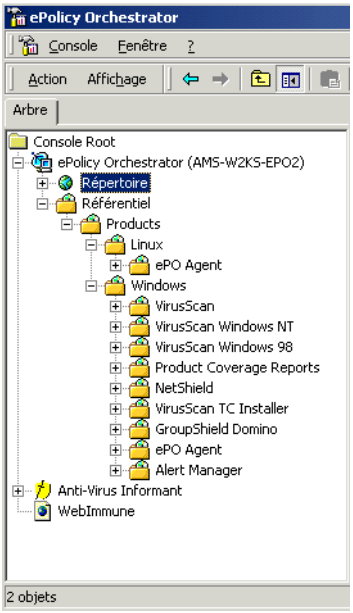


Figure 3-3. Arborescence de la console

Vous pouvez afficher immédiatement la structure complète de votre répertoire dans l'arborescence de la console. Voir Figure 3-3. Vous pouvez afficher la liste des logiciels installés dans le référentiel. Si l'arborescence d'Anti-Virus Informant était étendue, vous pourriez également voir les détails de l'installation du logiciel rapportés par Anti-Virus Informant.

La structure de l'arborescence de la console s'applique au mode de relation des noeuds entre eux et pas nécessairement à la relation en réseau entre les entités. L'administrateur peut modifier cette relation au niveau de la console, mais il faut veiller à préserver les relations des adresses IP et les dispositions des masques de sous-réseau. Déplacer des objets ne modifie pas les domaines ou les répertoires du réseau. L'administrateur les modifie à des fins de gestion du logiciel et de fourniture de services aux ordinateurs client. Le contenu de la portion du répertoire de l'arborescence de la console peut être modifié pour prendre en charge l'installation de l'anti-virus.

La structure du référentiel de logiciels et du noeud d'Anti-Virus Informant est déterminée par d'autres options, telles que l'installation du logiciel ou la création de rapports.

Noeuds

Chaque élément de l'arborescence de la console est un *noeud*. Voir Figure 3-4. Un noeud peut être un site ou un élément de programme. Les éléments principaux de l'arborescence de la console, à savoir le répertoire, le référentiel et les éléments d'Anti-Virus Informant, sont tous des noeuds.

Chaque noeud du répertoire représente un élément unique dans la configuration ePolicy Orchestrator. Un noeud unique peut être un parent ou un enfant. Il peut être un parent pour les noeuds qui se trouvent sous lui tout en étant un enfant pour un noeud qui se trouve au-dessus de lui.

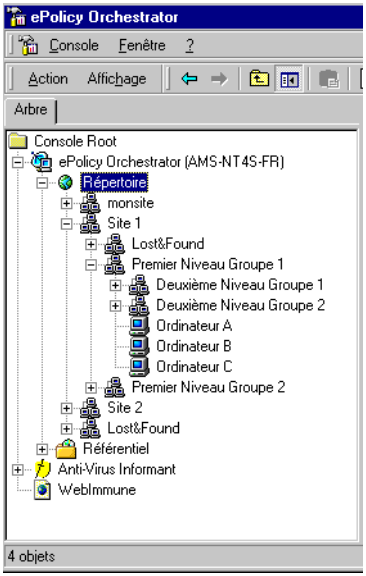


Figure 3-4. Arborescence de la console affichant le répertoire

Noeud parent

Les noeuds parents ont des sous-noeuds ou des branches placées en dessous d'eux. Ces sous-noeuds sont appelée enfants. Les sites peuvent uniquement être des noeuds parents dans cette structure.

Noeud enfant

Un noeud enfant peut être en même temps enfant d'un autre noeud et parent de noeuds enfants placés au-dessous. Au niveau le plus bas de l'arborescence, un enfant n'a aucun noeud placé en dessous de lui. Un enfant hérite des décisions que vous prenez concernant le site dans lequel il se trouve. Les noeuds de l'ordinateur peuvent uniquement être des noeuds enfants dans cette structure.

Un site peut avoir un groupe, un ordinateur ou un périphérique WebShield e-500 comme noeuds enfants. Un groupe peut avoir un autre groupe, un ordinateur ou un périphérique WebShield e-500 comme noeuds enfants. Vous ne pouvez pas placer un noeud sous un ordinateur ou un périphérique WebShield e-500 dans la structure de ce répertoire. Il peut y avoir plusieurs niveaux de noeuds enfants, appelés générations.

Dans la Figure 3-4 à la page 27, Répertoire est un parent du Site 1, Perdu & Trouvé, et du Site 2. Site 1, Perdu & Trouvé et Site 2 sont des noeuds enfants du répertoire. Site 1 est également un noeud parent de Groupe 1 de premier niveau et de Groupe 2 de premier niveau.

Héritage

Il est important de comprendre la relation qui existe entre les noeuds parents et les noeuds enfants, car les noeuds enfants peuvent hériter des stratégies des noeuds parents.

Héritage signifie qu'un noeud prend des stratégies ou en hérite du noeud parent. Lorsque vous définissez des stratégies ou programmez des tâches, vous décidez si vous souhaitez que les noeuds enfants héritent des stratégies ou tâches du noeud parent. Pour plus de détails sur ce sujet, consultez « Organisation du répertoire » à la page 55.

Volet Détails

Le *volet Détails* se trouve sur le côté droit de la console et affiche des détails sur l'élément que vous avez sélectionné dans l'arborescence de la console. Les informations affichées peuvent changer en fonction de l'élément sélectionné. Le volet Détails ne se divise en volets *supérieur* et *inférieur* uniquement lorsque vous sélectionnez un élément dans l'arborescence du répertoire ou lorsque vous sélectionnez l'onglet Stratégies dans le volet Détails. Voir Figure 3-5.

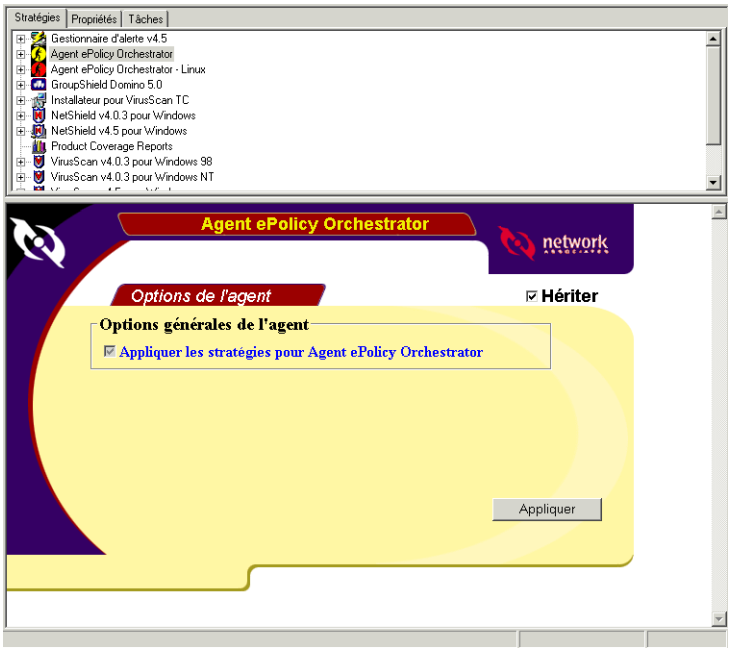


Figure 3-5. Volet Détails

- Le *volet supérieur des détails* comporte trois onglets.

  Stratégies — Répertorie les options configurables pour le logiciel dans le référentiel.

  Propriétés — Affiche les propriétés du noeud sélectionné, telles qu'elles sont rapportées par l'agent.

  Tâches — Répertorie les tâches programmées pour le noeud sélectionné.

- Le *volet inférieur des détails* affiche les stratégies configurables pour un progiciel. Il devient visible une fois que vous avez « complété » le répertoire et installé le logiciel dans le référentiel. Voir « Compléter le répertoire » à la page 36.

Configuration du référentiel

Référentiel

Le référentiel (Figure 3-6) est l'endroit dans ePolicy Orchestrator où vous stockez les logiciels McAfee (fichiers *.NAP) qui sont gérés pour votre réseau. Ces produits logiciels sont installés sur le serveur ePolicy Orchestrator lors de l'installation du produit ePolicy Orchestrator. Ils sont distribués via la console aux ordinateurs client installés sur le réseau.

Les fichiers *.NAP multilingues sont disponibles avec la version 2.0 du logiciel ePolicy Orchestrator.

Figure 3-6. Référentiel ePolicy Orchestrator

La fonctionnalité **Configurer le référentiel** fournit les outils nécessaires pour ajouter des logiciels, activer le déploiement de logiciels et mettre à jour des plug-ins.

Pour configurez le référentiel, procédez comme suit :

- **Ajouter de nouveaux logiciels à gérer** — Sélectionnez cette option pour installer de nouveaux fichiers .NAP de produits logiciels. Elle est requis si vous voulez ajouter de nouveaux logiciels à gérer par ePolicy Orchestrator.
- **Activer le déploiement de logiciels** — Sélectionnez cette option pour installer les fichiers d'installation (binaires) du produit pour chaque produit et langue à déployer. Elle est requise avant de déployer un logiciel anti-virus.
- **Mettre à jour le plug-in** — Sélectionnez cette option si vous avez une mise à jour de produit à installer. Les mises à jour de produit ou les plug-ins peuvent être sous la forme d'un fichier .NAP.

Ajout de nouveaux logiciels

Vous pouvez ajouter de nouveaux logiciels pour n'importe quel produit McAfee que vous souhaitez qu'ePolicy Orchestrator gère.

Pour ajouter un nouvelle progiciel :

1. Mettez en surbrillance **Référentiel** dans l'arborescence de la console, puis cliquez avec le bouton droit de la souris et sélectionnez **Configurer le référentiel**.

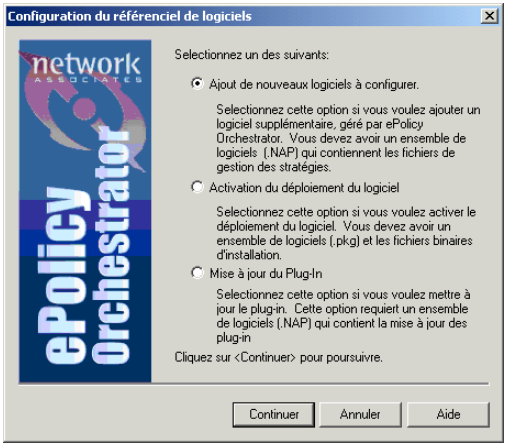


Figure 3-7. Configurer le référentiel

2. Sélectionnez **Ajouter de nouveaux logiciels à gérer**, puis cliquez sur **Continuer** pour ouvrir la fenêtre Sélectionner un ensemble de logiciels.
3. Utilisez le champ **Regarder dans** pour parcourir l'arborescence afin de localiser le fichier .NAP que vous voulez ajouter.
4. Mettez en surbrillance le fichier .NAP que vous voulez installer et cliquez sur **Ouvrir** pour commencer l'installation.
5. Répétez cette procédure de l'Etape 1 à l'Etape 4 pour chaque progiciel à ajouter.

Activation du déploiement de logiciels

Vous devez installer les fichiers d'installation (binaires) du produit McAfee pour chaque langue et produit anti-virus McAfee avant de pouvoir les déployer sur les ordinateurs client installés sur le réseau.

Vous avez besoin des fichiers .PKG spécifiques à la langue et au produit pour installer les fichiers d'installation du produit McAfee. Les fichiers .PKG sont fournis avec le logiciel ePolicy Orchestrator.

Pour activer le déploiement de logiciels :

1. Mettez en surbrillance **Référentiel** dans l'arborescence de la console, puis cliquez avec le bouton droit de la souris et sélectionnez **Configurer le référentiel**.
2. Sélectionnez l'option **Activer le déploiement de logiciels**, puis cliquez sur **Continuer** pour ouvrir la fenêtre Sélectionner un ensemble de logiciels.
    a. Utilisez le champ **Regarder dans** pour localiser l'endroit où vous avez installé ePolicy Orchestrator. Vous pouvez trouver les fichiers .PKG dans le dossier suivant :

    \Setup\Nap\<Produit>\<Version>\InstallFiles

Figure 3-8. Activer le déploiement – Sélectionner le fichier .PKG

3. Mettez en surbrillance le fichier .PKG spécifique à la langue que vous voulez installer et cliquez sur **Ouvrir**. La fenêtre Recherche d'un dossier s'affiche.

4. Recherchez, sur votre réseau, le dossier dans lequel se trouve le fichier d'installation du produit McAfee spécifique à la langue (Point Product), puis cliquez sur **OK**. Voir Figure 3-9.

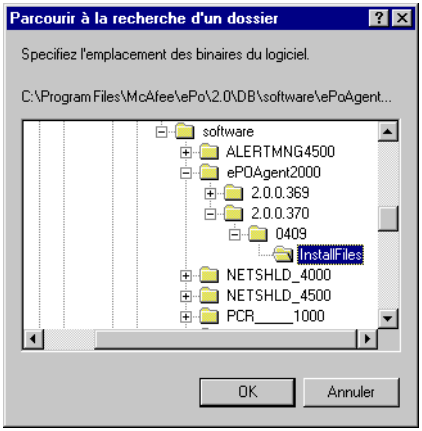


Figure 3-9. Activer le déploiement – Sélectionner le fichier binaire

5. Lorsque la configuration est terminée, vous recevez un message indiquant que la configuration du référentiel de logiciels a abouti. Cliquez sur **OK**.

6. Répétez cette procédure de l'Etape 1 à l'Etape 5 pour chaque produit et langue à déployer.

Mise à jour de plug-ins

Vous pouvez installer un fichier .NAP plug-in mis à jour pour n'importe quel produit pour lequel une mise à jour est disponible.

Pour mettre à jour le plug-in :

1. Mettez en surbrillance **Référentiel** dans l'arborescence de la console, puis cliquez avec le bouton droit de la souris et sélectionnez **Configurer le référentiel**.
2. Sélectionnez l'option **Mettre à jour le plug-in** et cliquez sur **Continuer** pour ouvrir la fenêtre Sélectionner un ensemble de logiciels.
3. Utilisez le champ **Regarder dans** pour localiser l'endroit où vous avez copié le fichier .NAP plug-in pour le produit à mettre à jour.
4. Mettez en surbrillance le fichier .NAP plug-in que vous voulez installer et cliquez sur **Ouvrir** pour commencer l'installation.
5. Répétez cette procédure de l'Etape 1 à l'Etape 4 pour chaque produit à mettre à jour.

> **REMARQUE :** Vous pouvez vérifier qu'il s'agit d'un fichier .NAP plug-in ou d'un fichier .NAP de gestion en affichant ses propriétés.

Suppression d'un logiciel

Vous pouvez supprimer des logiciels pour n'importe quel produit McAfee que vous que vous avez installés dans le référentiel.

Pour supprimer un progiciel :

1. Mettez en surbrillance le nom ou la version du produit que vous souhaitez supprimer dans le référentiel, puis cliquez avec le bouton droit de la souris et sélectionnez **Supprimer**.
2. Sélectionnez **Supprimer** pour supprimer tous les fichiers d'installation, de kit et de plug-in correspondant à toutes les langues du produit sélectionné.
3. Répétez cette procédure de l'Etape 1 à l'Etape 2 pour chaque progiciel à supprimer.

> **AVERTISSEMENT :** Lorsque vous supprimez du référentiel les fichiers d'installation (binaires), de plug-in ou de langue du produit McAfee, le fichier du produit logiciel McAfee (*.NAP) est également supprimé. Si vous supprimez par erreur un produit logiciel que vous souhaitiez conserver, vous devez à nouveau ajouter ce produit logiciel au référentiel. Voir « Ajout de nouveaux logiciels » à la page 31.

Compléter le répertoire

Le côté gauche de l'arborescence de la console contient le répertoire. Ce répertoire contient tous les sites que vous créez ou importez depuis le domaine du réseau.

Les premiers objets que vous créez sous le répertoire doivent être des sites. Ces sites de premier niveau possèdent des conditions spéciales qui leur sont associées, comme indiqué ci-dessous. Vous devez créer au moins un site sous le répertoire dans votre arborescence de la console. Généralement, les objets de ce site proviennent d'un domaine ou d'un fichier texte importé, mais vous pouvez également créer un site.

Une fois ces sites créés, vous pouvez ajouter des groupes de second niveau, des ordinateurs ou un périphérique WebShield e-500.

Sites

Un site est un groupe de premier niveau sous le répertoire dans l'arborescence de la console. Il existe des différences importantes entre un site (un groupe de premier niveau) et d'autres groupes de niveau (par exemple, groupe de second, de troisième et de quatrième niveau). Un site peut uniquement être ajouté au niveau du répertoire.

Un site possède des fonctions spéciales pour la gestion, comme la possibilité d'affecter une adresse IP et contient un groupe Perdu et Trouvé.

Il existe deux méthodes pour ajouter des sites. Vous pouvez importer un domaine existant ou créer un site.

Importation d'un domaine de réseau en tant que site

La méthode la plus courante pour compléter l'arborescence de la console au niveau du répertoire consiste à importer un domaine de réseau existant en tant que site. Vous pouvez limiter la plage d'adresses IP en modifiant le groupe. Vous pouvez également utiliser la fonction Modifier lors du processus d'importation pour inclure des noeuds enfants.

Vous pouvez utiliser la fenêtre Ajouter des sites pour ajouter un nouveau site créé ou parcourir la structure de domaine actuelle pour sélectionner un domaine à ajouter en tant que site.

Pour importer un domaine de réseau existant en tant que site :

1. Cliquez avec le bouton droit sur **Répertoire** dans l'arborescence de la console pour ouvrir le menu Action.
2. Placez le curseur sur **Nouveau**, puis sélectionnez **Site** dans le sous-menu (Figure 3-10).

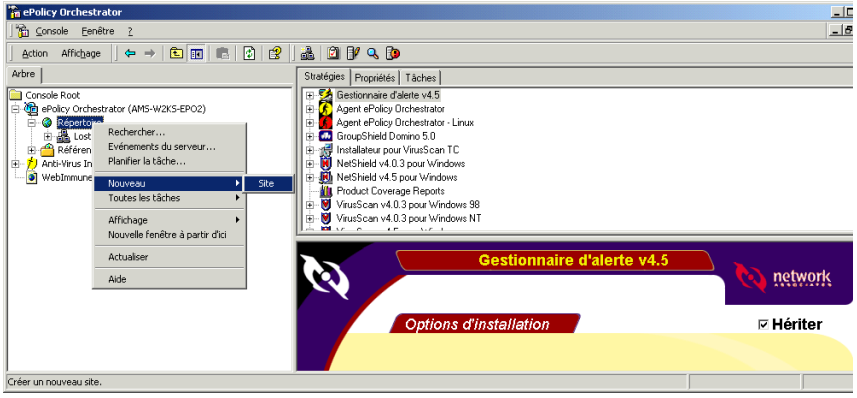


Figure 3-10. Importer un nouveau site

3. Cliquez sur **Parcourir...** pour ouvrir la boîte de dialogue Navigateur réseau qui vous propose des sélections de domaines disponibles.

4. Cliquez sur le signe plus ⊞ du niveau supérieur pour afficher la liste des domaines disponibles.

5. Sélectionnez le ou les domaines souhaité(s) et cliquez sur **OK** pour revenir à la fenêtre Ajouter des sites (Figure 3-11).

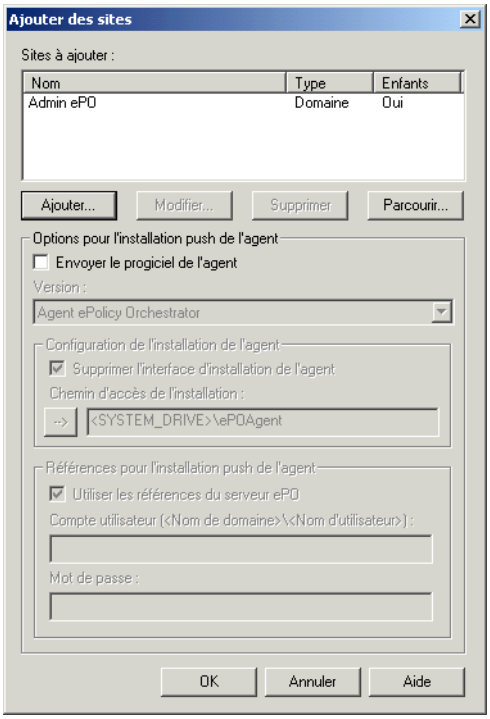


Figure 3-11. Ajouter des sites – Domaine importé

La fenêtre Ajouter des sites affiche à présent le ou les sites que vous venez de sélectionner. Vous pouvez ajouter ici des domaines existants ou n'importe quel groupe d'ordinateurs.

- Si la valeur Enfants est **Oui**, le domaine est importé en tant que nouveau site avec tous les ordinateurs qu'il comprend.
- Si la valeur Enfants est **Non**, seul le domaine est importé dans le nouveau site.

La fenêtre Ajouter des sites propose également plusieurs options supplémentaires :

- Elle vous indique si vous ajoutez un domaine et si le domaine détecté a des enfants.
- Lorsque vous importez un site, elle offre la possibilité d'envoyer l'agent à chaque ordinateur du site. Pour envoyer l'agent à l'ensemble des ordinateurs du domaine lorsque vous les importez, sélectionnez **Envoyer le progiciel de l'agent**.

  Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.

6. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePolicy Orchestrator. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.
   - **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
   - **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme. Consultez « Variables de stratégies » à la page 118 pour obtenir une définition de variables.
   - **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, le serveur ePolicy Orchestrator utilisera son compte utilisateur pour pousser les agents. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

   Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces fonctions sont désactivées.

7. Pour importer un autre domaine, répétez cette procédure de l'Etape 3 à l'Etape 6.
8. Cliquez sur **OK** pour valider le nouveau site et revenir à la console.

Ajout d'un nouveau site

Vous pouvez créer un nouveau site au niveau du répertoire. Cela est utile si vous avez défini une stratégie spécifique à appliquer pour sélectionner des ordinateurs dans différents domaines.

Pour créer un site dans l'arborescence de la console :

1. Mettez en surbrillance **Répertoire** dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Site** dans le sous-menu pour ouvrir la fenêtre Ajouter des sites.
2. Cliquez sur **Ajouter** pour créer un site.

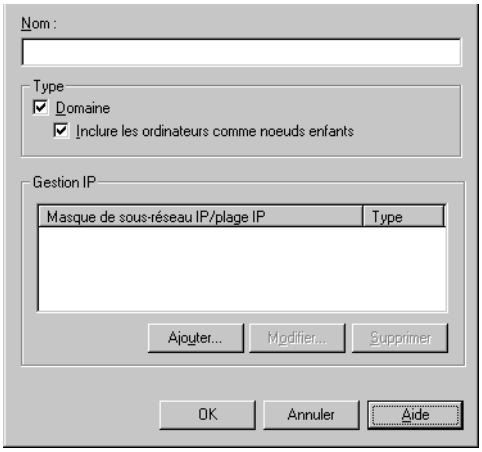


Figure 3-12. Ajouter un nouveau site

3. Entrez un **nom** pour le nouveau site.
4. Sélectionnez **Domaine** si le site que vous créez est un domaine NT. Ainsi l'option **Inclure les ordinateurs comme noeuds enfants** devient disponible.
5. Sélectionnez **Inclure les ordinateurs comme noeuds enfants** si vous voulez importer tous les ordinateurs dans le domaine en tant qu'enfants. Cela vous permet de créer un site qui ressemble à votre domaine NT et vous offre la possibilité d'appliquer des stratégies à partir du niveau supérieur en utilisant la fonction d'héritage du logiciel.
6. Cliquez sur **Ajouter** à la section Gestion IP pour ouvrir la fenêtre Gestion IP. Vous pouvez spécifier un masque de sous-réseau IP ou une plage d'adresses IP pour ce nouveau site.

7. Cliquez sur **OK** pour revenir à la fenêtre Ajouter des sites, qui montre le nouveau site créé (Figure 3-13).

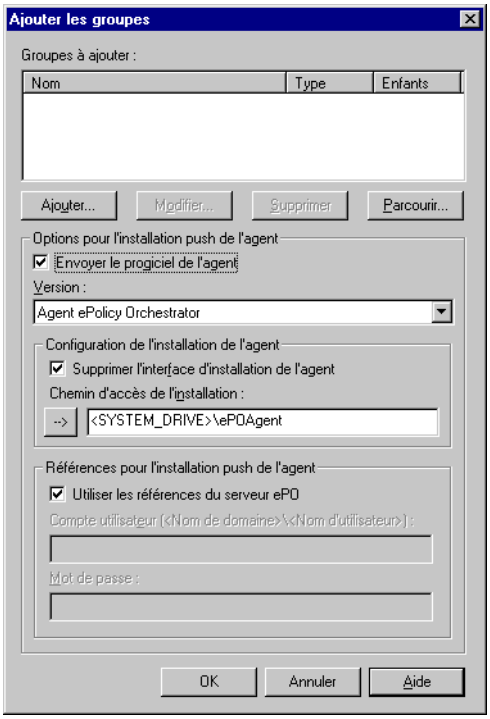


Figure 3-13. Fenêtre Ajouter des sites affichant le nouveau site

La fenêtre Ajouter des sites propose également plusieurs options supplémentaires :

- Elle vous indique si vous ajoutez un domaine et si le domaine détecté a des enfants. Vous ne pouvez pas modifier ces options.
- Lorsque vous importez un site, elle offre la possibilité d'envoyer l'agent à chaque ordinateur du site. Pour envoyer l'agent à l'ensemble des ordinateurs du domaine lorsque vous les importez, sélectionnez **Envoyer le progiciel de l'agent**.

  Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.

8. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePO pour Win32. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.

- **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Cet écran de message peut disparaître au bout de quelques secondes seulement. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
- **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur pour insérer une variable système ou une variable de fichiers programme (Figure 3-14). Consultez « Variables de stratégies » à la page 118 pour obtenir une définition de variables.

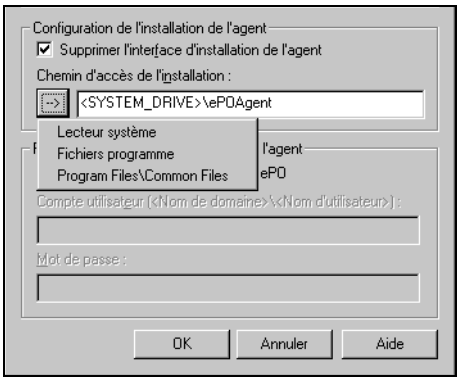


Figure 3-14. Fenêtre Envoyer le programme d'installation de l'agent – Insérer des variables

- **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push des agents et les fonctions Compte utilisateur et Mot de passe ne sont pas disponibles. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces fonctions sont désactivées.

9. Pour ajouter un autre site, répétez cette procédure de l'Etape 3 à l'Etape 8.
10. Cliquez sur **OK** pour ajouter le site. Cela vous renvoie à la console, affichant le nouveau site sous forme de noeud dans le répertoire.

Groupes

Un groupe peut être un noeud parent ou un noeud enfant. Il existe deux méthodes pour ajouter des groupes. Vous pouvez ajouter un groupe en important un groupe existant depuis un autre domaine ou en créant un groupe.

Importation d'un groupe

Vous pouvez importer un groupe au niveau du site ou du groupe.

Pour importer un groupe dans l'arborescence de la console :

1. Mettez en surbrillance un site ou un groupe dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Groupe** dans le sous-menu pour ouvrir la fenêtre Ajouter des groupes.
2. Cliquez sur **Parcourir...** pour ouvrir la boîte de dialogue Explorateur de répertoires qui vous propose des sélections de domaines disponibles.
3. Cliquez sur le signe plus ⊞ du niveau supérieur pour afficher la liste des groupes disponibles.
4. Sélectionnez les groupes souhaités et cliquez sur **OK** pour revenir à la fenêtre Ajouter des groupes.

   La fenêtre Ajouter des groupes affiche à présent les groupes que vous venez de sélectionner. Vous pouvez ajouter ici des domaines existants ou n'importe quel groupe d'ordinateurs.

   - Si la valeur Enfants est **Oui**, le domaine est importé en tant que nouveau groupe avec tous les ordinateurs compris dans le groupe.
   - Si la valeur Enfants est **Non**, seul le domaine est importé dans le nouveau groupe.

La fenêtre Ajouter des groupes propose également plusieurs options supplémentaires :

- Elle vous indique si vous ajoutez un domaine et si le domaine détecté a des enfants. Vous ne pouvez pas modifier ces options.
- Lorsque vous importez un groupe, elle offre la possibilité d'envoyer l'agent à chaque ordinateur du groupe. Pour envoyer l'agent à l'ensemble des ordinateurs du domaine lorsque vous les importez, sélectionnez **Envoyer le progiciel de l'agent**.

  Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.

5. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePO pour Win32. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.
   - **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
   - **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.
   - **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push des agents et les fonctions Compte utilisateur et Mot de passe ne sont pas disponibles. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

   Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces options sont désactivées.

6. Pour importer un autre groupe, répétez cette procédure de l'Etape 3 à l'Etape 5.
7. Cliquez sur **OK** pour valider le groupe importé et revenir à la console.

Ajout d'un nouveau groupe

Vous pouvez créer un groupe au niveau du site ou du groupe.

Pour ajouter un groupe dans l'arborescence de la console :

1. Mettez en surbrillance un site ou un groupe dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Groupe** dans le sous-menu pour ouvrir la fenêtre Ajouter des groupes.
2. Cliquez sur **Ajouter** pour créer un groupe.
3. Entrez un **nom** pour le nouveau groupe. Voir Figure 3-15.

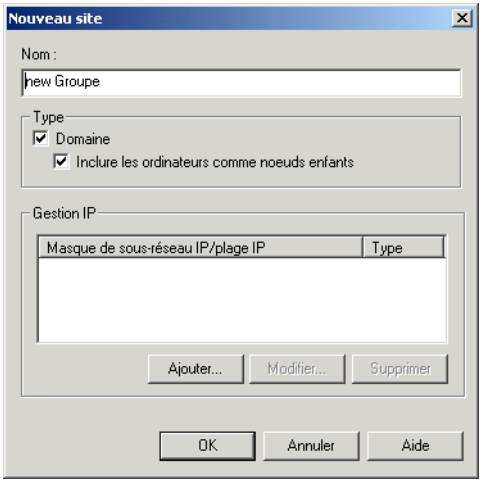


Figure 3-15. Fenêtre Ajouter un nouveau groupe affichant le nouveau groupe

4. Sélectionnez **Domaine** si le groupe que vous créez est un domaine NT. Ainsi l'option **Inclure les ordinateurs comme noeuds enfants** devient disponible.
5. Sélectionnez **Inclure les ordinateurs comme noeuds enfants** si vous voulez importer tous les ordinateurs dans le domaine en tant qu'enfants. Cela vous permet de créer un groupe qui ressemble à votre domaine NT et vous offre la possibilité d'appliquer des stratégies à partir du niveau supérieur en utilisant la fonction d'héritage du logiciel.
6. Cliquez sur **Ajouter** à la section Gestion IP pour spécifier un masque de sous-réseau IP ou une plage d'adresses IP pour ce nouveau groupe. La fenêtre Gestion IP s'ouvre.

7. Cliquez sur **OK** pour revenir à la fenêtre Ajouter des groupes, qui montre le nouveau groupe créé (Figure 3-16).

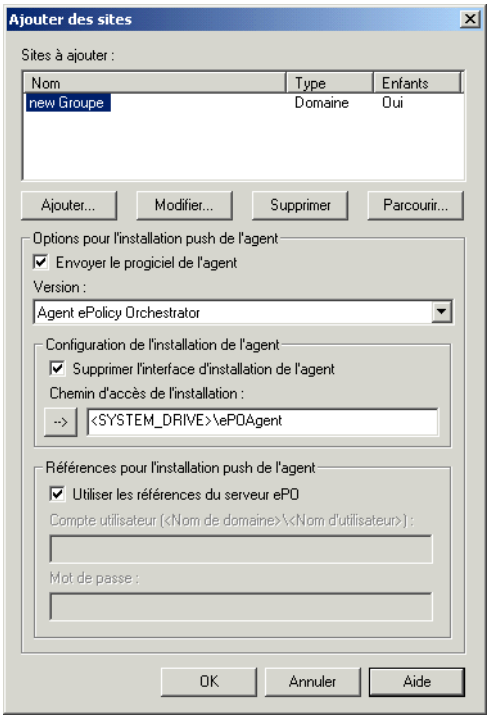


Figure 3-16. Fenêtre Ajouter des sites affichant le nouveau site

La fenêtre Ajouter des groupes propose également plusieurs options supplémentaires :

- Elle vous indique si vous ajoutez un domaine et si le domaine détecté a des enfants. Vous ne pouvez pas modifier ces options.
- Lorsque vous importez un groupe, elle offre la possibilité d'envoyer l'agent à chaque ordinateur du groupe. Pour envoyer l'agent à l'ensemble des ordinateurs du domaine lorsque vous les importez, sélectionnez **Envoyer le progiciel de l'agent**.

  Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.

8. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePO pour Win32. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.
   - **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Cet écran de message peut disparaître au bout de quelques secondes seulement. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
   - **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.
   - **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push des agents et les fonctions Compte utilisateur et Mot de passe ne sont pas disponibles. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

   Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces fonctions sont désactivées.

9. Pour ajouter un autre groupe, répétez cette procédure de l'Etape 3 à l'Etape 8.

10. Cliquez sur **OK** pour ajouter le nouveau groupe. Cela vous renvoie à la console, affichant le nouveau groupe sous forme de noeud dans l'arborescence.

Ordinateurs

L'entité Ordinateurs est toujours un noeud enfant. Il existe trois méthodes pour ajouter des ordinateurs. Vous pouvez importer un ordinateur depuis un domaine existant, créer un ordinateur ou importer un ordinateur d'un fichier texte.

Importation d'un ordinateur depuis un domaine

Vous pouvez importer un ordinateur au niveau du site ou du groupe.

Pour importer un ordinateur dans l'arborescence de la console :

1. Mettez en surbrillance un site ou un groupe dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Ordinateur** dans le sous-menu pour ouvrir la fenêtre Ajouter des ordinateurs.
2. Cliquez sur **Parcourir...** pour ouvrir la boîte de dialogue Recherche des ordinateurs qui vous propose des sélections de domaines disponibles.
3. Cliquez sur le signe plus ⊞ du niveau supérieur et du second niveau pour afficher la liste des ordinateurs disponibles.
4. Sélectionnez le ou les ordinateurs souhaité(s) et cliquez sur **OK** pour revenir à la fenêtre Ajouter des ordinateurs.

   La fenêtre Ajouter des ordinateurs propose plusieurs options supplémentaires :

   - Elle propose l'option d'envoyer l'agent à chaque ordinateur. Pour envoyer l'agent à l'ensemble des ordinateurs, sélectionnez **Envoyer le progiciel de l'agent**.

     Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.

5. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePO pour Win32. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.
   - **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
   - **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.
   - **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push des agents et les fonctions Compte utilisateur et Mot de passe ne sont pas disponibles. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

   Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces fonctions sont désactivées.

6. Pour importer un autre ordinateur, répétez cette procédure de l'Etape 3 à l'Etape 5.

7. Cliquez sur **OK** pour valider l'ordinateur importé et revenir à la console.

Ajout d'un ordinateur

Vous pouvez créer un ordinateur au niveau du site ou du groupe.

Pour ajouter un ordinateur à l'arborescence de la console :

1. Mettez en surbrillance un site ou un groupe dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Ordinateur** dans le sous-menu pour ouvrir la fenêtre Ajouter des ordinateurs.
2. Cliquez sur **Ajouter** pour ouvrir la fenêtre Nouvel ordinateur.
3. Entrez un nom d'ordinateur et cliquez sur **OK** pour revenir à la fenêtre Ajouter des ordinateurs.

   La fenêtre Ajouter des ordinateurs propose plusieurs options supplémentaires :

   - Elle propose l'option d'envoyer l'agent à chaque ordinateur. Pour envoyer l'agent à l'ensemble des ordinateurs, sélectionnez **Envoyer le progiciel de l'agent**.

     Pour plus d'informations sur le déploiement de l'agent, consultez la section « L'agent » à la page 85.
4. Lorsque vous sélectionnez **Envoyer le progiciel de l'agent**, vous activez d'autres options. Sélectionnez l'option appropriée :

   - **Version.** Actuellement, cette liste déroulante permet uniquement d'installer l'agent ePO pour Win32. Si plusieurs agents peuvent être déployés, cette liste propose des options supplémentaires.
   - **Supprimer le GUI d'installation de l'agent.** Normalement, lorsque l'agent est installé sur l'ordinateur client, une zone de message s'affiche brièvement à l'écran. Dès que l'installation est terminée, il disparaît. Si vous cochez cette case, ePolicy Orchestrator installe silencieusement l'agent sur le client. L'utilisateur final n'a pas connaissance de l'installation.
   - **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.

- **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push des agents et les fonctions Compte utilisateur et Mot de passe ne sont pas disponibles. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

Si vous ne cochez pas la case **Envoyer le progiciel de l'agent**, ces fonctions sont désactivées.

5. Pour créer un autre ordinateur, répétez cette procédure de l'Etape 3 à l'Etape 4.

6. Cliquez sur **OK** pour valider le nouvel ordinateur et revenir à la console.

Importation d'un groupe ou d'un ordinateur à partir d'un fichier texte

Vous pouvez créer des groupes et des ordinateurs en les important à partir d'un fichier.

Pour importer des fichiers :

1. Mettez en surbrillance un site ou un groupe dans l'arborescence de la console, cliquez avec le bouton droit de la souris et déplacez le curseur vers **Toutes les tâches**, puis sélectionnez **Importer l'ordinateur** dans le sous-menu pour ouvrir l'écran Importation d'ordinateurs à partir d'un fichier texte.

2. Cliquez sur **Continuer** pour ouvrir la fenêtre Importer du fichier (Figure 3-17).

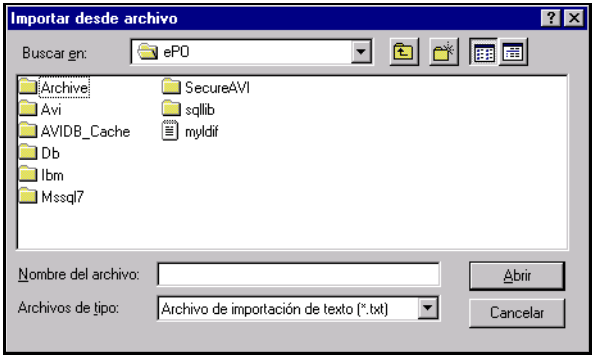


Figure 3-17. Fenêtre Importer du fichier

3. Sélectionnez le fichier que vous voulez importer. Cliquez sur **Ouvrir** pour importer le fichier sélectionné et ajouter les ordinateurs à l'arborescence de la console sous le noeud sélectionné. Si les ordinateurs n'apparaissent pas comme spécifié, consultez la section suivante.

Règles de formatage pour les fichiers texte à importer

REMARQUE : Cette fonction ne vérifie pas que le fichier importé contient des noms d'ordinateurs et de domaines valides. Vous devez revoir le fichier texte d'importation avant d'activer la fonction d'importation pour vous assurer que les informations que vous importez sont valides.

Les règles suivantes s'appliquent lorsque vous importez des noeuds d'une liste de fichiers :

- Chaque entrée doit commencer sur une nouvelle ligne.
- Les espaces dans les noms de domaines, les noms d'ordinateurs ou les commentaires d'ordinateurs ne sont pas ignorés. Par exemple, `MON MAC` n'est pas la même chose que `MONMAC`.
- Les lignes laissées vides sont ignorées.

Voici les trois types d'entrées que vous pouvez importer d'une liste :

- Entrée d'ordinateur unique, pas de domaine
- Entrée d'ordinateur unique avec un nom de domaine
- Entrée d'ordinateur multiple pour un nom de domaine unique

Entrée d'ordinateur unique, pas de domaine

Syntaxe

<Nom de l'ordinateur>

Nom de l'ordinateur Microsoft. Cette valeur ne doit pas nécessairement respecter la casse et comprend au maximum 15 caractères.

Exemples

```
Ordinateur A
Ordinateur B
```

Entrée d'ordinateur unique avec un nom de domaine

Syntaxe

<Nom de domaine>\<Nom de l'ordinateur>

Ce format vous permet d'ajouter de nombreux ordinateurs à un domaine Microsoft unique sans devoir préciser le nom de domaine à chaque fois. Ne placez pas de lignes vides entre le nom de domaine et l'un des noms d'ordinateurs suivants pour ce domaine.

Champ obligatoire

<Nom de domaine>

Indique le nom de domaine Microsoft qui contient ce nom d'ordinateur.

<Nom de l'ordinateur>

Nom de l'ordinateur Microsoft. Cette valeur ne respecte pas la casse et comprend au maximum 15 caractères.

Exemples

```
ZONEDOMAINE\MARKET5
ZONEDOMAINE\MARKET6
```

Entrée d'ordinateur multiple pour un nom de domaine unique

Syntaxe

<Nom de domaine>\<Nom de l'ordinateur>

Chaque paramètre a la même signification que ceux détaillés dans « Entrée d'ordinateur unique avec un nom de domaine ».

Exemples

```
B_DOMAIN\
WORK1
WORK2
C_DOMAIN\
MACH1
MACH2
```

Périphériques WebShield e-500

Un périphérique WebShield e-500 peut être ajouté à n'importe quel site ou groupe existant en tant que noeud enfant.

Pour ajouter un périphérique WebShield e-500 dans l'arborescence de la console :

1. Mettez en surbrillance un site, un groupe ou un ordinateur dans l'arborescence de la console, cliquez avec le bouton droit et déplacez le curseur vers **Nouveau**, puis sélectionnez **Périphérique WebShield e-500** dans le sous-menu pour ouvrir la fenêtre Configuration du nouveau périphérique WebShield e-500. (Figure 3-18).

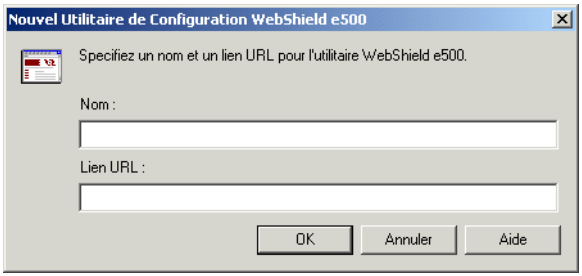


Figure 3-18. Ajouter un périphérique WebShield e-500

2. Entrez un nom pour le périphérique WebShield e-500.
3. Entrez le lien de l'URL pour le périphérique WebShield e-500.
4. Cliquez sur **OK** pour ajouter le périphérique e-500 au site ou au groupe.

L'ajout du périphérique WebShield e-500 facilite la gestion. Si vous souhaitez également consulter les informations de couverture, telles que les informations sur le matériel ou sur l'agent, vous devez ajouter un composant informatique pour chaque périphérique e-500.

REMARQUE : Si vous ajoutez à la fois un périphérique e-500 et un ordinateur, prenez soin de donner à chacun un nom différent. L'utilisation de noms en double risque d'entraîner une confusion lorsque vous contactez l'ordinateur ou le périphérique (en exécutant la commande ping), ou lorsque vous affichez des informations sur les propriétés.

Gestion du répertoire

Il existe plusieurs façons de gérer le répertoire :

- Organisation du répertoire
- Gestion IP
- Contrôles d'intégrité
- Mise à jour des domaines

Organisation du répertoire

L'organisation de vos éléments peut rendre le déploiement de l'agent et du logiciel simple et efficace. Vous pouvez utiliser les fonctions Couper et Coller pour déplacer des groupes et des ordinateurs à l'intérieur de sites, ou utiliser la fonction Rechercher pour rechercher et déplacer des ordinateurs dans le répertoire.

Déplacement d'éléments dans le répertoire avec les fonctions Couper et Coller

Vous pouvez déplacer des éléments à l'intérieur des groupes ou des sites pour réorganiser le répertoire ou compléter les nouveaux groupes créés.

Pour déplacer un élément dans le répertoire :

1. Mettez en surbrillance l'élément (groupe, ordinateur ou périphérique WebShield e-500) à déplacer, puis cliquez avec le bouton droit et sélectionnez **Couper** pour supprimer l'élément.
2. Déplacez le curseur vers le nouveau site ou groupe, puis cliquez avec le bouton droit et sélectionnez **Coller** pour placer l'élément dans le répertoire.
3. Effectuez un contrôle d'intégrité IP pour vous assurer de l'absence de tout conflit ou doublons d'adresses IP. Consultez la section « Contrôles d'intégrité d'adresse IP » à la page 69 pour plus de détails.

> **REMARQUE :** Vous devez posséder des droits d'administrateur général pour déplacer un groupe à partir du groupe Perdu & Trouvé général.

Recherche d'ordinateurs dans le répertoire

La nouvelle fonction Rechercher vous permet de rechercher facilement des ordinateurs dans le répertoire. Vous pouvez effectuer plusieurs actions sur un ordinateur ou un groupe d'ordinateurs. Ces actions comprennent le déplacement et la suppression d'ordinateurs.

Pour rechercher des ordinateurs dans le répertoire :

1. Mettez en surbrillance **Répertoire** dans l'arborescence de la console, puis cliquez avec le bouton droit et sélectionnez **Rechercher** pour ouvrir la fenêtre Recherche de répertoire.
2. Sélectionnez le critère de recherche dans la liste déroulante. Voici les options proposées :
   - Ordinateurs d'un domaine
   - Ordinateurs dans un groupe ou site spécifique
   - Ordinateurs avec une version DAT spécifique
   - Ordinateurs avec une version de moteur d'analyse spécifique
   - Noms d'ordinateurs en double
   - Agents ePolicy Orchestrator inactifs
   - Système d'exploitation
   - Ordinateurs spécifiques
   - Version de l'agent ePO spécifique
   - Version de l'agent ePO spécifique

3. Poursuivre la personnalisation de la recherche en entrant des critères de recherche supplémentaires.

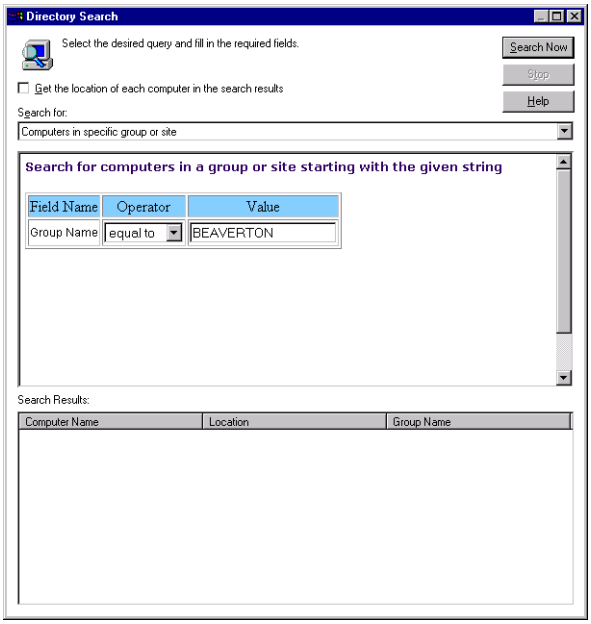


Figure 3-19. Fenêtre Recherche de répertoire

Les critères supplémentaires que vous pouvez entrer dépendent de l'option de recherche sélectionnée. Certaines options de recherche vous permettent de sélectionner un opérateur et d'entrer une valeur ; d'autres vous permettent d'entrer uniquement une valeur.

La valeur que vous entrez peut inclure des caractères normaux tels que du texte, ou si vous utilisez l'opérateur LIKE, vous pouvez entrer une chaîne qui recherche un modèle particulier. Le modèle peut inclure les caractères génériques SQL Server valides suivants :

Caractère générique	Description	Exemple
%	Toute chaîne contenant zéro caractère ou plus.	WHERE title LIKE '%computer%' recherche tous les titres de manuels contenant le terme « computer ».
_(caractère de soulignement)	N'importe quel caractère.	WHERE au_fname LIKE '_ean' recherche tous les noms composés de quatre lettres se terminant par « ean ». Par exemple, Dean et Sean.
[]	N'importe quel caractère dans la plage indiquée ([a-f]) ou l'ensemble ([abcdef]).	WHERE au_lname LIKE '[C-P]arsen' recherche les prénoms des auteurs qui se terminent par « arsen » et commence par n'importe quel caractère compris entre « C » et « P ». Carsen, Larsen et Parsen, par exemple.
[^]	N'importe quel caractère dans la plage indiquée ([^a-f]) ou l'ensemble ([^abcdef]).	WHERE au_lname LIKE 'de[^b]%' recherche tous les noms de famille d'auteurs qui commencent par « de » et dont la lettre qui suit n'est pas un « b ».

4. Cliquez sur **Rechercher** pour lancer la recherche.
5. Visualisez les résultats dans la section Résultats de la recherche de la fenêtre.
6. Sélectionnez les résultats en mettant en surbrillance les résultats individuels ou à l'aide des touches **Maj** et/ou **Ctrl** pour sélectionner plusieurs résultats.

7. Cliquez avec le bouton droit pour sélectionner l'action à effectuer pour les résultats sélectionnés (Figure 3-20). Voici les options proposées :

   - Envoyer le programme d'installation de l'agent
   - Appel de réveil de l'agent
   - Déplacer vers
   - Supprimer
   - Enregistrer sous
   - Imprimer

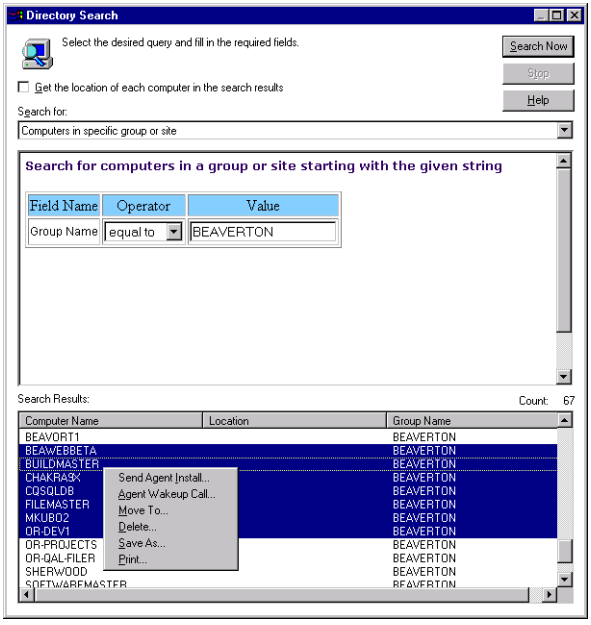


Figure 3-20. Recherche de répertoire – Sélectionner une action

Gestion IP

Le logiciel ePolicy Orchestrator permet de trier les éléments du répertoire par plages d'adresses IP et par masques de sous-réseau. Vous pouvez organiser le répertoire en blocs discrets qui correspondent à des affectations d'entreprises ou géographiques des adresses IP et des masques de sous-réseau au niveau du site. Les grandes entreprises peuvent ainsi gérer différents sites géographiques depuis une seule installation. Les fournisseurs de services gérés (MSP) ont la possibilité de fournir une protection anti-virus uniforme à tous leurs clients depuis une seule console tout en maintenant les sites séparément via l'affectation de plages d'adresses ou de masques de sous-réseau à leurs sites spécifiques.

Cette fonction améliore la sécurité en garantissant que les comptes au niveau du site ne peuvent voir que le site sur lequel ils possèdent des droits. Les agents répondant lors de l'intervalle de communication agent-serveur initial sont affectés au groupe Perdu & Trouvé au niveau du site qui se base sur leur adresse IP, en limitant l'accès aux seuls administrateur général et administrateur de site approprié.

Règles de tri des plages d'adresses IP et des masques de sous-réseau

Les règles de tri suivantes pour les plages d'adresses IP et les masques de sous-réseau ne s'appliquent que lors de la première communication de l'agent avec le serveur :

- Si une plage d'adresses IP ou un masque de sous-réseau n'est pas défini(e) pour un site, aucun groupe de ce site ne peut avoir de plage d'adresses IP ou de masque de sous-réseau affecté(e).
- Une plage d'adresses IP ou un masque de sous-réseau d'un groupe doit être un sous-ensemble du site auquel il(elle) appartient.
- Une plage d'adresses IP ou un masque de sous-réseau d'un site doit être un super-ensemble de tout groupe qui lui appartient.
- Une plage d'adresses IP ou un masque de sous-réseau d'un groupe ne doit pas chevaucher tout « enfant » ou groupe sur le même niveau qui appartient au même site ou groupe.

Après le contact initial, l'agent met à jour l'emplacement auquel il a été affecté. Si l'adresse IP dans l'ID unique de l'agent ne correspond pas à l'une des plages d'adresses IP ou ni à l'un des masques de sous-réseau affectés, l'agent est placé dans le groupe Perdu & Trouvé général pour qu'un administrateur général l'affecte à l'emplacement approprié. Si la plage d'adresses IP ou le masque de sous-réseau ne correspond pas à un des sites, les données de l'agent sont placées dans le groupe Perdu & Trouvé au niveau du site. L'administrateur de site affecte alors l'agent au groupe approprié.

Ordre de recherche

IMPORTANT : Pour activer la fonction Ordre de recherche lors de la première communication, vous devez installer l'agent à l'aide d'une méthode non push, comme des scripts de connexion. Vous ne pouvez pas utiliser cette fonction si l'agent est poussé. McAfee recommande l'utilisation d'un script de connexion. Consultez « Méthodes d'installation » à la page 92 pour avoir des instructions détaillées sur l'installation de l'agent.

Lorsqu'un agent contacte le serveur pour la première fois, ce dernier recherche le site ou approprié dont le masque IP ou la plage IP correspond à l'adresse IP de l'agent, en utilisant l'ordre suivant :

1. Masque/plage IP du site — Si le masque IP ou la plage IP du site correspond à l'adresse IP de l'agent, le serveur poursuit la recherche dans ce site. Si le masque IP ou la plage IP du site ne correspond pas à l'adresse IP de l'agent, la recherche se poursuit dans tous les autres sites pour lesquels aucun paramètre IP n'est défini.

   Si le masque IP ou la plage IP du site correspond à l'adresse IP de l'agent, mais que le serveur ne peut pas faire correspondre le masque IP ou la plage IP au niveau de l'ordinateur ou du domaine, le serveur crée un groupe de domaine sous le groupe Perdu & Trouvé du site, puis ajoute un noeud d'ordinateur sous ce groupe de domaine.

2. Nom de l'ordinateur — Si le noeud d'ordinateur dont le nom de noeud correspond au nom d'ordinateur de l'agent est trouvé, l'agent est lié à ce noeud.

3. Nom de domaine — Si le noeud de groupe dont le nom de noeud correspond au nom de domaine de l'agent est trouvé, le serveur poursuit la recherche dans le groupe le plus profond de ce domaine, pour le masque IP ou la plage IP correspondant. Si un masque IP ou une plage IP correspondant à l'adresse IP de l'agent est trouvé, le serveur crée un noeud d'ordinateur portant le même nom que l'agent, et lie l'agent à ce noeud d'ordinateur. Si aucun masque IP ou aucune plage IP correspondant à l'adresse IP de l'agent n'est trouvé, le serveur crée un noeud d'ordinateur sous le groupe de domaine.

4. Groupe le plus profond sous ce site qui correspond au masque IP — Si le noeud de groupe ne correspond pas à un nom de domaine de l'agent, le serveur poursuit la recherche du groupe le plus profond ayant un masque IP correspondant sous ce site. Une fois qu'un groupe correspondant est trouvé, le serveur crée un noeud d'ordinateur portant le même nom que l'agent, et lie l'agent à ce noeud d'ordinateur.

5. Aucune correspondance trouvée — Si le serveur ne trouve de correspondance IP avec aucun site du répertoire, il crée un groupe de domaine sous le groupe Perdu & Trouvé général, puis crée un noeud d'ordinateur sous ce groupe de domaine. Vous devez posséder des droits d'administrateur général pour déplacer un groupe à partir du groupe Perdu & Trouvé général.

La règle de recherche de nom de domaine est prioritaire sur la règle de groupe IP. Si vous souhaitez placer l'ordinateur dans le groupe IP approprié, vous devez soit créer le groupe IP sous le groupe de domaine, soit ne pas créer le groupe de domaine sous le site. Voici trois scénarios démontrant comment cela fonctionne :

Scénario A

Répertoire

|— SiteA (161.69.0.0/16)

|— Amérique_Nord (Groupe de domaine)

|— IPGroupA (161.69.82.0/24)

Scénario B

Répertoire

|— SiteA (161.69.0.0/16)

|— IPGroupA (161.69.82.0/24)

Scénario C

Répertoire

|— SiteA (161.69.0.0/16)

|— Amérique_Nord (Groupe de domaine)

|— IPGroupA (161.69.82.0/24)

Lorsque l'agent dont l'adresse IP est 161.69.82.100 se connecte au serveur dans les scénarios A et B, l'agent va correctement dans IPGroupA. Toutefois, dans le scénario C, l'agent va dans le groupe de domaine Amérique_Nord au lieu d'aller dans IPGroupA.

Groupes Perdu & Trouvé

Un groupe Perdu & Trouvé est un référentiel d'informations sur l'agent obtenues à partir d'un agent non identifié. Les informations sur l'agent sont placées dans l'un des répertoires Perdu & Trouvé lorsque l'agent envoie pour la première fois des propriétés au serveur.

Il existe deux types de groupes Perdu & Trouvé :

- **Groupe Perdu & Trouvé général.** Ce groupe contient des informations sur l'agent qui ne correspondent à aucun site du répertoire. Cela inclut les informations sur les adresses IP et les masques de sous-réseau si vous les utilisez pour gérer des groupes et des sites. Cela inclut également des noms de sites ou de groupes. Si vous importez des informations sur le site à l'aide de domaines de réseau existants, cela inclut un nom de domaine. Seuls les administrateurs généraux ont un accès total au groupe Perdu & Trouvé général.
- **Groupes Perdu & Trouvé spécifiques au site.** Les groupes Perdu & Trouvé au niveau du site contiennent des informations sur l'agent qui correspondent aux informations sur les adresses IP ou les masques de sous-réseau du site. Si vous n'utilisez pas d'informations sur les adresses IP ou sur les masques de sous-réseau pour gérer l'arborescence de la console, ePolicy Orchestrator fait correspondre les noms de site ou de groupe. Les administrateurs de site peuvent accéder aux noeuds Perdu & Trouvé spécifiques au site.

Si le serveur peut faire correspondre les informations sur l'agent à un ordinateur ou domaine existant dans l'arborescence de la console, il crée un objet ordinateur pour cet agent dans l'arborescence de la console, y place la liste pour cet ordinateur ou domaine et les informations s'affichent sur la console. Si, cependant, le serveur ne connecte pas les informations entrantes sur l'agent à un ordinateur ou domaine existant, les informations sont placées dans un des groupes Perdu & Trouvé jusqu'à ce qu'un administrateur déplace la fiche dans l'un des autres groupes.

Les groupes Perdu & Trouvé apparaissent au niveau du répertoire et de chaque site (groupe de premier niveau) dans l'arborescence de la console. La Figure 3-21 indique une structure d'arborescence de la console qui affiche les groupes Perdu & Trouvé dans les groupes de second niveau affichés, ainsi que le groupe Perdu & Trouvé pour le répertoire complet.

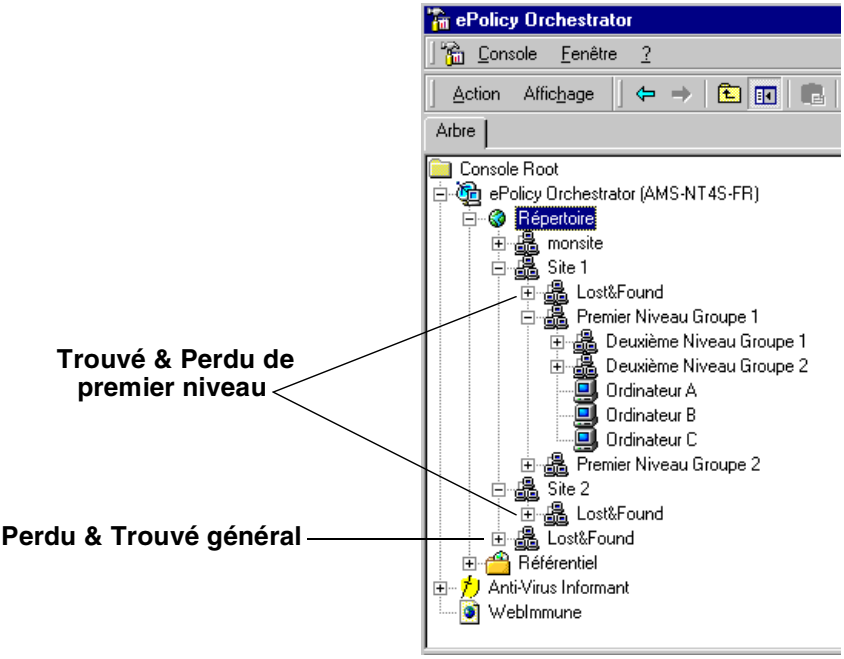


Figure 3-21. Arborescence de la console avec des groupes Perdu & Trouvé

Si vous supprimez un groupe, un ordinateur ou un utilisateur de l'arborescence de la console, mais que vous ne parvenez pas à supprimer le logiciel de l'agent de l'ordinateur client, l'agent réinitialise lors du prochain intervalle de communication agent-serveur et apparaît dans l'arborescence de la console dans un groupe Perdu & Trouvé ou à son emplacement d'origine. Si vous supprimez le logiciel de l'agent de l'arborescence de la console, vous devez également supprimer l'agent de l'ordinateur client.

Tri d'ordinateurs à l'aide de paramètres de gestion IP

Vous pouvez trier des ordinateurs en fonction de leur adresse IP dans le répertoire, en utilisant l'Assistant de tri des adresses IP. L'intégrité IP du répertoire doit être valide avant que l'Assistant puisse trier les ordinateurs.

L'assistant de tri des adresses IP utilise deux algorithmes de tri :

1. L'algorithme de tri non explicite, qui est l'option par défaut, effectue le tri de la façon suivante :

    a. Suivez les règles définies par l'algorithme de tri explicite, à moins que l'une des règles définies dans l'algorithme de tri non explicite soit prioritaire.

    b. Si l'ordinateur est un groupe pour lequel aucune plage IP n'est définie, mais que ce groupe se trouve sous un groupe qui correspond à la plage IP de l'ordinateur, laissez-le à l'endroit où il a été trouvé.

    c. Si un ordinateur se trouve sous un groupe qui est moins approprié qu'un autre groupe pour lequel une plage IP correcte est définie, l'ordinateur sera déplacé dans le groupe le plus approprié.

2. L'algorithme de tri explicite est une autre méthode de tri que vous pouvez activer en insérant une nouvelle clé dans le fichier CONSOLE.INI. L'algorithme de tri explicite effectue le tri de la façon suivante :

    a. L'adresse IP de l'ordinateur doit correspondre à la plage IP de son site parent. Si aucun site approprié n'est trouvé, l'ordinateur sera déplacé vers le site spécifié par l'utilisateur (par défaut, le groupe Perdu & Trouvé général).

    b. (Facultatif) — Si l'ordinateur appartient à un site, et qu'aucun autre groupe n'est valide sous ce site, un nouveau groupe doit être créé sous le groupe Perdu & Trouvé du site avant que l'ordinateur puisse être déplacé vers ce site. Le nouveau groupe doit être nommé après le domaine auquel appartient l'ordinateur. Seule l'option du fichier CONSOLE.INI permet d'activer cette fonctionnalité.

Pour activer l'algorithme de tri explicite, apportez les modifications suivantes au fichier CONSOLE.INI :

[Sorting]

UseExplicit=0

UseExplicit=0

L'option UseExplicitLostFound détermine la façon dont les systèmes qui doivent être déplacés vers le groupe Perdu & Trouvé et/ou un site sont traités. Si cette option est activée, les ordinateurs sont déplacés directement vers la racine du groupe Perdu & Trouvé ou du site. Si l'option UseExplicitLostFound n'est pas activée (valeur par défaut), et qu'un ordinateur doit être déplacé vers un site, l'ordinateur est déplacé vers le groupe Perdu & Trouvé au niveau du site. En outre, si un ordinateur doit être déplacé vers un groupe Perdu & Trouvé (y compris le déplacement explicite à partir du niveau du site), le domaine de l'ordinateur est créé en tant que groupe sous le groupe Perdu & Trouvé et l'ordinateur est déplacé sous le nouveau groupe Perdu & Trouvé/groupe de domaine.

Pour trier des ordinateurs en fonction de leur adresse IP :

1. Mettez en surbrillance **Répertoire** dans l'arborescence de la console, puis cliquez avec le bouton droit et sélectionnez **Toutes les tâches**, puis **Trier les ordinateurs en fonction de leur IP** afin de démarrer l'Assistant de tri des adresses IP.

2. Cliquez sur **Suivant** pour continuer.

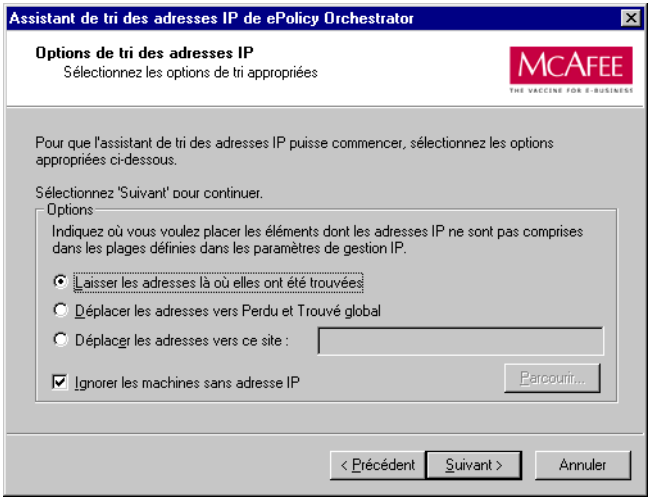


Figure 3-22. Assistant de tri des adresses IP

3. Spécifiez les options que vous souhaitez utiliser, puis cliquez sur **Suivant** pour continuer.

4. Observez l'avancement du tri par adresse IP, puis cliquez sur **Suivant** pour continuer.

5. Lorsque l'exécution de l'Assistant de tri des adresses IP est terminée, cliquez sur **Terminer**.

> **REMARQUE :** Si l'exécution de l'Assistant de tri des adresses IP n'aboutit pas, utilisez les « Contrôles d'intégrité d'adresse IP » à la page 69 pour vérifier la validité des paramètres de gestion IP.

Contrôles d'intégrité

La console fournit deux méthodes pour contrôler l'intégrité de la structure de votre répertoire ePolicy Orchestrator. Vous pouvez contrôler s'il y a des conflits concernant les noms d'éléments affichés dans le répertoire. Il est également possible de contrôler s'il existe des conflits ou des chevauchements dans les adresses IP de ces éléments. Accédez à ces options à partir du menu Toutes les tâches de la console.

Contrôles d'intégrité du répertoire

Un nom d'ordinateur ne peut exister que dans un seul endroit du répertoire.

Vous pouvez réaliser des contrôles d'intégrité pour vous assurer que chaque nom n'est associé qu'à un seul ordinateur de l'arborescence.

Pour effectuer un contrôle d'intégrité du répertoire :

1. Mettez en surbrillance **Répertoire** dans l'arborescence de la console, puis cliquez avec le bouton droit et placez le curseur sur **Toutes les tâches**, puis sélectionnez **Vérification de l'intégrité du répertoire** dans le sous-menu (Figure 3-23).

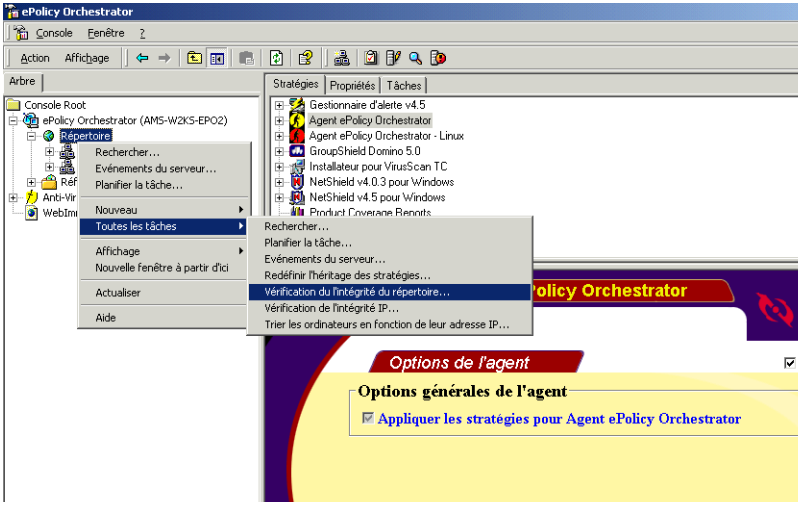


Figure 3-23. Console – menu Toutes les tâches

2. Cliquez sur **Rechercher** pour lancer le contrôle d'intégrité. S'il n'existe aucun conflit, le système vous renvoie le message correspondant. Les noms en double apparaissent dans le bas de la fenêtre sous Entrées en double trouvées.

3. Supprimez ou renommez tous les noms en double détectés :

   - **Pour supprimer un élément en double :**

     a. Double-cliquez sur l'entrée en double trouvée, puis affichez l'emplacement des doublons afin de déterminer quelle entrée en double vous souhaitez supprimer.

     b. Mettez en surbrillance le doublon dans le répertoire, cliquez avec le bouton droit de la souris, puis sélectionnez **Supprimer**.

     c. Cliquez sur **Oui** dans la zone de message lorsqu'elle vous invite à confirmer votre choix.

   - **Pour renommer un élément en double :**

     a. Double-cliquez sur l'entrée en double trouvée, puis affichez l'emplacement des doublons afin de déterminer quelle entrée en double vous souhaitez renommer.

     b. Mettez en surbrillance le doublon dans le répertoire, cliquez avec le bouton droit de la souris, puis sélectionnez **Renommer**.

     c. Saisissez un nouveau nom pour l'ordinateur sélectionné.

4. Lorsque vous avez renommé ou supprimé tous les éléments en double, cliquez sur **Fermer**.

Contrôles d'intégrité d'adresse IP

Les adresses IP en double ne sont pas autorisées à l'intérieur d'un site du répertoire. Pour déterminer si vous possédez des plages d'adresses IP en double ou des masques de sous-réseau IP se chevauchant, effectuez un contrôle d'intégrité des adresses IP. Si ce contrôle révèle un conflit d'adresses IP entre les groupes, examinez les conflits puis résolvez-les à l'aide des options affichées dans le volet Détails sous Gestion du sous-réseau IP.

AVERTISSEMENT : Les administrateurs de site ne peuvent voir que le site sur lequel ils possèdent des droits. Il peut exister des conflits entre des sites qui ne sont pas visibles pour les administrateurs de site.

Contrôle d'intégrité d'adresse IP

Exécutez cette procédure pour déterminer si le répertoire contient des plages d'adresses IP en double ou des masques de sous-réseau IP se chevauchant. Nous vous recommandons d'effectuer un contrôle d'intégrité des adresses IP après avoir réorganisé les éléments du répertoire.

Pour effectuer un contrôle d'intégrité des adresses IP :

1. Mettez en surbrillance **Répertoire** dans l'arborescence de la console, puis cliquez avec le bouton droit, placez le curseur sur **Toutes les tâches**, et sélectionnez **Vérification de l'intégrité IP** dans le sous-menu (Figure 3-24).

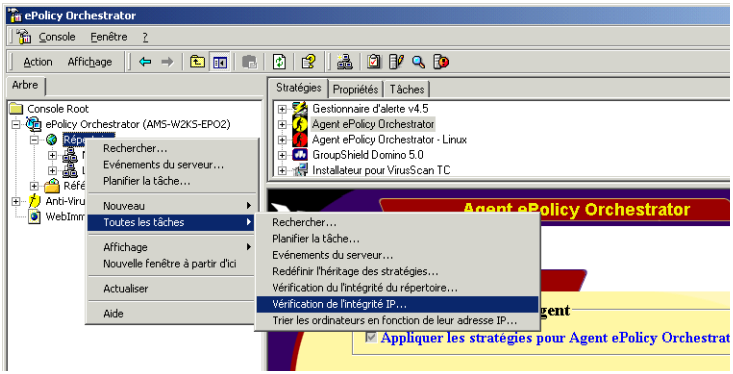


Figure 3-24. Console – menu Toutes les tâches

2. Cliquez sur **Démarrer** pour contrôler automatiquement l'intégrité des adresses IP.

   - S'il n'existe aucun conflit, le système vous envoie le message correspondant.
   - S'il existe un conflit d'adresses IP, le système fournit des descriptions des conflits dans le tableau de la fenêtre (Figure 3-25 à la page 71).

Deux types de conflits peuvent se produire : les conflits de *chevauchement* et les conflits de *sous-ensemble*.

- **Le conflit de chevauchement d'adresse IP** survient lorsque les adresses IP ou les masques de sous-réseau de deux groupes partagent une partie, mais pas la totalité, de leur plage d'adresses IP.
- **Le conflit de sous-ensemble d'adresse IP** survient lorsque la totalité des adresses IP ou du masque de sous-réseau d'un groupe risque de se trouver dans la plage d'adresses IP du second groupe. Le deuxième groupe peut avoir plus d'adresses IP que la plage du premier groupe, mais l'ensemble de la plage d'adresses IP (ou masque de sous-réseau) d'un groupe est contenu dans l'autre groupe.

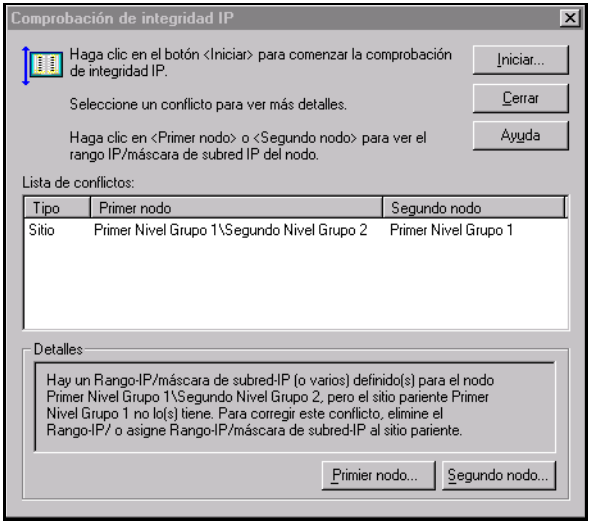


Figure 3-25. Contrôler l'intégrité IP, affichage des conflits

Etude d'un conflit IP

Suivez les étapes suivantes lorsqu'un contrôle d'intégrité IP détecte des conflits.

Pour étudier les conflits IP :

1. Consultez la liste des conflits dans la fenêtre Contrôler l'intégrité IP.
2. Cliquez sur l'étiquette **Type** pour mettre en surbrillance le conflit et activez les boutons en bas de la fenêtre.
3. Cliquez sur **Premier noeud...** pour afficher la plage d'adresses IP ou le masque de sous-réseau pour la première plage ; cliquez sur **Deuxième noeud...** pour afficher la plage d'adresses IP ou le masque de sous-réseau pour la deuxième plage.

   Ces informations sont affichées sur le volet Détails de la console dans la fenêtre Gestion de sous-réseau IP (Figure 3-26).

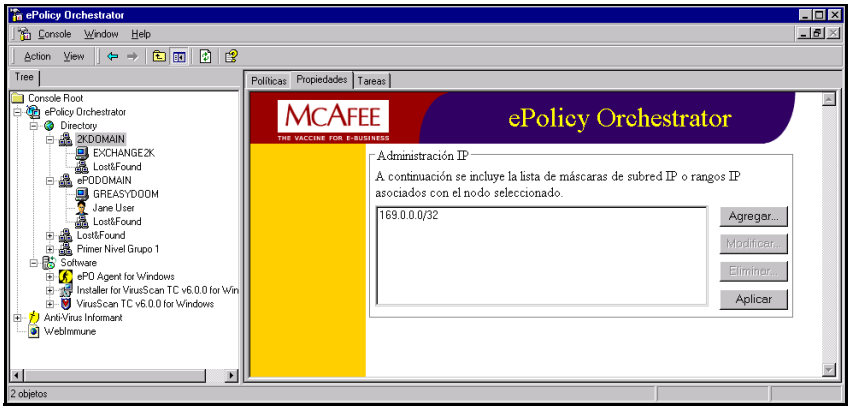


Figure 3-26. Affichage de la gestion de sous-réseau IP dans la console

Résolution d'un conflit IP

Sélectionnez la méthode de résolution du conflit. Le volet Détails vous offre les options pour ajouter, modifier ou supprimer l'adresse conflictuelle.

Pour ajouter une gamme ou un masque de sous-réseau :

1. Affichez la fenêtre **Gestion du sous-réseau IP** dans le volet Détails
2. Cliquez sur **Ajouter…** pour ouvrir la fenêtre Gestion IP qui affiche les données en conflit dans la zone appropriée.

   Vous pouvez ajouter un masque de sous-réseau IP ou une plage d'adresses IP.
3. Complétez les valeurs pour un masque de sous-réseau ou une gamme IP qui n'apparaît nulle part ailleurs dans le répertoire.
4. Cliquez sur **OK** pour fermer la fenêtre Gestion IP.
5. Cliquez sur **Appliquer** pour appliquer ces nouvelles valeurs au groupe désigné.
6. Effectuez un autre contrôle d'intégrité IP pour déterminer si le problème a été résolu. Pour ce faire, répétez les étapes de la section « Contrôle d'intégrité d'adresse IP » à la page 70.

Pour modifier une gamme ou un masque de sous-réseau :

1. Affichez la fenêtre **Gestion du sous-réseau IP** dans le volet Détails
2. Sélectionnez l'adresse souhaitée et cliquez sur **Modifier…** pour ouvrir la fenêtre Page Web d'ePolicy Orchestrator qui affiche les données en conflit dans la zone appropriée (Figure 3-27 à la page 74).

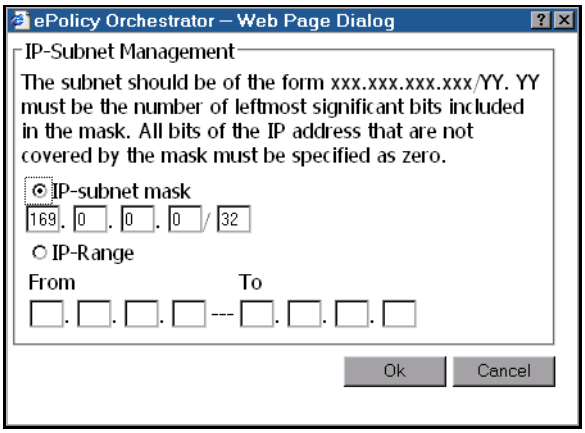


Figure 3-27. Fenêtre Page Web d'ePolicy Orchestrator

Vous pouvez modifier un masque de sous-réseau IP ou une plage d'adresses IP.

3. Complétez les valeurs pour un masque de sous-réseau ou une gamme IP qui n'apparaît nulle part ailleurs dans le répertoire.
4. Cliquez sur **OK** pour fermer la fenêtre Gestion du sous-réseau IP.
5. Cliquez sur **Appliquer** pour appliquer les valeurs modifiées au groupe désigné.
6. Effectuez un autre contrôle d'intégrité IP pour déterminer si le problème a été résolu. Pour ce faire, répétez les étapes de la section « Contrôle d'intégrité d'adresse IP » à la page 70.

Pour supprimer une gamme ou un masque de sous-réseau :

1. Affichez la fenêtre **Gestion du sous-réseau IP** dans le volet Détails.
2. Sélectionnez l'adresse souhaitée et cliquez sur **Supprimer...** pour supprimer l'entrée mise en surbrillance.
3. Cliquez sur **Appliquer**.
4. Effectuez un autre contrôle d'intégrité IP pour déterminer si le problème a été résolu. Pour ce faire, répétez les étapes de la section « Contrôle d'intégrité d'adresse IP » à la page 70.

Mise à jour des domaines

La fonction Mettre à jour les domaine règle votre domaine (site) importé de l'arborescence de la console pour correspondre à votre structure de domaine Windows NT. *Si* vous complétez l'arborescence de votre console avec un domaine et *si* vous conservez la structure du domaine importé, vous pouvez mettre à jour la structure du domaine à l'aide de cette fonction. Si vous modifiez un domaine importé dans ePolicy Orchestrator, puis utilisez cette fonction, vous perdez les modifications que vous avez apportées à l'arborescence de la console. Vous devez réorganiser manuellement votre site sur l'arborescence de la console selon vos besoins.

Pour mettre à jour un site avec des informations actuelles sur le domaine :

1. Mettez en surbrillance le site ou le groupe à mettre à jour dans l'arborescence de la console, puis cliquez avec le bouton droit, placez le curseur sur **Toutes les tâches** et sélectionnez **Mettre à jour le domaine** dans le sous-menu (Figure 3-28).

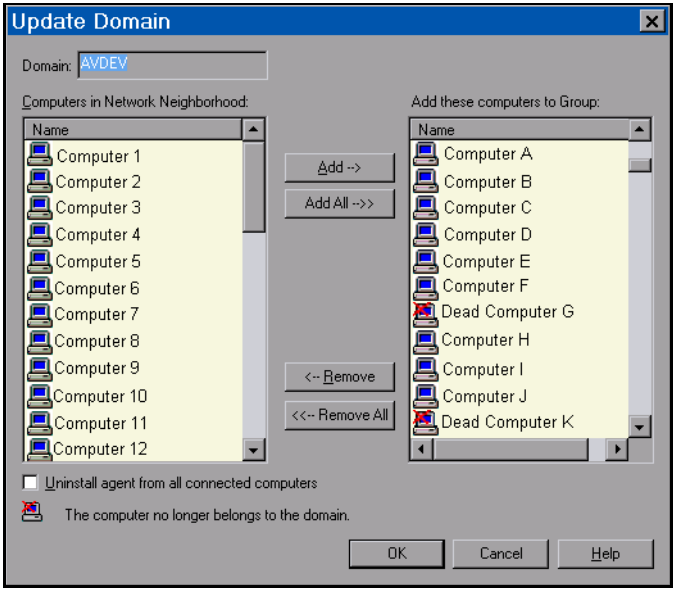


Figure 3-28. Mettre à jour le domaine

2. Pour ajouter des ordinateurs au site, sélectionnez-les dans la liste sous Ordinateurs dans Voisinage réseau, puis cliquez sur **Ajouter->**. Cette opération déplace les ordinateurs sélectionnés dans la liste des groupes à droite. Vous pouvez cliquer sur **Ajouter tous->** pour ajouter tous les ordinateurs du domaine au groupe.

   Tous les ordinateurs du site sélectionné qui ne correspondent pas à un ordinateur dans la liste Voisinage réseau s'affichent comme n'appartenant plus au domaine. Il peut s'agir d'ordinateurs que vous avez ajoutés au site après avoir importé le domaine pour les gérer avec le site, ou d'ordinateurs qui n'appartiennent plus au domaine dans le réseau.

3. Pour supprimer des ordinateurs du site ou du groupe, sélectionnez-les dans la liste située sous Ajouter ces ordinateurs à la liste des groupes, puis cliquez sur **<-Supprimer**. Cette opération supprime les ordinateurs sélectionnés de la liste des ordinateurs et les place dans la liste située à gauche. Vous pouvez cliquer sur **Supprimer tout->** pour supprimer tous les ordinateurs du groupe.

4. Pour supprimer les fichiers de l'agent d'un ordinateur que vous souhaitez supprimer du site, sélectionnez **Désinstaller l'agent de tous les ordinateurs connectés**.

5. Une fois la mise à jour du domaine terminée, cliquez sur **OK**.

Gestion de comptes

Présentation

Le produit ePolicy Orchestrator permet à l'administrateur du système de désigner différents administrateurs de site qui gèreront un plus petit nombre de systèmes, disposés par groupes dans l'arborescence de la console. En outre, ceux qui ont besoin de réviser les performances de la protection anti-virus de votre entreprise via ePolicy Orchestrator peuvent utiliser une console distante, avec des privilèges d'affichage uniquement. Ces réviseurs peuvent avoir un accès global pour afficher l'installation complète ou l'accès complet au site afin de visualiser l'opération pour un site spécifique.

Gestion du site

Une installation unique de ePolicy Orchestrator pour une entreprise peut comporter plusieurs sites. Ces sites ou groupements peuvent être physiques (différentes villes) ou logiques (différents services au même endroit). Chaque site peut comporter un administrateur qui applique la stratégie et définit des tâches pour ce seul emplacement.

Ces sites apparaissent sous forme de groupes dans l'arborescence de la console. Alors que l'installation ne comporte qu'un seul répertoire, l'administrateur général crée des groupes pour refléter les sites abordés dans ce chapitre. En général, ce manuel fait référence aux sites comme à des groupes de premier niveau dans l'arborescence de la console.

Pour faciliter l'administration, ce manuel différencie les niveaux globaux et de site à l'intérieur de l'arborescence de la console.

Global

Les actions prises au niveau global affectent la totalité des noeuds de l'arborescence de la console. En cas d'apparition de virus, vous pourriez souhaiter appliquer *globalement* une analyse à la demande pour rechercher et stopper automatiquement le virus.

Site

Les actions prises au niveau du site affectent la totalité des noeuds au niveau du site dans l'arborescence de la console. Ils affectent également la totalité des enfants de premier niveau au niveau du site.

Types de comptes

Il existe quatre types de comptes distincts dans le produit ePolicy Orchestrator : administrateurs généraux, réviseurs généraux, administrateurs de site et réviseurs de site. Les deux comptes d'administrateur offrent des possibilités de mise à jour et les deux comptes de réviseur offrent un accès en lecture seule. Les comptes de réviseur permettent aux autres employés d'afficher les performances de votre entreprise sans pour autant autoriser les modifications du système.

Administrateurs généraux

Les administrateurs généraux disposent de droits d'accès complets et d'un accès complet aux fonctions d'ePolicy Orchestrator. Ils peuvent effectuer les tâches suivantes dans toute l'entreprise :

- Affecter les comptes appropriés à tous les utilisateurs du système.
- Compléter l'arborescence de la console avec des groupes, des ordinateurs et des utilisateurs.
- Créer des arborescences et ajouter des noeuds.
- Mettre à jour des paramètres du serveur.
- Installer et supprimer un logiciel dans le référentiel.
- Pousser des installations d'agent sur tous les ordinateurs.
- Effectuer un glisser-déplacer de l'administration du site à travers tous les sites.
- Créer et appeler des tâches.
- Appliquer des stratégies.
- Ajouter des nouveaux comptes.
- Affecter des droits de compte.
- Modifier la configuration du serveur.
- Exécuter tous les rapports Anti-Virus Informant.
- Glisser-déplacer les éléments à travers les groupes.
- Déplacer les ordinateurs du groupe Perdu & Trouvé général dans un des groupes de premier niveau ou dans les groupes Perdu & Trouvé de premier niveau.
- Ajouter et supprimer les groupes de premier niveau.

Tous les administrateurs d'ePolicy Orchestrator version 1.x deviennent automatiquement des administrateurs généraux lorsque le produit est mis à niveau vers la version 2.0.

Tâches privilégiées pour les administrateurs généraux

Les tâches privilégiées ne sont disponibles que pour les administrateurs généraux. Ces tâches affectent toute l'installation, à tous les niveaux de noeuds.

- Installer des progiciels dans le référentiel ePolicy Orchestrator.
- Modifier des masques de sous-réseau IP au niveau du site.
- Créer des rapports Anti-Virus Informant à l'échelle de l'entreprise.
- Administrer les comptes.
- Ajouter ou supprimer des comptes.
- Administrer des groupes de premier niveau.
- Ajouter eu supprimer des groupes de premier niveau.

Réviseurs généraux

Les réviseurs généraux disposent d'un accès en lecture seule pour la totalité des paramètres d'ePolicy Orchestrator à travers l'entreprise. Un réviseur général peut afficher tous les éléments du système mais ne peut en modifier aucun. Ce compte est géré par l'administrateur général. Une entreprise peut comprendre un nombre illimité de réviseurs généraux.

Administrateurs de site

Un administrateur de site dispose d'un accès en lecture et écriture pour la totalité des logiciels d'ePolicy Orchestrator pour un site ou un groupe de premier niveau donné. Les droits d'accès incluent des groupes de premier niveau et leurs enfants de premier niveau. Les administrateurs de site disposent d'un accès complet à leurs sites spécifiés pour exécuter les tâches suivantes :

- Modifier des stratégies.
- Définir des stratégies de déploiement de logiciels.
- Ajouter, supprimer ou modifier des tâches.
- Ajouter ou supprimer des ordinateurs sur leur site.
- Pousser des installations d'agent sur les ordinateurs de leur site.

- Modifier des masques de sous-réseau IP au niveau du groupe pour leur site.
- Exécuter les rapports Anti-Virus Informant pour leur site.
- Déplacer des noeuds hors du groupe Perdu & Trouvé pour leur groupe de premier niveau vers les groupes de second niveau dans leurs groupes de premier niveau.

Les administrateurs de site ne peuvent pas :

- Modifier les configurations du serveur.
- Administrer les comptes.
- Installez les progiciels sur le serveur ePolicy Orchestrator.
- Modifier des masques de sous-réseau IP au niveau du répertoire ou au niveau global.

Réviseurs de site

Les réviseurs de site dispose d'un accès en lecture seule pour les paramètres d'installation d'ePolicy Orchestrator sur leur site. Ce site est représenté comme un groupe de premier niveau sur l'arborescence de la console. Un réviseur de site peut afficher les stratégies et les tâches pour son site ePolicy Orchestrator mais ne peut en modifier aucune. Ce compte est géré par l'administrateur général. Un groupe de premier niveau peut comprendre un nombre illimité de réviseurs de site.

Création et gestion de comptes

Dans cette section, vous apprendrez comment créer et gérer des comptes d'administrateur et de réviseur pour ePolicy Orchestrator. L'interface qui offre cette fonction est la fenêtre Gérer les administrateurs, à laquelle vous pouvez accéder depuis la console.

Accès à la fenêtre Gérer les administrateurs

La fenêtre Gérer les administrateurs permet à tout administrateur général d'ajouter, de supprimer ou de configurer des comptes, et de modifier des mots de passe pour d'autres utilisateurs. Chaque utilisateur peut modifier son propre mot de passe. Pour plus d'informations sur la distinction qui existe entre un administrateur général et d'autres rôles, consultez « Types de comptes » à la page 77.

REMARQUE : Les références citées dans ce manuel et qui se rapportent aux administrateurs généraux concernent les administrateurs de la console à proprement parler.

1. Connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur général.
2. Mettez en surbrillance **ePolicy Orchestrator** dans l'arborescence de la console.
3. Sélectionnez **Gérer les administrateurs** pour ouvrir la fenêtre Gérer les administrateurs (Figure 3-29).

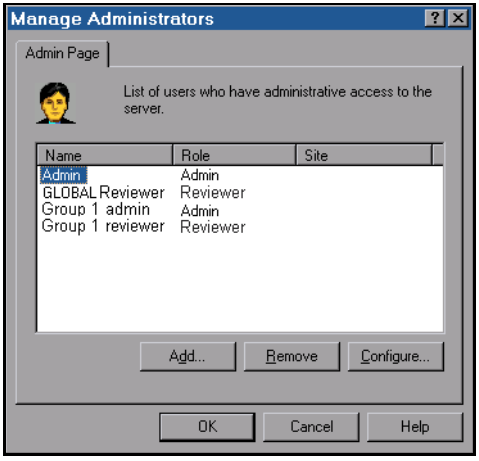


Figure 3-29. Gérer les administrateurs

Ajout de comptes

Cette procédure vous permet d'ajouter de nouveaux comptes. Seul un administrateur général peut effectuer cette tâche.

1. Si ce n'est pas déjà fait, connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur général et ouvrez la fenêtre **Gérer les administrateurs** dans le volet Détails de la console.
2. Cliquez sur **Ajouter...** pour ouvrir la fenêtre Ajouter un administrateur (Figure 3-30).

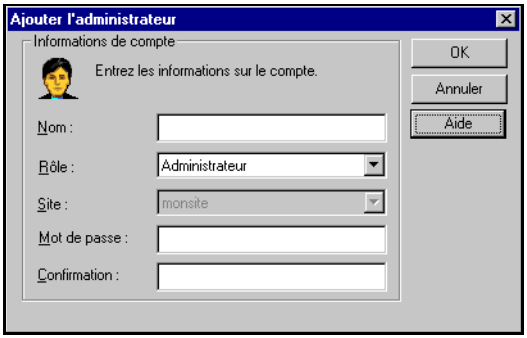


Figure 3-30. Ajouter un administrateur

3. Entrez le **nom** du nouvel utilisateur.
4. Sélectionnez l'un des quatre types de comptes dans la liste déroulante **Rôle** :

Administrateur (*général*) **Réviseur** (*général*)	Droits sur le répertoire complet
***Administrateur de site** ***Réviseur de site**	Droits sur un seul site spécifié

* Indisponible jusqu'à ce que vous ayez créé un site. Pour créer un site, consultez « Compléter le répertoire » à la page 36.

REMARQUE : Les administrateurs disposent de droits d'accès complets pour le répertoire complet (administrateur) ou pour leurs sites désignés (administrateur de site). Un réviseur peut uniquement voir le répertoire complet (réviseur) ou les sites pour lesquels il dispose de droits de lecture (réviseur de site). Pour plus d'informations sur les rôles, consultez « Types de comptes » à la page 77.

- Si le nouveau compte est un compte *général* (droits sur l'installation complète), passez à l'Etape 6.
- Si le nouveau compte est un compte *au niveau du site* (droits sur un seul site spécifié), la liste déroulante Site est activée et inclut la totalité des groupes au niveau du répertoire affichés dans l'arborescence de la console. Passez à l'Etape 5.

5. Sélectionnez un site parmi les options disponibles dans la liste déroulante **Site**. Vous ne pouvez sélectionner qu'un seul site par compte.
6. Entrez un mot de passe et confirmez-le.
7. Cliquez sur **OK** pour revenir à la fenêtre Gérer les administrateurs. Le nouveau compte apparaît sur la liste avec son rôle désigné.
8. Pour ajouter d'autres comptes, répétez cette procédure de l'Etape 2 à l'Etape 7.
9. Cliquez sur **OK** pour revenir à la console. Le nouvel utilisateur peut maintenant se connecter.

Suppression de comptes

Cette procédure vous permet de supprimer des comptes existants. Seul un administrateur général peut effectuer cette tâche.

1. Si ce n'est pas déjà fait, connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur général et ouvrez la fenêtre **Gérer les administrateurs** dans le volet Détails de la console.
2. Sélectionnez le compte que vous voulez supprimer.
3. Cliquez sur **Supprimer**. Si le nom de compte est supprimé, le rôle n'existe plus.
4. Cliquez sur **OK** pour revenir à la console.

Configuration des informations sur le compte

Les administrateurs généraux peuvent modifier les droits d'un utilisateur spécifique. Ces droits incluent la modification des types d'utilisateurs (tels que l'administrateur de site, le réviseur de site, l'administrateur général, etc.), la modification du site auquel ils sont associés (pour les utilisateurs de site) et les modification des mots de passe des utilisateurs. Tous les détenteurs de compte peuvent modifier leur propre mot de passe.

1. Si ce n'est pas déjà fait, connectez-vous au serveur ePolicy Orchestrator en tant qu'administrateur général et ouvrez la fenêtre **Gérer les administrateurs** dans le volet Détails de la console (Figure 3-31).
2. Sélectionnez le compte que vous voulez configurer.
3. Cliquez sur **Configurer...** pour ouvrir la fenêtre Modifier les informations sur le compte.

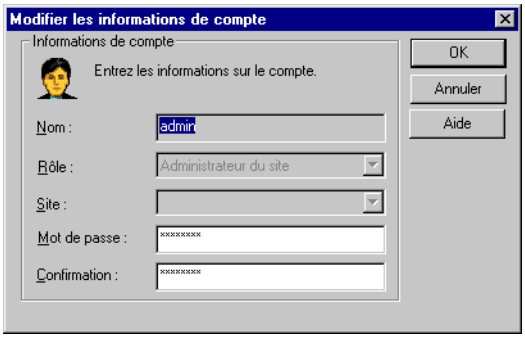


Figure 3-31. Fenêtre Modifier les informations sur le compte

4. Entrez un mot de passe et confirmez-le.
5. Cliquez sur **OK** pour revenir à la boîte de dialogue Gérer les administrateurs.
6. Cliquez sur **OK** pour revenir à la console.

L’agent

Présentation

L'agent ePolicy Orchestrator est un programme logiciel qui s'exécute sur les ordinateurs client (également appelés hôtes d'agent). Les fonctions de l'agent comprennent l'installation automatique, la collecte des informations relatives aux événements et aux propriétés, l'application de la stratégie, la communication des statuts, la gestion des clés publiques, l'exécution des tâches planifiées et l'installation des produits.

L'agent s'installe et s'exécute en arrière-plan, sans que les utilisateurs le voient. Il travaille avec le serveur ePolicy Orchestrator pour surveiller l'activité éventuelle des virus sur le réseau, installer le logiciel anti-virus et faire respecter les stratégies concernant le logiciel qui ont été configurées à l'aide de la console.

Après avoir installé l'agent avec succès, retournez au chapitre 4, « Déploiement du logiciel », pour installer les produits logiciels anti-virus et au chapitre 5, « Gestion du logiciel anti-virus McAfee », afin d'utiliser l'agent pour créer et faire respecter la stratégie de votre société en matière de défense contre les virus dans l'ensemble de l'entreprise. Pour afficher l'activité de l'agent sur l'ordinateur installé, vous pouvez utiliser l'interface Agent Monitor. Pour plus d'informations, reportez-vous au chapitre 9, « Utilitaires et outils », page 201.

Fonctions de l’agent

L'agent d'ePolicy Orchestrator s'exécute de façon transparente sur les ordinateurs client de votre réseau. Après l'installation, l'agent recueille alors les propriétés de l'ordinateur et les transmet au serveur. Il informe également le serveur de tout événement ou activité concernant des virus éventuels et installe le logiciel anti-virus McAfee sur l'ordinateur. Il exécute les tâches programmées via la console. Ce sommaire indique plusieurs fonctions utiles de l'agent ePolicy Orchestrator.

Installation facile

Vous pouvez déployer l'agent via différents canaux, depuis la technologie « push » jusqu'aux disquettes diffusées manuellement. Vous devez installer l'agent après que le programme ePolicy Orchestrator a été installé sur le serveur et configuré par l'intermédiaire de la console. L'administrateur dirige la diffusion de l'agent de la manière la plus appropriée au réseau.

Collecte de propriétés et création de rapport sur les propriétés

Après l'interrogation initiale, l'agent ePolicy Orchestrator contrôle l'installation du logiciel anti-virus McAfee et son état d'activité et collecte les propriétés générales du système sur son ordinateur hôte. Ces informations sont utiles pour la planification de stratégies anti-virus complètes. Une fois les données rassemblées, l'agent les transmet au serveur au cours de la seconde transmission de retour vers ce dernier. Le serveur enregistre ces informations dans la base de données d'ePolicy Orchestrator pour permettre à l'administrateur de les utiliser dans ses rapports sur le réseau ou sur son ordinateur.

L'administrateur utilise la console pour définir la fréquence de la collecte des informations sur les propriétés et l'émission de rapports.

Déploiement de logiciels anti-virus

Une des fonctions les plus utiles de l'agent est sa capacité à déterminer le statut du logiciel anti-virus McAfee sur son hôte et à demander l'installation du logiciel au serveur ePolicy Orchestrator. Après avoir interrogé le serveur et recueilli en retour les propriétés de l'hôte et le statut du logiciel anti-virus, l'agent peut demander l'installation de la dernière version du logiciel anti-virus ou bien des mises à jour. L'agent informe également le serveur du succès de l'installation du logiciel. Le chapitre 4, « Déploiement du logiciel », fournit des détails sur le processus de déploiement.

Application de stratégies

L'agent applique immédiatement la stratégie dès qu'il la recueille du serveur. Les stratégies peuvent être définies dans le volet de détail (côté droit) de la console pour chaque produit logiciel anti-virus. Voir « Gestion de stratégie » à la page 120.

Exécution de tâches programmées

L'agent exécute toutes les instructions transmises à partir du serveur, d'après le programme établi par l'administrateur. Les tâches sont planifiées à partir des menus de l'arborescence de la console. Voir « Planification de tâches » à la page 123.

Héritage

L'option **Hériter** peut être utilisée pour appliquer les tâches et stratégies du niveau sélectionné à tous les niveaux inférieurs.

Si la case **Hériter** est activée sur une fenêtre de stratégie (le volet inférieur des détails de la console) pour le noeud courant, le noeud prend la valeur du noeud parent. Lorsque la case **Hériter** est activée, tous les champs de la page sont désactivés.

Si la case **Hériter** est désactivée, le noeud prend les valeurs définies dans l'écran de stratégie affiché. Si la case **Hériter** n'est pas activée, tous les champs de la page sont activés.

Déploiement de l'agent

Le déploiement de l'agent se compose de trois actions différentes :

- Installer et/ou personnaliser le fichier d'installation de l'agent (POAGINST.EXE).
- Configurer les options de l'agent.
- Installer l'agent sur les ordinateurs réseau à l'aide de méthodes diverses.
- Une fois l'installation terminée, l'agent contacte le serveur.
  - Dans ce contact initial, l'agent communique sa seule étiquette d'identification et transmet immédiatement les propriétés qu'il collecte sur son ordinateur hôte, y compris les installations logicielles anti-virus McAfee actuelles.
  - L'agent extrait ensuite toutes les tâches stockées par le serveur à son intention. Cela peut inclure une installation logicielle, une autre collection de propriétés ou d'événements ou des stratégies à appliquer sur l'ordinateur client.

  A la fin de cette période de communication initiale, l'agent est entièrement déployé.

Installer et personnaliser le fichier d'installation de l'agent

Le fichier d'installation de l'agent (POAGINST.EXE) est utilisé pour installer l'agent.

Vous pouvez installer le fichier d'installation de l'agent à partir de la console ePolicy Orchestrator, ou le copier et le coller à partir de n'importe quel emplacement. Si vous l'installez à partir de la console ePolicy Orchestrator, vous pouvez également intégrer les références de l'utilisateur dans le fichier d'installation.

Installation et personnalisation du fichier POAGINST.EXE à partir de la console

Vous pouvez créer un fichier d'installation de l'agent (POAGINST.EXE) personnalisé à partir de la console ePolicy Orchestrator et l'installer à partir de n'importe quel emplacement. La personnalisation de ce fichier permet à tout utilisateur d'intégrer des références d'utilisateur dans le fichier d'installation, puis d'installer l'agent en utilisant les informations de connexion intégrées. Les utilisateurs peuvent ainsi installer l'agent quelles que soient les autorisations dont ils disposent.

Pour installer ou personnaliser le fichier d'installation de l'agent :

1. Cliquez avec le bouton droit sur **ePolicy Orchestrator** dans la console, sélectionnez **Toutes les tâches**, puis sélectionnez **Personnaliser le progiciel de l'agent** pour ouvrir l'Assistant de configuration de l'agent.
2. Cliquez sur **Suivant**.
3. Entrez le nom d'utilisateur et le mot de passe, puis confirmer le mot de passe spécifié pour les informations de connexion que vous souhaitez intégrer dans le progiciel d'installation de l'agent.
4. Cliquez sur **Suivant**.
5. Cliquez sur **Parcourir** pour ouvrir la fenêtre de recherche et sélectionnez le chemin d'accès de l'emplacement où vous souhaitez enregistrer le fichier d'installation de l'agent.
6. Cliquez sur **Suivant** pour créer le fichier d'installation de l'agent (POAGINST.EXE) personnalisé.
7. Cliquez sur **Suivant**, puis sur **Terminer**.

Copie et collage du fichier POAGINST.EXE

Vous pouvez installer manuellement le fichier d'installation de l'agent (POAGINST.EXE) en le copier et en le collant à l'emplacement souhaité.

Pour copier et coller le fichier d'installation de l'agent :

1. Copiez le fichier **POAGINST.EXE** à partir de l'emplacement d'installation d'ePolicy Orchestrator, puis collez-le à l'emplacement souhaité. Si vous l'avez installé dans son emplacement par défaut, vous le trouverez dans le chemin suivant :

   C:\Program Files\McAfee\ePO\2.0\DB\Software\ePOAgent2000\2.0.0.XXX\0409\Installfiles

   Contrôlez toujours la date de création de ce fichier avant de l'utiliser car le serveur crée un nouveau fichier d'installation de l'agent chaque fois qu'il met à jour sa configuration.

Configurer les options de l'agent

La *stratégie* pour l'agent, qui englobe les différentes options de l'agent, détermine le comportement de l'agent après l'installation. Vous pouvez configurer des options pour l'agent avant son installation ou installer l'agent avec les paramètres par défaut et modifier ces paramètres après l'installation. McAfee vous recommande de configurer les options de l'agent avant d'installer l'agent.

Si vous installez l'agent avec les options par défaut et que vous modifiez ensuite ces paramètres, vous devez attendre qu'un processus de communication agent à serveur complet soit achevé pour que les nouvelles stratégies soient appliquées.

Pour configurer les options de l'agent :

1. Sélectionnez l'élément (site, groupe ou ordinateur) du répertoire dans lequel vous souhaitez installer l'agent.

2. Sélectionnez l'onglet **Stratégies** dans le volet supérieur des détails de la console, puis mettez en surbrillance **Configuration** sous l'**agent ePolicy Orchestrator**. (Figure 3-32).

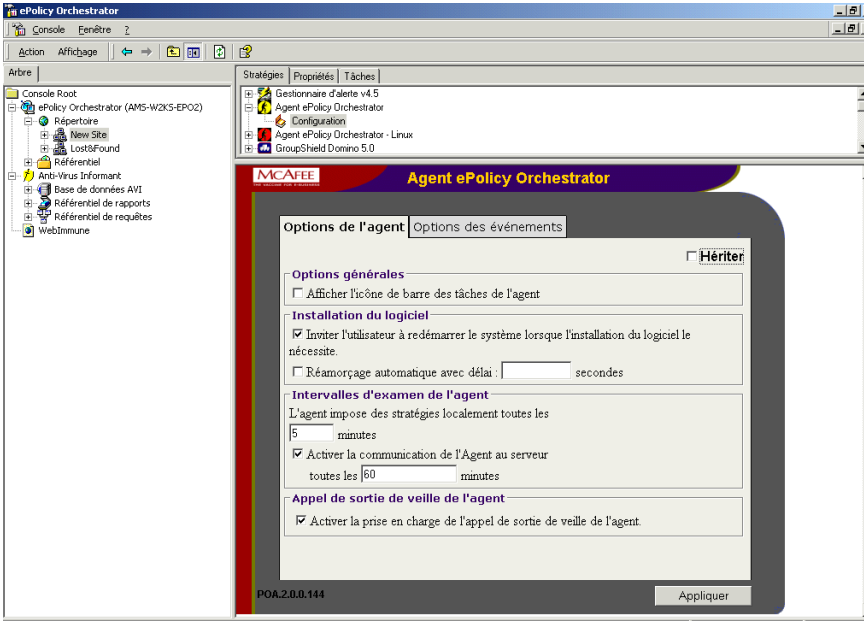


Figure 3-32. Console – Configuration de l'agent

3. Sélectionnez l'onglet **Options de l'agent** et désélectionnez **Hériter** pour activer les options de cette page.

4. Dans la zone Options générales, sélectionnez **Afficher l'icône d'état de l'agent** si vous voulez que l'icône de l'agent apparaisse dans la barre des tâches de l'ordinateur client. Cette fonction est particulièrement utile si vous suivez le comportement d'agent sur les ordinateurs client.

5. Dans la zone d'installation du logiciel, vous pouvez sélectionner une option ou les deux. Dans certains cas, l'ordinateur client peut devoir redémarrer pour terminer l'installation du logiciel anti-virus que vous avez demandée. Plus ce redémarrage est effectué rapidement (lorsqu'il est nécessaire), plus vite l'installation sera terminée. Consultez les guides de configuration de vos logiciels anti-virus pour déterminer si l'installation nécessite un redémarrage.

    - Sélectionnez **Interroger l'utilisateur lorsque l'installation nécessite un redémarrage** pour que l'agent affiche le message correspondant à l'attention de l'utilisateur.
    - Sélectionnez **Redémarrage automatique avec un délai de X secondes** pour que, le cas échéant, l'ordinateur client redémarre indépendamment de l'action de l'utilisateur sur l'ordinateur à ce moment-là.
    - Désélectionnez les deux options, si l'installation du logiciel peut être terminée lorsque l'utilisateur décide de redémarrer au cours d'opérations classiques.

6. Dans la zone Intervalles de communication de l'agent, vous pouvez modifier l'une ou l'autre des options, ou les deux options, ou bien garder les valeurs par défaut.

    - La valeur par défaut de **Intervalle d'application de stratégies toutes les X minutes** est de 5 minutes. Vous pouvez modifier cet intervalle pour l'adapter à vos besoins de bande passante et à l'urgence de la collection vos propriétés. N'oubliez pas que la réduction de l'intervalle entraîne l'augmentation de la quantité de bande passante utilisée.
    - La valeur par défaut de l'option **Activer l'intervalle de communication agent à serveur toutes les X minutes** est 60 minutes. Vous pouvez modifier cet intervalle pour l'adapter à vos besoins de bande passante. Il se peut que vous souhaitiez réduire l'intervalle lors de l'apparition de virus. Définissez cette valeur à 0 pour désactiver cette fonction.

7. Dans la zone Appel de réveil de l'agent, vous pouvez sélectionner **Activer la prise en charge de l'appel de réveil de l'agent** pour permettre au serveur d'appeler l'agent lorsque vous voulez que l'agent demande immédiatement des stratégies au serveur. Cette fonction doit être activée dans ce volet pour que l'appel de réveil de l'agent fonctionne. Elle indique à l'agent de se tenir à l'écoute d'un appel de réveil, ce qui est particulièrement important pour le traitement en cas d'apparition de virus.

   Pour envoyer un appel de réveil une fois que tous vos agents ont reçu cette stratégie, consultez « Appel de réveil de l'agent » à la page 109. Pour plus d'informations sur la gestion des infections virales, consultez « Traitement des apparitions de virus » à la page 231.

Méthodes d'installation

Il existe plusieurs façons d'installer l'agent sur des ordinateurs client. façons : Des informations détaillées sur chaque méthode d'installation sont fournies ci-après.

Installation push

Vous pouvez utiliser la technologie push pour déployer l'agent. L'administrateur définit les stratégies à suivre pour l'agent à partir de la console. Ensuite, avec des droits d'administrateur de domaine, l'administrateur déploie l'agent sur les ordinateurs client de façon organisée, en considérant les contraintes dues à la bande passante de votre réseau.

Pour effectuer une installation push, l'administrateur doit sélectionner un ou plusieurs ordinateurs ou groupes pour la diffusion de l'agent. Ce groupe d'ordinateurs peut être importé directement à partir d'un domaine Windows NT ou d'un fichier correctement structuré (pour plus d'informations, voir « Compléter le répertoire » à la page 36). Si c'est un groupe qui est choisi, le progiciel d'installation de l'agent est envoyé à tous les ordinateurs du groupe sélectionné à condition que le client se trouve dans le domaine du serveur ePolicy Orchestrator. Si c'est un ordinateur qui est choisi, le progiciel d'installation de l'agent est envoyé à l'ordinateur sélectionné. Tous les ordinateurs de la liste d'installation qui n'exécutent pas le logiciel Windows NT s'affichent dans Evénements de serveur.

Installation push sur plusieurs domaines

Il existe deux méthodes pour installer l'agent sur plusieurs domaines :

1. **Domaine local —** Lorsque vous utilisez un compte de domaine local pour effectuer une installation push vers différents domaines, le compte utilisateur spécifié pour effectuer cette opération à partir du domaine actuel doit disposez de droits d'administrateur sur les systèmes client installés sur le domaine distant.

2. **Domaine distant —** Lorsque vous utilisez un domaine distant pour effectuer l'installation push de l'agent ePolicy Orchestrator, le domaine dans lequel le serveur ePolicy Orchestrator est installé doit approuver le domaine distant (sélectionnez *Approuvé* pour le paramètre Relation d'approbation).

Installation avec image prédéfinie

Si votre société crée une image d'ordinateur client standard pour configurer de nouvelles stations de travail ou de nouveaux ordinateurs personnels, vous pouvez installer l'agent sur le système qui est utilisé pour l'image. Lors du premier démarrage de l'ordinateur, l'agent remplace son ID par une valeur unique qui décrit le nouveau PC avant l'interrogation du serveur ePolicy Orchestrator.

Autres méthodes de distribution

En outre, le fichier POAGINST.EXE peut être distribué via des partages réseau, des supports amovibles ou des scripts de connexion. Dans chacune de ces méthodes, l'administrateur ou l'utilisateur doit exécuter le fichier manuellement sur chaque ordinateur.

REMARQUE : La procédure présentée dans la section « Installation push de l'agent sur des ordinateurs sélectionnés » à la page 97 s'applique spécifiquement aux installations push effectuées sur des ordinateurs Windows 95, Windows 98 et Windows 2000 uniquement. Si vous déployez l'agent sur ces systèmes en utilisant une autre méthode d'installation décrite ici, vous n'avez pas besoin d'effectuer un partage de fichiers et d'imprimantes sur ces machines.

Installation push

REMARQUE : Pour qu'un administrateur d'ePolicy Orchestrator puisse « pousser » un agent vers un ordinateur client, il faut que le compte de l'administrateur appartienne au groupe des administrateurs locaux sur tous les clients.

La procédure suivante décrit comment pousser l'agent vers les clients Windows NT du même domaine.

Pour effectuer une installation push sur des clients Windows NT :

1. Cliquez avec le bouton droit sur le site, le groupe ou l'ordinateur du répertoire qui doit recevoir l'agent, puis sélectionnez **Envoyer le programme d'installation de l'agent...** (Figure 3-33).

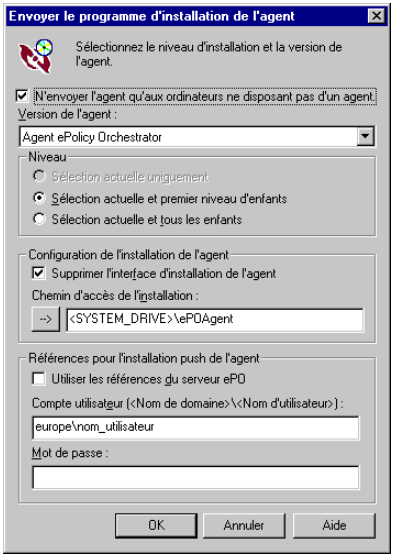


Figure 3-33. Envoyer le programme d'installation de l'agent

2. Sélectionnez **N'envoyer l'agent qu'aux ordinateurs ne disposant pas d'un agent** si vous voulez envoyer l'agent uniquement aux ordinateurs qui n'en ont pas. Si vous installez l'agent sur tous les ordinateurs, comme dans le cas d'une mise à jour, désélectionnez cette option.

3. Sélectionnez le niveau de cette installation. Il y a trois niveaux reconnus dans cette procédure :

   - **Sélection actuelle uniquement** : Le noeud de l'ordinateur sélectionné.

   - **Sélection actuelle et premier niveau d'enfants** : ce niveau et les noeuds situés *immédiatement* en dessous. Ce niveau d'installation déploie l'agent vers l'ensemble des sites, groupes et ordinateurs du niveau actuel et vers tous les groupes et/ou ordinateurs du niveau inférieur suivant. Les enfants des groupes sous le premier niveau ne reçoivent pas l'agent via cette transaction. Par exemple, si vous sélectionnez un site ayant quatre groupes sous lui et que chacun de ces groupes a quatre ordinateurs sous lui, le site sélectionné ainsi que les quatre groupes directement en dessous reçoivent l'agent, mais pas les ordinateurs. Vous devez utiliser une autre transaction pour installer l'agent sur ces ordinateurs. Cela peut s'avérer utile si vous souhaitez limiter la bande passante utilisée.

   - **Sélection actuelle et tous les enfants** : ce niveau et *tous* les noeuds situés en dessous. Si nous reprenons l'exemple du site qui a quatre groupes sous lui, ayant eux-mêmes quatre ordinateurs chacun, tous les éléments qui se trouvent sous le site sélectionné reçoivent l'agent à partir d'une seule transaction. Ce choix est conseillé, si le volume du groupe complet est réduit ou si la bande passante ne pose pas de problème.

4. Sélectionnez **Supprimer l'installation d'agent GUI** pour une installation d'agent silencieuse. De cette manière, l'agent est installé sans que l'utilisateur s'en aperçoive.

5. **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.

6. **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push de l'agent et les options Compte utilisateur et Mot de passe sont désactivées. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

7. Cliquez sur **OK** pour démarrer la procédure d'installation.

   Il existe deux scénarios d'installation :

   - **Installation d'agent GUI supprimée**. Pendant l'installation, si l'administrateur a supprimé l'installation d'agent GUI, aucune indication n'est faite concernant l'installation de l'agent en cours. La première indication concernant le succès de l'installation survient lorsque le nouvel agent interroge le serveur et fait un rapport des propriétés de l'ordinateur.
   - **GUI d'installation de l'agent ouverte**. Cette fenêtre de message, qui n'est généralement visible que pendant quelques secondes, s'ouvre sur l'ordinateur client.

8. Une fois l'installation terminée, sélectionnez l'ordinateur client dans le répertoire, puis cliquez sur l'onglet Propriétés du volet Détails pour afficher ses propriétés.

Installation push de l'agent sur des domaines non approuvés

Vous pouvez pousser l'agent uniquement à partir d'un compte d'utilisateur possédant des droits sur le domaine sur lequel vous déployez l'agent ou sur un domaine approuvé. Si votre réseau contient des domaines non approuvés, créez un compte d'administrateur de domaine dans chaque domaine qui doit recevoir l'agent.

IMPORTANT : Le compte d'administrateur de chaque domaine doit posséder des droits d'administrateur de domaine pour que l'installation push réussisse.

Pour pousser l'agent vers un nouveau domaine :

1. A partir de la console, ouvrez la fenêtre **Services** (dans le **Panneau de configuration** du **menu Démarrer**).
2. Sélectionnez le service **Serveur McAfee ePolicy Orchestrator 2.0** et cliquez sur **Arrêter**.
3. Cliquez sur **Démarrage** pour ouvrir la fenêtre Service.
4. Sélectionnez **Ce compte** et saisissez les informations nécessaires pour le compte d'administration du domaine (admin) déjà défini, puis cliquez sur **OK**.

5. Redémarrez le service en sélectionnant **Serveur McAfee ePolicy Orchestrator 2.0**, puis en cliquant sur **Démarrer**.
6. Poussez l'agent vers le nouveau domaine. Pour obtenir des instructions, consultez la section « Installation push » à la page 94.
7. Répétez ces étapes pour tous les domaines non approuvés.

Installation push de l'agent sur des ordinateurs sélectionnés

L'agent peut également être poussé vers des ordinateurs client qui utilisent Windows 98, Windows 95 ou Windows ME lorsque les conditions suivantes sont respectées :

- L'administration à distance doit être activée sur l'ordinateur client.
- L'ordinateur client doit être configuré pour gérer le partage des fichiers et de l'impression.
- L'ordinateur client doit avoir configuré correctement le contrôle d'accès au niveau utilisateur.
- La sécurité doit être définie au niveau utilisateur sur l'ordinateur client.
- Pour les installations push de l'agent uniquement, l'ordinateur doit être redémarré ; cela fait partie de la procédure d'installation de l'agent. Ce logiciel ne possède pas de fonction de service à distance.

Pour pousser l'agent vers des ordinateurs sélectionnés :

1. Cliquez avec le bouton droit sur l'ordinateur du répertoire qui doit recevoir l'agent, puis sélectionnez **Envoyer le programme d'installation de l'agent...**
2. Sélectionnez **N'envoyer l'agent qu'aux ordinateurs ne disposant pas d'un agent** si vous voulez envoyer l'agent uniquement aux ordinateurs qui n'en ont pas. Si vous installez l'agent sur tous les ordinateurs, comme dans le cas d'une mise à jour, désélectionnez cette option.
3. Sélectionnez le niveau de cette installation. Il y a trois niveaux reconnus dans cette procédure.
4. Sélectionnez **Supprimer l'installation d'agent GUI** pour une installation d'agent silencieuse. De cette manière, l'agent est installé sans que l'utilisateur s'en aperçoive.
5. **Chemin d'accès de l'installation.** Entrez le chemin d'accès de l'installation ou cliquez sur  pour insérer une variable système ou une variable de fichiers programme.

6. **Références pour l'installation push d'agent.** Si l'option **Utiliser les références du serveur ePO** est sélectionnée, ces références sont utilisées pour l'installation push de l'agent et les options Compte utilisateur et Mot de passe sont désactivées. Si l'option **Utiliser les références du serveur ePO** est désélectionnée, l'administrateur peut entrer un compte utilisateur et un mot de passe de domaine qui seront utilisés pour l'installation push des agents.

7. Cliquez sur **OK** pour démarrer la procédure d'installation.

   Il existe deux scénarios d'installation :

   - **Installation d'agent GUI supprimée**. Pendant l'installation, si l'administrateur a supprimé l'installation d'agent GUI, aucune indication n'est faite concernant l'installation de l'agent en cours. La première indication concernant le succès de l'installation survient lorsque le nouvel agent interroge le serveur et fait un rapport des propriétés de l'ordinateur.
   - **GUI d'installation de l'agent ouverte**. Cette fenêtre de message, qui n'est généralement visible que pendant quelques secondes, s'ouvre sur l'ordinateur client.

8. Redémarrez l'ordinateur pour terminer l'installation.

9. Une fois l'installation terminée, sélectionnez l'ordinateur client dans le répertoire, puis cliquez sur l'onglet Propriétés du volet Détails pour afficher ses propriétés.

Installation de l'agent en utilisant le fichier POAGINST.EXE

Dans certains cas, vous pouvez être amené à installer l'agent manuellement, par le biais d'une disquette, d'un CD-ROM ou d'un répertoire réseau comme source pour le fichier.

Pour installer manuellement l'agent en utilisant le fichier POAGINST.EXE

1. Copiez le fichier **POAGINST.EXE** à partir de l'emplacement d'installation d'ePolicy Orchestrator. Si vous l'avez installé dans son emplacement par défaut, vous le trouverez dans le chemin suivant :

   C:\Program Files\McAfee\ePO\2.0\DB\Software\ePOAgent2000\2.0.0.XXX\0409\Installfiles

   Contrôlez toujours la date de création de ce fichier avant de l'utiliser car le serveur crée un nouveau fichier d'installation de l'agent chaque fois qu'il met à jour sa configuration.

2. Insérez la disquette ou le CD-ROM dans le lecteur approprié de chaque ordinateur client.

3. Exécutez le programme d'installation d'agent **POAGINST.EXE** sur l'ordinateur client via l'option **Exécuter** du menu **Démarrer** ou via une invite de commande. Sur la ligne de commande, tapez :

   `poaginst.exe[/s][/installpath="ePOAgentInstallPath"]`

   - **`/s`:** mode silencieux, GUI non visible
   - **`/installpath="ePOAgentInstallPath"`:** Répertoire d'installation de l'agent d'ePolicy Orchestrator

     Le chemin d'installation prend également en charge les trois macros suivantes :

Macro	Description
<SYSTEM_DRIVE>	Lecteur sur lequel est installé le système d'exploitation.
<PROGRAM_FILES_DIR>	Chemin complet du répertoire « Program Files » du système d'exploitation. Par exemple : C:\Program Files\
<PROGRAM_FILES_COMMON_DIR>	Chemin complet du répertoire « Common Files » du système d'exploitation. Par exemple : C:\Program Files\Common Files

REMARQUE : L'emplacement spécifié doit déjà exister.

Codes de retour pour POAGINST.EXE

Codes de retour	Description
-1 AGINST_RETURN_UNKNOWN_ERROR	Erreur non spécifiée.
0 AGINST_RETURN_SUCCEEDED	L'installation a abouti
1 AGINST_RETURN_IMPERSONATE_FAILED	La référence intégrée est incorrecte et la personnification a échoué.
2 AGINST_RETURN_COPYFILE_FAILED	La copie du fichier dans le répertoire d'installation de l'agent a échoué.
3 AGINST_RETURN_UPDATE_REG_FAILED	Echec de la mise à jour du registre du système.
4 AGINST_RETURN_INSTALL_SERVICE_FAILED	Echec de l'installation du service de l'agent ePO.
5 AGINST_RETURN_START_SERVICE_FAILED	Echec du démarrage du service de l'agent ePO.
6 AGINST_RETURN_INSTALL_CANCELLED	L'installation a été annulée.
7 AGINST_RETURN_INSTANCE_EXISTED	Une instance poaginst est en cours d'exécution.
8 AGINST_RETURN_CREATE_MUTEX_FAILED	Echec de création mutex pour identifier l'instance poaginst.
9 AGINST_RETURN_INITIALIZE_COMMAND_LINE_FAILED	Ligne de commande incorrecte.

Installation de l'agent sur un ordinateur muni d'une image prédéfinie

Lorsque vous créez un système en tant qu'ordinateur standard pour les images, vous pouvez installer l'agent avant de créer l'image. L'agent se renomme lui-même et contacte le serveur ePolicy Orchestrator en tant que nouvel agent la première fois que l'ordinateur se connecte au réseau.

Pour installer l'agent sur un ordinateur muni d'une image prédéfinie

1. A partir du serveur ePolicy Orchestrator, installez l'agent sur le système qui est utilisé comme ordinateur standard. Utilisez l'une des méthodes décrites dans « Méthodes d'installation » à la page 92).

2. Sur l'ordinateur standard, exécutez le programme d'installation d'agent **POAGINST.EXE** via l'option **Exécuter** du menu **Démarrer** ou via une invite de commande. Sur la ligne de commande, tapez :

   ```
   poaginst.exe[/s][/installpath="ePOAgentInstallPath"]
   ```

C'est tout ce que vous avez à faire. A chaque fois que l'agent démarre, il extrait l'adresse IP et le nom de l'ordinateur où il est installé, puis il insère ces deux valeurs dans l'ID d'agent unique qu'il envoie au serveur. Si l'une de ces valeurs a été modifiée depuis la dernière exécution de l'agent, ce dernier apparaît sur le serveur ePolicy Orchestrator comme étant un agent différent.

Ainsi, si vous installez l'agent sur le système principal pour un ordinateur sur lequel une image a été définie, l'agent se différencie automatiquement de lui-même lors du démarrage du nouvel ordinateur muni d'une image. L'ordinateur sur lequel une image a été définie (ou copie de l'image principale) apparaît comme agent unique vis-à-vis du serveur ePolicy Orchestrator.

Gestion de l'agent par ligne de commande

L'utilitaire de ligne de commande de l'agent, **CmdAgent**, est un exécutable par ligne de commande qui envoie des commandes au service de l'agent. Cet utilitaire a été conçu pour des cas spécifiques afin de contrôler à distance l'activité de l'agent. Il est particulièrement utile lorsque l'administrateur souhaite qu'un agent contacte immédiatement le serveur une fois que l'utilisateur s'est connecté à l'ordinateur de l'agent. L'utilitaire s'exécute sur l'ordinateur client à l'aide d'un script de connexion.

Les commandes actuellement prises en charge sont les suivantes :

- Créer et envoyer des propriétés et des événements.
- Appliquer des stratégies.
- Vérifier l'existence de nouvelles stratégies/tâches.

Pour utiliser l'utilitaire de ligne de commande :

1. Sur l'ordinateur client, ouvrez une **Invite de commande** dans le menu **Démarrer**.
2. Passez au répertoire **EPOAgent**.
3. Tapez la commande suivante avec un commutateur approprié :

   ```
   CmdAgent  /P /E /C
   ```

   Les commutateurs sont les suivants :

   `/P` Créer et envoyer des propriétés et des événements au serveur

   `/E` Appliquer des stratégies et exécuter des tâches

   `/C` Vérifier l'existence de nouvelles stratégies
4. Tapez **`Quitter`** pour fermer la fenêtre d'invite de commande.

Suppression de l'agent

Vous pouvez supprimer l'agent à partir de la console ePolicy Orchestrator ou directement à partir de l'ordinateur client.

Pour supprimer l'agent de la console :

1. Mettez en surbrillance le site, le groupe ou l'ordinateur duquel vous souhaitez supprimer l'agent, puis cliquez avec le bouton droit de la souris et sélectionnez **Supprimer**.
2. Cliquez sur **Désinstaller l'agent de tous les ordinateurs connectés**.

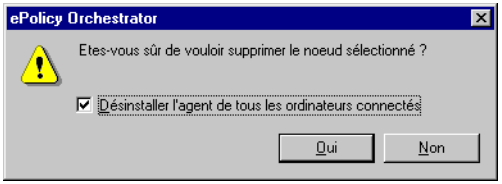


Figure 3-34. Désinstallation de l'agent

3. Cliquez sur **Oui**.

Pour supprimer l'agent directement à partir de l'ordinateur client :

1. Sur l'ordinateur client, ouvrez une **Invite de commande** dans le menu **Démarrer**.
2. Passez au répertoire **EPOAgent**.
3. Tapez la ligne suivante et appuyez sur **ENTRÉE** :

```
aginst32 /remove
```

4. Tapez **Quitter** pour fermer la fenêtre d'invite de commande.
5. A partir du Gestionnaire de fichiers, supprimez le répertoire **EPOAgent**.

Caractéristiques et fonctions de l'agent

Cette section décrit les caractéristiques et les fonctions d'un agent installé. Les sujets abordés sont les suivants :

- Intervalle de communication agent à serveur.
- Structure du répertoire d'un agent installé.
- Informations sur l'adresse IP dans l'agent.
- Appel de réveil de l'agent. Cette fonction permet à l'administrateur d'exécuter la commande *ping* (contacter) sur l'agent et de lui demander de contacter immédiatement le serveur. Cet outil est particulièrement utile en cas d'infection, où la mise à jour immédiate du fichier .DAT peut être cruciale.

En plus des fonctions décrites ici, l'agent applique également les stratégies qu'il collecte sur le serveur, une fois que l'administrateur à défini ces stratégies sur la console. L'agent exécute également des tâches définies par l'administrateur et signale les infections virales au serveur en appliquant la stratégie de l'administrateur. Vous trouverez davantage d'informations sur ces fonctions au chapitre 5 à la page 117.

Comment déterminer si un agent est en cours d'exécution

La façon la plus facile de déterminer si un agent est en cours d'exécution sur un ordinateur particulier est de contrôler le noeud sur la console ou de consulter le rapport « Computers with No Anti-Virus Protection » (No AV Protection Summary) [« Ordinateurs non protégés contre les virus » (Résumé de l'absence de protection AV)]. Contrôlez la dernière mise à jour des propriétés. Si elle est normale par rapport aux valeurs définies par l'administrateur, il est probable que l'agent fonctionne correctement. Si la dernière mise à jour des propriétés remonte à plus de 24 heures, l'agent se trouve sur un portable qui n'est pas connecté au serveur en ce moment ou bien l'agent ne fonctionne pas correctement. L'administrateur peut promouvoir de nouveau l'agent, faire apparaître l'icône d'état de l'agent et contrôler le fonctionnement de l'agent à partir de l'ordinateur client ou bien attendre la prochaine mise à jour de l'agent. Toutefois, l'absence de réponse de la part de l'agent peut être due uniquement à des problèmes de communication.

Communication agent-serveur

L'agent communique de façon sûre avec le serveur en utilisant un mécanisme de signature à infrastructure de clé publique (PKI) basé sur la technologie de chiffrement PGP de Network Associates. L'agent signe et authentifie chaque message de façon numérique. Si la validation de la signature échoue d'un côté ou de l'autre, le message est ignoré et éliminé. La fréquence d'interrogation par défaut est déterminée par l'administrateur via la console.

Peu de temps après l'installation réussie de l'agent, celui-ci envoie un message d'interrogation sécurisé au serveur pour proposer un identificateur d'agent univoque. Le serveur crée un enregistrement dans la base de données pour cet identificateur unique de façon à conserver les informations que l'agent transmet.

L'agent transmet les propriétés de l'ordinateur et le statut des logiciels anti-virus McAfee installés à intervalles prédéfinis. En fonction des stratégies définies à partir de la console, l'agent peut également rapporter des virus ou des événements logiciels demandés par l'administrateur. L'agent reçoit toutes les nouvelles stratégies de la part de l'administrateur depuis la dernière période d'interrogation, si l'administrateur a défini ces stratégies sur la console.

Si l'agent réside sur un ordinateur qui se connecte au réseau par accès à distance (DUN), chaque fois que l'utilisateur lance un appel sur le réseau, l'agent se met automatiquement à jour dès la première connexion. L'agent met automatiquement à jour les propriétés et applique les stratégies et les tâches.

Fréquence de communication agent à serveur

Ce tableau indique les intervalles recommandés pour les communications agent à serveur, en fonction de l'importance du réseau.

Tableau 3-1. Intervalles de création d'états recommandés pour un fonctionnement normal basé sur une couverture de 10 000 noeuds

Taille du réseau	Intervalle de communication agent
100 Mo réseau local (LAN) uniquement	60 minutes
10 Mo réseau local (LAN) uniquement	180 minutes
Réseau étendu (WAN)	6 heures (360 minutes)
Accès à distance/RAS*	6 heures (360 minutes)
100 Mo réseau local (LAN) uniquement	60 minutes

* Lorsque vous vous connectez à un intranet d'entreprise via l'accès à distance/RAS, l'agent détecte la connexion réseau et la communique au serveur ePolicy Orchestrator.

REMARQUE : Voir « Traitement d'une attaque », page 234 pour obtenir davantage d'informations sur l'utilisation de la fonction Appel de réveil de l'agent pour la gestion des infections virales.

Structure du répertoire de l'agent

Voici une structure de répertoire normale pour un agent résidant sur l'ordinateur client.

Tableau 3-2. Structure de répertoire pour l'agent

Répertoire et sous-répertoires	Objet
[DRIVE]:\EPOAgent	L'emplacement peut être personnalisé
\AgArchive	Non utilisé actuellement
\AgUnpack	Utilisé comme chemin d'extraction temporaire pour les fichiers compressés traités par l'agent ePolicy Orchestrator.
\AgentDb	Contient les sous-répertoires suivants :
\Data	Utilisé pour les logiciels téléchargés à partir du serveur ePolicy Orchestrator avant leur installation.
\Event	Utilisé pour stocker les fichiers .EVT (fichiers d'événement) qui seront téléchargés vers le serveur ePolicy Orchestrator (Anti-Virus Informant).
\Policy	Utilisé pour stocker des fichiers policy.ini qui seront appliqués sur des produits Anti-Virus Informant locaux.
\Tasks	Utilisé pour stocker des fichiers TASK.INI destinés à l'exécution de l'agent.

Informations sur l’adresse IP dans l’agent

Pour pouvoir localiser le serveur ePolicy Orchestrator, l'agent doit chercher l'adresse IP du serveur ou bien utiliser le nom d'ordinateur de ce dernier (nom NetBIOS). Si l'adresse IP est modifiée, le serveur met automatiquement à jour POAGINST.EXE, fichier d'installation de l'agent, afin d'inclure ces nouvelles informations.

Lorsqu'une méthode de distribution manuelle est utilisée pour livrer l'agent, il faut bien s'assurer que c'est la dernière copie de l'agent qui est installée sinon il se peut que le serveur ne reconnaisse pas l'agent lors des rapports. McAfee recommande d'utiliser la technologie push.

Collecte des propriétés

Dès que l'agent est installé, il recueille un ensemble général de propriétés du client et les transfère au serveur. Ces informations sont enregistrées dans la base de données d'ePolicy Orchestrator. Elles sont affichées sur la console sur l'onglet Propriétés du volet de détails lorsque l'ordinateur de l'agent est sélectionné dans l'arborescence de la console.

Deux ensembles de propriétés sont répertoriés. Les propriétés générales comprennent des informations concernant le système et ses informations uniques d'identification, ainsi que des éléments tels que l'espace disponible sur le disque. Ces propriétés sont décrites dans le tableau 3-3 à la page 108.

Tableau 3-3. Définition des propriétés spécifiques d'ePolicy Orchestrator

Propriétés	Définition
Chemin utilisé pour l'installation	Chemin d'accès à l'agent sur l'ordinateur client
Version du produit	Le numéro de version du produit ePolicy Orchestrator doit être 2.0.0.XXX
GUID de l'agent	Identificateur unique pour cette installation de l'agent
Afficher l'interface de l'agent	1 = Indiquer la présence à l'utilisateur par une icône dans la barre d'état 0 = Masquer la présence à l'utilisateur
Afficher l'interface de redémarrage	1 = Afficher la demande de redémarrage à l'utilisateur et attendre qu'il redémarre le système 0 = Ne pas afficher la demande de redémarrage à l'utilisateur
Délai de redémarrage	Intervalle en minutes en fonction duquel le système redémarre automatiquement pour continuer l'installation.
Intervalle de recréation des propriétés de l'agent local	Intervalle en secondes en fonction duquel l'agent prend un nouveau profil de l'ordinateur hôte
Intervalle de communication agent à serveur (ASCI)	Intervalle en secondes en fonction duquel l'agent interroge le serveur (se connecte au serveur)
Version du plug-in	Numéro de version du plug-in ePolicy Orchestrator

Les noeuds inférieurs de l'arborescence indiquent des propriétés du logiciel anti-virus installé sur le noeud sélectionné dans l'arborescence de la console sur le côté gauche de celle-ci. Les informations sur ces propriétés sont décrites dans les manuels du logiciel spécifique.

Affichage des propriétés de l'agent à partir de la console

Pour afficher les propriétés d'un agent spécifique :

1. Dans le répertoire, sélectionnez l'ordinateur client que vous souhaitez afficher.
2. Sélectionnez l'onglet **Propriétés** dans le volet Détails pour afficher la liste des propriétés définies pour l'agent sélectionné.

Appel de réveil de l'agent

L'appel de réveil de l'agent permet à l'administrateur de contacter tous les agents d'un site ou d'un groupe donné et de leur demander de contacter immédiatement le serveur. Il doit être utilisé en cas d'infection afin d'imposer à tous les agents sélectionnés un délai de 0 à 60 minutes qui peut être randomisé. L'administrateur peut définir l'intervalle de randomisation à 0 pour exécuter immédiatement l'appel de réveil de l'agent, ou randomiser le contact sur une période maximale de 60 minutes.

La fonction d'appel de réveil utilise un port défini par l'administrateur (la valeur par défaut est 8081) pour effectuer ce réveil configurable. La fonction de réveil peut être arrêtée ou démarrée dynamiquement. Le port utilisé pour le réveil de l'agent peut être modifié dynamiquement. Toutefois, si l'appel de réveil est désactivé, il ne peut être réactivé que lors du prochain intervalle de communication agent à serveur.

En outre, si le port est laissé ouvert, la fonction appel de réveil fonctionne par le biais d'un pare-feu.

IMPORTANT : Avant d'utiliser cette fonction vous devez activer un appel de réveil de l'agent en utilisant l'écran d'options de l'agent pendant un intervalle de communication agent à serveur complet, *au minimum*. Sinon, l'agent n'écoute pas l'appel de réveil et ne contacte pas le serveur jusqu'au prochain intervalle régulièrement planifié. Pour configurer cette option, consultez « Configurer les options de l'agent » à la page 89.

Pour réveiller les agents après avoir activé l'appel de réveil dans les options de l'agent :

1. Cliquez avec le bouton droit sur un site ou un groupe dans le répertoire, sélectionnez **Toutes les tâches**, puis sélectionnez **Appel de réveil de l'agent...** pour ouvrir la fenêtre Appel de réveil de l'agent (Figure 3-35).

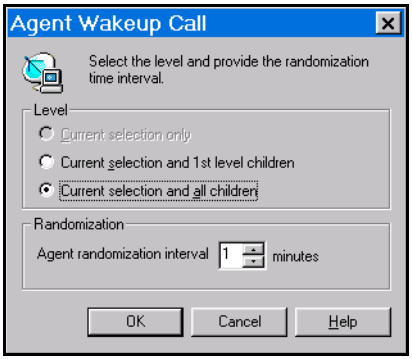


Figure 3-35. Fenêtre Appel de réveil de l'agent

2. Sélectionnez le niveau de contact lié à cet appel de réveil. Si votre sélection dans l'arborescence de la console s'applique à un ordinateur ou un utilisateur, vous ne pouvez choisir que **Sélection actuelle uniquement**. Si votre sélection dans l'arborescence de la console s'applique à un site ou à un groupe, sélectionnez **Sélection actuelle et enfants de premier niveau** ou, si vous souhaitez élargir l'étendue de l'appel de réveil, **Sélection actuelle et tous les enfants**.

3. Sélectionnez un intervalle de randomisation compris entre 0 et 60 minutes. L'intervalle de randomisation désigne le délai pendant lequel les agents peuvent démarrer une tâche. Dans ce cas, la tâche contacte le serveur et l'appel de réveil demande à l'agent d'envoyer un message à une heure aléatoire comprise dans l'intervalle.

   - Un délai de randomisation plus court active l'agent plus rapidement mais augmente la quantité de bande passante réseau requise avec des contacts simultanés.
   - Un délai de randomisation plus long active l'agent plus lentement, jusqu'à 60 minutes, mais permet de réduire l'impact sur la bande passante réseau.

4. Cliquez sur **OK** pour envoyer l'appel de réveil à tous les agents sélectionnés.

Déploiement du logiciel 4

Présentation

Ce chapitre décrit la façon de déployer les produits anti-virus McAfee pris en charge par le programme ePolicy Orchestrator. Une fois le logiciel ePolicy Orchestrator installé sur le serveur, le déploiement de logiciels activé et l'agent correctement installé sur un ordinateur client, l'administrateur peut définir une stratégie pour que le produit logiciel soit déployé.

Procédure

Voici la procédure pour installer le logiciel sur un seul ordinateur :

1. Quand l'agent interroge pour la première fois le serveur d'ePolicy Orchestrator, il transmet les informations concernant les installations actuelles du logiciel anti-virus McAfee, y compris les numéros de version et les états. Ces informations de profil sont stockées dans le serveur et apparaissent sur la console comme expliqué dans « Informations sur l'adresse IP dans l'agent » à la page 107.
2. L'action suivante dépend de l'état du logiciel anti-virus McAfee installé sur l'ordinateur client.
    - Si le logiciel anti-virus McAfee souhaité n'est pas installé du tout, l'agent interroge le serveur au moment programmé pour la communication et indique que le logiciel désiré n'est pas installé sur l'ordinateur du client.
    - Si la version souhaitée du logiciel anti-virus MacAfee est installée sur l'ordinateur client, l'agent s'attache à ce logiciel pour pouvoir interagir avec lui et créer un rapport sur lui. Il ne remplace pas le logiciel. L'agent signale également au serveur que le logiciel McAfee est déjà installé.
3. Le serveur envoie le produit désiré à l'agent dans le message de réponse.
4. L'agent accepte et installe le produit sur le serveur client.
5. L'agent renvoie un message d'état au serveur lui indiquant que l'installation s'est déroulée avec succès.

Si une version du produit logiciel anti-virus McAfee est déjà installée, le système ne la mettra pas à niveau avec une version plus récente. Par exemple, si le logiciel VirusScan 4.03 est installé sur le système, l'agent signale que le produit VirusScan est déjà installé et le logiciel VirusScan 4.5, plus récent, ne sera pas installé. L'administrateur doit définir une stratégie pour le logiciel VirusScan 4.5 s'il souhaite que cet agent en force l'installation.

Application du déploiement du logiciel anti-virus

Le logiciel ePolicy Orchestrator applique toutes les stratégies d'installation définies par l'administrateur. Cela signifie que si un utilisateur final supprime un produit qu'il gère, ePolicy Orchestrator réinstalle ce produit.

L'agent collecte les propriétés avant chaque transmission au serveur. Si l'agent renvoie des informations différentes des stratégies définies par l'administrateur ePolicy Orchestrator sur la console, les stratégies sont automatiquement appliquées. Le serveur envoie automatiquement à nouveau tous les logiciels ne fonctionnant pas lors du prochain intervalle de communication agent-console. L'agent réinstalle le logiciel et rapporte les informations mises à jour.

Déploiement des produits logiciels anti-virus McAfee

Le produit ePolicy Orchestrator vous permet de déployer le logiciel anti-virus McAfee sur n'importe quel ordinateur doté d'un agent ePolicy Orchestrator. Vous pouvez déployer un produit sur un agent ou plusieurs produits sur plusieurs agents installés différents. Vous pouvez aussi déployer simultanément un produit sur l'ensemble de l'entreprise.

Pour installer des produits via la console ePolicy Orchestrator :

1. Planifiez votre déploiement.
   a. Déterminez la portée de cette installation. Combien d'ordinateurs recevront quels produits et sur quelle période ? Si vous connaissez le nombre d'ordinateurs sur lesquels les produits risquent de devoir être installés et le délai de l'installation, vous pouvez optimiser la planification de l'installation.
   b. Déterminez le meilleur moment de transmission des divers téléchargements de logiciels sur le réseau. La bande passante peut constituer une restriction lorsque vous déployez de nombreuses copies. Si vous téléchargez trop de copies en même temps, vous pouvez affecter les performances de l'ensemble du réseau durant le téléchargement initial du produit.
   c. Pour effectuer le déploiement, créez un plan auquel vous pourrez vous référer durant la configuration des installations.
2. Passez en revue la structure du répertoire à l'aide de la console. Si toutes vos tâches de déploiement dépendent d'un site unique, vous pouvez effectuer une installation sur le site et inclure tous les enfants dans le déploiement, en laissant en attente les remarques sur le volume évoquées ci-dessus.

Vous ne pouvez sélectionner qu'un seul site à la fois. Si vous devez installer des logiciels sur des ordinateurs de différents sites, vous devez réaliser ces étapes pour chaque site.

Si vous planifiez de déployer des logiciels vers des ordinateurs sélectionnés dans plusieurs sites ou groupes, pensez à restructurer le répertoire en utilisant les procédures décrites dans « Organisation du répertoire » à la page 55. Vous simplifiez ainsi le déploiement en planifiant une tâche unique ou en appliquant une fois la stratégie.

REMARQUE : La réorganisation de la structure du répertoire n'affecte pas l'emplacement physique ou réseau des ordinateurs. McAfee fournit cette fonction de gestion afin de simplifier l'application de votre stratégie anti-virus.

---

3. Utilisez un rapport Anti-Virus Informant pour vous assurer que tous les ordinateurs cible disposent d'agents opérationnels. Consultez « Déploiement de l'agent » à la page 87 pour obtenir des informations concernant l'installation de l'agent ; consultez « Rapports et requêtes » à la page 135 pour obtenir des informations concernant les rapports.

4. Sélectionnez un site ou un groupe dans l'arborescence de la console, puis cliquez sur l'onglet Stratégies dans le volet de détails supérieur pour afficher la liste des logiciels disponibles (Figure 4-1).

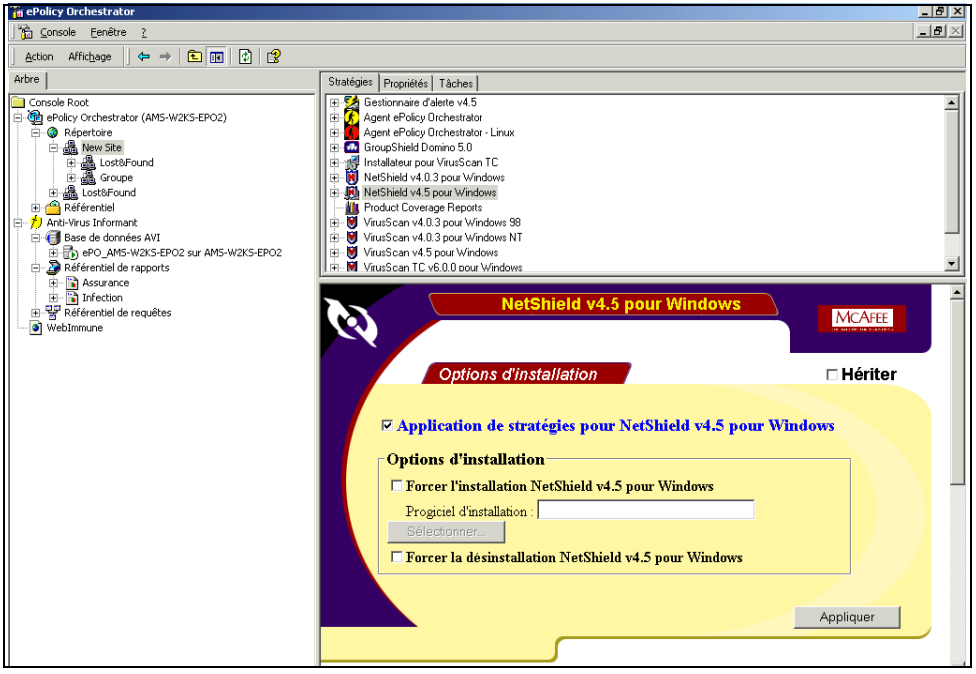


Figure 4-1. Options d'installation du logiciel

Le volet de détails inférieur affiche les options de stratégie d'installation. Cet affichage reflète la propriété d'installation actuelle pour le logiciel sélectionné dans le volet supérieur des détails, telle qu'elle s'applique au groupe ou à l'ordinateur sélectionné dans l'arborescence de la console.

5. Une fois que vous avez sélectionné le site, le groupe ou l'ordinateur et le logiciel anti-virus McAfee à installer, passez en revue les options d'installation du volet de détails inférieur.

   La page d'options (Figure 4-1) propose les options d'installation standard. Il offre trois possibilités à l'administrateur : l'héritage, l'installation forcée du progiciel anti-virus sur le(s) ordinateur(s) client du groupe sélectionné et la suppression forcée du même progiciel sur le même groupe.

   - **Héritage** : Lorsqu'un groupe hérite, il prend des stratégies, ou en hérite, d'un groupe parent. Si l'option **Hériter** est sélectionnée pour le groupe (l'agent) actuel, il obtient ses valeurs du groupe parent. Si l'option **Hériter** n'est pas sélectionnée, ce groupe prend les valeurs définies dans l'écran de stratégie affiché.

     Lorsque la case **Hériter** est cochée, tous les champs de stratégie sont désactivés. Lorsque la case **Hériter** n'est pas cochée, les stratégies peuvent être sélectionnées.

     Si la case **Hériter** est cochée pour un groupe enfant, il obtient ses valeurs directement du groupe parent. Que le groupe parent possède des valeurs personnalisées ou des valeurs héritées n'a pas d'importance.

   - **Forcer l'installation** : Si vous sélectionnez **Forcer l'installation** pour le logiciel sélectionné, ce dernier est installé sur tous les ordinateurs d'agent du groupe.

     Désélectionnez **Hériter**. Sélectionnez **Forcer l'installation**, cliquez ensuite sur **Sélectionner**, puis choisissez le kit et la langue que vous souhaitez déployer. Pour pouvoir sélectionner le kit ici, le déploiement de logiciels doit avoir été au préalable activé pour cette version du produit et pour cette langue. Reportez-vous au paragraphe « Activation du déploiement de logiciels » à la page 32 pour de plus amples informations.

   - **Forcer la désinstallation** : Si vous sélectionnez **Forcer la désinstallation**, toute instance du logiciel existant pour un ordinateur à ce niveau et pour tous les groupes enfants est supprimée. Si vous désélectionnez la case **Hériter**, seul le logiciel au niveau du groupe est supprimé.

6. Sélectionnez l'option qui s'applique à cette installation :

   - Pour installer le logiciel choisi sur le groupe sélectionné et sur tous les groupes enfants, désélectionnez **Hériter**. Sélectionnez **Forcer l'installation…**, cliquez ensuite sur **Sélectionner**, puis choisissez le kit et la langue que vous souhaitez déployer. Pour pouvoir sélectionner le kit ici, le déploiement de logiciels doit avoir été au préalable activé pour cette version du produit et pour cette langue. Reportez-vous au paragraphe « Activation du déploiement de logiciels » à la page 32 pour de plus amples informations.

     Une fois cette opération effectuée, sélectionnez à nouveau l'option **Hériter**.

   - Pour installer le logiciel souhaité uniquement sur le groupe sélectionné, désélectionnez **Hériter**. Sélectionnez **Forcer l'installation…**, cliquez ensuite sur **Sélectionner**, puis choisissez le kit et la langue que vous souhaitez déployer. Pour pouvoir sélectionner le kit ici, le déploiement de logiciels doit avoir été au préalable activé pour cette version du produit et pour cette langue. Reportez-vous au paragraphe « Activation du déploiement de logiciels » à la page 32 pour de plus amples informations.

     Une fois cette opération effectuée, sélectionnez à nouveau l'option **Hériter**.

7. Une fois que vous avez sélectionné toutes les cases appropriées pour le logiciel anti-virus MacAfee que vous souhaitez installer, cliquez sur **Appliquer** pour commencer l'installation.

8. Lorsque le processus d'installation est terminé, vous pouvez définir les stratégies pour le groupe. Reportez-vous au paragraphe « Gestion de stratégie » à la page 120 pour de plus amples informations.

REMARQUE : Certains produits anti-virus McAfee peuvent nécessiter le redémarrage de l'ordinateur durant l'installation, en fonction de la plate-forme d'exploitation. Consultez les guides de configuration de ces installations pour obtenir des informations spécifiques au produit.

---

9. Consultez le fichier journal des événements du serveur pour collecter les informations sur les échecs d'installation. Cela vous permettra de trouver une méthode pour terminer l'installation sur ces ordinateurs. Une installation de logiciel peut échouer pour plusieurs raisons :

   - Il se peut qu'il n'y ait pas assez d'espace disque dur sur le lecteur système de l'ordinateur client. Si tel est le cas, le logiciel s'interrompt avant même le téléchargement. L'agent envoie un message d'échec d'agent au journal d'événements du serveur concernant le manque d'espace disque.
   - Il se peut qu'il y ait assez de place pour télécharger le logiciel sur l'ordinateur client, mais que pour une raison quelconque, le logiciel n'arrive pas à réussir l'installation sur la machine. Si tel est le cas, l'agent envoie un message d'échec d'installation au journal d'événements du serveur.

   Pour obtenir plus d'informations sur la façon d'ouvrir et de consulter le journal des événements du serveur, consultez la section « Interface des événements du serveur » à la page 203.

Gestion du logiciel anti-virus McAfee 5

Présentation

Ce chapitre fournit des informations sur l'utilisation d'ePolicy Orchestrator pour gérer les produits anti-virus McAfee que vous avez installés sur des ordinateurs client. Avant d'effectuer cette gestion, vérifiez que vous avez installé et configuré le logiciel ePolicy Orchestrator sur le serveur. Voir « Installation et configuration du produit » à la page 21 pour plus de détails.

Vous pouvez effectuer la gestion des tâches depuis la console ePolicy Orchestrator. Trois éléments de la console constituent les principaux outils de gestion de logiciels :

- **Onglet Stratégies** situé dans le volet de détails supérieur. Définissez les options de stratégies logicielles et exécutez des tâches de gestion des stratégies.
- **Onglet Tâches** situé dans le volet de détails.
- **Options de stratégie** situées dans le volet de détails inférieur.

Chaque produit logiciel anti-virus McAfee inclut une documentation qui décrit la méthode de configuration et d'utilisation de ce logiciel. Ce chapitre décrit les outils intégrés au produit ePolicy Orchestrator qui servent à *gérer* le logiciel anti-virus McAfee. Les manuels de chaque produit logiciel anti-virus se trouvent sur le CD-ROM d'ePolicy Orchestrator.

Comparaison des tâches et des stratégies

Les tâches et les stratégies constituent les outils de gestion du logiciel anti-virus McAfee que vous installez. Un groupe de stratégies par défaut est en place la première fois que vous exécutez ePolicy Orchestrator. Un groupe de stratégies par défaut existe pour chaque logiciel anti-virus que vous déployez avec ce logiciel. Les stratégies sont décrites dans le volet Détails de la console pour chaque produit logiciel et pour chaque agent installé.

Les *stratégies* sont des règles strictes qui régissent les logiciels anti-virus. Il peut s'agit d'une option de configuration ou d'une option de déploiement. Les stratégies comprennent des éléments tels que les types de virus à rechercher, ou l'analyse du courrier électronique entrant pour vérifier la présence de virus. Un agent applique une stratégie dès qu'il la reçoit.

Les *tâches* sont des instructions que l'administrateur peut programmer pour être exécutées immédiatement ou à des heures précises. Elles peuvent comprendre des instructions pour des analyses à la demande à exécuter immédiatement, une mise à jour des fichiers .DAT ou une mise à niveau des moteurs d'analyse. Alors que le logiciel doit appliquer des stratégies pour pouvoir fonctionner, vous pouvez choisir de ne pas programmer des tâches, bien que cela diminue votre capacité à protéger votre réseau. La programmation d'une tâche inclut la programmation d'analyses à la demande dans un produit logiciel anti-virus McAfee.

Variables de stratégies

Vous pouvez utiliser des variables de tâches et de stratégies qui peuvent changer d'un ordinateur client à un autre. Par exemple, vous pouvez souhaiter installer des logiciels sur le lecteur système, mais celui-ci varie d'un ordinateur à un autre. Vous pouvez utiliser la variable <SYSTEM_DRIVE> pour résoudre le problème des lecteurs système différents pour chaque ordinateur. Une variable est remplacée par l'agent ePolicy Orchestrator sur l'ordinateur pendant la phase de compilation de la stratégie ou de la tâche.

Vous pouvez utiliser les variables prédéfinies ou créer vos propres variables.

Lors de la configuration de stratégies, vous pouvez cliquer sur pour insérer une variable. Les variables suivantes ont été prédéfinies :

Tableau 5-1. Variables

Variable	Définition
<SYSTEM_DRIVE>	Lecteur du système d'exploitation. Par exemple : • C:\ • D:\.
<SYSTEM_ROOT>	Répertoire racine du système d'exploitation. Par exemple : • C:\windows pour WIN9x • C:\windows pour NT.
<SYSTEM_DIR>	Répertoire système du système d'exploitation. Par exemple : • C:\windows\system pour WIN9x • C:\winnt\system32 pour les machines NT.
<TEMP_DIR>	Répertoire temporaire du système d'exploitation. Par exemple : • C:\temp.
<PROGRAM_FILES_DIR>	Répertoire d'installation de l'application Win32. Par exemple : • C:\Program Files sur la version anglaise du système Windows • C:\Programme sur la version allemande du système Windows
<PROGRAM_FILES_COMMON_DIR>	Répertoire commun de l'application Win32. Par exemple : • C:\Program Files\Common Files
<SOFTWARE_INSTALLED_DIR>	Répertoire d'installation de tout logiciel Point Product. Macro traduite par un plug-in Point Product.
<COMPUTER_NAME>	Nom de l'ordinateur local. Nom NetBIOS sur les systèmes Windows, nom DNS sur les systèmes Unix et nom NDS sur les systèmes Netware.
<USER_NAME>	Nom de connexion de l'utilisateur.
<DOMAIN_NAME>	Nom de domaine ou nom de groupe de travail de l'utilisateur connecté.

Gestion de stratégie

Flux de données

Une fois que le serveur et la console ePolicy Orchestrator sont installés, que le logiciel est activé et que l'agent est déployé sur les ordinateurs client, vous pouvez définir des stratégies pour toute l'entreprise.

- A l'aide de la console, vous pouvez définir les stratégies sur le serveur où elles sont gérées dans la base de données d'ePolicy Orchestrator.
- Quand l'agent interroge le serveur, celui-ci lui envoie toute nouvelle stratégie une fois l'authentification de l'agent terminée.
- L'agent envoie les stratégies au logiciel anti-virus McAfee installé sur son ordinateur client.
- Le logiciel anti-virus McAfee contrôle s'il peut exécuter la stratégie et communique à l'agent tout problème rencontré.
- En cas de problème, l'agent informe le serveur.
- La console affiche le problème que l'administrateur doit résoudre après l'avoir diagnostiqué à l'aide du journal d'événements du serveur. Voir « Interface des événements du serveur » à la page 203.

Définition des stratégies

L'onglet Stratégies situé dans le volet Détails supérieur et les informations du volet inférieur Détails vous permettent de définir les stratégies utilisées pour exécuter l'application des stratégies. Dans le volet supérieur des détails, cliquez sur ⊞ , près d'un progiciel, pour ouvrir la liste des options que vous pouvez configurer. Voir Figure 5-1 à la page 121. Pour de plus amples informations sur chaque stratégie, reportez-vous à la documentation concernant chaque produit logiciel anti-virus McAfee.

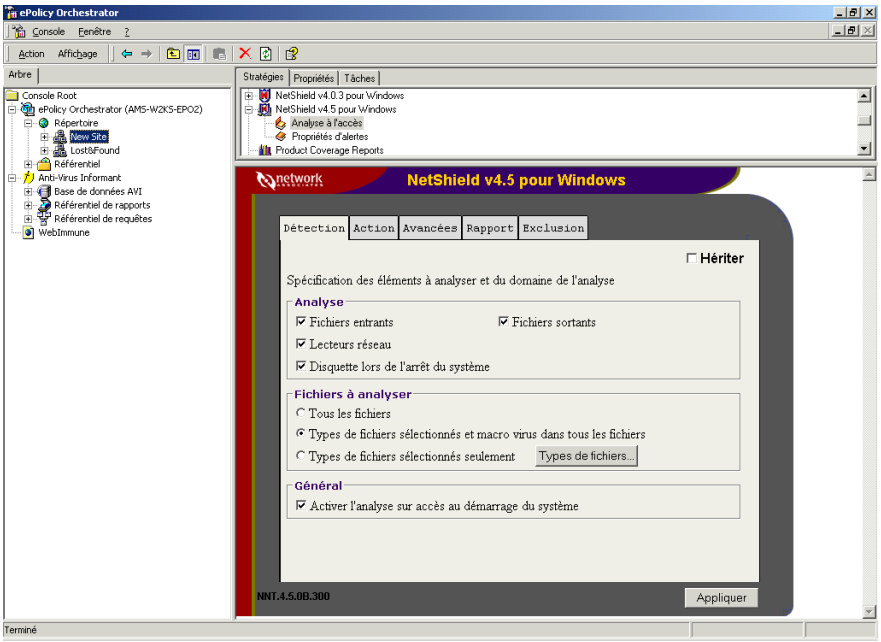


Figure 5-1. Options de stratégie

Pour configurer une stratégie logicielle :

1. Avant de définir une stratégie, vérifiez que les conditions suivantes sont remplies :

   - Chaque logiciel anti-virus McAfee que le programme ePolicy Orchestrator gère doit être installé dans le référentiel de logiciels et le déploiement de logiciels doit être activé. Reportez-vous au paragraphe « Activation du déploiement de logiciels » à la page 32 pour de plus amples informations.

   - L'agent est installé sur les clients que vous souhaitez gérer.

2. Dans l'arborescence de la console, sélectionnez le noeud à gérer. Il peut s'agir d'un groupe d'ordinateurs ou d'un seul ordinateur.

3. Lorsque l'onglet **Stratégies** est activé dans le volet supérieur Détails, sélectionnez le produit que vous souhaitez gérer et cliquez sur ⊞ près de son nom pour afficher ses fonctions.

4. Sélectionnez la fonction du produit que vous souhaitez configurer (par exemple, analyse à l'accès). Le volet inférieur de détails affiche la page des options de stratégie (Figure 5-1).

La page des options des stratégies du logiciel comprend toujours les options Détection, Action et Rapport ; certains logiciels incluent des options supplémentaires.

5. Passez en revue les options des stratégies dans le volet inférieur Détails. Si une option est grisée, elle est désactivée et ne peut être modifiée.

6. Supprimez la coche de la case **Hériter** pour activer les stratégies sur cette page. Si la case Hériter est sélectionnée, vous ne pouvez pas modifier les stratégies à ce niveau.

7. Sélectionnez les stratégies à appliquer, puis fournissez les informations nécessaires. Pour obtenir des informations détaillées sur la configuration des produits logiciels McAfee, consultez le guide de configuration du produit, disponible sur le CD-ROM ePolicy Orchestrator.

8. Sélectionnez de nouveau **Hériter**, si nécessaire, pour rétablir les propriétés d'héritage de ce produit.

9. Cliquez sur **Appliquer** pour appliquer la stratégie.

IMPORTANT : Vous devez toujours cliquer sur **Appliquer** pour chaque onglet que vous modifiez, afin d'appliquer les stratégies. Si vous modifiez toutes les stratégies dans cet onglet, mais que vous ne cliquez pas sur **Appliquer,** les nouveaux paramètres de stratégie ne sont pas enregistrés.

Planification de tâches

Le programme ePolicy Orchestrator vous aide à gérer les événements logiciels anti-virus de votre entreprise en définissant des tâches et en configurant le programme pour l'exécution de ces tâches. Une fois que les stratégies sont définies, vous pouvez planifier des tâches pour un seul agent ou pour tout un noeud de groupe. Vous pouvez planifier des mises à niveau de logiciel, des mises à jour automatiques des propriétés depuis les agents et des analyses de virus.

Vous pouvez planifier des tâches pour qu'elles démarrent immédiatement quand vous avez terminé la planification ou à une date ultérieure. La section suivante décrit en détail tous les composants de la planification d'une tâche ainsi que l'interface du Planificateur. Pour planifier le démarrage d'une tâche pour une date ultérieure, consultez « Options de planification avancées » à la page 132.

- **REMARQUE :** Tâches en attente. Si vous utilisez cette fonction pour planifier une tâche pour un groupe et que le logiciel anti-virus n'est pas installé pour la tâche sur certains ordinateurs du groupe, l'agent sur ces ordinateurs maintient la tâche en attente jusqu'à l'installation du logiciel anti-virus approprié. Si vous installez le logiciel nécessaire par la suite, la tâche s'exécutée comme programmée.

  Par exemple, si votre ordinateur client n'a pas installé VirusScan 4.5 lors de la collecte d'une tâche par l'agent visant à mettre à jour le fichier .DAT pour VirusScan 4.5, l'agent maintient la tâche. Lorsque vous installez VirusScan 4.5, la mise à jour du fichier .DAT s'exécute comme programmée.

  Si vous ne souhaitez pas qu'une tâche affecte les installations d'agent à venir, vous pouvez définir une date d'expiration pour la tâche lorsque vous programmez celle-ci.

Pour planifier une tâche :

1. Dans le répertoire, cliquez avec le bouton droit sur l'élément pour lequel vous voulez planifier une tâche, puis sélectionnez **Planifier la tâche...** (Figure 5-2).

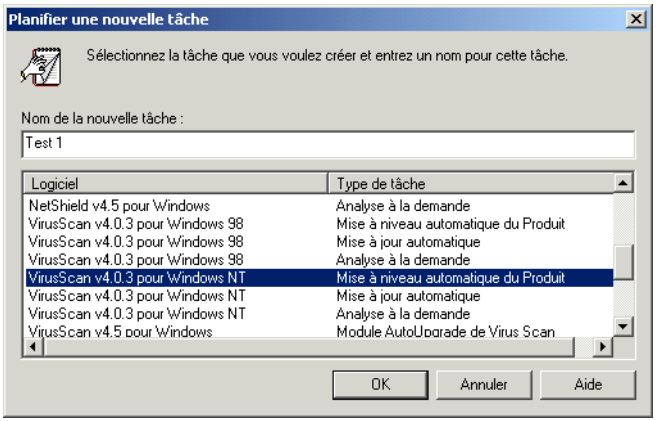


Figure 5-2. Planifier une nouvelle tâche

2. Entrez un nouveau nom de tâche.

3. Sélectionnez le **Logiciel** et le **Type de tâche** dans la liste. Les types de tâches sont les suivants :

   - **AutoUpdate** : Met automatiquement à jour le logiciel à l'aide des derniers fichiers de définitions de virus (*.DAT).
   - **AutoUpgrade** : Met automatiquement à niveau le logiciel anti-virus McAfee avec la dernière version disponible. Cette fonction peut également être utilisée pour mettre à jour le logiciel anti-virus McAfee avec le dernier moteur anti-virus et les derniers fichiers de définitions de virus (*.DAT).
   - **Analyse à la demande** : Effectue une analyse de virus sur l'ordinateur client, y compris dans tous les sous-répertoires.
   - **Site Mirror AutoUpdate** : Créez un miroir du site de mise à jour.

   REMARQUE : Tous les types de tâches ne sont pas disponibles pour l'ensemble des produits anti-virus McAfee. Consultez le guide de configuration du produit que vous gérez pour connaître les tâches disponibles.

4. Cliquez sur **OK** pour planifier la tâche sélectionnée.

5. Sélectionnez le site, le groupe ou l'ordinateur pour lequel vous avez planifié la tâche, puis cliquez sur l'onglet **Tâche** dans le volet de détails supérieur (Figure 5-3).

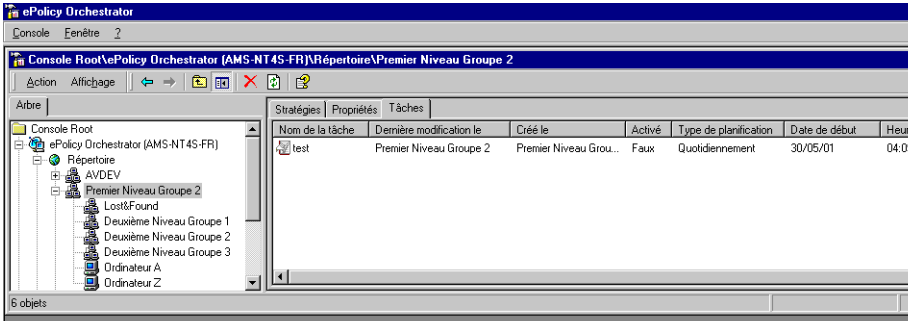


Figure 5-3. Sélectionner une tâche à planifier

6. Double-cliquez sur la tâche pour ouvrir la fenêtre Planificateur ePolicy Orchestrator et afficher les paramètres de l'onglet Tâche.

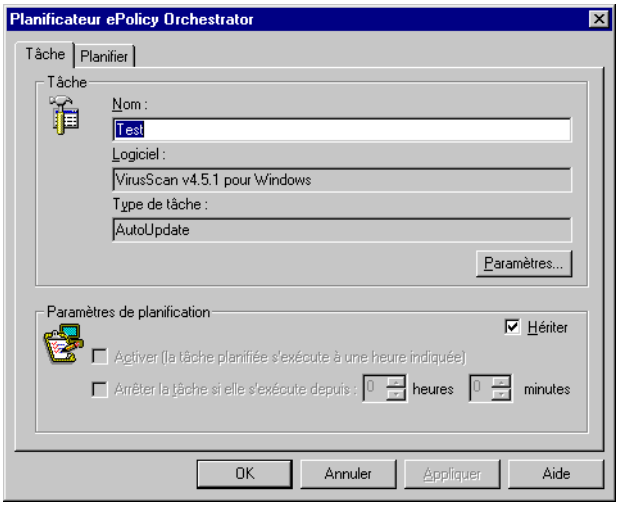


Figure 5-4. Planificateur — Onglet Tâche

7. Cliquez sur **Paramètres** pour passer en revue les stratégies pour la tâche planifiée. La modification des stratégies sur cette page affecte uniquement les noeuds déjà sélectionnés dans l'arborescence de la console.

   Les informations de la page Paramètres de la tâche varient en fonction du produit anti-virus McAfee installé sur votre serveur. Si un paramètre est désactivé, vous ne pouvez pas le modifier. Comme l'illustre la Figure 5-5, vous pouvez avoir plusieurs onglets à configurer, tels que Détection, Action, Avancé et Rapport ; cela varie en fonction du produit logiciel installé.

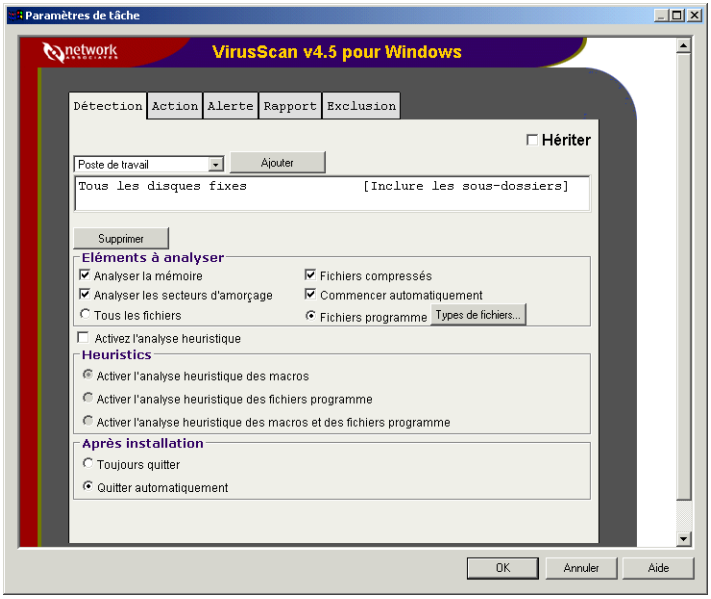


Figure 5-5. Paramètres de la tâche — Onglet Détection

8. Pour modifier ces stratégies, vous devez d'abord désélectionner **Hériter** sur chaque onglet, puis effectuer les modifications. Assurez-vous de sélectionner **Hériter** une nouvelle fois sur chaque onglet après avoir sélectionné des stratégies si vous souhaitez qu'elles soient héritées.

9. Cliquez sur **OK** pour revenir au planificateur ePolicy Orchestrator (Figure 5-2 à la page 124), puis cliquez sur **Appliquer** pour appliquer les modifications effectuées.

10. Cliquez sur l'onglet **Planifier** (Figure 5-6 à la page 127). Cet onglet vous permet de définir la planification des dates de début et de fin (ou l'absence de date de fin). Il vous offre également la possibilité de répéter la tâche à intervalles réguliers.

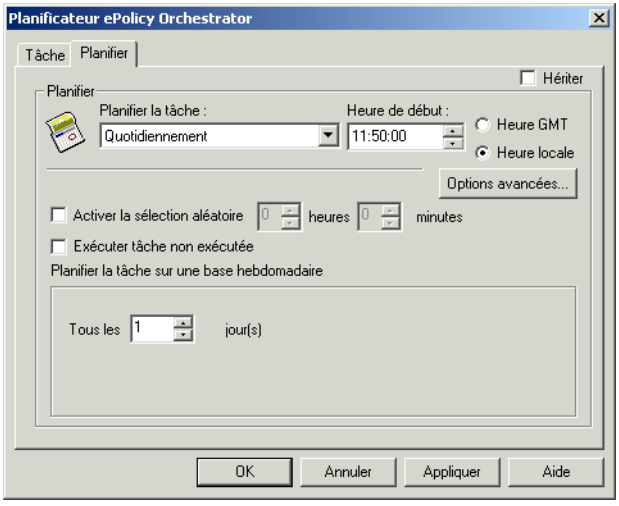


Figure 5-6. Planificateur — Onglet Planifier

11. Sélectionnez la fréquence de votre choix pour cette tâche spécifique dans le menu déroulant **Planifier la tâche**. Vous pouvez choisir : par jour, par semaine, par mois, une fois, au démarrage du système, à la connexion, au repos, exécuter immédiatement et exécuter à la numérotation.

    La sélection de la fréquence de la tâche modifie les informations disponibles dans le reste de l'onglet Planifier.

    Sélectionnez l'une des options de fréquence suivantes :

    - **Par jour** : Définit l'heure de début et la période d'exécution.
        - Entrez l'heure de début souhaitée au format HH:MM ou modifiez l'heure en cliquant sur les flèches de direction.
        - Sélectionnez **GMT** (heure de Greenwich) ou **Heure locale**.

REMARQUE : GMT est utile si votre installation d'ePolicy Orchestrator gère des domaines dans différents fuseaux horaires. Si tous vos domaines se trouvent dans le même fuseau horaire, vous pouvez préférer l'heure locale.

- La sélection de **Heure locale** correspond à l'heure qu'il est, de l'avis de l'agent. Si vos agents sont déployés sur différents fuseaux horaires, ceci vous permet de définir l'exécution d'une tâche à 02h00 (2:00 am), localement. La tâche sera exécutée sur l'ordinateur client lorsqu'il indique à l'agent qu'il est 02h00. Cela peut s'avérer utile pour une tâche qui accède au serveur et utilise la bande passante.
- La sélection de **GMT** (Greenwich Mean Time) pour une tâche revient à sélectionner 02h00 à Greenwich, Angleterre, comme l'heure de début de la tâche. Ceci signifie que l'ensemble de vos agents programmés pour exécuter une tâche à 02h00 GMT commenceront tous à la même heure. Ceci peut s'avérer utile lors de situations d'apparition lorsque vous souhaitez que TOUS vos agents commencent une analyse à la demande exactement à la même heure. Cette option est également utile lorsque la tâche ne demande pas de bande passante réseau.

– Définissez l'intervalle entre les exécutions de cette tâche en modifiant le nombre dans la zone **Tous les X jours**. La valeur par défaut est 1, mais vous pouvez la modifier pour l'adapter à votre convenance. La tâche sera exécutée tous les X jours, en fonction de votre sélection.

– Si vous cliquez sur **Avancé...**, la boîte de dialogue Options de planification avancées s'ouvre. Utilisez-la pour planifier la date de début d'exécution des tâches. Voir « Options de planification avancées » à la page 132 pour plus de détails.

- **Par semaine** : Cette sélection vous permet de définir le jour de la semaine au cours duquel sera exécutée cette tâche.
  - Entrez l'heure de début souhaitée au format HH:MM ou modifiez l'heure en cliquant sur les flèches de direction à droite de la zone Heure de début.
  - Sélectionnez **GMT** (heure de Greenwich) ou **Heure locale**. Pour plus de détails, consultez la REMARQUE, page 128.
  - Sélectionnez le nombre de semaines entre les exécutions de la tâche en entrant un nombre dans la zone **Toutes les X semaines**. Sélectionnez le jour de la semaine souhaité pour exécuter cette tâche.
  - Si vous cliquez sur **Avancé...**, la boîte de dialogue Options de planification avancées s'ouvre. Utilisez-la pour planifier la date de début d'exécution des tâches. Voir « Options de planification avancées » à la page 132 pour plus de détails.
- **Par mois** : Vous pouvez définir l'heure de début et la période d'exécution.
  - Entrez l'heure de début souhaitée au format HH:MM ou modifiez l'heure en cliquant sur les flèches de direction à droite de la zone Heure de début.
  - Sélectionnez **GMT** (heure de Greenwich) ou **Heure locale**. Pour plus de détails, consultez la REMARQUE, page 128.
  - Choisissez le bouton radio du haut pour sélectionner le jour du calendrier de chaque mois pour cette tâche ou le bouton radio du bas pour sélectionner le même jour de la même semaine pour cette tâche.

    Le bouton du haut vous permet de choisir le jour de chaque mois au cours duquel la tâche sera exécutée, par exemple, chaque premier jour du mois.

    Le bouton du bas vous permet d'indiquer que la tâche sera exécutée le même jour de la semaine, la même semaine du mois, par exemple, tous les derniers dimanches du mois.

  - Cliquez sur **Sélectionner les mois** pour ouvrir la liste des douze mois. Sélectionnez chacun des mois au cours desquels vous désirez exécuter cette tâche et cliquez sur **OK** pour retourner au planificateur ePolicy Orchestrator.
  - Si vous cliquez sur **Avancé...**, la boîte de dialogue Options de planification avancées s'ouvre. Utilisez-la pour planifier la date de début d'exécution des tâches. Voir « Options de planification avancées » à la page 132 pour plus de détails.

- **Une fois** : Vous pouvez définir une seule exécution de la tâche.
  - Entrez l'heure de début souhaitée au format HH:MM ou modifiez l'heure en cliquant sur les flèches de direction à droite de la zone Heure de début.
  - Sélectionnez **GMT** (heure de Greenwich) ou **Heure locale**. Pour plus de détails, consultez la REMARQUE, page 128.
  - Sélectionnez la date d'exécution de cette tâche en cliquant sur les flèches de direction à la droite de la zone **Exécuter le**. Cela ouvre un calendrier Windows standard dans lequel la date du jour est sélectionnée. Utilisez les flèches de direction pour modifier le mois le cas échéant, puis cliquez sur la date à laquelle vous désirez exécuter la tâche. La date que vous sélectionnez s'affiche dans la zone Date de l'onglet Planifier.
  - Si vous cliquez sur **Avancé...**, la boîte de dialogue Options de planification avancées s'ouvre. Utilisez-la pour planifier la date de début d'exécution des tâches. Voir « Options de planification avancées » à la page 132 pour plus de détails.

    REMARQUE : Si vous sélectionnez cette fonction alors que vous planifiez une tâche pour une seule fois, vous devez la transformer en tâche à répétition avant de pouvoir faire un choix dans ce menu.

- **Exécuter à la connexion** ou **Exécuter au démarrage du système** : Le reste des options de l'onglet disparaissent ou sont grisées, à l'exception de l'option **N'exécuter cette tâche qu'une fois par jour**. Quand vous avez terminé les actions de l'onglet, la tâche commence selon votre sélection.

- **Au repos** : Cette sélection affiche un minuteur d'intervalle, **lorsque l'ordinateur est resté inactif pendant X minutes**. Définissez l'intervalle pour exécuter la tâche une fois, uniquement après ce nombre de minutes d'inactivité de l'ordinateur.
- **Exécuter immédiatement** : L'exécution immédiate signifie que la tâche sera exécutée dès que l'agent la télécharge à partir du serveur, pendant le prochain intervalle de communication agent-serveur.

  Si vous sélectionnez **Activer la randomisation**, elle sera exécutée pendant la période définie comme temps de randomisation. Si vous associez ce paramètre à l'appel de réveil de l'agent (voir « Appel de réveil de l'agent » à la page 109), vous pouvez immédiatement mettre à jour vos ordinateurs protégés. McAfee vous recommande de sélectionner **Activer la randomisation** pour diminuer la charge de la bande passante.
- **Exécuter à la numérotation** : L'exécution à la numérotation signifie que l'agent télécharge cette tâche à partir du serveur pendant le prochain intervalle de numérotation et l'exécute.

  Si vous sélectionnez **Activer la randomisation**, elle sera exécutée pendant la période définie comme temps de randomisation. Si vous associez ce paramètre à l'appel de réveil de l'agent (voir « Appel de réveil de l'agent » à la page 109), vous pouvez immédiatement mettre à jour vos ordinateurs protégés. McAfee vous recommande de sélectionner **Activer la randomisation** pour diminuer la charge de la bande passante.

  Si vous sélectionnez **N'exécuter cette tâche qu'une fois par jour**, elle sera exécutée une seule fois par jour.

12. Sélectionnez **Activer la randomisation**, si nécessaire. L'activation de cette boîte de dialogue permet à l'administrateur de définir une période de randomisation en heures ou minutes. Le fait d'activer la randomisation de l'exécution des tâches pour une période définie peut réduire l'influence des tâches sur la vitesse du réseau. C'est une fonction idéale à utiliser lorsque la tâche demande que de nombreux agents accèdent au serveur. La randomisation de la tâche permet de limiter le ralentissement simultané du trafic réseau par l'action push ou pull de l'agent et de rendre les fonctions du réseau plus efficaces.

13. Sélectionnez **Exécuter la tâche manquée**, si nécessaire. Cette fonction demande à l'agent d'exécuter la tâche lorsqu'il redémarre, si l'agent était hors ligne au moment de l'exécution planifiée de la tâche. Elle permet d'assurer l'entière protection des utilisateurs distants et du réseau, même s'ils sont hors ligne au moment de l'exécution planifiée de la tâche. En outre, sans cette fonction utile pour une tâche non répétitive, telle que la tâche à « exécuter une fois », si l'agent était hors ligne pour l'exécution prévue de la tâche, il ignorerait celle-ci au redémarrage et ne l'exécuterait jamais. Par contre, lorsque cette fonction est activée, vous pouvez demander à l'agent d'exécuter la tâche, même s'il a manqué l'heure d'origine planifiée pour la tâche.

    L'administrateur peut activer l'option Tâche manquée pour que, lorsqu'il redémarre, l'agent exécute toutes les tâches qu'il a manquées lorsqu'il était hors ligne. Si l'option n'est pas activée, l'agent ignore les tâches manquées au redémarrage.

14. Cliquez sur **Appliquer** pour définir vos choix.

15. Cliquez sur **OK** pour fermer le Planificateur et retourner à la console principale. La tâche s'affiche maintenant sur l'onglet Tâches de la console pour l'objet ou le groupe.

REMARQUE : La tâche ne sera exécutée que la valeur de la section Activé de l'onglet Tâches est « True ». Voir Figure 5-3 à la page 125. Si la valeur de la section Activé de l'onglet Tâches est « False », la tâche ne sera pas exécutée.

Options de planification avancées

Vous pouvez entrer des options de planification avancées lorsque vous sélectionnez des fréquences quotidienne, hebdomadaire, mensuelle ou unique.

Pour utiliser la fenêtre Options de planification avancées :

1. Définissez une tâche, selon la procédure « Pour planifier une tâche : » à la page 124.

    Les tâches futures récurrentes doivent être planifiées pour une exécution quotidienne, hebdomadaire ou mensuelle. Les tâches qui sont exécutées une fois peuvent être définies comme des tâches futures dans la partie inférieure de l'onglet Planifier.

2. Cliquez sur **Avancées...** sur l'onglet Planifier pour ouvrir la fenêtre Options de planification avancées (Figure 5-7).

Figure 5-7. Fenêtre Options de planification avancées

3. Sélectionnez la flèche de la liste déroulante dans la zone **Date de début** pour ouvrir le calendrier. Acceptez la date d'aujourd'hui ou utilisez les flèches de direction pour sélectionner une date future. Si vous indiquez une date dans le passé, la tâche sera exécutée dès sa planification.

4. Sélectionnez la date souhaitée pour revenir à la fenêtre Options de planification avancées, puis cliquez sur **OK** pour revenir à l'onglet Planifier.

Rapports et requêtes 6

Anti-Virus Informant, qui est installé avec ePolicy Orchestrator, offre une fonction de rapport puissante à l'échelle de l'entreprise. Vous pouvez générer toute une série de rapports et de requêtes utiles à partir des informations recueillies par ePolicy Orchestrator.

REMARQUE : Le logiciel ePolicy Orchestrator ne peut recevoir que les informations provenant des ordinateurs sur lesquels des agents ont été installés et qui fonctionnent correctement. Pour de plus amples informations concernant l'installation de l'agent sur vos ordinateurs, consultez le « L'agent » à la page 85.

Ce chapitre décrit Anti-Virus Informant, son mode d'utilisation, ainsi que son interaction avec le serveur ePolicy Orchestrator. Les fonctions supplémentaires d'Anti-Virus Informant sont décrites au chapitre 7, « Modèles de rapports par défaut ».

A propos d'Anti-Virus Informant

Vous pouvez alors utiliser une console pour accéder à la base de données Anti-Virus Informant et générer des rapports et des requêtes (Figure 6-1 à la page 136). La base de données recueille deux types d'informations :

- **Informations sur les propriétés du produit et de l'ordinateur**

  Ces informations sur les propriétés comprennent les numéros de version des produits anti-virus et les fichiers de définition de virus (DAT) utilisés par les ordinateurs.

- **Informations d'alerte et d'activité anti-virus**

  Ces informations d'alerte comprennent les types de virus détectés et les actions entreprises par les produits anti-virus pour éviter toute infection.

La Figure 6-1 montre comment les informations provenant des produits anti-virus (sur les ordinateurs où ont été installés les agents ePolicy Orchestrator) sont collectées par le serveur ePolicy Orchestrator et mises à la disposition d'Anti-Virus Informant.

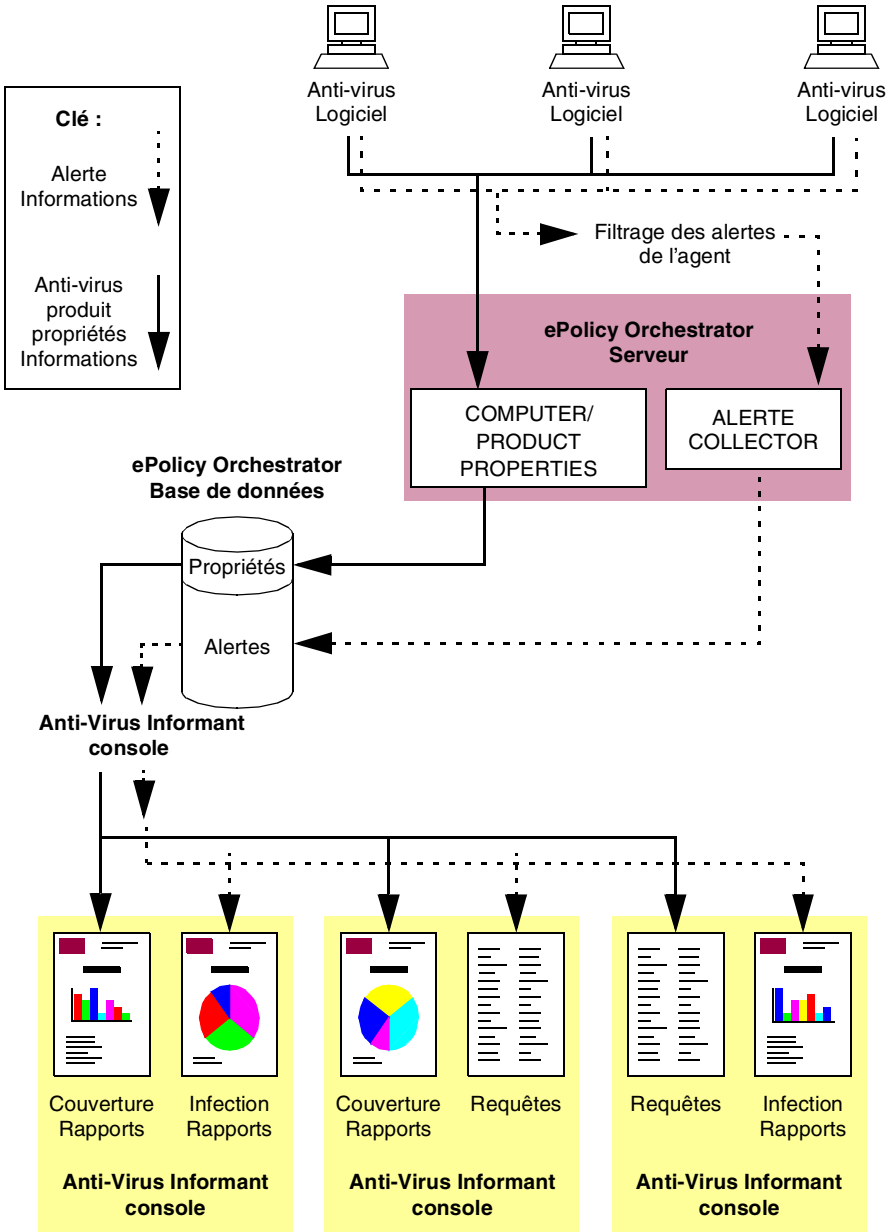


Figure 6-1. Les informations circulent par le serveur ePolicy Orchestrator vers le serveur et les consoles Anti-Virus Informant

Accès aux serveurs ePolicy Orchestrator multiples

Si plusieurs serveurs ePolicy Orchestrator sont installés sur votre réseau, vous pouvez vous connecter à eux via Anti-Virus Informant pour configurer les options de rapports et générer ces derniers. Le processus de configuration, ainsi que les informations disponibles pour vos rapports (depuis la base de données du serveur), dépendent des privilèges du compte que vous utilisez lorsque vous vous connectez aux serveurs.

Fonctions d'Anti-Virus Informant

Anti-Virus Informant vous permet de :

- Configurer les options générales Voir « Configuration des options générales d'Anti-Virus Informant » à la page 139.
- Configurer le filtre d'alertes de la base de données d'un serveur, de façon à ce que l'agent de la base de données n'envoie que les informations d'alerte que vous voulez recueillir et rejette les autres informations d'alerte. Cela vous permet de vous concentrer sur les informations qui vous intéressent et d'empêcher la base de données de se développer trop excessivement et trop rapidement. Voir « Filtrage de la base de données ePolicy Orchestrator » à la page 143.
- Générer des rapports graphiques à partir des informations contenues dans la base de données et, le cas échéant, personnaliser les rapports. Vous pouvez imprimer les rapports et les exporter pour les utiliser dans d'autres logiciels. Voir « Noms de noeuds » à la page 149.
- Générer des requêtes sur les informations contenues dans la base de données. Voir « Génération de requêtes » à la page 158.

Rapports graphiques

Anti-Virus Informant offre plus de 20 modèles de rapports par défaut que vous pouvez utiliser pour générer différents types de rapports d'information, tels que la fréquence de détection d'un virus particulier. Vous pouvez personnaliser vos rapports pour vous concentrer sur les informations désirées, telles que la fréquence de détection d'un virus particulier *pendant une semaine*.

Vous pouvez également ajouter vos propres modèles de rapports personnalisés à Anti-Virus Informant ; consultez « Création de vos propres modèles de rapports » à la page 157.

Vous pouvez générer deux types de rapports pour vos serveurs ePolicy Orchestrator. Les rapports comportent des informations pour les ordinateurs gérés par les serveurs et ils peuvent être restreints à un sous-ensemble d'ordinateurs, en fonction des privilèges du compte ePolicy Orchestrator que vous utilisez pour vous connecter aux serveurs :

- Les **Rapports d'infection** fournissent un historique des alertes et de l'activité anti-virus relatif à vos produits anti-virus. Un rapport d'infection peut, par exemple, détailler le nombre de virus détectés. Reportez-vous au paragraphe « Rapports d'infection » à la page 174 pour de plus amples informations.

- Les **Rapports de couverture** fournissent des « instantanés » de la protection anti-virus actuellement active sur vos ordinateurs, telles qu'ils sont collectés par le serveur. Un rapport de couverture peut, par exemple, détailler les versions actuellement installées des fichiers de définition de virus (.DAT) et des moteurs anti-virus.

  Deux des rapports de couverture fournissent des informations sur les produits anti-virus non compatibles. Il s'agit des **Rapports de couverture du produit**. Le Résumé de l'absence de protection AV (No AV Protection Summary) et le Résumé de la protection du produit (Product Protection Summary) collectent des informations sur les versions 5.0, 6.0, 7.0 et 7.5 des produits Norton Anti-Virus Corporate. Reportez-vous au paragraphe « Domaines d'application » à la page 167 pour de plus amples informations.

Vos rapports peuvent être imprimés ou exportés dans différents formats, afin que vous puissiez les incorporer à votre travail et les partager avec vos collègues, y compris :

- Microsoft Word pour Windows (.DOC)
- Fichiers .RTF (Rich Text Format)
- Hyper Text Markup Language (HTML) à utiliser comme page Web

Accès à Anti-Virus Informant

Anti-Virus Informant permet à l'administrateur de générer des rapports basés sur les rôles pour contrôler les installations anti-virus et identifier la source des infections virales.

Configuration des options générales d'Anti-Virus Informant

Vous pouvez configurer des options générales pour Anti-Virus Informant qui affectent le mode de fonctionnement de la console.

Pour configurer des options générales pour Anti-Virus Informant :

1. Dans l'arborescence de la console Anti-Virus Informant, cliquez avec le bouton droit de la souris sur **Anti-Virus Informant**, puis sélectionnez **Options** dans le menu qui apparaît.
2. Dans la zone **Général**, sélectionnez les options souhaitées et désélectionnez les options non souhaitées :
   - **Ajouter une machine locale à la liste des serveurs si un serveur ePO est détecté**
     Si vous utilisez Anti-Virus Informant sur le même ordinateur que le serveur ePolicy Orchestrator, le logiciel inclut automatiquement le serveur dans les **Bases de données AVI**.
   - **Crypter et enregistrer les mots de passe entre les sessions** — Le logiciel encode et enregistre les mots de passe pour les serveurs dans les **Bases de données AVI**, de sorte que vous n'avez pas besoin de vous connecter aux serveurs pendant chaque session de la console.

     REMARQUE : Si vous avez des droits d'administrateur sur un ou plusieurs serveurs, McAfee vous recommande de vérifier que votre ordinateur est protégé par un mot de passe afin que d'autres utilisateurs ne puissent pas accéder directement aux serveurs via la console.

     Si d'autres utilisateurs peuvent accéder à la console, ils peuvent modifier les paramètres de Anti-Virus Informant pour les serveurs (ceux accédés avec des comptes d'administrateur) et supprimer la totalité des alertes de la base de données.

3. Dans la zone **Connexion SQL**, modifiez les valeurs des délais de connexion et de requête qu'Anti-Virus Informant utilise lorsqu'il accède à la base de données. Cela vous permet d'étendre les heures si vous rencontrez des retards ou des erreurs de réseau, comme des délais SQL au travers d'un lien WAN (Wide Area Network). Les valeurs s'expriment en secondes.
4. Dans la zone **Requêtes**, sélectionnez les tableaux temporaires Regenerate après la valeur. Les valeurs sont exprimées en secondes.
5. Une fois les options générales configurées, cliquez sur **X** pour fermer la fenêtre.

Accès à un serveur ePolicy Orchestrator

Avant de pouvoir utiliser Anti-Virus Informant pour configurer et générer des rapports pour un serveur ePolicy Orchestrator, vous devez :

1. Ajouter le serveur au groupe de serveurs du logiciel.

   Si vous utilisez Anti-Virus Informant sur le même ordinateur que le serveur ePolicy Orchestrator, le serveur est, par défaut, automatiquement inclus dans le groupe de serveurs. Vous pouvez configurer Anti-Virus Informant pour qu'il n'ajoute pas le serveur.

   Vous pouvez ajouter plusieurs serveurs ePolicy Orchestrator au groupe de serveurs. Vous avez besoin d'ajouter un serveur une seule fois, car les informations du serveur sont stockées par Anti-Virus Informant.

2. Vous connecter au serveur à l'aide du compte ePolicy Orchestrator requis.

   A chaque ouverture d'une session Anti-Virus Informant, vous devez vous connecter à un serveur avant de pouvoir configurer et générer des rapports pour ce serveur.

   Les droits du compte que vous utilisez pour vous connecter au serveur déterminent le niveau de configuration que vous pouvez exécuter ainsi que les informations qui sont disponibles pour vos rapports (depuis la base de données du serveur).

Pour ajouter un serveur au groupe de serveurs d'Anti-Virus Informant :

1. Dans l'arborescence de la console Anti-Virus Informant, cliquez avec le bouton droit de la souris sur **Bases de données AVI**, puis sélectionnez **Ajouter un nouveau serveur** (Figure 6-2).

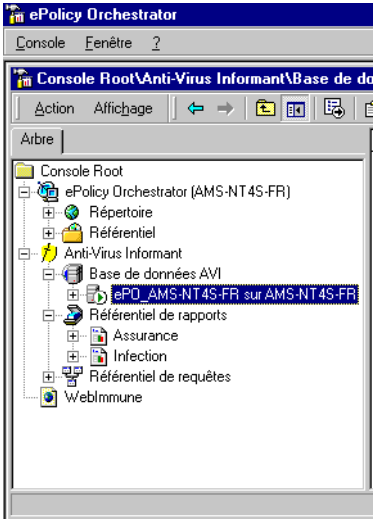


Figure 6-2. Ajouter un nouveau serveur de base de données AVI

2. Sélectionnez le **nom du serveur**.
3. Sélectionnez le **type d'authentification** dans la liste déroulante :

   - **Utilisateur actuellement connecté —** Sélectionnez ce type si vous voulez utiliser les références de l'utilisateur actuellement connecté.
   - **Authentification ePO —** Sélectionnez ce type si vous voulez utiliser les références d'ePolicy Orchestrator. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.
   - **Authentification SQL —** Sélectionnez ce type si vous configurez votre base de données MSDE ou SQL Server 7 pour qu'elle utilise l'authentification SQL. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.

- **Authentification Windows NT —** Sélectionnez ce type si vous configurez votre base de données MSDE ou SQL Server 7 pour qu'elle utilise l'authentification NT. En sélectionnant cette option, vous activez également **Domaine**. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur, un mot de passe et un domaine valides.

4. Cliquez sur **OK**.

La console ajoute le serveur au groupe de serveurs. Cela peut prendre quelques minutes, en fonction de l'état d'occupation de votre réseau. Lorsque la console s'est connectée, une icône du serveur s'affiche dans les bases de données AVI.

Pour vous connecter à un serveur :

1. Dans l'arborescence de la console Anti-Virus Informant, mettez en surbrillance l'icône de serveur requise dans **Bases de données AVI**, puis cliquez avec le bouton droit et sélectionnez **Connecter**.
2. Entrez le **nom d'utilisateur** et le **mot de passe** dans la zone Informations de compte.
3. Cliquez sur **Options** pour entrer les informations de connexion.

   REMARQUE : Le compte d'utilisateur doit être configuré pour le serveur dans la console ePolicy Orchestrator que vous utilisez. Si le compte d'utilisateur ne possède pas de droits d'administrateur général :

   - Vous ne pouvez pas *configurer* les options de rapport du serveur, mais vous pouvez *afficher* les paramètres.
   - Vos rapports et requêtes créés se limitent aux informations (depuis la base de données du serveur) qui portent sur les ordinateurs affectés à votre compte d'utilisateur.

   Pour des informations sur la configuration de comptes d'utilisateur ePolicy Orchestrator, consultez « Gestion de comptes » à la page 76.

   ---

4. Cliquez sur **OK**.

   Vous pouvez désormais utiliser Anti-Virus Informant avec le serveur ePolicy Orchestrator.

Filtrage de la base de données ePolicy Orchestrator

Le logiciel Anti-Virus Informant vous permet de configurer le filtre d'alertes de la base de données d'un serveur, de manière à ce que la base de données n'enregistre que les informations d'alerte que vous voulez recueillir (Figure 6-3). Les informations d'alerte non requises sont éliminées afin de ne pas augmenter la taille de la base de données.

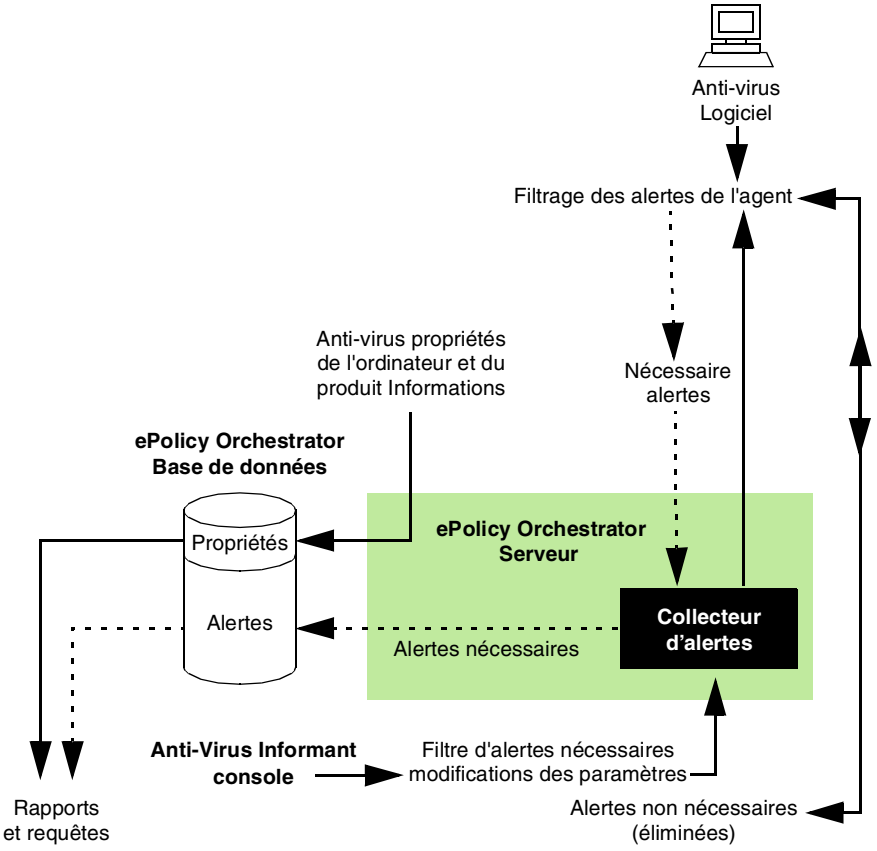


Figure 6-3. Filtre d'alertes

Par défaut, le filtre d'alertes est configuré pour rejeter les alertes de service, telles que celles générées lors du démarrage et de l'arrêt des produits anti-virus. La plupart des messages d'alerte de ce type peuvent être générés, augmentant ainsi la taille de la base de données.

Avant de générer des rapports ou des requêtes, vous souhaiterez peut-être configurer le filtre pour garantir que vos rapports et requêtes futurs n'incluront pas d'informations non souhaitées.

Vous pouvez également supprimer des alertes de la base de données ; voir « Suppression d'alertes de la base de données d'ePolicy Orchestrator » à la page 146.

REMARQUE : Le filtre d'alertes n'affecte *pas* les informations de propriétés de l'ordinateur et du produit qui sont enregistrées dans la base de données.

Pour configurer le filtre d'alertes d'un serveur :

1. Dans l'arborescence de la console des bases de données AVI, naviguez vers l'élément **Alertes** sous le serveur.

   Vous devez posséder des droits d'administrateur général pour *configurer* le filtre d'alertes du serveur. Les autres utilisateurs peuvent *afficher* les paramètres.

2. Cliquez sur l'élément **Alertes**.

   Le volet Détails de la console affiche l'écran Filtrage des alertes (Figure 6-4), indiquant ainsi les paramètres actuels du filtre.

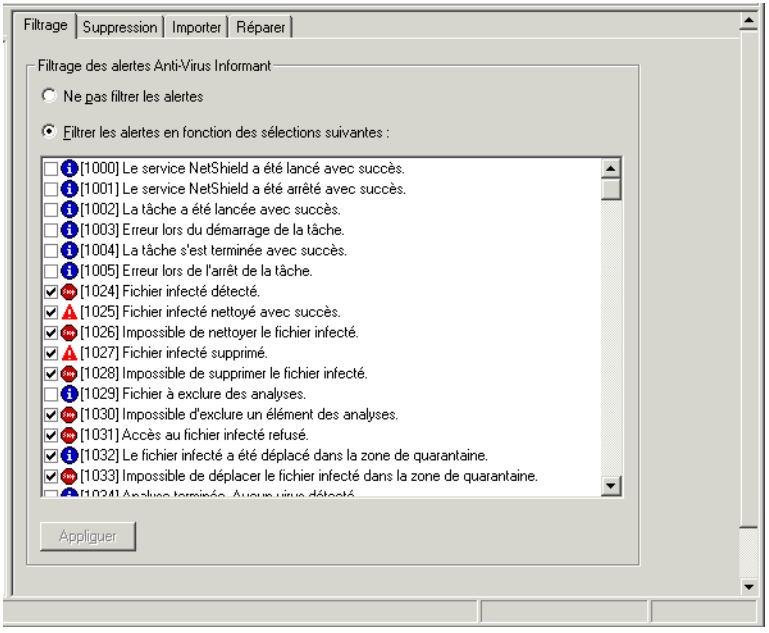


Figure 6-4. Filtrage des alertes

Si le filtre est activé, l'écran énumère les différents messages d'alerte qui peuvent être enregistrés dans la base de données. Les éléments suivants s'affichent pour chaque message d'alerte :

- Une case à cocher qui indique si le message d'alerte a été filtré.

  Les messages d'alerte sélectionnés sont enregistrés dans la base de données du serveur pour être utilisés dans vos rapports et requêtes. Les autres messages d'alerte sont éliminés.

- Une icône de gravité. La gravité est dictée par vos produits anti-virus. Les niveaux de gravité (dans l'ordre) sont :

   Informationnel

   Avertissement

   Mineur

   Majeur

   Critique

- Un numéro ID unique.
- Une description.

3. Le filtre est activé par défaut. Pour désactiver le filtre, sélectionnez **Ne pas filtrer les alertes**.
4. Dans la zone de liste :
   - Décochez les cases des messages d'alerte à supprimer.
   - Cochez les cases des messages d'alerte à conserver.

   AVERTISSEMENT : Si vous désactivez le filtre ou que vous conservez des messages d'alerte qui sont générés lors du démarrage et de l'arrêt des produits anti-virus, tels que des alertes de service, la base de données risque d'augmenter excessivement. McAfee vous recommande d'activer le filtre et de désélectionner ces alertes.

5. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

> **REMARQUE :** Le filtre n'affecte pas les alertes qui se trouvent *déjà* dans la base de données.

Pour de plus amples informations concernant la génération de rapports basés sur les informations contenues dans la base de données, consultez « Noms de noeuds » à la page 149.

Suppression d'alertes de la base de données d'ePolicy Orchestrator

Anti-Virus Informant vous permet de supprimer de la base de données des alertes qui ne vous sont plus nécessaires. La suppression de ces alertes réduit la taille de la base de données.

> **REMARQUE :** McAfee vous recommande de sauvegarder votre base de données *avant* d'effectuer cette action, afin que vous puissiez rétablir la base de données si nécessaire ; voir « Sauvegarde et restauration de la base de données d'ePolicy Orchestrator » à la page 210, pour plus informations.

Pour supprimer des alertes de la base de données d'ePolicy Orchestrator :

1. Exécutez la procédure de l'Etape 1 à l'étape 2 à la page 144.
2. Cliquez sur l'onglet **Suppression**.
3. Sélectionnez les événements d'alerte que vous souhaitez supprimer de la base de données. Spécifiez des jours ou des dates, si nécessaire.
4. Cliquez sur **Démarrer**.

   Un message apparaît, signalant que le processus de suppression des alertes ne peut être exécuté et demandant si vous souhaitez poursuivre la suppression de ces alertes.
5. Cliquez sur **Oui**.

   Anti-Virus Informant supprime les alertes de la base de données du serveur. La zone de texte au bas de l'écran affiche l'état du processus de suppression.

Importation d'alertes de la base de données d'ePolicy Orchestrator

Le logiciel Anti-Virus Informant vous permet d'importer des alertes d'une autre base de données dans la base de données actuelle. Par exemple, vous souhaitez :

- Accéder aux alertes d'une base de données créée par le logiciel Anti-Virus Informant 1.x. La base de données du logiciel Anti-Virus Informant 2.0 comporte un schéma de base de données légèrement différent, de sorte que vous devez importer les alertes de la base de données 1.x dans une base de données 2.0 avant de pouvoir les utiliser avec le logiciel 2.0.
- Importez les alertes d'une ancienne base de données dans la base de données actuelle, de sorte que vous pouvez inclure les alertes dans vos rapports.

IMPORTANT : McAfee vous recommande de sauvegarder votre base de données *avant* d'effectuer cette action, afin que vous puissiez rétablir la base de données si nécessaire ; voir « Sauvegarde et restauration de la base de données d'ePolicy Orchestrator » à la page 210, pour plus informations.

Pour importer des alertes de la base de données d'ePolicy Orchestrator :

1. Exécutez la procédure de l'Etape 1 à l'étape 2 à la page 144.
2. Cliquez sur l'onglet **Importer**.
3. Sélectionnez la base de données SQL qui contient la base de données dans laquelle sont stockées les alertes que vous souhaitez importer.
4. Entrez le nom de la base de données.
5. Entrez l'**ID de connexion SQL** et le **Mot de passe** pour la base de données.

   REMARQUE : Vous devez utiliser un compte administratif global ePolicy Orchestrator.

6. Pour importer uniquement les alertes qui ne figurent pas déjà dans la base de données actuelle, laissez sélectionné **Importer uniquement les événements qui n'ont pas déjà été importés**. Sinon, sélectionnez **Importer tous les événements**.

   REMARQUE : Vous devez savoir qu'utiliser l'option **Importer tous les événements** peut introduire des alertes en double dans la base de données.

7. Cliquez sur **Démarrer**.

   Anti-Virus Informant importe les alertes dans la base de données actuelle.

8. Exécutez la fonction de réparation ; exécutez l'étape 2 à la page 149 et l'étape 3 à la page 149.

Réparation des alertes de la base de données

Le logiciel Anti-Virus Informant enregistre les identificateurs uniques globaux (ou ID), ainsi que les alertes dans la base de données afin d'identifier les ordinateurs qui les ont générés et afin que vous puissiez créer des rapports d'infection précis.

Chaque ordinateur possède un ID unique. Dans certaines circonstances, les ID peuvent toutefois changer, ce qui entraînerait la mise hors phase des ID de la base de données avec les ordinateurs de votre réseau. Ces informations sont les suivantes :

- Utilisation d'une image couramment enregistrée (du logiciel et du matériel) pour reconstruire un ou plusieurs de vos ordinateurs.
- Modification de la carte d'interface réseau (NIC) dans un ou plusieurs de vos ordinateurs.
- Mise à niveau de l'agent de la version 1.x à la version 2.0, ce qui crée un nouvel ID.

Anti-Virus Informant possède une fonction qui peut réparer les ID de la base de données en les synchronisant par nom d'ordinateur.

IMPORTANT : Si des informations incorrectes sur les ID ne sont pas réparées, vos rapports d'infection peuvent contenir des informations inexactes.

Il est recommandé de sauvegarder votre base de données *avant* d'effectuer cette action, afin que vous puissiez rétablir la base de données si nécessaire. Reportez-vous au paragraphe « Sauvegarde et restauration de la base de données d'ePolicy Orchestrator » à la page 210 pour de plus amples informations.

Pour réparer des alertes de la base de données d'ePolicy Orchestrator :

1. Exécutez la procédure de l'Etape 1 à l'étape 2 à la page 144.
2. Cliquez sur l'onglet **Réparer**.
3. Cliquez sur **Démarrer**.

   Anti-Virus Informant vérifie les alertes de la base de données et répare les informations sur les ID aux emplacements nécessaires.

   REMARQUE : La fonction de réparation utilise les noms d'ordinateurs pour réparer les alertes. Si un ordinateur a été renommé, ses alertes ne peuvent pas être réparées. Vous pouvez exécuter le script SQL suivant sur la base de données pour remplacer le nom d'ordinateur des alertes appropriées par le nouveau nom de l'ordinateur :

   ```
   UPDATE Events SET HostName='Newname' WHERE
   HostName='Oldname'
   ```

   Où `Newname` et `Oldname` sont les noms de l'ordinateur.

Noms de noeuds

Les événements sont liés aux noeuds. Il est donc important de comprendre comment cette relation affecte les informations qui s'affichent dans les rapports.

Le cas échéant, les rapports d'infection affichent le nom du noeud ePO associé à chaque événement. Les utilisateurs qui ne disposent pas de droits d'administrateur voient toujours le champ de nom du noeud, car ils ne peuvent voir que les événements associés aux noeuds qu'ils sont autorisés à voir. Il est important que les utilisateurs ne disposant pas de droits d'administrateur réparent les événements perdus, afin que les noeuds s'affichent correctement dans les rapports.

Les utilisateurs disposant de droits d'administrateur doivent être en mesure d'afficher tous les événements du système, y compris les événements sans ID correspondant (ou dont l'ID est perdu) et les événements des ordinateurs qui ont récemment été supprimés d'ePolicy Orchestrator (orphelins). Lorsqu'un filtre de rapports est défini, les utilisateurs administratifs ne voient que le champ contenant le nom du noeud dans les rapports d'infection. Dans le cas contraire, la valeur par défaut du champ de nom de noeud est <Un-Named>. Les utilisateurs administratifs peuvent afficher des événements sans devoir au préalable se connecter aux noeuds.

Génération de rapports

Anti-Virus Informant vous permet de générer des rapports pour les serveurs ePolicy Orchestrator auxquels vous êtes connecté. Ces rapports se fondent sur un sous-ensemble d'informations de la base de données du serveur, en fonction des éléments suivants :

- Les droits de votre compte ; voir page 142.
- Le filtre de rapports actuel. Vous pouvez générer des rapports pour un *sous-ensemble* des ordinateurs affectés à votre compte de site ; voir page 151.
- Le rapport et sa personnalisation éventuelle ; voir page 152.

Types de rapports

Le logiciel possède plus de 20 rapports graphiques différents que vous pouvez personnaliser à votre convenance. Les rapports se divisent en deux groupes :

- Les **rapports d'infection** fournissent un historique des alertes et de l'activité anti-virus relatif à vos produits anti-virus.

  Ces rapports se fondent sur les informations d'alerte enregistrées dans la base de données du serveur (Figure 6-5 à la page 151). McAfee vous recommande de configurer le filtre d'alertes de la base de données *avant* de générer un rapport, de façon à ce que vos rapports futurs ne comprennent aucune information non nécessaire. Voir « Filtrage de la base de données ePolicy Orchestrator » à la page 143.

- Les **rapports de couverture** fournissent des « instantanés » de la protection anti-virus actuellement active sur vos ordinateurs.

  Ces rapports se fondent sur les informations relatives aux propriétés de l'ordinateur et du produit, enregistrées dans la base de données du serveur (Figure 6-5 à la page 151).

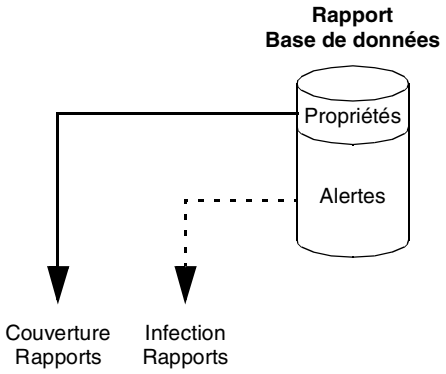


Figure 6-5. Génération de rapports

Pour de plus amples informations concernant les modèles de rapports par défaut que vous pouvez utiliser, consultez « Modèles de rapports par défaut » à la page 167. Pour utiliser vos propres modèles de rapports personnalisés créés avec le produit Crystal Report Designer de Seagate Software, consultez « Création de vos propres modèles de rapports » à la page 157.

Définition d'un filtre de rapports

Chaque serveur ePolicy Orchestrator rassemble des informations depuis les ordinateurs de votre réseau, en fonction des paramètres de votre serveur. Lorsque vous vous connectez à un serveur ePolicy Orchestrator, vous pouvez générer des rapports et des requêtes pour les ordinateurs qui sont affectés au compte de site que vous utilisez. Anti-Virus Informant vous permet de définir un filtre de rapports, de sorte que vous pouvez générer des rapports pour un *sous-ensemble* d'ordinateurs. Définir un filtre de rapports peut permettre d'améliorer les temps de réponse des rapports et requêtes.

Par exemple, si votre compte de réviseur peut générer des rapports et des requêtes pour deux services, comme le service commercial et la finance, vous souhaiterez peut-être générer des rapports pour un seul service.

REMARQUE : Le filtre de rapports n'est *pas* le même que le filtre d'alertes. Le filtre de rapports s'applique à Anti-Virus Informant que vous utilisez (à l'intérieur de la console ePolicy Orchestrator) et il n'est *pas* copié sur le serveur ePolicy Orchestrator.

Pour des informations sur la configuration de comptes de réviseur ePolicy Orchestrator, consultez « Gestion de comptes » à la page 76.

Pour définir le filtre de rapports :

1. Dans l'arborescence de la console Anti-Virus Informant, cliquez avec le bouton droit de la souris sur l'icône du serveur requis dans les **Bases de données AVI**, puis sélectionnez **Définir un filtre de rapports** dans le menu qui apparaît.

   La fenêtre Filtrage des rapports s'affiche.

   > **REMARQUE :** Le filtre de rapports affiche les groupes d'ordinateurs qui sont affectés au compte de site que vous utilisez. Le filtre de rapports n'affiche pas les groupes vides et les ordinateurs sur lesquels les agents ePolicy Orchestrator ne sont pas installés.

2. Sélectionnez le groupe requis pour lequel vous souhaitez générer des rapports et des requêtes. Vos rapports et requêtes incluent les informations pour tous les ordinateurs du groupe et tous les groupes subordonnés.
3. Cliquez sur **OK**.

Génération et personnalisation d'un rapport

Pour générer un rapport :

1. Dans l'arborescence de la console Anti-Virus Informant, ouvrez le **Référentiel de rapports**, puis sélectionnez **Couverture**, **Infection** ou votre propre groupe de rapports.

   Si vous avez récemment installé le serveur ePolicy Orchestrator, il est possible que la base de données ne contienne *pas* d'informations étant donné que le serveur n'a pas reçu ces informations des agents ePolicy Orchestrator de vos ordinateurs. Si c'est le cas, un message s'affiche et vous informe qu'il n'y a pas de données dans la base de données. Les rapports que vous générez dépendent de ces informations, c'est pourquoi vous devez attendre que ces informations filtrent à travers la base de données.

L'écran Rapport (Figure 6-6) situé dans le volet Détails de la console répertorie les modèles de rapports pour l'élément de rapports que vous avez sélectionné.

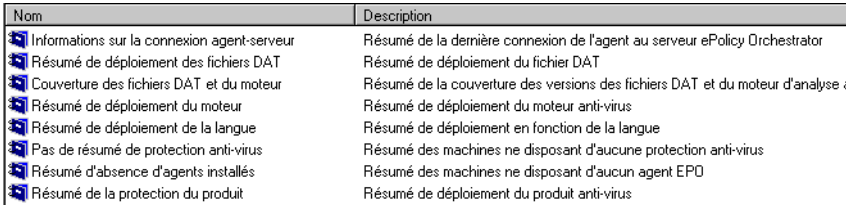


Figure 6-6. Rapports de couverture

Les éléments suivants s'affichent pour chaque modèle de rapport :

- Nom du modèle.
- Description de ce que le modèle est configuré pour indiquer.
- Nom de fichier du modèle.

Pour des détails concernant les modèles de rapports par défaut et les informations qu'ils peuvent fournir, consultez « Modèles de rapports par défaut » à la page 167.

2. Double-cliquez sur le rapport que vous voulez générer.

   Une fenêtre s'affiche et vous demande si vous voulez personnaliser le rapport. La personnalisation de votre rapport vous permet de vous concentrer sur le sous-ensemble d'informations que vous voulez afficher. Par exemple, si vous affichez la fréquence de détection d'un virus, vous pouvez spécifier les virus qui vous intéressent.

3. Choisissez si vous voulez personnaliser le rapport :

   - Pour personnaliser le rapport, cliquez sur **Oui**.
   - Pour générer le rapport sans le personnaliser, sélectionnez **Non**.

4. Si vous générez un rapport de couverture, vous pourriez être amené à entrer des informations pertinentes pour le rapport, comme la version .DAT requise. Entrez les informations nécessaires, puis cliquez sur **OK**.

   Si vous choisissez de personnaliser le rapport (à l'étape 3 à la page 153), passez à l'Etape 5 ci-dessous. Sinon, passez à l'étape 10 à la page 156.

5. La fenêtre Configurer le rapport s'affiche (Figure 6-7 à la page 154). Elle contient les pages de propriétés des différents *types* d'informations que vous pouvez personnaliser pour le rapport.

Chaque page de propriétés vous permet de spécifier les conditions d'identification des valeurs requises pour ce type d'informations. Par défaut, toutes les conditions des pages de propriétés sont configurées sur « toute valeur ».

Vous pouvez utiliser des pages de propriétés multiples pour cibler plus avant votre rapport. Par exemple, si vous voulez vous concentrer sur un type de virus pendant une période de temps, vous devez spécifier les conditions requises dans les pages de propriété Nom du virus et Heure et date de l'événement.

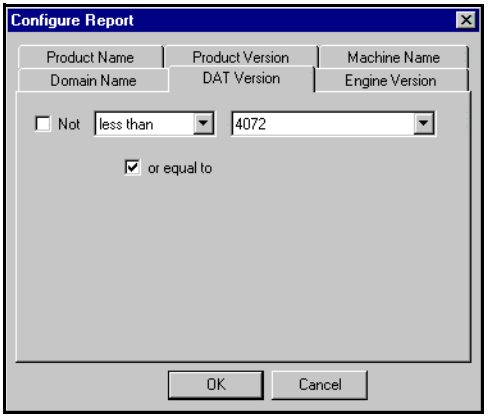


Figure 6-7. Configurer le rapport

Pour spécifier les conditions d'un type d'informations :

a. Cliquez sur l'onglet du type d'informations, tel que **Nom du produit**.

   La page de propriétés du type d'informations s'affiche.

b. Sélectionnez l'opérateur nécessaire pour cette condition, tel que « égal à ».

   Selon l'opérateur sélectionné, un ou plusieurs champs supplémentaires s'affichent dans la page de propriétés. Ceux-ci vous permettent de compléter la condition en spécifiant les valeurs requises.

   Une case à cocher **Ne pas** peut s'afficher. Si vous sélectionnez cette option, elle nie l'opérateur. Par exemple, si vous avez spécifié « égal à », la sélection de cette case à cocher rend l'opérateur « non égal à ».

c. Sélectionnez les valeurs requises.

La première fois que vous sélectionnez une valeur, Anti-Virus Informant accède à la base de données pour compléter ses champs avec des valeurs réelles de votre base de données.

6. Lorsque vous avez fini de spécifier toutes les conditions dont vous avez besoin pour personnaliser votre rapport, cliquez sur **OK**.

Une fenêtre s'affiche et vous donne un récapitulatif de vos conditions.

7. Pour indiquer vos conditions dans votre rapport, sélectionnez **Afficher dans le rapport**.

Les conditions apparaissent sous la forme de quelques lignes de texte dans le rapport, identifiant ainsi la méthode de personnalisation du rapport. Cela est utile pour :

- Mettre en surbrillance le fait que le rapport se base sur un *sous-ensemble* d'informations de la base de données.
- Se rappeler les conditions que vous avez utilisées, au cas où vous devriez restaurer le rapport dans le futur.

8. Pour générer votre rapport, cliquez sur **OK**. Sinon, cliquez sur **Annuler**.

9. Pour certains rapports, une fenêtre de paramètres supplémentaire s'ouvre lorsque vous cliquez sur **OK**. Par exemple, pour le rapport Informations sur la connexion agent-serveur (Figure 6-8).

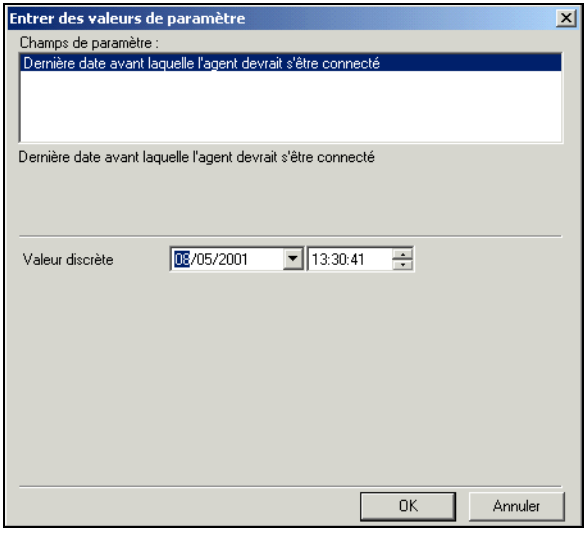


Figure 6-8. Valeurs des paramètres du rapport

Si cette fenêtre s'ouvre pour le rapport, entrez de nouvelles valeurs ou acceptez les valeurs par défaut, puis cliquez sur **OK**.

10. Anti-Virus Informant génère le rapport en fonction des informations contenues dans la base de données correspondant au type de rapport et remplit toutes les conditions que vous avez spécifiées (si vous avez personnalisé votre rapport). Le processus de génération peut prendre du temps si votre base de données est volumineuse.

    Le rapport généré s'affiche dans le volet Détails ; consultez « Fonctionnement d'un rapport généré » à la page 156. Lorsque vous souhaitez générer un rapport différent, cliquez sur le groupe de rapports dans l'arborescence de la console, à votre convenance, pour afficher les autres rapports qui sont disponibles. Si vous souhaitez générer le rapport pour un groupe d'ordinateurs différent à l'intérieur de votre compte d'utilisateur, il vous suffit de modifier le filtre de rapports ; voir « Définition d'un filtre de rapports » à la page 151.

Fonctionnement d'un rapport généré

Lorsque vous avez généré votre rapport, il apparaît dans le volet Détails avec une barre d'icônes située en haut du volet. La partie droite de la barre d'icônes affiche les éléments suivants :

- Nombre total d'enregistrements dans la base de données.
- Pourcentage d'enregistrements correspondant au rapport en question.
- Nombre d'enregistrements correspondants en fonction du nombre total d'enregistrements présents dans la base de données.

Hiérarchisation vers le bas pour de plus amples informations

Vous pouvez hiérarchiser votre rapport vers le bas pour afficher des informations textuelles plus détaillées relatives aux différentes zones, barres ou segments à secteurs du rapport. Votre pointeur de souris se transforme en icône en forme de loupe  lorsque vous le déplacez d'un élément à un autre pour lequel vous pouvez hiérarchiser vers le bas.

Pour hiérarchiser vers le bas, double-cliquez sur l'élément lorsque l'icône en forme de loupe  s'affiche. Le volet Détails se modifie pour afficher une page d'informations concernant cet élément. Certains rapports vous permettent de hiérarchiser vos rapports encore plus vers le bas pour afficher plus de pages d'informations. Lorsque vous avez fini d'afficher les informations, revenez au rapport ou à la page d'informations précédente en cliquant sur  .

Tâches Rapports

Vous pouvez exécuter les actions suivantes :

- Imprimer le rapport ou la page d'informations détaillées, en cliquant sur  .
- Restaurer le rapport en cliquant sur  , pour le mettre à jour les nouvelles informations entrées dans la base de données de rapports depuis la création du rapport.
- Exporter le rapport ou la page d'informations détaillées en cliquant sur  .

  Utilisez la fenêtre qui s'affiche pour spécifier le type d'exportation requis ainsi que l'emplacement et le nom du fichier que vous voulez créer.
- Recherchez dans le rapport un mot ou une expression en tapant sur le clavier le mot ou la phrase dans la zone de texte, puis en cliquant sur  .
- Choisissez l'agrandissement nécessaire du volet Détails afin de réduire ou d'agrandir son contenu.

Lorsque vous avez terminé d'utiliser le rapport, fermez-le en cliquant avec le bouton droit de la souris n'importe où dans le rapport, puis en choisissant **Fermer** dans le menu qui s'affiche.

Création de vos propres modèles de rapports

Si vous disposez du produit Crystal Report Designer v7 de Seagate Software, vous pouvez créer vos propres modèles de rapports personnalisés et les utiliser avec Anti-Virus Informant. Pour de plus amples informations concernant l'utilisation du produit Crystal Report Designer, veuillez vous reporter à la documentation fournie avec le produit.

Après avoir créé vos propres modèles de rapports, vous devez ajouter les fichiers de modèles (.RPT) à Anti-Virus Informant avant de pouvoir les utiliser.

Pour ajouter vos modèles de rapports personnalisés à la console Anti-Virus Informant :

1. Ouvrez la console ePolicy Orchestrator. Voir « Accès à Anti-Virus Informant » à la page 139 pour plus de détails.
2. Dans l'arborescence de la console Anti-Virus Informant, étendez le **Référentiel de rapports** en cliquant sur ⊞ près du groupe pour afficher les groupes de rapports actuels.

3. Pour créer un nouveau groupe de rapports dans lequel vous pouvez ajouter votre modèle de rapport, cliquez avec le bouton droit de la souris sur **Référentiel de rapports**, puis sélectionnez **Nouveau groupe de rapports**.

   La fenêtre Nouveau groupe de rapports s'ouvre. Entrez le nom du nouveau groupe, puis cliquez sur **OK**.

   REMARQUE : Vous pouvez créer des groupes de rapports à l'intérieur d'autres groupes de rapports.

4. Cliquez avec le bouton droit de la souris sur le groupe de rapports auquel vous souhaitez ajouter votre modèle de rapport, puis sélectionnez **Ajouter le modèle de rapport**.

5. Dans la zone de texte **Nom du rapport**, entrez le nom que vous voulez utiliser pour identifier le rapport dans l'écran Rapport.

6. Dans la zone **Fichier du rapport**, définissez le fichier pour le modèle de rapport.

   Vous pouvez localiser le fichier en cliquant sur **>>**, en sélectionnant le fichier puis en cliquant sur **OK**.

7. Dans la zone de texte **Description**, entrez une brève description du rapport que vous voulez afficher dans l'écran Rapport.

8. Lorsque vous êtes prêt à ajouter le modèle de rapport, cliquez sur **OK**.

   Anti-Virus Informant ajoute le modèle de rapport au groupe de rapports. Le groupe **Référentiel de rapports** est dupliqué dans le groupe **Rapports** pour chaque serveur du **Groupe de serveurs ePO** de la console, ce qui vous permet de générer votre rapport pour les serveurs. Pour de plus amples informations sur la génération de rapports, consultez « Noms de noeuds » à la page 149.

Génération de requêtes

Le logiciel Anti-Virus Informant vous permet de générer des requêtes pour les serveurs ePolicy Orchestrator auxquels vous êtes connecté. Ces requêtes dépendent d'un sous-ensemble d'informations de la base de données du serveur, en fonction des éléments suivants :

- Les privilèges de votre compte ; voir page 142.
- Le filtre de rapports actuel : Vous pouvez générer des requêtes pour un *sous-ensemble* des ordinateurs affectés à votre compte de site ; voir page 151.
- La requête.

Types de requêtes

Le logiciel possède plus de 10 requêtes différentes que vous pouvez utiliser. Elles se divisent en trois groupes :

- Les **ordinateurs** fournissent des informations sur les ordinateurs de votre entreprise.

  Ces requêtes se fondent sur les informations relatives aux propriétés de l'ordinateur et du produit, enregistrées dans la base de données du serveur (Figure 6-9), recueillies dans la base de données à intervalles réguliers.

- Les **événements** fournissent des informations sur les alertes de la base de données, notamment les alertes de virus.

  Ces requêtes dépendent des informations relatives aux alertes, enregistrées dans la base de données du serveur (Figure 6-9). McAfee vous recommande de configurer le filtre d'alertes de la base de données *avant* de générer une requête, de façon à ce que vos requêtes futures ne comprennent aucune information non nécessaire. Voir « Filtrage de la base de données ePolicy Orchestrator » à la page 143.

- Les **installations** fournissent des informations sur les produits anti-virus installés sur vos ordinateurs.

  Ces requêtes se fondent sur les informations relatives aux propriétés de l'ordinateur et du produit, enregistrées dans la base de données du serveur (Figure 6-9), recueillies dans la base de données à intervalles réguliers.

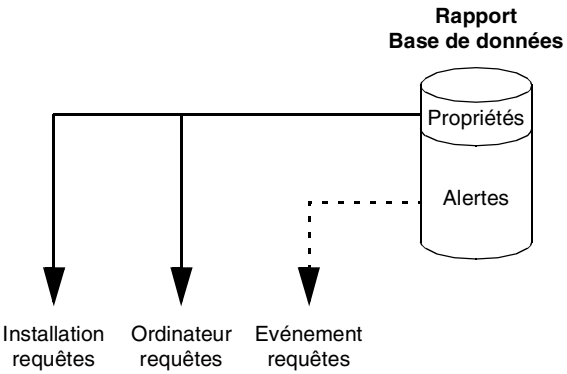


Figure 6-9. Génération de requêtes

Pour utiliser vos propres requêtes avec Anti-Virus Informant, consultez « Création de vos propres requêtes » à la page 161.

Génération d'une requête

Pour générer une requête pour un serveur :

1. Ouvrez la console ePolicy Orchestrator. Voir « Accès à Anti-Virus Informant » à la page 139 pour plus de détails.

2. Si ce n'est pas déjà fait, ajoutez le serveur requis à la console et connectez-le à celle-ci à l'aide d'un compte d'administrateur ou de réviseur.

3. Dans l'arborescence de la console Anti-Virus Informant, naviguez vers les éléments **Ordinateurs**, **Evénements** ou **Installations** dans le groupe **Requêtes**, en fonction du type de requête que vous souhaitez générer. Si vous avez créé votre propre groupe de requêtes, cliquez sur le groupe si nécessaire.

4. Cliquez sur le groupe de requêtes requis, tel que **Ordinateurs**.

   Si vous avez récemment installé le serveur ePolicy Orchestrator, il est possible que la base de données ne contienne *pas* d'informations étant donné que le serveur n'a pas reçu ces informations des agents ePolicy Orchestrator de vos ordinateurs. Si c'est le cas, un message s'affiche et vous informe qu'il n'y a pas de données dans la base de données. Les requêtes que vous générez dépendent de ces informations, c'est pourquoi vous devez attendre que ces informations filtrent à travers la base de données.

   Le volet Détails de la console affiche l'écran Requêtes, qui répertorie les requêtes disponibles dans l'élément de requêtes que vous avez sélectionné (Figure 6-10).

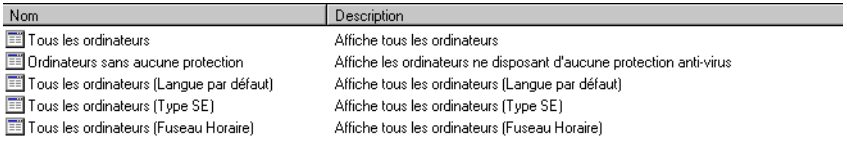


Figure 6-10. Rapports de requêtes

Les éléments suivants s'affichent pour chaque requête :

- Le nom de la requête.
- Description de ce que la requête est configurée pour afficher.
- Le nom de fichier de la requête.

5. Double-cliquez sur la requête que vous voulez générer.

   Anti-Virus Informant génère la requête basée sur les informations de la base de données qui sont pertinentes pour la requête. Le processus de génération peut prendre du temps si votre base de données est volumineuse.

   La requête générée s'affiche dans le volet Détails. Pour générer une requête différente, cliquez sur les groupes de requêtes dans l'arborescence de la console, à votre convenance, pour afficher les autres requêtes disponibles. Pour générer la requête pour un groupe d'ordinateurs différent à l'intérieur de votre compte d'utilisateur, il vous suffit de modifier le filtre de rapports. Voir « Définition d'un filtre de rapports » à la page 151.

Création de vos propres requêtes

Vous pouvez créer vos propres requêtes personnalisées pour les utiliser avec Anti-Virus Informant. Vous devez ajouter les requêtes à Anti-Virus Informant avant de pouvoir les utiliser.

Pour ajouter vos requêtes personnalisées à Anti-Virus Informant :

1. Dans l'arborescence de la console Anti-Virus Informant, étendez le **Référentiel de requêtes** en cliquant sur ⊞ en regard du groupe pour afficher les groupes de requêtes actuels.

2. Pour créer un nouveau groupe de requêtes, cliquez avec le bouton droit sur **Référentiel de requêtes**, puis sélectionnez **Nouveau groupe de requêtes**.

   La fenêtre Nouveau groupe de requêtes s'ouvre. Entrez le nom du nouveau groupe de requêtes, puis cliquez sur **OK**. Le nouveau groupe apparaît dans l'arborescence de la console.

   REMARQUE : Vous pouvez créer des groupes de requêtes à l'intérieur d'autres groupes de requêtes.

3. Cliquez avec le bouton droit de la souris sur le groupe de requêtes auquel vous souhaitez ajouter votre requête, puis sélectionnez **Ajouter le modèle de requête** dans le menu qui s'affiche.

   La fenêtre Nouvelle définition de la requête s'affiche (Figure 6-11).

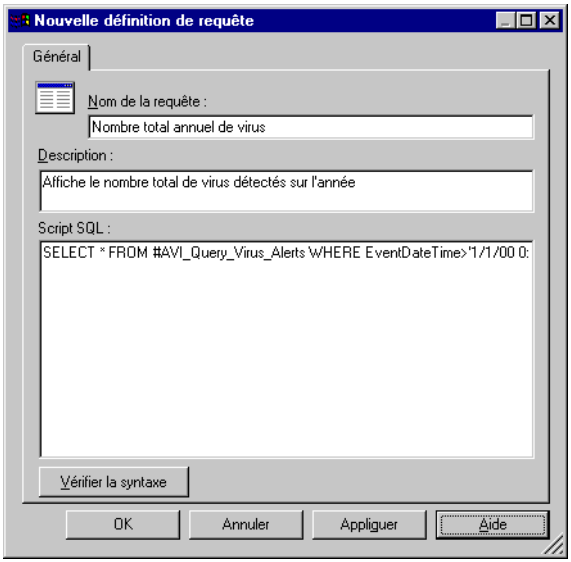


Figure 6-11. Nouvelle définition de la requête

4. Dans la zone de texte **Nom de la requête**, entrez le nom que vous voulez utiliser pour identifier la requête dans l'écran Requête.

5. Dans la zone de texte **Description**, entrez une brève description de la requête que vous voulez afficher dans l'écran Requête.

6. Dans la zone de texte **Script SQL**, entrez le script SQL qui extrait les informations requises des tables temporaires du logiciel lors de l'exécution de la requête.

REMARQUE : Vous ne pouvez pas créer des requêtes qui possèdent plusieurs sous-ensembles de résultats, tels que l'exécution de procédures enregistrées.

Le format de la requête SQL est :

```
SELECT * FROM <tablename> WHERE <field>='<value>'
```

Par exemple, pour obtenir les alertes de virus pour l'année, entrez cette requête :

```
SELECT * FROM Events WHERE EventDateTime>'1/1/00
0:00:01 AM'
```

ASTUCE : Pour afficher les champs et les formats des valeurs utilisés par une table temporaire, créez une requête de connexion avec la syntaxe suivante :

```
SELECT * FROM <tablename>
```

Par exemple :

```
SELECT * FROM Events
```

Lorsque vous générez la requête, la requête résultante affiche le contenu complet de la table, ce qui vous permet d'afficher les champs et les formats des valeurs.

Les administrateurs peuvent écrire une instruction Select SQL pour afficher n'importe quelle table de la base de données d'ePolicy Orchestrator. Les requêtes provenant de comptes non administrateurs sont filtrées pour s'assurer qu'elles ne renvoient pas de données autres que celles que le compte a le droit d'afficher. Ces utilisateurs peuvent uniquement afficher directement des données provenant des tables de rapports principales:

- Evénements
- Propriétés du produit
- Propriétés de l'ordinateur

Les données d'autres tables peuvent être affichées uniquement si elles sont rattachées à l'une de ces tables.

7. Pour tester le script SQL, cliquez sur **Vérifier la syntaxe**.

   Si plusieurs serveurs figurent dans les **bases de données AVI**, la fenêtre Choisir un serveur qui apparaît vous permet de choisir le serveur sur lequel vous souhaitez tester le script. Sélectionnez le serveur et cliquez sur **OK**.

   Si le script SQL est valide, le message résultant confirme qu'il a vérifié le script. Cliquez sur **OK** pour fermer le message.

   Si le script n'est pas valide, vous devez le corriger.

8. Lorsque vous êtes prêt à ajouter la requête, cliquez sur **OK**.

   Anti-Virus Informant ajoute la requête au groupe de requêtes. Le groupe **Référentiel de requêtes** est dupliqué dans le groupe **Requêtes** pour chaque serveur des **Bases de données AVI** de la console, ce qui vous permet de générer votre requête pour les serveurs. Pour de plus amples informations sur la génération de requêtes, consultez « Génération de requêtes » à la page 158.

Rapports de requêtes par défaut

Les requêtes par défaut suivantes sont fournies avec le logiciel.

Requêtes d'ordinateurs

- **Toutes les connexions —** Cette requête affiche le détail des propriétés de tous les ordinateurs connectés au serveur, en fonction du nom d'ordinateur.
- **Ordinateurs non protégés —** Cette requête affiche le détail des propriétés de tous les ordinateurs sur lesquels aucun produit de protection contre les virus n'est installé. Elle est triée par le nom de noeud ePO.
- **Ordinateurs par ID de langue —** Cette requête affiche le détail des propriétés de tous les ordinateurs en fonction de l'ID de langue et du nom de noeud ePO. Elle indique les paramètres de langue de l'ordinateur et peut aider l'utilisateur à prendre des décisions sur l'installation du produit.
- **Ordinateurs par type de système d'exploitation —** Cette requête affiche le détail des propriétés de tous les ordinateurs en fonction du type de système d'exploitation et du nom de noeud ePO. Elle peut aider l'utilisateur à prendre des décisions sur l'installation du produit.
- **Ordinateurs par fuseau horaire —** Cette requête affiche le détail des propriétés de tous les ordinateurs en fonction du fuseau horaire et du nom de noeud ePO. Elle peut aider l'utilisateur à prendre des décisions de planification et de trafic réseau.

- **Ordinateurs par noeud ePO —** Cette requête affiche le détail des propriétés de tous les ordinateurs en fonction du nom du noeud ePO. Le nom du noeud ePO est une fusion du nom du noeud de l'ordinateur et de celui de son parent. Ce champ peut faciliter la localisation du noeud de l'ordinateur dans la console ePolicy Orchestrator.
- **Nombre total d'ordinateurs connectés —** Cette requête affiche le nombre total d'ordinateurs connectés et liste leurs propriétés dans la base de données du serveur ePolicy Orchestrator.

Requêtes d'événements

- **Tous les événements —** Cette requête affiche tous les événements par date et heure.
- **Tous les événements par noeud ePO —** Cette requête affiche tous les événements par nom de noeud ePO, puis par date et heure.
- **Nombre total d'événements —** Cette requête affiche le nombre total d'événements.
- **Nombre total d'annonces de virus —** Cette requête affiche le nombre total d'annonces de virus.
- **Annonces de virus —** Cette requête affiche tous les événements de virus par date et heure.
- **Attaques de virus —** Cette requête affiche tous les événements de virus par nom de virus, puis par date et heure.

Requêtes d'installation

- **Toutes les installations AVI —** Cette requête affiche toutes les installations anti-virus par produit et nom de noeud ePO.
- **Toutes les installations —** Cette requête affiche toutes les installations (moteurs d'analyse anti-virus et produits de support) par produit et nom de noeud ePO.
- **Toutes les installations par noeud ePO —** Cette requête affiche toutes les installations (moteurs d'analyse anti-virus et produits de support) par nom de noeud ePO, puis par produit.
- **Nombre total d'installations AVI —** Cette requête affiche le nombre total d'installations Anti-Virus Informant.
- **Nombre total d'installations —** Cette requête affiche le nombre total d'installations.

Modèles de rapports par défaut 7

Ce chapitre décrit les modèles de rapports par défaut qui sont fournis avec Anti-Virus Informant. Lorsque vous produisez ces rapports, n'oubliez pas que vous pouvez les parcourir afin d'afficher des informations plus détaillées. Voir « Fonctionnement d'un rapport généré » à la page 156.

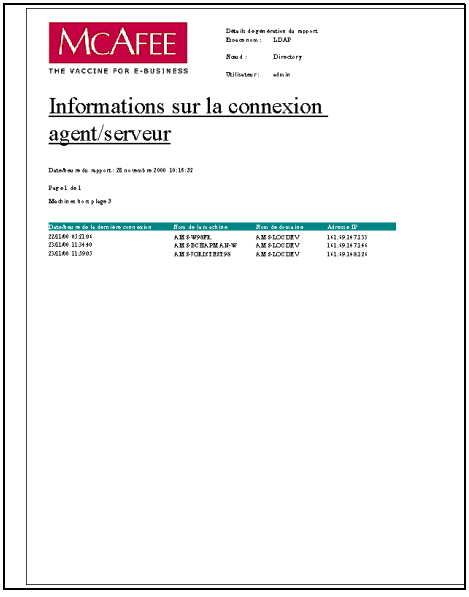
Domaines d'application

Les rapports de couverture fournissent des « instantanés » de la protection anti-virus actuellement active sur vos ordinateurs, telles qu'elles sont collectées par la base de données MSDE ou SQL Server.

Intervalle de connexion agent à serveur

Ce rapport répertorie les connexions ePolicy Orchestrator d'agent à serveur qui ne se sont pas produites dans l'intervalle spécifié.

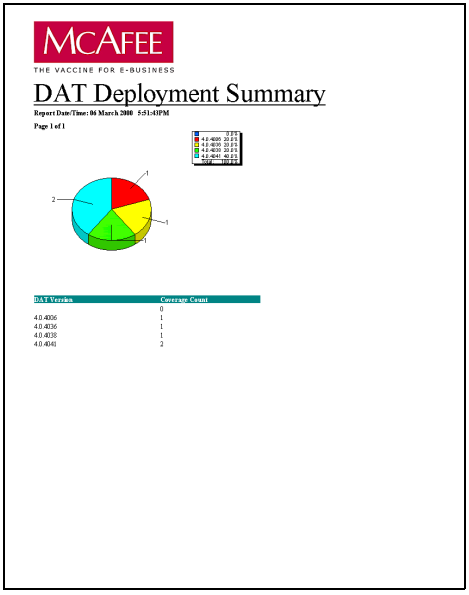
Cela permet de détecter tout problème éventuel au niveau de l'agent ou du réseau.



Résumé de déploiement des fichiers DAT

Ce rapport affiche un diagramme à secteurs des *versions* des *fichiers de définitions de virus (.DAT)* actuellement utilisés sur vos ordinateurs. Les tailles des segments sont proportionnelles au nombre d'ordinateurs qui utilisent les versions en question. Pour savoir quels ordinateurs utilisent les différentes versions, parcourez vers le bas les segments correspondants.

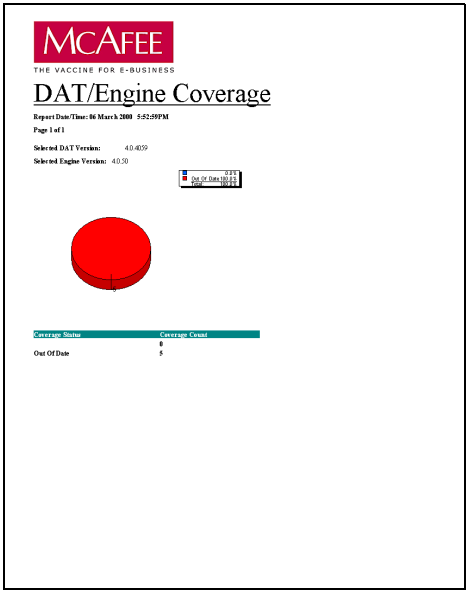
Ce rapport fournit une bonne vue d'ensemble de la méthode de mise à jour de la protection anti-virus de vos ordinateurs et il signale les ordinateurs qui ont besoin d'être mis à jour.



Couverture des fichiers DAT/du moteur

Ce rapport vous demande de spécifier les *versions* du dernier *moteur anti-virus* et *du dernier fichier de définitions de virus (DAT)*. Il affiche ensuite un diagramme à secteurs des ordinateurs qui sont à jour et de ceux qui doivent l'être. Les tailles des segments sont proportionnelles au nombre d'ordinateurs de chaque catégorie. Pour savoir quels ordinateurs ont besoin d'être mis à jour, parcourez vers le bas les segments correspondants.

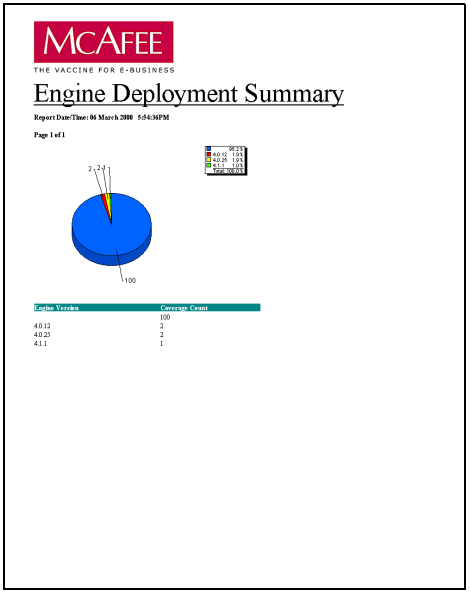
Ce rapport fournit une bonne vue d'ensemble de la méthode de mise à jour de la protection anti-virus de vos ordinateurs et il signale les ordinateurs qui ont besoin d'être mis à jour.



Résumé de déploiement du moteur

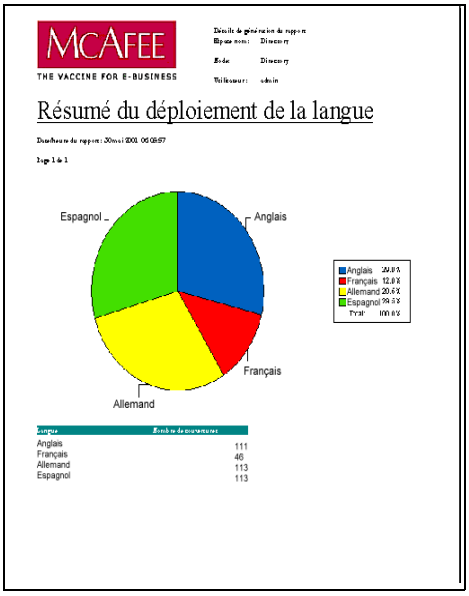
Ce rapport affiche un diagramme à secteurs des *versions* des *moteurs anti-virus* actuellement utilisés sur vos ordinateurs. Les tailles des segments sont proportionnelles au nombre d'ordinateurs qui utilisent les versions en question. Pour savoir quels ordinateurs utilisent les différentes versions, parcourez vers le bas les segments correspondants.

Ce rapport fournit une bonne vue d'ensemble de la méthode de mise à jour de la protection anti-virus de vos ordinateurs et il signale les ordinateurs qui ont besoin d'être mis à jour.



Résumé de déploiement de la langue

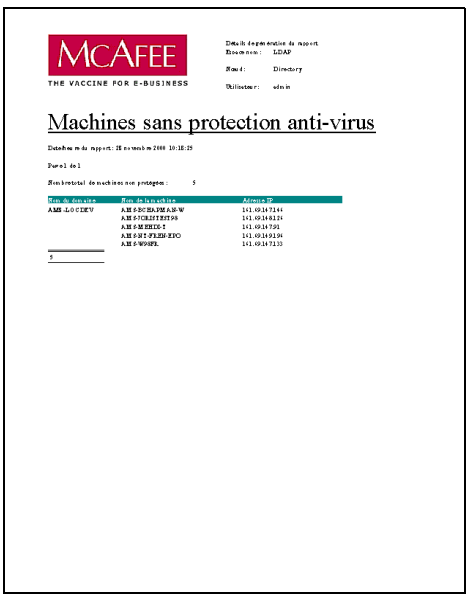
Ce rapport vous demande de spécifier les *versions* du dernier *moteur anti-virus* et *du dernier fichier de définitions de virus (DAT)*. Il affiche ensuite un diagramme à secteurs des numéros de versions, par langue, des produits anti-virus installés. Ce diagramme présente les versions des langues des produits, et non pas les paramètres de langue de la machine. Pour affiche une liste détaillée des occurrences d'une langue donnée, parcourez vers le bas les segments correspondants.



Machines sans aucune protection anti-virus

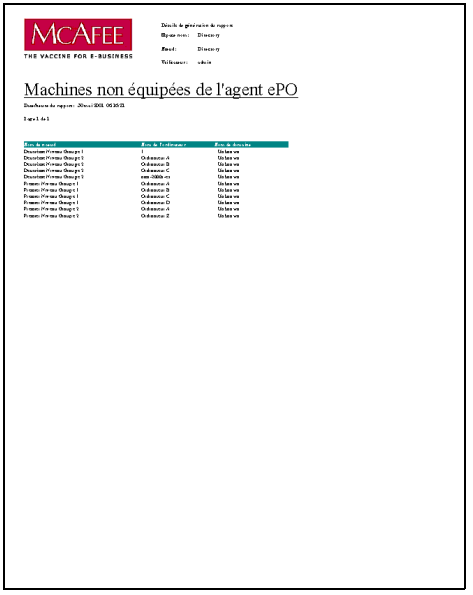
Ce rapport répertorie les ordinateurs qui ne sont pas protégés par les produits anti-virus McAfee ou Network Associates.

Ce rapport de couverture du produit est très utile pour détecter d'éventuelles lacunes (notamment les produits anti-virus non compatibles) dans la protection anti-virus de votre entreprise.



Machines sur lesquelles l'agent ePO n'est pas installé

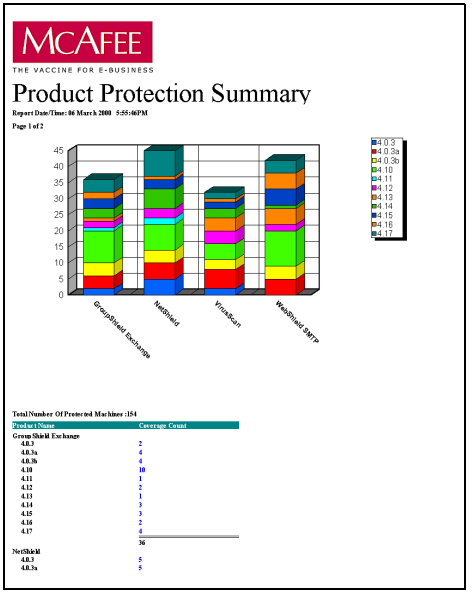
Ce rapport répertorie les *ordinateurs* ne disposant pas d'un *agent* de connexion ePolicy Orchestrator. L'agent n'a pas été installé ou bien n'a pas été connecté au serveur.



Résumé de la protection du produit

Ce rapport affiche un diagramme à barres des *produits anti-virus* actuellement utilisés sur vos ordinateurs et dont chaque barre est divisée en différentes portions de versions du produit. Pour savoir quels ordinateurs utilisent les différentes versions des produits anti-virus, parcourez vers le bas les portions correspondantes des barres.

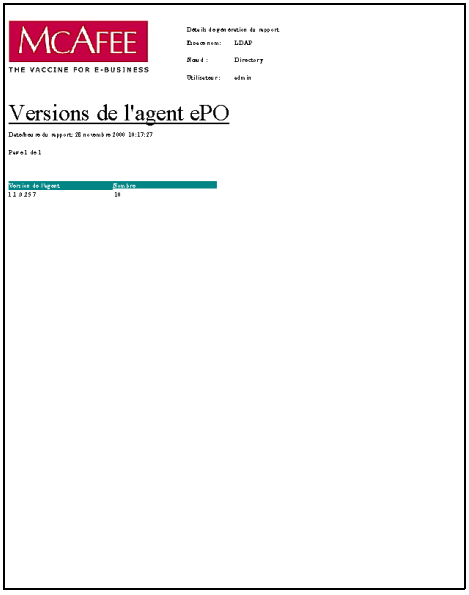
Ce rapport de couverture du produit fournit une bonne vue d'ensemble de l'action des produits anti-virus (notamment les produits anti-virus non compatibles) utilisés sur vos ordinateurs.



Versions de l'agent ePO

Ce rapport répertorie les *versions* des *agents* ePolicy Orchestrator actuellement utilisées sur vos ordinateurs. Parcourez vers le bas la version appropriée de l'agent pour savoir quels ordinateurs l'utilisent.

Ce rapport fournit une bonne vue d'ensemble de l'ancienneté des agents sur vos ordinateurs.



Rapports d'infection

Les rapports d'infection fournissent un historique des alertes et de l'activité anti-virus relatif à vos produits anti-virus. Il existe trois catégories de rapports d'infection :

- Les **Rapports de résumés d'action** donnent des informations concernant les actions exécutées par les produits anti-virus en cas de détection de virus ; voir ci-dessous.
- Les rapports des **10 premiers** donnent des informations concernant les 10 occurrences principales, telles que les 10 utilisateurs les plus contaminés ; voir page 180.
- Les **Rapports de détection** indiquent les virus détectés pour une durée déterminée ; voir page 184.

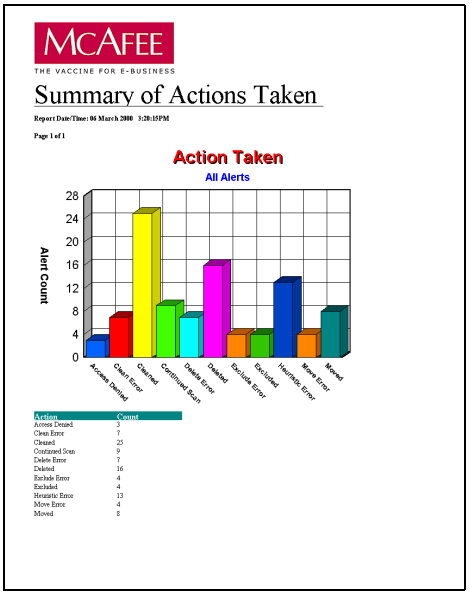
Rappelez-vous que vous pouvez personnaliser vos rapports pour vous concentrer sur le sous-ensemble d'informations qui vous intéresse.

Rapports de résumés d'action

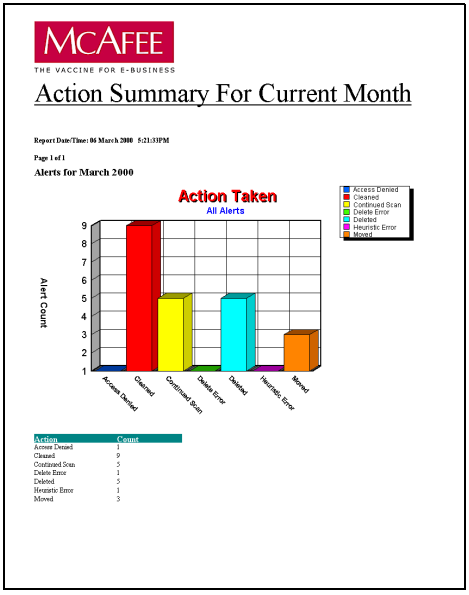
Résumé des actions effectuées

Ce rapport affiche un diagramme à barres de *toutes* les actions exécutées par les produits anti-virus, en cas de détection de virus. Il fournit une bonne vue d'ensemble de l'activité de détection de votre entreprise et peut indiquer l'efficacité de votre configuration anti-virus actuelle.

Parcourez vers le bas une action pour afficher le nombre d'alertes par nom de produit, suivi de la version du produit, puis de la liste détaillée des occurrences pour cette action, ce produit et ce virus.



Résumé de l'action du mois en cours



Ce rapport affiche un diagramme à barres de *toutes* les actions exécutées *durant le mois en cours* par les produits anti-virus, en cas de détection de virus. Il fournit une bonne vue d'ensemble de l'activité de détection de votre entreprise durant le dernier mois et peut indiquer l'efficacité de votre configuration anti-virus actuelle.

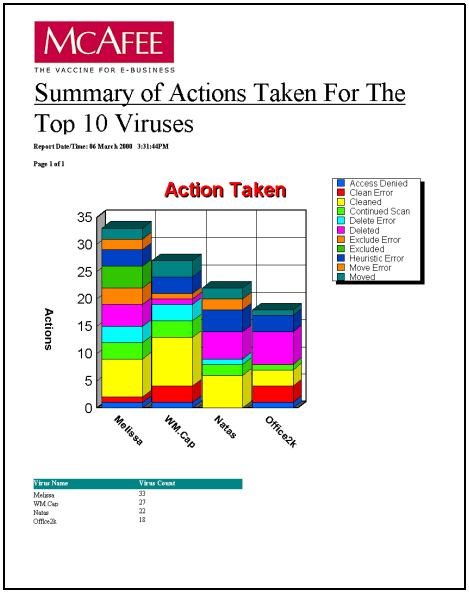
Le mois en cours est évalué comme mois calendaire en cours et non comme un nombre de jours fixe à partir de la production du rapport. C'est pourquoi la création d'un rapport durant les premiers jours du mois n'affiche que les informations relatives à ces jours-là.

Parcourez vers le bas une action pour afficher le nombre d'alertes par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour cette action, ce produit et ce virus.

Résumé des actions effectuées sur les 10 premiers virus

Ce rapport affiche un diagramme à barres de *toutes* les actions exécutées par les produits anti-virus, concernant les 10 virus détectés le plus souvent. Chaque barre est divisée en différentes portions présentant les actions exécutées. Il donne une bonne indication des virus les plus communs qui sont détectés par votre entreprise, ainsi que les actions exécutées pour les empêcher de contaminer votre entreprise.

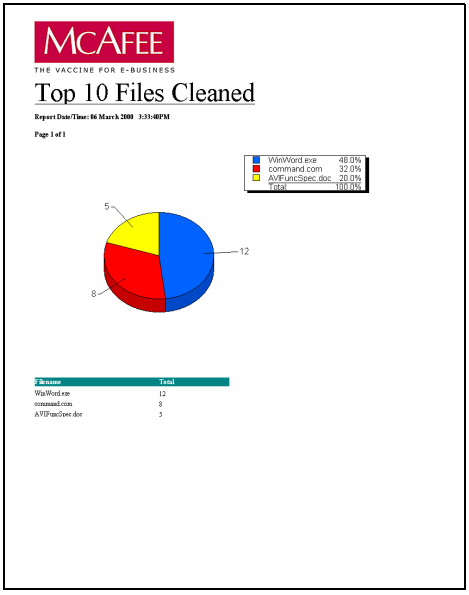
Parcourez vers le bas une action de virus pour afficher le nombre de virus par nom de produit, suivi de la version du produit, puis de la liste détaillée des occurrences pour cette action, ce produit et ce virus.



10 premiers fichiers nettoyés

Ce rapport affiche un diagramme à secteurs des 10 fichiers les plus contaminés et dont les virus ont été *éliminés* par les produits anti-virus. Les tailles des segments sont proportionnelles à la fréquence de détection et de suppression des virus des fichiers contaminés. Il donne une bonne indication des fichiers les plus communément contaminés qui sont détectés par votre entreprise.

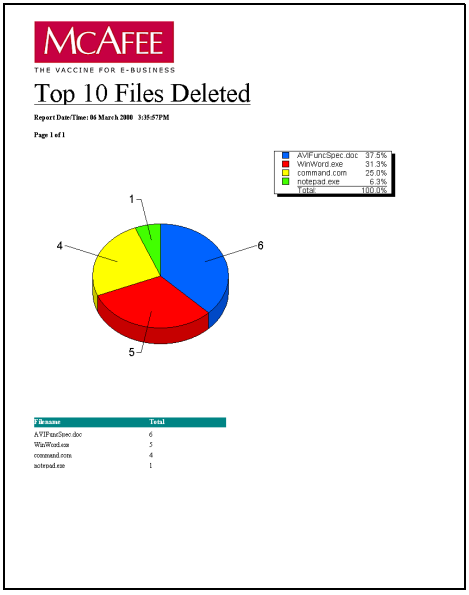
Parcourez vers le bas un nom de fichier pour afficher le nombre de fichiers infectés par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour ce fichier, ce produit et ce virus.



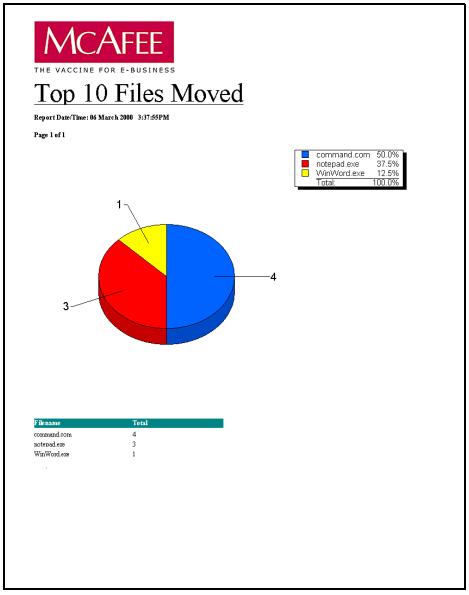
10 premiers fichiers supprimés

Ce rapport affiche un diagramme à secteurs des 10 fichiers les plus contaminés qui ont été *effacés* par les produits anti-virus. Les tailles des segments sont proportionnelles à la fréquence de détection et d'effacement des fichiers contaminés. Il donne une bonne indication des fichiers les plus communément contaminés qui sont détectés par votre entreprise.

Parcourez vers le bas un nom de fichier pour afficher le nombre de fichiers infectés par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour ce fichier, ce produit et ce virus.



10 premiers fichiers déplacés



Ce rapport affiche un diagramme à secteurs des 10 fichiers les plus contaminés et qui ont été *déplacés* par les produits anti-virus, tels que ceux qui ont été déplacés dans un dossier de quarantaine pour être soumis à une inspection. Les tailles des segments sont proportionnelles à la fréquence de détection et de déplacement des fichiers contaminés. Il donne une bonne indication des fichiers les plus communément contaminés qui sont détectés par votre entreprise.

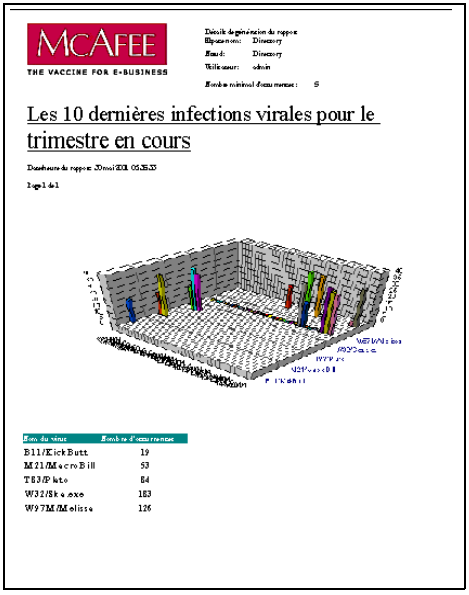
Parcourez vers le bas un nom de fichier pour afficher le nombre de fichiers infectés par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour ce fichier, ce produit et ce virus.

Rapports des dix premiers

10 premières apparitions de virus pour le trimestre en cours

Ce rapport affiche un diagramme à barres tridimensionnel des infections détectées au cours d'une apparition de virus. Il indique le nombre de détections de virus au cours d'une semaine. Une apparition de virus est définie comme un nombre minimum d'occurrences au cours d'une semaine, chacune se produisant au cours d'une durée maximale (spécifiée en heures) entre les occurrences. Les valeurs par défaut de ces deux paramètres sont cinq détections, avec une durée maximale de 24 heures entre les occurrences. Ce rapport vous permet de redéfinir ces paramètres pour étendre ou réduire la définition d'une apparition de virus.

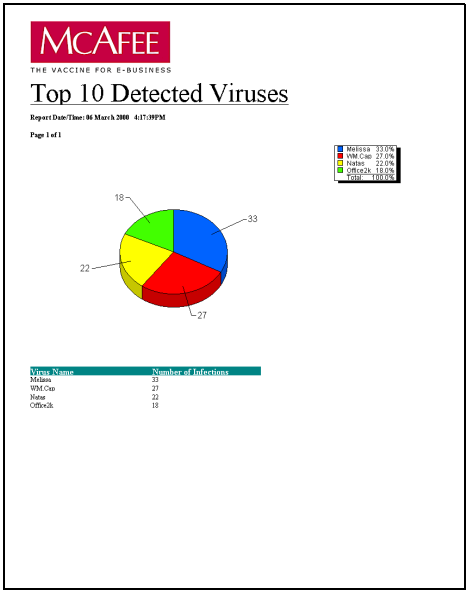
Parcourez vers le bas le rapport pour afficher une liste détaillée des occurrences pour un jour donné.



10 premiers virus détectés

Ce rapport affiche un diagramme à secteurs des 10 *virus* les plus détectés. Les tailles des segments sont proportionnelles à la fréquence de détection des virus. Il vous permet d'identifier les virus les plus communs qui sont détectés par votre entreprise.

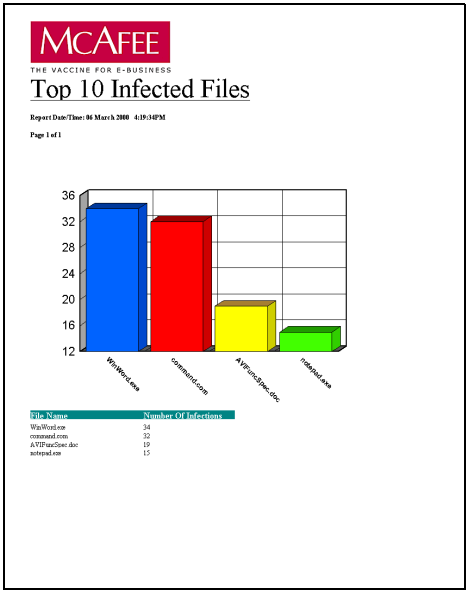
Parcourez vers le bas un nom de virus pour afficher le nombre de virus par nom de produit, suivi de la version du produit, puis de la liste détaillée des occurrences pour ce produit et ce virus.



10 premiers fichiers infectés

Ce rapport affiche un diagramme à barres des 10 *fichiers les plus contaminés*. Il vous permet d'identifier les fichiers les plus communément contaminés qui sont détectés par votre entreprise.

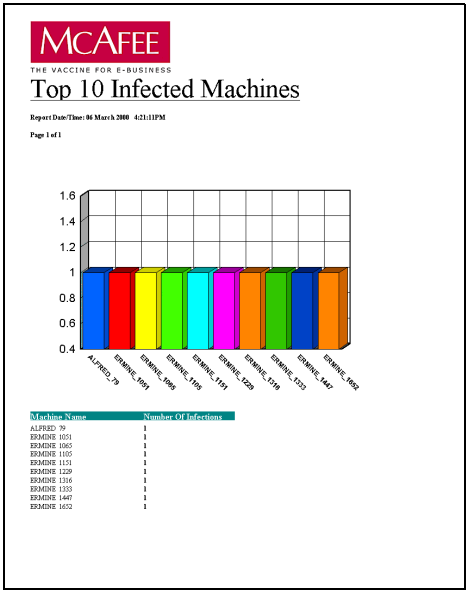
Parcourez vers le bas des fichiers pour afficher le nombre de fichiers infectés par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour ce fichier, ce produit et ce virus.



10 premières machines infectées

Ce rapport affiche un diagramme à barres des 10 *machines les plus contaminées*. Il vous permet d'identifier les ordinateurs de votre entreprise qui tentent le plus d'accéder à des fichiers contaminés. Il se peut que vous vouliez savoir comment les ordinateurs sont utilisés et que vous vouliez connaître les sources d'informations extérieures auxquelles ils ont accès (sources éventuelles de contamination).

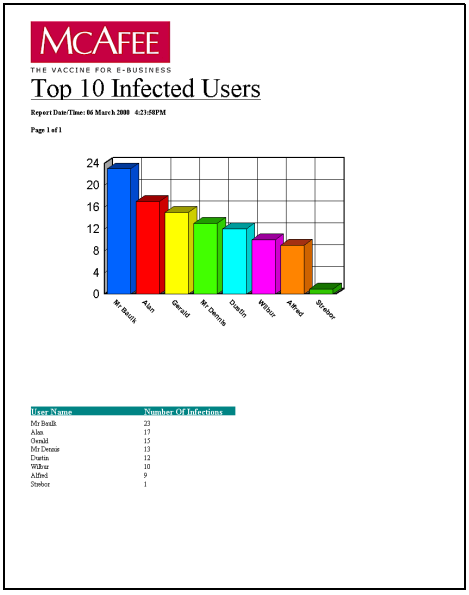
Parcourez vers le bas des machines pour afficher le nombre de machines infectées par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour cette machine, ce produit et ce virus.



10 premiers utilisateurs infectés

Ce rapport affiche un diagramme à barres des 10 *utilisateurs les plus contaminés*. Il vous permet d'identifier les utilisateurs de votre entreprise qui tentent le plus d'accéder à des fichiers contaminés. Il se peut que vous vouliez savoir comment ils utilisent les ordinateurs et que vous vouliez connaître les sources d'informations extérieures auxquelles ils ont accès (sources éventuelles de contamination).

Parcourez vers le bas des utilisateurs pour afficher le nombre d'utilisateurs infectés par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour cet utilisateur, ce produit et ce virus.



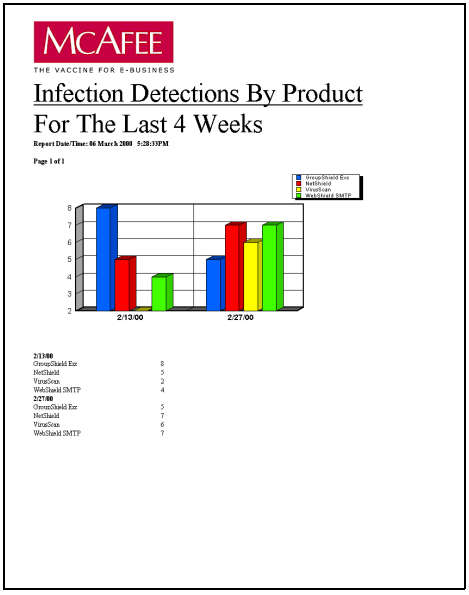
Rapports de détection

Infections détectées par produit durant les 4 dernières semaines

Ce rapport affiche un diagramme à barres des contaminations détectées par *chacun* des produits anti-virus de vos ordinateurs durant les *quatre dernières semaines*. Il vous permet de comparer les produits anti-virus dans votre entreprise et d'identifier les méthodes d'intrusion de virus les plus communes (telles que les messages électroniques ou les disquettes).

Les quatre semaines sont comptées comme étant les 28 jours précédents.

Parcourez vers le bas un produit pour afficher le nombre de virus par version du produit, suivi du nom du virus, puis de la liste détaillée des occurrences pour ce produit et ce virus.

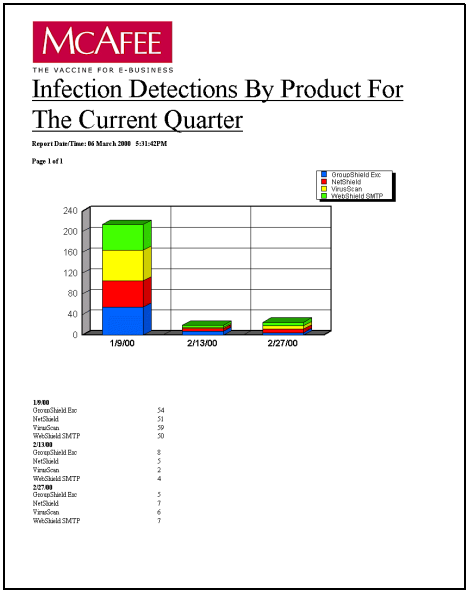


Infections détectées par produit durant le trimestre actuel

Ce rapport affiche un diagramme à barres des contaminations détectées par *chacun* des produits anti-virus de vos ordinateurs durant le *trimestre en cours mois*. Il vous permet de comparer les niveaux de détection des produits anti-virus durant ces trois mois.

Le trimestre en cours est compté à partir du trimestre calendaire en cours et non comme un nombre de jours fixe à dater de la création du rapport. C'est pourquoi la création d'un rapport durant le premier mois du trimestre n'affiche que les informations relatives à ce mois-là. Les trimestres en question sont les suivants : Janvier–Mars, Avril–Juin, Juillet–Septembre, Octobre–Décembre.

Parcourez vers le bas un produit pour afficher le nombre de virus par version du produit, suivi du nom du virus, puis de la liste détaillée des occurrences pour ce produit et ce virus.

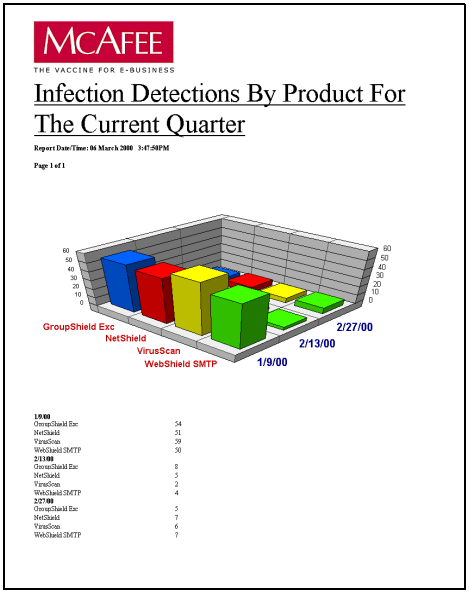


Infections détectées par produit durant le trimestre actuel — diagramme à barres tridimensionnel

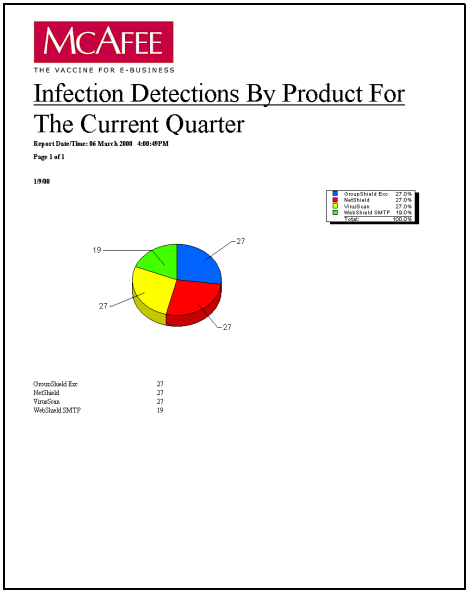
Ce rapport affiche un diagramme à barres tridimensionnel des contaminations détectées par *chacun* des produits anti-virus de vos ordinateurs durant le *trimestre actuel*. Il vous permet de comparer les niveaux de détection des produits anti-virus durant ces trois mois.

Le trimestre en cours est compté à partir du trimestre calendaire en cours et non comme un nombre de jours fixe à dater de la création du rapport. C'est pourquoi la création d'un rapport durant le premier mois du trimestre n'affiche que les informations relatives à ce mois-là. Les trimestres en question sont les suivants : Janvier–Mars, Avril–Juin, Juillet–Septembre, Octobre–Décembre.

Parcourez vers le bas un produit pour afficher le nombre de virus par version du produit, suivi du nom du virus, puis de la liste détaillée des occurrences pour ce produit et ce virus.



Infections détectées par produit durant le trimestre actuel — diagramme à secteurs



Ce rapport affiche un diagramme à secteurs des contaminations détectées par *chacun* des produits anti-virus de vos ordinateurs durant le *trimestre actuel*. Les tailles des segments sont proportionnelles à la fréquence de détection des contaminations. Il vous permet de comparer les niveaux de détection généraux des produits anti-virus durant ces trois mois.

Le trimestre en cours est compté à partir du trimestre calendaire en cours et non comme un nombre de jours fixe à dater de la création du rapport. C'est pourquoi la création d'un rapport durant le premier mois du trimestre n'affiche que les informations relatives à ce mois-là. Les trimestres en question sont les suivants : Janvier–Mars, Avril–Juin, Juillet–Septembre, Octobre–Décembre.

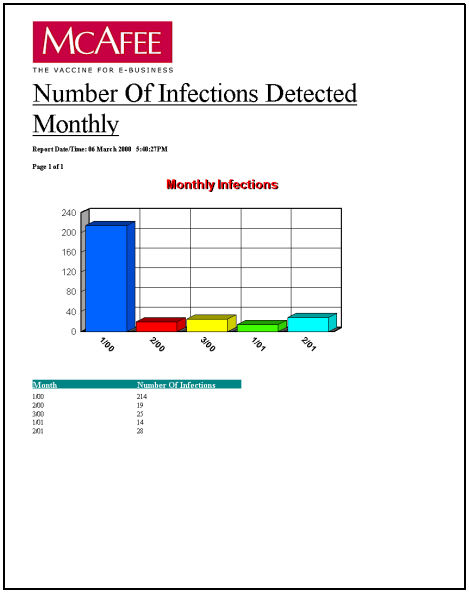
Parcourez vers le bas un produit pour afficher le nombre de virus par version du produit, suivi du nom du virus, puis de la liste détaillée des occurrences pour ce produit et ce virus.

Nombre d'infections détectées par mois

Ce rapport affiche un diagramme à barres des *contaminations* détectées par *mois*. Il vous permet de comparer les niveaux de contamination par mois.

Les mois sont comptés comme mois calendaires et non comme un nombre de jours fixe à partir de la création du rapport.

Parcourez vers le bas un mois pour afficher le nombre de virus par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour ce mois, ce produit et ce virus.

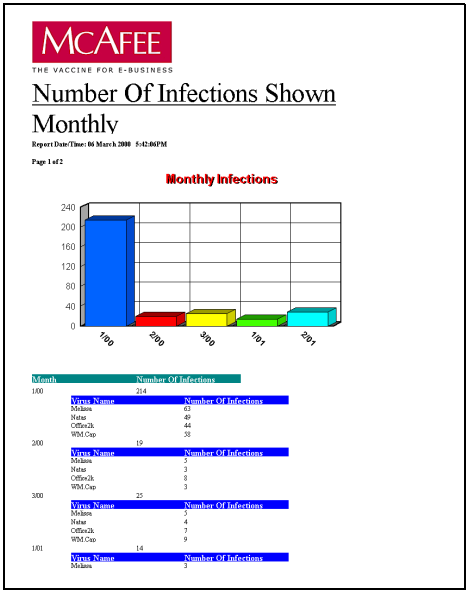


Nombre d'infections affichées par mois

Ce rapport affiche les *contaminations* détectées par *mois*, avec une interruption des niveaux individuels de *chaque* virus. Il vous permet d'afficher les niveaux de contamination mensuels, avec des détails supplémentaires pour chaque virus.

Les mois sont comptés comme mois calendaires et non comme un nombre de jours fixe à partir de la création du rapport.

Parcourez vers le bas un nom de virus pour afficher le nombre de virus par nom de produit, suivi de la version du produit, puis de la liste détaillée des occurrences pour ce mois, ce produit et ce virus.

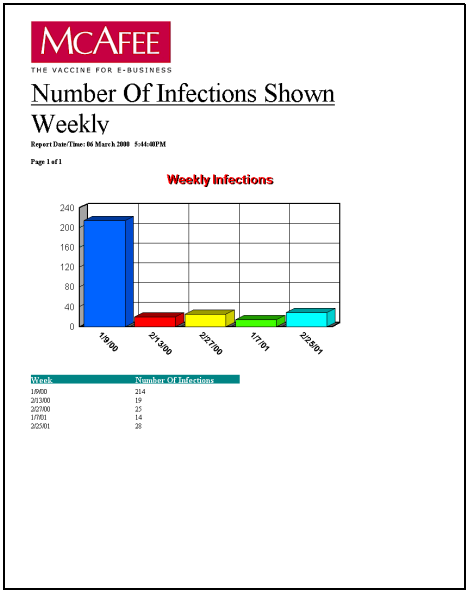


Nombre d'infections affichées par semaine

Ce rapport affiche un diagramme à barres des *contaminations* détectées par *semaine*. Il vous permet de comparer les niveaux de contamination hebdomadaires.

Les semaines sont comptées comme semaines calendaires (à partir de dimanche) et non comme un nombre de jours fixe à partir de la création du rapport.

Parcourez vers le bas une semaine pour afficher le nombre de virus par nom de produit, suivi de la version du produit, du nom du virus, puis de la liste détaillée des occurrences pour cette semaine, ce produit et ce virus.

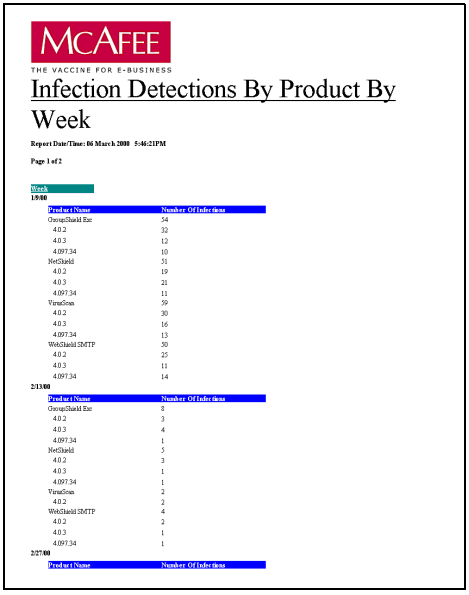


Infections détectées par produit par semaine

Ce rapport affiche les *contaminations* détectées par *semaine*, avec une interruption des niveaux individuels de *chaque* produit anti-virus. Il vous permet de comparer les niveaux de contamination hebdomadaires, avec des détails supplémentaires pour chaque produit anti-virus.

Les semaines sont comptées comme semaines calendaires (à partir de dimanche) et non comme un nombre de jours fixe à partir de la création du rapport.

Parcourez vers le bas un nom de virus pour afficher le nombre de virus par nom de produit, suivi de la version du produit, puis de la liste détaillée des occurrences pour cette semaine, ce produit et ce virus.


MCAFEE
THE VACCINE FOR E-BUSINESS

Infection Detections By Product By Week

Report Date/Time: 06 March 2000 5:46:21PM

Page 1 of 2

Week

1/9/00

Product Name	Number Of Infections
GroupShield Exc	54
4.0.2	32
4.0.3	12
4.097.34	10
NetShield	51
4.0.2	19
4.0.3	21
4.097.34	11
VirusScan	59
4.0.2	30
4.0.3	16
4.097.34	13
WebShield SMTP	50
4.0.2	25
4.0.3	11
4.097.34	14

2/13/00

Product Name	Number Of Infections
GroupShield Exc	8
4.0.2	3
4.0.3	4
4.097.34	1
NetShield	5
4.0.2	3
4.0.3	1
4.097.34	1
VirusScan	2
4.0.2	2
WebShield SMTP	4
4.0.2	2
4.0.3	1
4.097.34	1

2/27/00

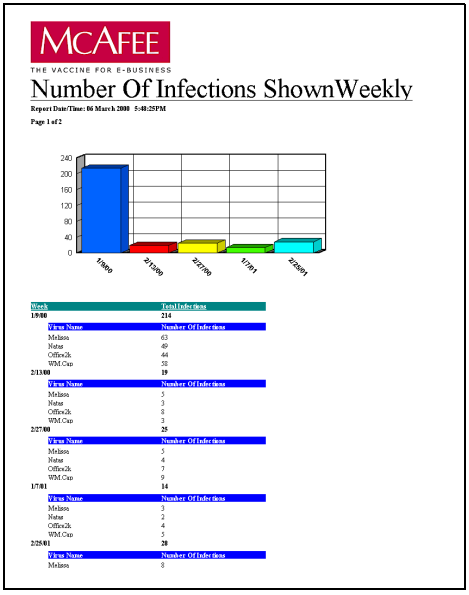
Product Name	Number Of Infections

Nombre d'infections affichées par semaine

Ce rapport affiche un diagramme à barres des *contaminations* détectées par *semaine*, avec une interruption des niveaux individuels pour *chaque* virus. Il vous permet de comparer les niveaux de contamination hebdomadaires, avec des détails supplémentaires pour chaque virus.

Les semaines sont comptées comme semaines calendaires (à partir de dimanche) et non comme un nombre de jours fixe à partir de la création du rapport.

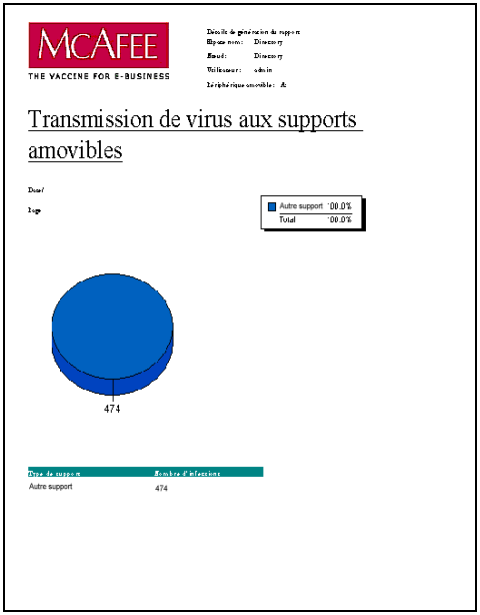
Parcourez vers le bas un produit pour afficher le nombre de virus par version du produit, suivi du nom du virus, puis de la liste détaillée des occurrences pour cette semaine, ce produit et ce virus.



Transmission des virus aux supports amovibles

Ce rapport affiche un diagramme à secteurs du nombre de virus détectés sur un support amovible tel qu'un lecteur de disquette. Spécifiez la lettre du lecteur (par défaut, a:) ; le rapport indique alors le nombre de virus provenant de ce lecteur par rapport à ceux provenant d'autres sources.

Parcourez vers le bas un numéro de règle pour afficher une liste détaillée des occurrences pour ce type de support précis.

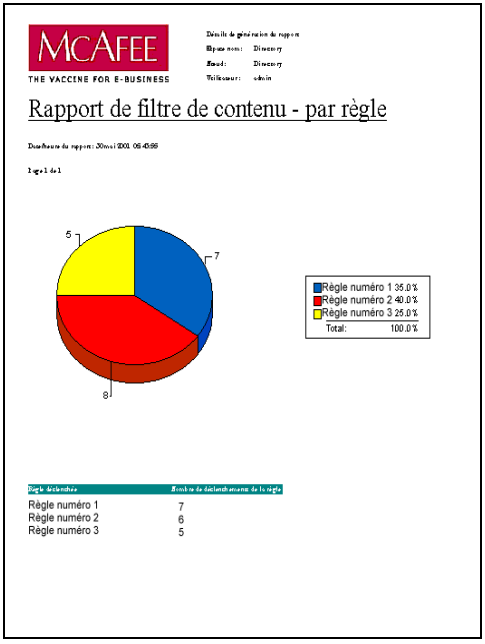


Rapports WebShield

Rapport du filtre de contenu par règle

Ce rapport affiche un diagramme à secteurs du nombre de règles déclenchées par le produit WebShield.

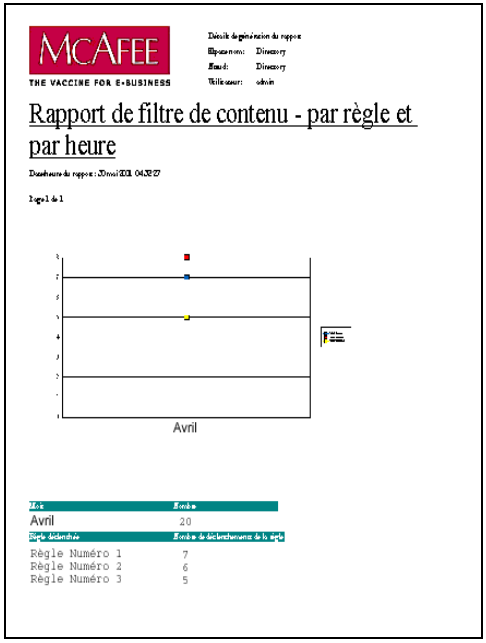
Parcourez vers le bas un numéro de règle pour afficher le nombre de règles par mois, suivi du nombre par semaine, par jour, par heure, puis de la liste détaillée des occurrences pour une période donnée.



Rapport du filtre de contenu par règle et par heure

Ce rapport affiche un diagramme en courbes du nombre de règles déclenchées sur plusieurs mois.

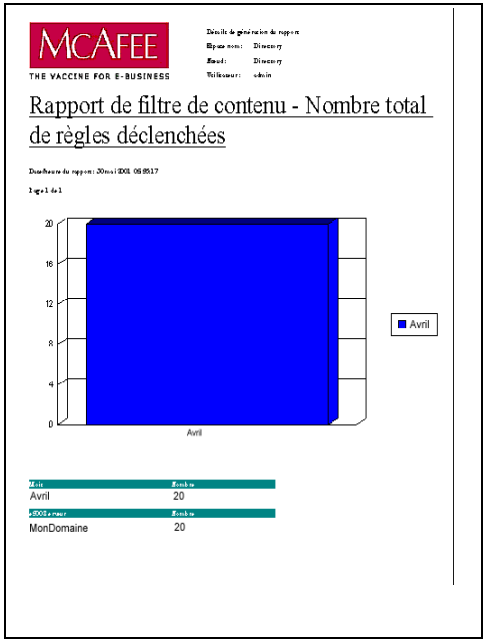
Parcourez vers le bas un mois pour afficher le nombre de règles par mois, suivi du nombre par semaine, par jour, par heure, puis de la liste détaillée des occurrences pour une période donnée.



Rapport du filtre de contenu par règle déclenchée

Ce rapport affiche un diagramme à barres du nombre de règles déclenchées par domaine sur plusieurs mois.

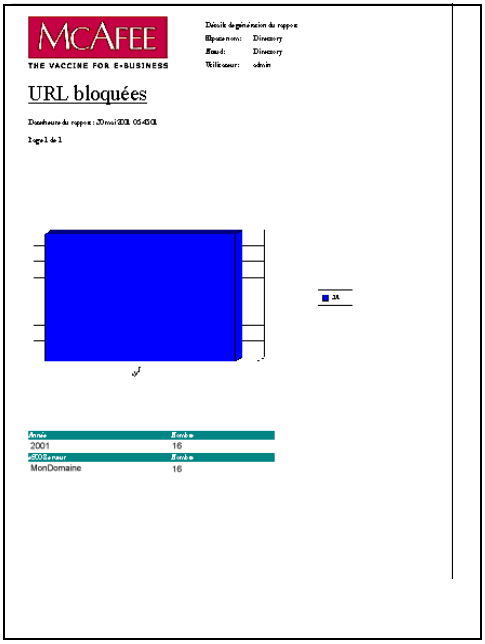
Parcourez vers le bas un domaine pour afficher le nombre de règles par mois, suivi du nombre par semaine, par jour, par heure, par règle, par numéro, puis de la liste détaillée des occurrences pour une période et un domaine donnés.



URL bloquées

Ce rapport affiche un diagramme à barres du nombre d'URL bloquées par domaine au cours d'une année.

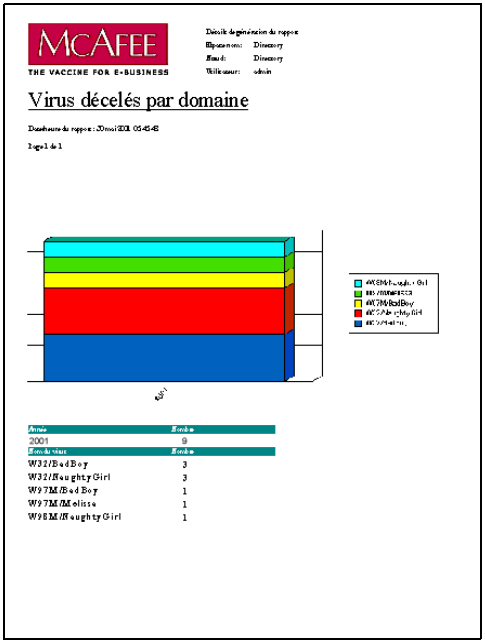
Parcourez vers le bas un domaine pour afficher le nombre de blocages par trimestre, suivi du nombre par mois, par semaine, par jour, par heure, puis de la liste détaillée des occurrences pour une période et un domaine donnés.



Virus attrapés par domaine

Ce rapport affiche un diagramme à barres du nombre de virus attrapés au cours d'une année, chaque barre étant divisée en différentes portions qui affichent le nom des virus.

Parcourez vers le bas un nom de virus pour afficher le nombre de virus par trimestre, suivi du nombre par mois, par semaine, par jour, par heure, puis de la liste détaillée des occurrences pour une période et un virus donnés.



Utilisation d'ePolicy Orchestrator sur Internet 8

Introduction

Ce chapitre passe brièvement en revue l'utilisation sur Internet de ce produit.

Le programme ePolicy Orchestrator a été conçu pour une utilisation sur Internet. Il permet une communication agent-serveur sur Internet si le pare-feu est configuré de façon à permettre une plage d'adresses IP correcte.

Scénarios Internet

Les options suivantes sont décrites dans ce chapitre :

Derrière le pare-feu

- Service d'accès à distance Microsoft (RAS) (Microsoft Remote Access Service), lorsqu'un utilisateur distant (agent) établit une connexion avec l'un des ports pour accéder au réseau derrière le pare-feu.
- VPN (Virtual Private Networks), lorsque des utilisateurs distants (agents) établissent une connexion avec un port fourni par un opérateur commercial, mais que l'accès se trouve toujours derrière un seul pare-feu.

Ouvert sur Internet

- Fournisseur de services Internet (ISP - Internet Service Provider) pour lequel des transactions entre l'utilisateur (agent) et le serveur ne peuvent être contenues derrière un pare-feu étant donné que l'adresse IP reste ouverte sur Internet.

Accès à distance à l'aide de VPN et RAS

Plusieurs situations impliquent que les consoles ou les agents ePolicy Orchestrator soient déployés en dehors du périmètre physique de l'intranet d'entreprise. Pour réduire les problèmes de configuration et de sécurité, il est hautement recommandé que les agents ou les consoles à distance accèdent au serveur par une connexion VPN ou Microsoft RAS. L'utilisation de serveurs proxy n'est pas prise en charge.

Intranet d'entreprise

Il existe différents types de topologies de réseau dans lesquelles il est possible de déployer ePolicy Orchestrator et ses composants. Le déploiement le plus simple et le niveau de sécurité le plus élevé sont atteints lorsque tous les composants d'ePolicy Orchestrator sont déployés dans un Intranet d'entreprise particulier, derrière un pare-feu unique. Dans ce scénario, tous les composants de la topologie de réseau sont situés dans des emplacements physiques fixes et ils sont tous caractérisés par un accès approprié à l'Intranet d'entreprise.

Cette topologie est la plus simple à mettre en oeuvre pour un administrateur système.

Dans ce scénario, les administrateurs peuvent optimiser une infrastructure d'entreprise existante pour permettre un accès transparent aux services ePolicy Orchestrator. Tout problème de pare-feu est masqué par les transports VPN et RAS.

Connexion à l'aide d'un fournisseur de services Internet et d'un pare-feu

Agent

L'agent peut accéder aux serveurs ePolicy Orchestrator grâce à un fournisseur de services avec plusieurs restrictions :

- Le fournisseur de services Internet doit être en mesure de résoudre l'adresse IP du serveur ePolicy Orchestrator.
- Le fournisseur de services peut utiliser le protocole DHCP pour attribuer des adresses IP pour accès direct, ce que le pare-feu d'entreprise doit accepter.
- Le serveur ePolicy Orchestrator ne peut pas effectuer des diffusions vers l'agent ePolicy Orchestrator à travers un pare-feu. Dans cet environnement, l'agent doit être transmis via d'autres supports.

- Le port du pare-feu utilisé pour la communication agent-serveur est le **Port 80**. Il doit être configuré pour un trafic agent-serveur entrant et sortant. Ce système utilise par défaut le port 80, mais vous pouvez choisir un autre numéro de port durant l'installation du serveur.
- Le port du pare-feu utilisé pour la communication console-serveur est le **Port 81**. Ce système utilise par défaut le port 81, mais vous pouvez choisir un autre numéro de port durant l'installation du serveur.
- Le port du pare-feu utilisé pour les appels de réveil d'agent est **8081**. Vous pouvez changer cette valeur en temps réel en utilisant la fonction de configuration du serveur, décrite dans « Paramètres du serveur » à la page 202.

Console

L'utilisation d'un ISP pour connecter la console au serveur est fortement déconseillée pour les raisons suivantes :

- La console ePolicy Orchestrator n'est pas exécutée dans le cas de certains anciens pare-feu, car elle utilise la fonction HTTP « Connexions persistantes » pour la plupart de ses transactions. La suppression de la fonction HTTP « Connexions persistantes » de la console aurait un impact significatif sur les performances des scénarios d'usage habituel, pour lesquels la console se trouve « à l'intérieur » de l'intranet d'entreprise.
- L'accès au serveur SQL dans le pare-feu de l'entreprise crée un risque de sécurité important.

Configuration du pare-feu pour ePolicy Orchestrator

Chacune des trois options suivantes permet d'activer les communications agent-serveur :

Aucun pare-feu

- Lorsqu'il n'y a pas de pare-feu, la communication agent-serveur est ouverte.

Pare-feu avec port HTTP ouvert

- Lorsque le port HTTP est déjà ouvert dans le pare-feu, aucune action n'est nécessaire. Des communications sont ouvertes.

Pare-feu sans port HTTP ouvert

Règle de destination

- Crée une règle de destination pour la configuration du pare-feu qui ouvre uniquement le serveur ePolicy Orchestrator pour communiquer avec les agents en dehors du pare-feu. Une règle de destination spécifie uniquement l'adresse IP du serveur ePolicy Orchestrator comme destination du trafic HTTP entrant.

Règle de source

- Crée une règle de source dans la configuration du pare-feu qui permet uniquement aux ordinateurs client désignés de communiquer avec le serveur ePolicy Orchestrator. Cela permet à une plage d'adresses IP d'accéder au serveur par le port. Des précautions doivent être prises pour éviter que quelqu'un détourne les adresses IP et les utilise de façon incorrecte.

Taille des paquets lors des communications d'agent à serveur

Voici un exemple de tailles de paquets :

Tableau 8-1. Taille de paquet habituelle pour Intervalle de communication agent à serveur

Activité (par machine)	Taille totale en Ko*	Taille incrémentielle en Ko*
L'agent envoie des propriétés	10	2
L'agent regarde s'il y a de nouvelles stratégies (pas de nouvelle stratégie)	2	
L'agent regarde s'il y a de nouvelles stratégies (nouvelles stratégies)	5–9	

*La taille des paquets peut varier considérablement selon la collection d'événements.

Utilitaires et outils 9

Présentation

Ce chapitre décrit plusieurs fonctions qui sont utiles mais pas souvent utilisées. Il s'agit de :

- La fonction **Paramètres serveur** offre une interface permettant de modifier les paramètres du serveur à l'intérieur du logiciel ePolicy Orchestrator.
- L'**Observateur d'événements du serveur** est une interface qui affiche les événements du serveur lors de leur inscription dans le journal.
- Le **Contrôleur de l'agent** est une interface qui permet de suivre l'activité de l'agent sur l'ordinateur client installé. Il fournit un moyen simple de surveiller l'activité de chaque agent.
- Vous pouvez facilement **supprimer le logiciel ePolicy Orchestrator** à l'aide de la fonction Ajout/Suppression de programmes du Panneau de configuration.
- L'utilitaire de **sauvegarde et de restauration de base de données** est un utilitaire permettant de sauvegarder et de restaurer facilement votre base de données.
- L'outil **fusion de la base de données** permet de combiner le contenu d'un certain nombre de bases de données dans une base de données fusionnée, nouvelle ou existante.
- L'**utilitaire de configuration** permet de modifier la base de données d'ePolicy Orchestrator ou le nom d'utilisateur et le mot de passe que vous utilisez pour administrer votre base de données SQL, ou de passer en revue la base de données AVI.

Paramètres du serveur

Cette section propose des procédures pour modifier les paramètres du serveur à l'intérieur du logiciel ePolicy Orchestrator.

Pour accéder à l'interface Paramètres serveur :

1. Mettez en surbrillance **ePolicy Orchestrator** sur l'arborescence de la console pour afficher les options disponibles.
2. Cliquez sur **Paramètres serveur** pour ouvrir la fenêtre Paramètres serveur et configurer les informations générales du serveur.

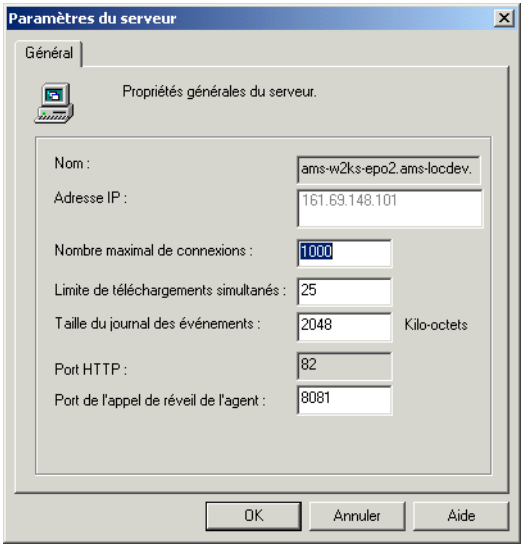


Figure 9-1. Ecran Paramètres serveur, onglet Général

Les champs **Nom**, **Adresse IP** et **Port HTTP** sont désactivés. Les valeurs indiquées ont été sélectionnées au cours de l'installation du produit.

Nombre maximal de connexions vous permet de déterminer le nombre d'agents pouvant être connectés au serveur en même temps. Cela inclut les agents qui se connectent au serveur, qui mettent à jour les propriétés ou les événements, qui reçoivent de nouvelles stratégies ou qui téléchargent des logiciels.

Limite de téléchargements simultanés vous permet de déterminer le nombre maximum de téléchargements de logiciels simultanés à partir du serveur vers les agents. Cette activité risque d'affecter les performances du réseau si le nombre en question est trop élevé.

Taille du journal des événements vous permet de limiter la taille du journal des événements du serveur. La taille par défaut est de 2 Mo. Lorsque le journal des événements atteint cette limite, le plus ancien des événements est supprimé. Vous disposez toujours des événements les plus récents dans le journal. Vous pouvez enregistrer ou imprimer périodiquement le fichier journal du serveur en utilisant la procédure décrite dans « Interface des événements du serveur » à la page 203.

Port d'appel de réveil d'agent configure le port pour la fonction de réveil de l'agent. Pour plus d'informations sur cette fonction, reportez-vous à « Appel de réveil de l'agent » à la page 109.

Interface des événements du serveur

L'Observateur d'événements du serveur affiche les événements du serveur tels qu'ils sont enregistrés. Il affiche la date et l'heure à côté du nom de l'événement, présenté ici dans Figure 9-2.

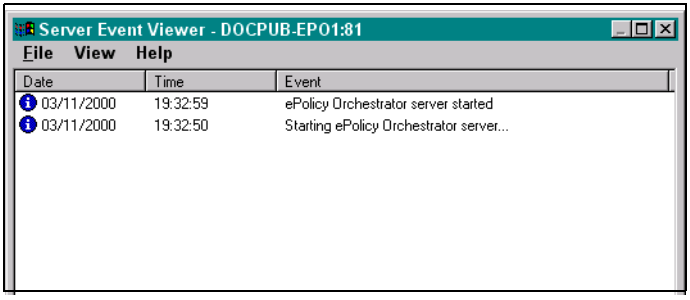


Figure 9-2. Observateur d'événements du serveur

Pour afficher les événements du serveur :

1. Cliquez avec le bouton droit sur **ePolicy Orchestrator** ou sur tout élément du **répertoire**, puis sélectionnez **Evénements du serveur**.
2. Double-cliquez dans le champ de date de l'un des événements du journal pour ouvrir la fenêtre des détails des événements du serveur, laquelle offre une description complète de cet événement.
3. Une fois que vous consulté ces informations, cliquez sur **Fermer**.

Enregistrement de fichiers journaux

La fonction Evénements du serveur vous autorise à enregistrer le fichier journal comme un fichier texte. Vous pouvez enregistrer tout le fichier ou simplement des événements particuliers que vous sélectionnez.

Pour enregistrer le journal sous la forme d'un fichier texte :

1. Sélectionnez les éléments à enregistrer dans le journal. Pour sélectionner plusieurs éléments, maintenez la touche **CTRL** enfoncée.
2. Sélectionnez **Enregistrer sous...** dans le menu **Fichier** pour ouvrir la fenêtre Enregistrer sous.
3. Sélectionnez les éléments à enregistrer dans la fenêtre Enregistrer sous.
4. Tapez un nom pour le fichier et indiquez dans quel répertoire vous souhaitez l'enregistrer.
5. Cliquez sur **Enregistrer** pour enregistrer le fichier.

   Un message s'affiche pour vous informer que le journal des événements du serveur a bien été enregistré.

Impression des fichiers journaux

Pour imprimer le contenu d'un fichier journal :

1. Dans le fichier journal ouvert, sélectionnez la plage d'entrées à imprimer.
2. Cliquez sur **Imprimer** à partir du menu **Fichier**.
3. Vous êtes invité à indiquer si vous souhaitez imprimer le fichier journal des événements du serveur. Cliquez sur **Oui** pour l'imprimer.
4. Fermez l'Observateur d'événements du serveur.

Actualiser les événements du serveur

Pour actualiser la liste des événements et garder la trace des événements en cours, cliquez sur **Actualiser** dans le menu **Afficher** de l'Observateur d'événements du serveur. Cela met à jour la liste des événements du serveur avec les événements les plus récents.

Contrôleur d'agent

Le Contrôleur d'agent est une interface qui permet de suivre l'activité de l'agent sur l'ordinateur client. Il permet de surveiller l'activité de chaque agent. Grâce au Contrôleur d'agent, vous pouvez afficher le journal de l'agent sur l'écran ou enregistrer ce journal dans un fichier puis l'imprimer à partir d'un éditeur de texte. Cette fonction permet de conserver les journaux de chaque agent. Vous devez intervenir à deux niveaux pour afficher un Contrôleur d'agent :

- Définissez la stratégie au niveau de la console de façon à afficher l'icône d'état de l'agent sur l'ordinateur client. Vous pouvez attendre tout un intervalle de communication agent-serveur après la définition de cette stratégie pour voir le Contrôleur d'agent. Mais vous pouvez aussi définir la stratégie, puis envoyer un appel de réveil d'agent à l'ordinateur client que vous souhaitez voir pour modifier cette stratégie.
- Affichez le Contrôleur d'agent au niveau de l'ordinateur client. Cela n'est possible que si l'icône de l'agent est visible dans la barre des tâches de l'ordinateur client.

Pour rendre l'icône du Contrôleur d'agent visible sur l'ordinateur client :

1. Sélectionnez l'ordinateur client dans l'arborescence de la console ePolicy Orchestrator.
2. Dans le volet supérieur des détails, sélectionnez **Configuration** sous l'agent ePolicy Orchestrator, puis sélectionnez l'onglet **Stratégies**. La page des options de l'agent s'affiche dans le volet inférieur des détails (Figure 9-3 à la page 206).

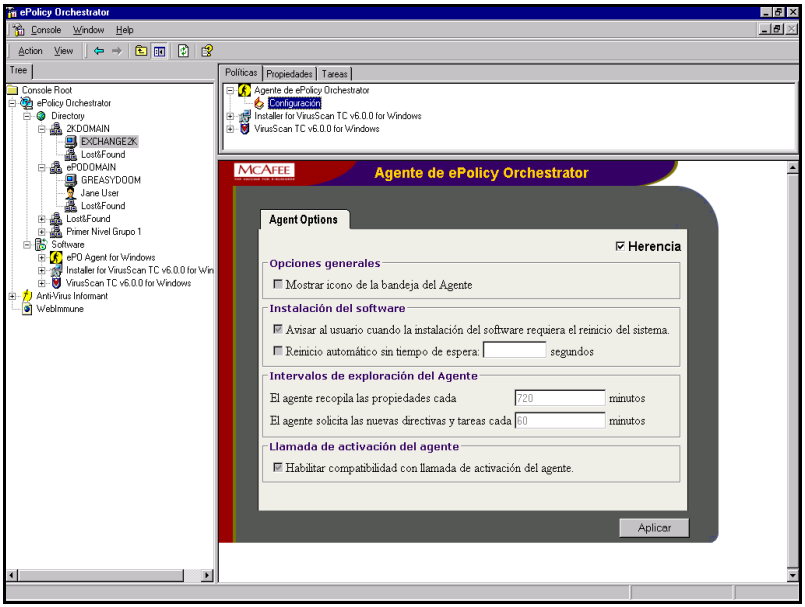


Figure 9-3. Console ePolicy Orchestrator, page des options de l'agent.

3. Sélectionnez **Afficher l'icône d'état de l'agent** dans la zone Options générales.

   Si cette case est sélectionnée, l'icône de l'agent  apparaît dans la barre des tâches de l'ordinateur client.

4. Cliquez sur **Appliquer**.

   Une fois que vous avez sélectionné cette option et cliqué sur le bouton **Appliquer**, vous avez renforcé la stratégie. Après la communication agent-serveur, l'icône de l'agent s'affiche dans la barre des tâches sur l'écran de l'ordinateur client.

Pour afficher le Contrôleur d'agent au niveau de l'ordinateur client :

1. Sur l'ordinateur client, double-cliquez sur l'icône de l'agent dans la barre des tâches pour ouvrir le Contrôleur d'agent (Figure 9-4).

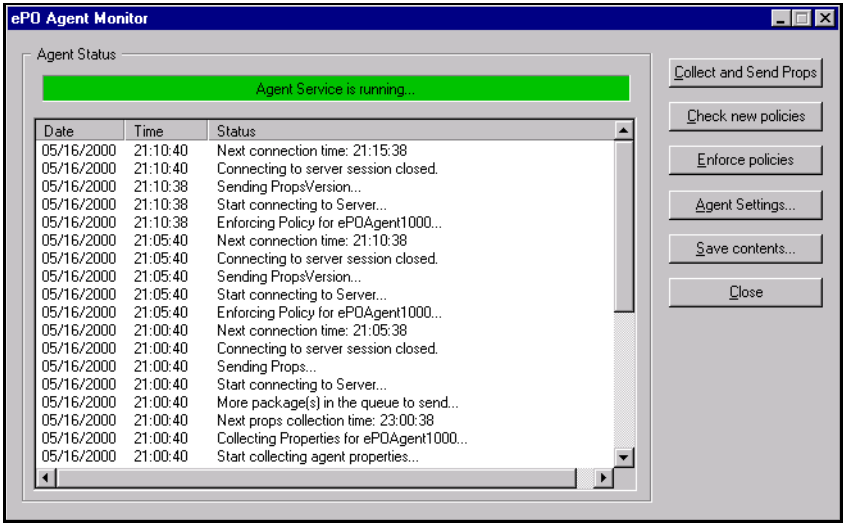


Figure 9-4. Contrôleur de l'agent ePolicy Orchestrator

2. Le Contrôleur d'agent propose les fonctions suivantes :

   - **Rassembler et envoyer les propriétés** force l'agent à recueillir les propriétés du système et celles du logiciel anti-virus et à les transmettre immédiatement au serveur. Cette collecte est planifiée pour une exécution périodique, décrite dans « Communication agent-serveur » à la page 105.

   - **Vérifier les nouvelles stratégies** force l'agent à sonder le serveur pour appliquer de nouvelles stratégies immédiatement. Le fait de cliquer sur cette option est utile si vous souhaitez recueillir les dernières stratégies anti-virus ou si vous contrôlez la communication agent-serveur.

   - **Appliquer les stratégies** force l'agent à appliquer les stratégies recueillies sur le serveur. Si vous cliquez sur cette option immédiatement après avoir cliqué sur Vérifier les nouvelles stratégies, les dernières stratégies sont appliquées à cet ordinateur.

- **Paramètres de l'agent** ouvre la fenêtre Options de l'agent d'ePolicy Orchestrator illustrée à la Figure 9-5 à la page 208. Bien que les valeurs affichées dans cette boîte de dialogue ne puissent être modifiées, elles indiquent à l'administrateur des propriétés importantes de cet agent et affichent l'identificateur univoque de l'agent.
- **Enregistrer le contenu** vous permet d'enregistrer les entrées dans le contrôleur sous la forme de fichier journal de statut d'agent au format *.TXT.
- **Fermer** arrête le contrôleur de l'agent mais laisse l'agent lui-même s'exécuter.

Autres fonctions de l'icône de l'agent

Les options suivantes s'affichent lorsque vous cliquez sur l'icône de l'agent avec le bouton droit sur l'ordinateur client :

- **Contrôleur de statut...** ouvre le contrôleur de statut (Figure 9-4 à la page 207).
- **Paramètres…** ouvre la fenêtre Options de l'agent d'ePolicy Orchestrator (Figure 9-5). Bien que les valeurs affichées dans cette boîte de dialogue ne puissent être modifiées, elles indiquent à l'administrateur des propriétés importantes de cet agent et affichent l'identificateur univoque de l'agent.

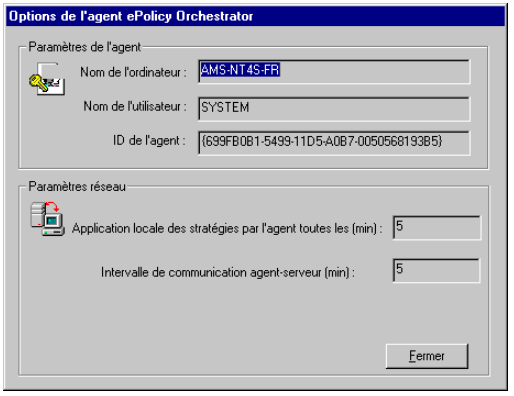


Figure 9-5. Options de l'agent

- **Quitter ePO Monitor** ouvre la fenêtre de confirmation. Celle-ci offre à l'utilisateur la possibilité de refermer le service agent. Cliquez sur **Oui** pour refermer le contrôleur.
- **A propos** ouvre un message qui indique les informations de copyright pour le contrôleur.

Récupération des informations du journal de l'agent

Pour récupérer les informations du journal de l'agent sur un ordinateur individuel :

1. Sur la console, activez la barre des icônes Contrôleur de l'agent correspondant à l'ordinateur en question. Voir Étape 1 à la page 207.
2. Au niveau de l'ordinateur client, ouvrez le Contrôleur d'agent. Voir Étape 1 à la page 207.
3. Dans l'écran du Contrôleur d'agent, choisissez **Enregistrer le contenu** pour ouvrir la fenêtre d'enregistrement du journal d'état de l'agent.
4. Tapez un nom pour le fichier et indiquez son emplacement. Vous pouvez l'enregistrer sur un lecteur du réseau.
5. Cliquez sur **Enregistrer** pour enregistrer le Contrôleur d'agent.
6. Refermez le Contrôleur d'agent.

Les fichiers de l'agent peuvent être affichés ou imprimés à partir de n'importe quel éditeur de texte.

Suppression du logiciel ePolicy Orchestrator

Si vous devez supprimer intégralement le serveur ePolicy Orchestrator ou la console, suivez cette procédure.

Pour supprimer le logiciel ePolicy Orchestrator :

1. Connectez-vous au serveur en tant qu'administrateur de domaine.
2. Fermez la console ePolicy Orchestrator.
3. Cliquez sur **Démarrer** et sélectionnez **Panneau de configuration** dans le menu **Paramètres**.
4. Sélectionnez **Ajouter/Supprimer programmes** depuis le panneau de configuration.
5. Sélectionnez **ePolicy Orchestrator 2.0**.
6. Cliquez sur **Ajouter/Supprimer**.
7. Cliquez sur **Oui** pour confirmer aussi la suppression des fichiers utilisateur. Cela lance la suppression. Une fenêtre de message s'affiche pour vous permettre de suivre le déroulement de la suppression.

Sauvegarde et restauration de la base de données d'ePolicy Orchestrator

Nous vous recommandons de sauvegarder régulièrement la base de données afin de la protéger contre toute panne matérielle. Vous pouvez alors restaurer la base de données au cas où vous devriez réinstaller le logiciel.

Si vous utilisez Microsoft SQL Server 7 pour votre base de données, veuillez vous reporter à la documentation jointe au logiciel pour toute information concernant la sauvegarde et la restauration de la base de données.

Si vous utilisez MSDE et n'avez pas effectué la mise à jour vers SQL Server, vous pouvez utiliser l'utilitaire de sauvegarde de la base de données pour sauvegarder et restaurer votre base de données. L'utilitaire de sauvegarde de la base de données est automatiquement installé avec le logiciel ePolicy Orchestrator. Si vous avez installé les fichiers programme dans le répertoire par défaut, l'utilitaire sera installé dans le chemin suivant :

C:\Program Files\McAfee\ePO

L'utilitaire de sauvegarde de la base de données (DBBak.EXE) est un exécutable autonome que vous pouvez exécuter à partir d'une console ou d'un serveur. Dans les deux cas, les fichiers de sauvegarde sont chargés dans le serveur de la base de données.

Pour sauvegarder la base de données d'ePolicy Orchestrator :

1. Arrêtez le service serveur ePolicy Orchestrator sur le serveur ePolicy Orchestrator, fermez toutes les consoles, et assurez-vous que le service SQL Server est en cours d'exécution avant de commencer le processus de restauration.

   Pour accéder à ces services, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration** pour ouvrir la fenêtre Panneau de configuration. Ensuite, localisez et double-cliquez sur le panneau de configuration **Services** pour ouvrir la boîte de dialogue Services. Arrêtez les services spécifiés ci-dessus.

2. Allez au répertoire dans lequel est installé l'utilitaire DBBak.EXE.

3. Double-cliquez sur le fichier **DBBak.EXE** pour exécuter l'utilitaire. Cet utilitaire doit être exécuté à partir de son emplacement d'installation (Figure 9-6 à la page 211).

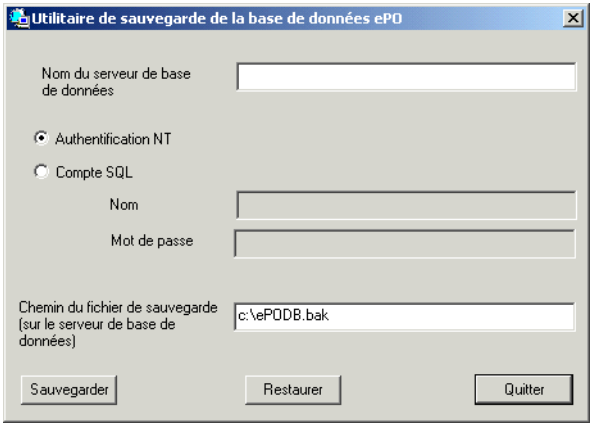


Figure 9-6. Utilitaire de sauvegarde de la base de données

4. Entrez le **nom du serveur de base de données**.
5. Sélectionnez **Authentification NT** ou **Compte SQL**.

   Si vous sélectionnez **Compte SQL**, entrez un nom et un mot de passe valides pour cette base de données.
6. Entrez le **chemin du fichier de sauvegarde**.
7. Cliquez sur **Sauvegarder**.
8. Cliquez sur **OK** lorsque le programme de sauvegarde est terminé.
9. Démarrez le service serveur ePolicy Orchestrator sur le serveur ePolicy Orchestrator, ouvrez toutes les consoles, et assurez-vous que le service SQL Server est en cours d'exécution avant de commencer le processus de restauration.
10. Pour accéder à ces services, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration** pour ouvrir la fenêtre Panneau de configuration. Ensuite, localisez et double-cliquez sur le panneau de configuration **Services** pour ouvrir la boîte de dialogue Services. Démarrez les services spécifiés ci-dessus.

Pour restaurer la base de données d'ePolicy Orchestrator :

1. Arrêtez le service serveur ePolicy Orchestrator sur le serveur ePolicy Orchestrator, fermez toutes les consoles, et assurez-vous que le service SQL Server est en cours d'exécution avant de commencer le processus de restauration.

   Pour accéder à ces services, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration** pour ouvrir la fenêtre Panneau de configuration. Ensuite, localisez et double-cliquez sur le panneau de configuration **Services** pour ouvrir la boîte de dialogue Services. Arrêtez les services spécifiés ci-dessus.

2. Allez au répertoire dans lequel est installé l'utilitaire DBBak.EXE.

3. Double-cliquez sur le fichier **DBBak.EXE** pour exécuter l'utilitaire. Cet utilitaire doit être exécuté à partir de son emplacement d'installation.

4. Entrez le **nom du serveur de base de données**.

5. Sélectionnez **Authentification NT** ou **Compte SQL**.

   Si vous sélectionnez **Compte SQL**, entrez un nom et un mot de passe valides pour cette base de données.

6. Entrez le **chemin du fichier de sauvegarde**.

7. Cliquez sur **Restaurer**.

8. Une fenêtre d'avertissement s'ouvre, indiquant que cette commande écrasera l'ensemble de la base de données ePolicy Orchestrator, et vous demande si vous êtes sûr de vouloir effectuer cette opération. Cliquez sur **Oui** pour continuer.

9. Cliquez sur **OK** lorsque le programme de restauration est terminé.

10. Démarrez le service serveur ePolicy Orchestrator sur le serveur ePolicy Orchestrator, ouvrez toutes les consoles, et assurez-vous que le service SQL Server est en cours d'exécution avant de commencer le processus de restauration.

11. Pour accéder à ces services, cliquez sur **Démarrer**, pointez sur **Paramètres**, puis sélectionnez **Panneau de configuration** pour ouvrir la fenêtre Panneau de configuration. Ensuite, localisez et double-cliquez sur le panneau de configuration **Services** pour ouvrir la boîte de dialogue Services. Démarrez les services spécifiés ci-dessus.

Fusion de la base de données

L'outil de fusion de la base de données vous permet d'intégrer le contenu d'un certain nombre de bases de données à une base de données de fusion nouvelle ou existante. Cet outil est très utile si vous possédez plusieurs serveurs ePolicy Orchestrator et si vous souhaitez produire des rapports et des requêtes SQL combinés pour certains serveurs.

Pour produire des rapports pour certaines bases de données, vous devez :

1. Créer une base de données de fusion à partir des bases de données sources. Voir « Création d'une base de données de fusion » à la page 214.

   REMARQUE : Les bases de données sources doivent être des bases de données 2.0. Si tel n'est pas le cas, le processus de fusion échoue. Si vous souhaitez utiliser les alertes d'une base de données 1.x, vous devez les importer dans une base de données 2.0 ; voir « Importation d'alertes de la base de données d'ePolicy Orchestrator » à la page 147.

2. Vous connecter à la base de données de fusion dans la partie **Bases de données AVI** de l'arborescence de la console Anti-Virus Informant et produire les rapports requis. Voir « Connexion à la base de données de fusion » à la page 223.

L'outil de fusion importe les informations sur les alertes (événements) et sur la couverture (données sur les propriétés du produit et de l'ordinateur) dans la base de données de fusion, en fonction des options de fusion que vous choisissez.

ASTUCE : L'outil de fusion comporte des fonctions supplémentaires qui vous permettent de le lancer de plusieurs façons, à partir, par exemple, d'un programme de planificateur. Voir « Méthodes de lancement supplémentaires » à la page 224.

Création d'une base de données de fusion

Pour créer une base de données de fusion à l'aide de l'outil de fusion :

1. A l'aide de l'Explorateur Windows, ouvrez le répertoire d'installation d'Anti-Virus Informant. Si vous avez installé le logiciel à son emplacement par défaut, vous trouverez ce répertoire à l'emplacement suivant :

   C:\Program Files\McAfee\ePO\2.0\Avi

2. Double-cliquez sur le fichier **AVIDB_Merge_Tool.EXE** pour ouvrir l'outil de fusion (Figure 9-7).

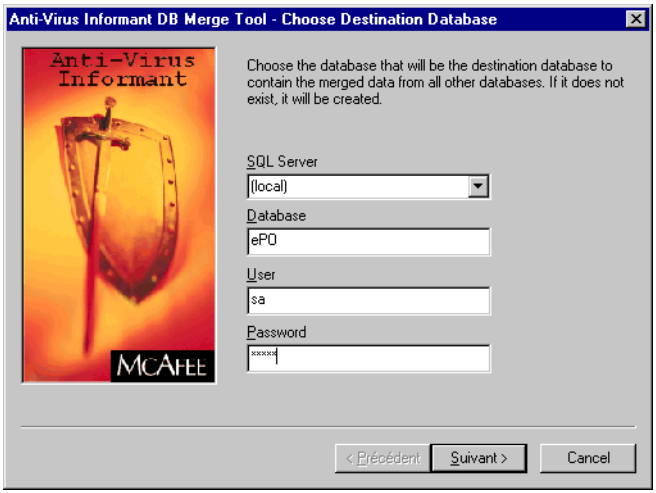


Figure 9-7. Outil de fusion — Fenêtre Choisir une base de données de destination

3. Entrez les informations relatives au **serveur SQL**, à la **base de données**, à l'**utilisateur** et au **mot de passe**.

4. Cliquez sur **Suivant** pour continuer.

5. Dans la zone de liste **Serveur SQL**, choisissez le serveur qui contient la base de données existante ou le serveur sur lequel vous souhaitez créer la nouvelle base de données.

   La zone de liste contient les serveurs SQL qui figurent dans le domaine réseau actuel. Si le serveur requis n'est pas répertorié, entrez le nom du serveur. Si vous souhaitez choisir l'ordinateur sur lequel vous exécutez l'outil de fusion, sélectionnez « (local) » ou entrez le nom du serveur local, si « (local) » n'est pas disponible.

   ☕ **IMPORTANT :** Le logiciel SQL v7 ou MSDE doit être installé sur le serveur.

   ---

6. Dans la zone de texte **Base de données**, entrez le nom de la base de données SQL.

   Vous pouvez utiliser une base de données de fusion existante.

7. Dans les zones de texte **Utilisateur** et **Mot de passe**, entrez le nom d'utilisateur SQL et le mot de passe pour le serveur que vous avez choisi à l'Etape 5.

   Vous devez utiliser un compte d'utilisateur avec des droits d'administrateur pour le serveur SQL.

8. Cliquez sur **Suivant>**.

   L'outil de fusion accède au serveur à l'aide du nom d'utilisateur SQL et du mot de passe que vous avez spécifiés. S'il ne peut pas se connecter au serveur, un message d'erreur apparaît. Cliquez sur **OK** et vérifiez les informations que vous avez spécifiées.

   L'écran Choisir des bases de données sources qui apparaît (Figure 9-8 à la page 216) vous permet d'indiquer les bases de données sources dont vous souhaitez importer le contenu dans la base de données de fusion.

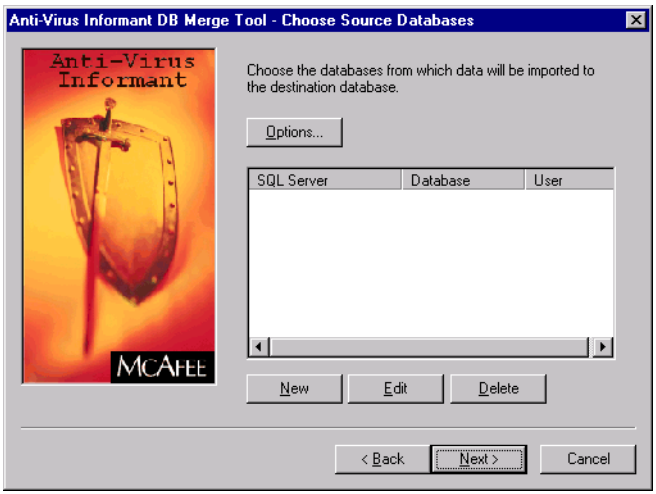


Figure 9-8. Outil de fusion – Fenêtre Choisir des bases de données sources

La liste affiche les bases de données sources spécifiées. Elle est vide si vous n'avez pas exécuté précédemment l'outil de fusion. Vous pouvez ajouter plusieurs bases de données sources, notamment les bases de données de fusion que vous avez créées au cours de précédentes sessions de fusion.

9. Cliquez sur **Nouveau** pour spécifier la nouvelle base de données (Figure 9-9).

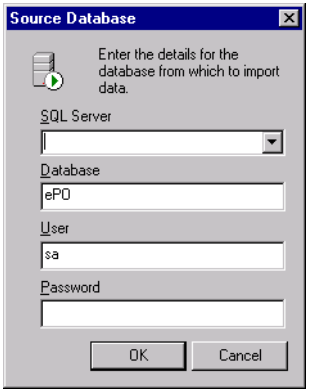


Figure 9-9. Fenêtre Base de données source

10. Cliquez sur **OK**.

11. Dans la fenêtre Choisir des bases de données sources :

    a. Dans la zone de liste **Serveur SQL**, choisissez le serveur qui contient la base de données source.

    La zone de liste contient les serveurs SQL qui figurent dans le domaine réseau actuel. Si le serveur requis n'est pas répertorié, entrez le nom du serveur. Si vous souhaitez choisir l'ordinateur sur lequel vous exécutez l'outil de fusion, sélectionnez « (local) » ou entrez le nom du serveur local, si « (local) » n'est pas disponible.

    b. Dans la zone de texte **Base de données**, indiquez le nom de la base de données existante. Ce nom est généralement `ePO`.

    REMARQUE : La base de données doit être une base de données 2.0. Si tel n'est pas le cas, le processus de fusion échoue. Si vous souhaitez utiliser les alertes d'une base de données 1.x, vous devez les importer dans une base de données 2.0 ; voir « Importation d'alertes de la base de données d'ePolicy Orchestrator » à la page 147.

    c. Dans les zones de texte **Utilisateur** et **Mot de passe**, entrez le nom d'utilisateur et le mot de passe pour le serveur que vous avez choisi à l'Etape a.

    Vous devez utiliser un compte d'utilisateur avec des droits d'administrateur pour le serveur SQL.

12. Cliquez sur **OK**.

    L'outil de fusion accède au serveur à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés. S'il ne peut pas se connecter au serveur, un message d'erreur apparaît. Voir « Modification du protocole de connexion du serveur » à la page 222.

    La base de données source est ajoutée à la liste dans l'écran Choisir des bases de données sources.

13. Pour modifier les options de fusion :

    a. Cliquez sur **Options**.

    La fenêtre Options qui apparaît (Figure 9-10 à la page 218) vous permet de modifier les options de fusion.

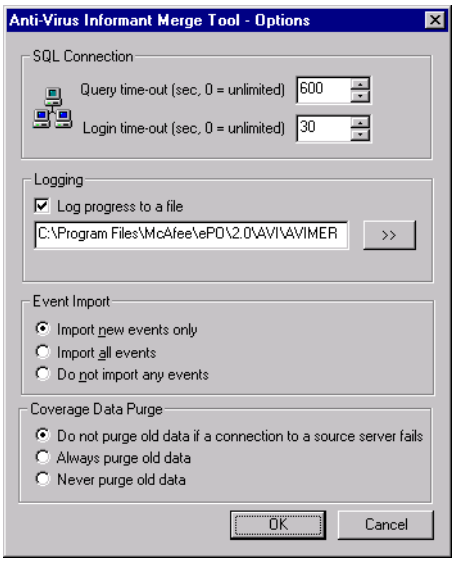


Figure 9-10. Fenêtre Options

b. Pour modifier les durées des délais de connexion et de requête, indiquez les valeurs requises dans la zone **Connexion SQL**.

   Les valeurs par défaut suffisent à la plupart des réseaux. Vous devez uniquement modifier ces valeurs si vous rencontrez des retards sur votre réseau.

c. Pour enregistrer la progression de l'outil de fusion dans un fichier journal, sélectionnez **Progression dans un fichier journal**, puis indiquez le nom et le chemin d'accès Windows complet pour le fichier journal. L'emplacement et le fichier par défaut sont :

   `<répertoire d'installation>\AVIMERGE.LOG`

   Vous pouvez choisir un fichier existant ou indiquer un nouveau fichier. Si vous choisissez un fichier existant, l'outil de fusion ajoute ses entrées de journal à la fin du fichier.

   Pour localiser un fichier, cliquez sur **>>**, puis choisissez le fichier requis. Cliquez sur **OK**.

d. Choisissez les événements (alertes) à importer dans la base de données de fusion :

- **Importer uniquement les nouveaux événements** — Importe les événements qui sont *plus récents* que ceux déjà contenus dans la base de données de fusion. Ceci est l'option par défaut.

  La base de données de fusion enregistre le dernier événement qu'elle contient pour chaque base de données et pour chaque serveur. L'outil de fusion utilise cet enregistrement pour identifier de nouveaux événements.

  Si la base de données ou le serveur est récent(e), l'outil de fusion importe *tous* ses événements.

  REMARQUE : Les enregistrements de la base de données de fusion ne sont pas désélectionnés si la base de données ne contient pas d'événements (alertes). Par conséquent, si vous souhaitez importer de nouveau la totalité des événements, vous devez choisir **Importer la totalité des événements**.

- **Importer la totalité des événements** — Importe *la totalité* des événements dans la base de données de fusion, quel que soit son contenu.

  REMARQUE : L'outil de fusion ne supprime pas les événements de la base de données de fusion avant d'ajouter de nouveaux événements. L'utilisation multiple de cette option peut introduire des événements en double dans la base de données de fusion. McAfee vous recommande d'utiliser uniquement cette option si vous avez vidé la base de données de fusion.

- **Ne pas importer d'événements** — N'importe pas d'événements. Cela est utile si vous souhaitez uniquement mettre à jour les informations sur les propriétés de l'ordinateur et du produit. Voir l'Etape e ci-après.

e. Choisissez le type d'informations (de couverture) sur les propriétés de l'ordinateur et du produit que vous souhaitez supprimer (purger) de la base de données de fusion.

   Le processus de purge s'exécute après l'importation des alertes et il purge les données de couverture qui se trouvent déjà dans la base de données de fusion (les bases de données sources ne sont *pas* affectées).

Voici les options de purge proposées :

- **Ne pas purger les anciennes données en cas d'échec de la connexion au serveur source** — Purge les anciennes informations sur les propriétés de l'ordinateur et du produit pour les bases de données et les serveurs, *à l'exception de* celles auxquelles le processus de fusion ne peut pas se connecter. Ceci empêche les informations sur les propriétés de l'ordinateur et du produit d'être supprimées de façon incorrecte. Ceci est l'option par défaut.
- **Toujours purger les anciennes données** — Purge les anciennes informations MSDE ou SQL Server. Ceci est risqué car le processus de fusion supprime les informations MSDE ou SQL Server pour les bases de données et les serveurs auquel il ne peut pas se connecter.
- **Ne jamais purger les anciennes données** — Ne purge pas les anciennes informations MSDE ou SQL Server. Ceci est utile si vos informations de couverture ne se modifient pas et si vous rassemblez simplement des informations sur les alertes.

> **REMARQUE :** Toutes ces options importent de *nouvelles* informations sur les propriétés de l'ordinateur et du produit pour les bases de données et les serveurs auquel le processus de fusion ne peut pas se connecter.

f. Cliquez sur **OK**.

14. Dans l'écran Choisir des bases de données sources, cliquez sur **Suivant>**.

    L'écran Importer des données apparaît (Figure 9-11), ce qui vous permet d'enregistrer les paramètres actuels de l'outil de fusion et de lancer le processus de fusion.

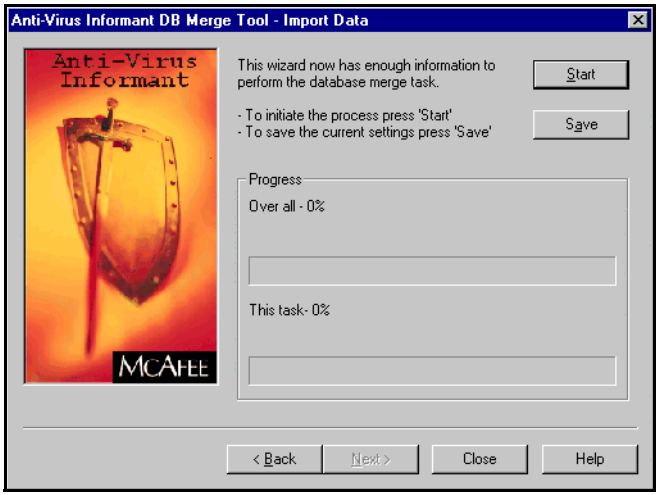


Figure 9-11. Outil de fusion – Fenêtre Importer des données

15. Cliquer sur **Enregistrer** pour enregistrer les paramètres actuels.

16. Dans la fenêtre Enregistrer sous, indiquez l'emplacement et le nom du fichier texte (.TXT) que vous souhaitez créer, puis cliquez sur **Enregistrer**.

17. Dans la fenêtre Importer des données (Figure 9-11 à la page 221), cliquez sur **Démarrer** pour exécuter le processus de fusion. L'écran rapporte la progression du processus de fusion.

    Si vous avez choisi **Importer uniquement les nouveaux événements** (Étape d à la page 219), vous pouvez arrêter le processus de fusion à tout instant en cliquant sur **Annuler**.

18. Lorsque le processus de fusion est terminé, cliquez sur **Fermer**.

    Si le processus de fusion ne peut pas se connecter à un serveur, la base de données de fusion n'est pas créée ; voir « Modification du protocole de connexion du serveur » à la page 222.

    Vous pouvez désormais vous connecter au rapport et produire les rapports requis. Voir « Connexion à la base de données de fusion » à la page 223.

    L'outil de fusion comporte des fonctions supplémentaires qui vous permettent de le lancer de plusieurs façons, à partir, par exemple, d'un programme de planificateur. Voir « Méthodes de lancement supplémentaires » à la page 224.

Modification du protocole de connexion du serveur

Un problème de connexion peut survenir lorsque la console tente de se connecter à un serveur. Par défaut, le protocole SQL « Canaux nommés » est utilisé pour tous les serveurs. Le protocole recommandé est TCP/IP.

Pour modifier le protocole de connexion du serveur :

1. A partir du menu **Démarrer** de Windows, sélectionnez **Exécuter**.

   La fenêtre Exécuter s'affiche.

2. Tapez le texte suivant :

   ```
   CLICONFG.EXE
   ```

3. Cliquez sur **OK**.

   L'utilitaire réseau client/serveur SQL apparaît (Figure 9-12).

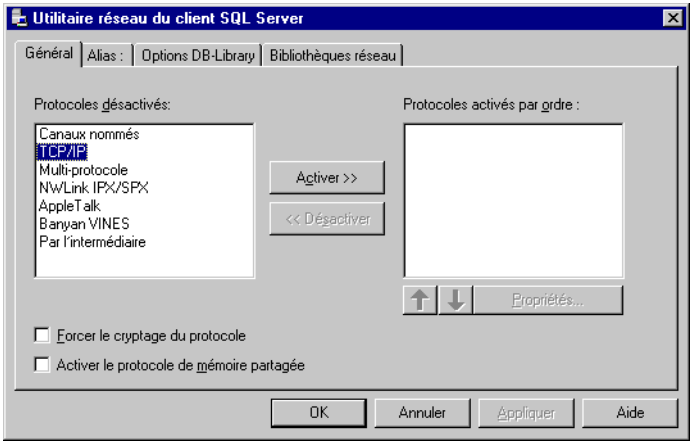


Figure 9-12. Utilitaire réseau client/serveur SQL

4. Sélectionnez **TCP/IP**.

5. Cliquez sur **OK**.

   Vous pouvez maintenant tenter de nouveau l'action qui a essayé de se connecter au serveur.

Connexion à la base de données de fusion

Lorsque vous avez créé votre base de données de fusion, vous pouvez vous connecter à celle-ci depuis la console et produire les rapports et requêtes nécessaires.

Pour se connecter à une base de données de fusion :

1. Dans l'arborescence de la console, sous Anti-Virus Informant, cliquez avec le bouton droit de la souris sur **Base de données AVI**, puis sélectionnez **Ajouter un nouveau serveur** dans le menu qui apparaît.
2. Sélectionnez le serveur qui contient la base de données de fusion.

   La zone de liste contient les serveurs SQL qui figurent dans le domaine réseau actuel. Si le serveur requis n'est pas répertorié, entrez le nom du serveur. Si vous souhaitez choisir l'ordinateur sur lequel vous exécutez la console ePolicy Orchestrator, sélectionnez **(local)**.
3. Entrez le nom de la base de données de fusion. Il doit correspondre au nom que vous avez entré lors de la création de la base de données de fusion.
4. Sélectionnez le **type d'authentification** dans la liste déroulante :
   - **Utilisateur actuellement connecté** — Sélectionnez ce type si vous voulez utiliser les références de l'utilisateur actuellement connecté. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.
   - **Authentification ePO** — Sélectionnez ce type si vous voulez utiliser les références d'ePolicy Orchestrator.

     REMARQUE : L'authentification ePO fonctionne uniquement avec les bases de données en cours d'utilisation par le service ePolicy Orchestrator (NAIMSERV). Une base de données fusionnée est généralement prise à partir de bases de données ePolicy Orchestrator. Il est donc improbable que vous puissiez utiliser l'authentification ePO pour vous connecter à une base de donnée fusionnée.
   - **Authentification SQL** — Sélectionnez ce type si vous configurez votre base de données MSDE ou SQL Server 7 pour qu'elle utilise l'authentification SQL. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.

- **Authentification Windows NT** — Sélectionnez ce type si vous configurez votre base de données MSDE ou SQL Server 7 pour qu'elle utilise l'authentification NT. Lorsque vous sélectionnez cette option, la zone **Domaine** devient disponible. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur, un mot de passe et un domaine valides.

5. Cliquez sur **OK**.

   Vous pourriez être invité à vous connecter à l'ordinateur sur lequel est installé le serveur ePolicy Orchestrator. Fournissez les informations demandées.

   La console ajoute la base de données de fusion au **Groupe de bases de données AVI**. Cela peut prendre quelques minutes, en fonction de l'état d'occupation de votre réseau. Lorsque la console s'est connectée, une icône s'affiche dans le groupe pour la base de données de fusion. S'il ne peut pas se connecter au serveur, un message d'erreur apparaît. Voir « Modification du protocole de connexion du serveur » à la page 222.

   Vous pouvez maintenant produire des rapports et des requêtes pour la base de données de fusion, et notamment définir un filtre de rapports, comme vous le feriez pour un serveur du Groupe de serveurs.

Méthodes de lancement supplémentaires

L'outil de fusion possède des fonctions supplémentaires qui vous permettent de :

- Ouvrir l'outil et utiliser des paramètres précédemment enregistrés ; voir page 225.
- Exécuter l'outil avec des paramètres précédemment enregistrés ; voir page 226.
- Exécuter l'outil depuis une ligne de commande avec des paramètres précédemment enregistrés ; voir page 226.

> **ASTUCE :** Cette méthode vous permet également d'exécuter silencieusement l'outil. Si vous possédez un programme de planificateur qui peut exécuter les applications 32 bits de Windows depuis une ligne de commande, vous pouvez l'utiliser pour exécuter l'outil à tout moment.

Pour ouvrir l'outil et utiliser des paramètres précédemment enregistrés :

1. A l'aide de l'Explorateur Windows, ouvrez le répertoire d'installation d'Anti-Virus Informant. Si vous avez installé le logiciel à son emplacement par défaut, vous trouverez ce répertoire à l'emplacement suivant :

1. C:\Program Files\McAfee\ePO\2.0\Avi

2. Double-cliquez sur le fichier **AVIDB_Merge_Tool.EXE** pour ouvrir l'outil de fusion.

   L'outil de fusion apparaît, affichant la fenêtre Choisir la base de données de destination.

3. A l'aide de l'Explorateur Windows, localisez le fichier texte (.TXT) des paramètres de fusion que vous avez enregistrés lors d'un précédent processus de fusion (Étape 15 à la page 221).

4. Glissez-déplacez le fichier sur l'outil de fusion (Figure 9-13).

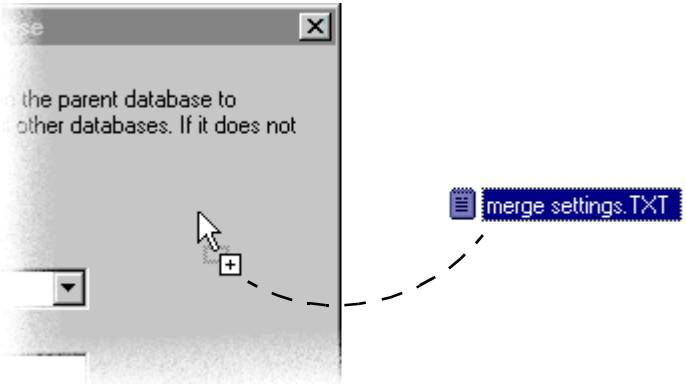


Figure 9-13. Déplacement du fichier des paramètres sur l'outil de fusion

L'outil de fusion importe les paramètres de fusion depuis le fichier texte et modifie ses écrans pour refléter ces paramètres. Vous pouvez maintenant utiliser l'outil de fusion et apporter davantage de modifications qui s'avèrent nécessaires.

Pour exécuter l'outil avec des paramètres précédemment enregistrés :

1. A l'aide de l'Explorateur Windows, ouvrez le répertoire d'installation d'Anti-Virus Informant *et* localisez le fichier texte (.TXT) des paramètres de fusion que vous avez enregistrés lors d'un précédent processus de fusion (Étape 15 à la page 221).

2. Glissez-déplacez le fichier sur l'icône de l'outil de fusion tout en maintenant enfoncé le bouton de la souris, puis relâchez le bouton de la souris.

   L'outil de fusion importe les paramètres de fusion depuis le fichier texte et exécute automatiquement le processus de fusion. L'écran Importer des données qui apparaît (Figure 9-11 à la page 221) vous permet d'afficher la progression du processus de fusion. L'écran disparaît lorsque le processus est terminé.

Pour exécuter l'outil depuis une ligne de commande avec des paramètres précédemment enregistrés :

1. Depuis le menu **Démarrer** de Windows, pointez sur **Programmes**, puis sélectionnez **Invite de commande**.

2. Dans la ligne de commande, entrez la commande suivante :

   ```
   <emplacement et nom de l'outil de fusion> <emplacement et nom du fichier de paramètres>
   ```

   REMARQUE : Vérifiez qu'il existe suffisamment d'espace entre les deux chemins d'emplacement. Si le chemin de l'outil de fusion comprend des espaces, vous devrez peut-être mettre le chemin entre guillemets. *Ne mettez pas* le chemin du fichier des paramètres entre guillemets.

   Par exemple, si l'outil de fusion se trouve dans C:\Program Files\logiciel ePolicy Orchestrator et si le nom et le chemin du fichier des paramètres sont C:\settings.txt, entrez :

   ```
   "C:\Program Files\logiciel ePolicy Orchestrator\AVIDB_Merge_Tool.exe" C:\settings.txt
   ```

   L'outil de fusion importe les paramètres de fusion depuis le fichier texte et exécute automatiquement le processus de fusion. La fenêtre Importer des données qui apparaît vous permet d'afficher la progression du processus de fusion. Cette fenêtre disparaît lorsque le processus est terminé.

3. Pour exécuter silencieusement l'outil, ajoutez `/silent` entre les deux chemins d'emplacement ; par exemple :

```
"C:\Program Files\logiciel ePolicy
Orchestrator\AVIDB_Merge_Tool.exe" /silent
C:\settings.txt
```

REMARQUE : Vérifiez qu'il existe un espace entre le chemin d'emplacement du fichier de paramètres et le `/silent`.

L'outil de fusion importe les paramètres de fusion depuis le fichier texte et exécute automatiquement le processus de fusion, *sans* afficher la fenêtre Importer des données. La tâche de fusion apparaît sur la barre des tâches de Windows (Figure 9-14) pour indiquer que le processus de fusion est en cours d'exécution.

Figure 9-14. Tâche de fusion sur la barre des tâches

ASTUCE : Si vous possédez un programme de planificateur qui peut exécuter les applications 32 bits de Windows depuis une ligne de commande, vous pouvez l'utiliser pour exécuter l'outil à tout moment. Pour plus d'informations sur cette procédure, consultez la documentation livrée avec le programme du planificateur.

Utilitaire de configuration

Cet utilitaire vous permet de modifier la base de données d'ePolicy Orchestrator, ainsi que le nom d'utilisateur et le mot de passe que vous utilisez pour administrer votre base de données SQL et pour passer en revue la base de données AVI.

L'utilitaire de configuration est automatiquement installé avec le logiciel ePolicy Orchestrator. Si vous avez installé les fichiers programme dans le répertoire par défaut, l'utilitaire sera installé dans le chemin suivant :

C:\Program Files\McAfee\ePO\2.0

L'utilitaire de configuration (CFGNAIMS.EXE) est un exécutable autonome que vous pouvez exécuter à partir d'une console ou d'un serveur.

Pour modifier la base de données :

1. Allez au répertoire dans lequel est installé l'utilitaire cfgnaims.EXE.
2. Double-cliquez sur le fichier **CFGNAIMS.EXE** pour exécuter l'utilitaire.
3. Cliquez sur l'onglet **Serveur SQL** pour modifier la base de données. Sélectionnez **Nom du serveur SQL** et entrez le **nom de la base de données**. La base de données que vous sélectionnez doit déjà exister.

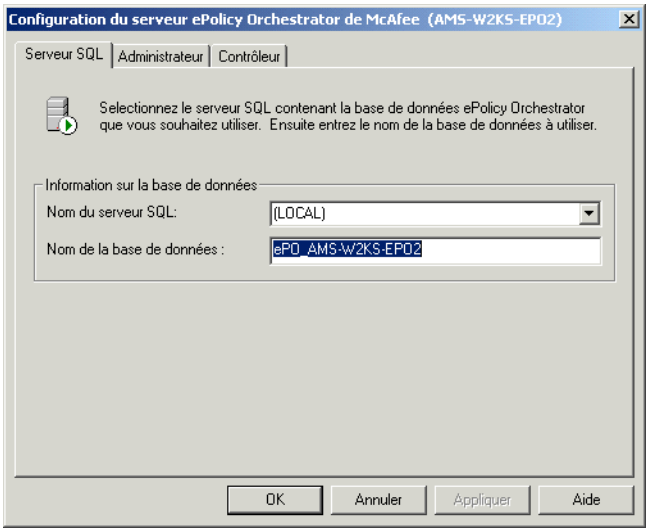


Figure 9-15. Outil de configuration – Serveur SQL

Pour modifier les références de l'utilisateur administrateur :

1. Cliquez sur l'onglet **Administrateur** pour modifier le nom d'utilisateur et le mot de passe que vous utilisez pour administrer la base de données SQL.

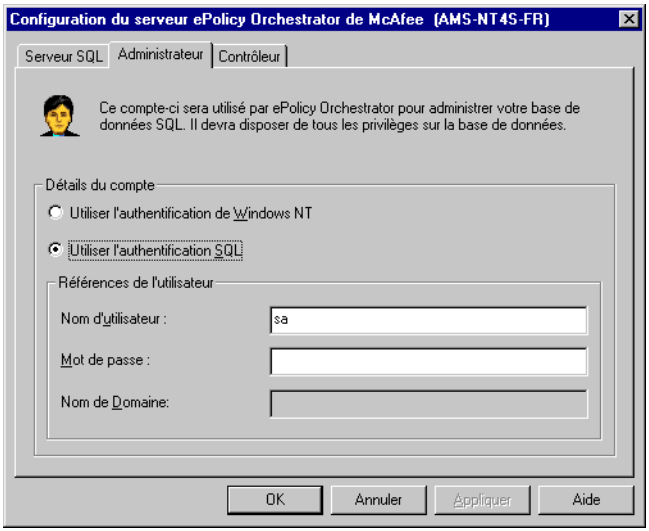


Figure 9-16. Outil de configuration — Administrateur

2. Sélectionnez **Utiliser l'authentification Windows NT** ou **Utiliser l'authentification SQL**.

   - Sélectionnez **Utiliser l'authentification Windows NT** si vous configurez votre base de données MSDE ou SQL Server 7 pour utiliser l'authentification NT. Lorsque vous sélectionnez cette option, le champ **Nom de domaine** devient disponible. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur, un mot de passe et un domaine valides.

   - Sélectionnez **Utiliser l'authentification SQL** si vous configurez votre base de données MSDE ou SQL Server 7 pour utiliser l'authentification SQL. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.

Le compte de réviseur est utilisé exclusivement par Anti-Virus Informant lors de la connexion à la base de données pendant l'authentification ePO, lorsqu'un compte d'utilisateur non général est utilisé. Cela fournit une sécurité supplémentaire en limitant l'accès des utilisateurs ne disposant pas de droits d'administrateur.

Pour modifier les références de l'utilisateur contrôleur :

1. Cliquez sur l'onglet **Contrôleur** pour modifier le nom d'utilisateur et le mot de passe que vous utilisez pour la base de données Anti-Virus Informant.

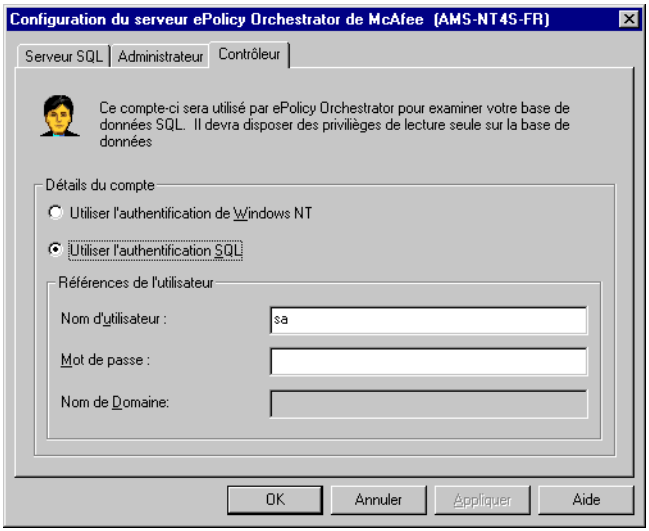


Figure 9-17. Outil de configuration — Contrôleur

2. Sélectionnez **Utiliser l'authentification Windows NT** ou **Utiliser l'authentification SQL**.

   - Sélectionnez **Utiliser l'authentification Windows NT** si vous configurez votre base de données MSDE ou SQL Server 7 pour utiliser l'authentification NT. Lorsque vous sélectionnez cette option, le champ **Nom de domaine** devient disponible. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur, un mot de passe et un domaine valides.
   - Sélectionnez **Utiliser l'authentification SQL** si vous configurez votre base de données MSDE ou SQL Server 7 pour utiliser l'authentification SQL. Si vous sélectionnez cette option, vous devez entrer un nom d'utilisateur et un mot de passe valides pour la base de données.

3. Cliquer sur **OK** pour accepter les modifications apportées.

REMARQUE : Vous devez redémarrer l'ordinateur pour que ces modifications soient prises en compte.

Traitement des apparitions de virus

A

Présentation

Après avoir installé ePolicy Orchestrator, installé et configuré votre logiciel anti-virus, déployé les agents et examiné les rapports, vous pouvez maintenant unir ces outils pour une réponse cohérente aux apparitions de virus.

La meilleure réponse face aux virus est le développement d'une stratégie efficace de réaction aux apparitions de virus. Ces outils vous offrent une possibilité de réponse efficace si vous les intégrez dans la réponse globale de votre société face aux dangers des virus informatiques.

Cette annexe comporte des instructions que vous pouvez suivre pour prévenir les infections et un scénario d'utilisation possible de réponse à une infection. Le logiciel ePolicy Orchestrator comprend certaines fonctionnalités, comme l'appel de réveil de l'agent, qui peuvent permettre de réduire le délai de réponse de l'ensemble de votre société.

Développement d'un plan

L'aspect le plus important du traitement des apparitions de virus est de créer une stratégie exploitable et efficace pour votre site ou votre société, puis de suivre le plan. Une stratégie efficace comporte un volet prévention en plus de la réponse.

Prévention

Une action préventive en tant qu'administrateur devrait comporter les éléments suivants :

- Installation et configuration d'un produit logiciel anti-virus McAfee, comme VirusScan 4.5, sur vos stations de travail et/ou serveurs client.
- Obtention des dernières mises à jour du fichier .DAT auprès de McAfee. Surveillez la fréquence et la procédure d'obtention des mises à jour du fichier .DAT.
- Contrôle des indicateurs de performance du réseau, comme la fonction serveur de messagerie ou bande passante disponible.

- Test des communications pour déterminer les meilleurs intervalles pour les réponses normales et les réponses aux apparitions de virus. Par exemple, test des intervalles pour :
  - Communications d'agent à serveur.
  - Appel de réveil de l'agent.
  - Collecte des propriétés et application des stratégies de l'agent.
  - Intervalles de téléchargement, dont le nombre maximal de téléchargements simultanés.
  - Randomisation optimale en utilisation normale et lors d'apparition de virus.
- Besoins de bande passante pour votre réseau (ils déterminent les types de réponse dont vous avez besoin lors d'une apparition de virus).

Besoins pour une stratégie efficace

Pour obtenir des résultats optimum d'une procédure telle que celle qui vous est présentée ici, vous *devez* disposer de tous les éléments suivants :

- **Une implémentation actuelle, intégralement installée, de ePolicy Orchestrator**. Si vous disposez d'une couverture inférieure à 100 % sur vos stations de travail et vos serveurs (serveurs Web et de messagerie inclus), vous ne disposez pas d'une couverture à 100 %.
- **Les fichiers .DAT mis à jour pour chaque produit anti-virus géré avec ePolicy Orchestrator**. L'efficacité de votre programme anti-virus dépend de la mise à jour des fichiers de définition de virus et de l'utilisation des moteurs d'analyse les plus récents. Consultez les guides de configuration de chaque produit anti-virus pour obtenir des informations pour conserver vos fichiers .DAT et votre moteur d'analyse à jour.
- **Une option d'appel de réveil de l'agent activée pour tous les agents**. Lorsque vous activez cette option, l'administrateur peut forcer tous les agents d'un groupe donné à contacter le serveur dans un délai précis et aider les agents à télécharger les fichiers nécessaires pour combattre une apparition de virus. Pour obtenir des instructions plus détaillées, consultez la section « Appel de réveil de l'agent » à la page 109.

- **WebImmune**. Un service de recherche de virus basé sur le Web de McAfee AVERT. Ce service utilise la technologie AVERT AutoImmune pour analyser les fichiers via la soumission d'une page Web et renvoie des réponses en temps réel au client. Les clients peuvent utiliser WebImmune pour soumettre des fichiers à AVERT. Si WebImmune ne peut pas répondre à la question du client, il transfère l'exemple à AVERT. Les réponses sont renvoyées au client via le Web et le client peut consulter le rapport en temps réel, ou quand cela lui convient. Pour plus d'informations, connectez-vous au site www.webimmune.net.

- **Une stratégie de réponse aux apparitions de virus pour votre société ou votre site qui comprend tous ces éléments**. Testez les fonctionnalités répertoriées ici avant une apparition de virus pour déterminer quel est votre délai de réponse opérationnel et quels intervalles utiliser pour optimiser vos feedback. Cela peut comprendre tous les éléments répertoriés dans la section « Prévention » à la page 231.

Les éléments présentés ici ne sont que des suggestions, et peuvent ne pas prendre en compte toutes les considérations nécessaires à votre installation.

Reconnaissance d'une attaque

Il existe plusieurs façons de savoir que votre réseau subit une attaque virale. Par exemple :

- Vous pouvez constater une baisse de la bande passante sur le réseau, ou que votre serveur de messagerie ne fonctionne plus.
- Vous pouvez entendre parler d'un nouveau virus par les médias.
- Si vous vous abonnez au service SecureCast de McAfee, vous pouvez recevoir des avertissements dès qu'un virus est identifié.
- Vous pouvez déterminer des normes spécifiques utilisées par votre société.

Lorsque vous êtes averti d'une nouvelle apparition de virus par SecureCast, le gestionnaire d'alerte ou Outbreak Manager de McAfee, ou par tout autre moyen, le logiciel ePolicy Orchestrator peut vous aider à réagir rapidement en utilisant plusieurs fonctionnalités de façon combinée.

Traitement d'une attaque

La fonctionnalité d'appel de réveil de l'agent vous permet de gérer la réponse de votre réseau aux apparitions de virus, de façon simple et rapide, avec votre logiciel ePolicy Orchestrator installé. Vous pouvez mettre à jour vos fichiers .DAT, configurer une stratégie ou définir une tâche, puis envoyer un appel de réveil à vos agents pour leur demander de contrôler et de collecter les nouvelles données. Cette section propose une suggestion de procédure utilisant l'appel de réveil de l'agent pour contenir une attaque virale.

Pour traiter une apparition avec ePolicy Orchestrator :

1. Mettez vos fichiers .DAT à jour avec les fichiers .DAT les plus récents. Consultez les guides de configuration de vos logiciels anti-virus pour obtenir des informations sur la façon de procéder pour chaque produit anti-virus géré avec ePolicy Orchestrator.
2. Planifiez une tâche de mise à jour définie sur « Exécuter immédiatement » pour déployer les fichiers .DAT mis à jour grâce à ePolicy Orchestrator. Pour plus de détails, reportez-vous à la section « » à la page 122.
3. Envoyez un appel de réveil de l'agent aux agents de votre installation. Définissez la randomisation sur le temps que vous avez prétesté pour optimiser la couverture d'apparition de virus. Consultez la section « Appel de réveil de l'agent » à la page 109 pour plus de détails.
4. Contrôlez l'activité de l'agent pendant l'apparition de virus. Vérifiez que vos agents collectent la stratégie et mettent les fichiers .DAT à jour sur chaque ordinateur.
5. Vérifiez la couverture de l'agent pour les nouveaux fichiers .DAT en utilisant les rapports de couverture du logiciel Anti-Virus Informant. Pour obtenir plus d'informations sur ces rapports et sur leur utilisation, consultez la section « Domaines d'application » à la page 167.

Forum aux questions B

Installation

Q. Puis-je copier le programme d'installation à un emplacement quelconque avant d'exécuter l'installation ?

R. Non. Actuellement, il existe une limitation à la longueur du chemin où s'effectue l'installation. C'est pour cette raison qu'il est recommandé d'exécuter l'installation à partir d'un répertoire temporaire tel que C:\Temp ou de créer un répertoire dans le répertoire principal, avec un nom ayant huit caractères au maximum.

Q. Tous les services appropriés sont lancés mais lorsque j'essaie de lancer le Serveur NAI d'ePolicy Orchestrator, j'obtiens une erreur 2140 ; à quel niveau se situe le problème ?

R. Vérifiez que vous n'avez pas démarré des services serveur Web tels que IIS (pour « World Wide Web Publishing Service »).

Q. Je n'arrive pas à connecter ma console distante au serveur ePolicy Orchestrator. Quel est le problème ?

R. Assurez-vous que le nom du serveur dans la boîte de dialogue de connexion est correct. Utilisez par défaut le système local.

Q. De combien de licences dois-je disposer pour le serveur SQL et ePolicy Orchestrator ?

R. Vous devez disposer de cinq licences, plus une pour chaque console distante installée après la première.

Déploiement

Q. Dois-je disposer de droits d'administrateur pour « pousser » l'agent ePolicy Orchestrator vers un système ?

R. Vous devez disposer de droits d'administrateur pour « pousser » l'agent ePolicy Orchestrator, à moins que l'administrateur spécifie un autre compte en utilisant la fonctionnalité de références intégrées.

Q. Comment ePolicy Orchestrator détermine-t-il le compte à utiliser pour pousser l'agent ?

R. ePolicy Orchestrator utilise le compte de service du serveur, à moins que l'administrateur ne spécifie un autre compte en utilisant la fonctionnalité de références intégrée.

Q. J'essaye de pousser vers un système Windows 95 ou Windows 98 sans aucun résultat. Quel est le problème ?

R. Vérifiez que les paramètres suivants sont définis correctement sur le système :

1. Activez « Partage de fichiers et de l'impression pour les réseaux Microsoft » sur le système.
2. Activez « Contrôle d'accès au niveau utilisateur » sous Voisinage réseau.
3. « Administration à distance » doit être activée dans Panneau de configuration/Mots de passe, et « Admins de domaine » doit se trouver sur la liste.
4. Vérifiez que votre nom se trouve également dans la liste si vous n'êtes pas un « Admin de domaine ».
5. Une fois que vous avez réussi à pousser l'agent, vous devez redémarrer le système avant de terminer l'installation.

Q. J'essaie de configurer un ordinateur et de le rechercher mais je ne le vois pas sur la liste. A quel niveau se situe l'erreur ?

R. Si le système est Windows 98 ou Windows 95, il n'est probablement pas prédéfini sur Annoncer LM et en conséquence il n'apparaît sur aucune liste. Essayez d'effectuer la recherche sur le Voisinage réseau et de voir s'il apparaît. S'il n'apparaît pas, vous devez soit le configurer sur Annoncer, soit l'ajouter manuellement.

Q. Dans Mettre à jour domaine, je vois un certain nombre d'ordinateurs dont l'icône est marquée d'une croix rouge alors que je suis sûr qu'elles font partie du domaine. Qu'est-ce que cela signifie ?

R. Le système Windows 95 ou Windows 98 qui a désactivé Annoncer LM s'affiche également de cette même manière. Vous pouvez laisser tel quel ou bien vous pouvez activer Annoncer LM et les icônes reprennent leur apparence normale.

Stratégies

Q. Comment dois-je définir une stratégie pour modifier les paramètres d'AutoUpdate ou d'AutoUpgrade dans le produit McAfee ?

R. Actuellement, l'unique méthode consiste à créer une tâche planifiée et de l'appliquer aux systèmes à modifier.

Q. J'active la fonctionnalité « Afficher l'icône d'état de l'agent », puis je pousse un agent, mais il ne s'affiche pas tout de suite. A quel niveau se situe l'erreur ?

R. Le paramètre par défaut est désactivé pour tous les agents. Une fois que vous avez poussé un agent vers un système il détermine au hasard une période de temps, comprise entre une et dix minutes, à l'issue de laquelle il contactera votre serveur et réactivera cette stratégie.

Q. Je crée une tâche planifiée pour une analyse à la demande et l'applique, mais elle n'apparaît pas sur le produit McAfee. Ais-je commis une erreur ?

R. A la différence des autres stratégies, la tâche à la demande est une tâche ePolicy Orchestrator interne uniquement et est exécutée par le planificateur de l'agent et non pas par le planificateur du produit McAfee.

Q. Je définis une stratégie sur le serveur, je vérifie que l'agent l'a appliquée et je m'aperçois qu'il ne l'a pas fait. A quel niveau se situe l'erreur ?

R. Les cas les plus courants d'échecs d'application sont répertoriés ci-après :

1. Vérifiez que l'option du serveur « Appliquer les stratégies » est activée pour la page que vous êtes en train de modifier.
2. Assurez-vous d'avoir cliqué sur le bouton « Appliquer » ou « OK » pour enregistrer vos paramètres. Si vous n'enregistrez pas les modifications apportées, les paramètres reprennent leur valeur d'origine.
3. Vérifiez que l'agent a communiqué avec le serveur depuis la modification et qu'il a reçu ces modifications pour les appliquer.
4. Si vous appliquez ces modifications à un groupe et que vous contrôlez un ordinateur dans ce groupe, vérifiez que cet ordinateur est prédéfini pour « Hériter » les modifications sinon il annule les paramètres de groupe.

Questions supplémentaires

Q. Avec quels systèmes d'exploitation ePolicy Orchestrator fonctionne-t-il ?

R. Le serveur ePolicy Orchestrator nécessite Windows NT 4.0/SP5, ou Windows 2000 Server ou Advanced Server. L'agent ePolicy Orchestrator nécessite Windows NT Workstation 4.0/SP5 ou version ultérieure, Windows NT Server 4.0/SP5 ou version ultérieure, Windows 2000 Server, Windows 2000 Workstation ou Windows 9x. Internet Explorer 5.0 avec le Service Pack 1 est requis pour utiliser le serveur ePolicy Orchestrator.

Q. Quels programmes anti-virus McAfee interagissent avec ePolicy Orchestrator ?

R. ePolicy Orchestrator prend en charge la gestion de stratégies et la création de rapports pour : VirusScan 4.03a/4.5/4.5.1, VirusScan TC 6.0.0, NetShield 4.03a/4.5, GroupShield Domino 5.0, Alert Manager 4.5, WebShield 4.5/e-50/e-500, WebShield SMTP et GroupShield Exchange 4.5.

Q. ePolicy Orchestrator peut-il prendre en charge Windows 2000 ?

R. Oui, ePolicy Orchestrator peut prendre en charge Windows 2000.

Q. Le serveur ePolicy Orchestrator peut-il envoyer des alertes SNMP ?

R. Non, il ne peut pas. Les produits McAfee sur les ordinateurs client exécutent toutes les fonctions du gestionnaire d'alerte. Définissez une alerte centralisée pour le(s) produit(s) chez le client. ePolicy Orchestrator ne permet pas d'exécuter une configuration de gestionnaire d'alerte pour les produits McAfee. Cependant, des options du gestionnaire d'alerte pour les systèmes précédemment configurés peuvent être définies et appliquées.

Q. Pourquoi reçois-je l'avertissement « Vérifier la configuration du site » lorsque je me connecte ?

R. Si un serveur ePolicy Orchestrator fonctionne correctement depuis un certain temps. Lorsque vous vous connectez à ePolicy Orchestrator, celui-ci indique que le mot de passe est incorrect, mais le mot de passe n'a pas changé.

Cette situation peut se produire si vous modifiez les paramètres proxy sous Internet Explorer 5 (IE 5), même si le serveur fonctionne correctement depuis un certain temps.

Q. L'agent fonctionne-t-il sur un ordinateur qui utilise DHCP ?

R. Oui. L'agent peut toujours communiquer avec le serveur si DHCP est installé.

Q. Que dois-je faire lorsque je reçois le message d'erreur suivant dans Server.log ?

Naispipe : La signature SPIPE ne correspond pas, kit ignoré par « ORDINATEUR_X »

R. Ce message d'erreur indique que « ORDINATEUR_X » n'a pas réussi à authentifier le kit SPIPE avec le serveur ePolicy Orchestrator et que cet ordinateur ne pourra pas communiquer avec le serveur ePolicy Orchestrator.

Pour résoudre le problème, remettez en place l'agent vers cet ordinateur.

Q. Que dois-je faire lorsque je reçois le message d'erreur suivant dans Server.log ?

Naisipe : Impossible de créer le kit, espace disque insuffisant.

R. Ce message d'erreur indique qu'il n'y a pas suffisamment d'espace disque sur le serveur ePolicy Orchestrator pour recevoir des kits.

Veuillez libérer suffisamment d'espace disque dur pour que le serveur ePolicy Orchestrator puisse recevoir des kits de l'agent ePolicy Orchestrator.

Q. Que dois-je faire lorsque je reçois le message d'erreur suivant dans Server.log ?

Naihttp : Impossible de se connecter à « ORDINATEUR_X »

R. Ce message d'erreur indique que le serveur ePolicy Orchestrator n'a pas réussi à envoyer un appel de réveil de l'agent à l'ordinateur « ORDINATEUR_X »

Assurez-vous que l'ordinateur de l'agent est en ligne et que le port ping de l'agent (dont la valeur par défaut est 8081) n'est pas bloqué par un firewall interne pour le trafic sortant.

Q. Que dois-je faire lorsque je reçois le message d'erreur suivant dans Server.log ?

Naihttp : Impossible d'établir une liaison avec le port « 80 »

R. Ce message d'erreur indique que le serveur SPIPE HTTP n'a pas réussi à établir une liaison avec le port HTTP 80 spécifié.

Vérifiez si un autre serveur Web est en cours d'exécution sur le même ordinateur serveur ePolicy Orchestrator. Si tel est le cas, reconfigurez le numéro de port de votre serveur Web en lui affectant un autre numéro de port HTTP ePolicy Orchestrator.

Q. Quels sont les paramètres régionaux correspondant aux langues prises en charge par le programme d'installation et la console d'ePolicy Orchestrator ?

R. Le programme d'installation et la console recherchent une correspondance exacte pour les langues suivantes :

Anglais — Anglais (USA)

Allemand — Allemand (Allemagne)

Espagnol — Espagnol (Traditionnel)

Français — Français (France)

Si aucune correspondance exacte n'est trouvée, la langue utilisée est, par défaut, l'anglais.

Glossaire

Administrateur de site

Type de compte permettant d'accéder à un site particulier de l'arborescence de la console et d'exécuter toutes les fonctions disponibles dans le logiciel sur ce site uniquement.

Comparer à *Administrateur général* et *Réviseur de site*.

Administrateur général

Type de compte permettant l'accès à l'intégralité de l'installation du logiciel ePolicy Orchestrator et l'exécution toutes les fonctions disponibles dans le logiciel sur chaque noeud de l'arborescence de la console.

Comparer à *Administrateur de site* et *Réviseur général*.

Agent

Un des trois composants du produit ePolicy Orchestrator. L'agent est un petit programme qui réside sur un ordinateur hôte (client), qui applique les stratégies et active les tâches que définit l'administrateur. L'agent interroge périodiquement le serveur ePolicy Orchestrator pour manifester sa présence, pour rendre compte de la configuration de la machine hôte de l'agent, pour donner des informations sur le logiciel installé et pour signaler des événements de virus identifiés par le logiciel anti-virus McAfee.

Voir aussi *Console* et *Serveur*.

analyse à la demande

Examen des fichiers sélectionnés pour déterminer s'ils contiennent un virus ou tout autre code malveillant. Cette analyse peut avoir lieu immédiatement, au moment de votre choix ou à intervalles réguliers.

Comparer à *Analyse à l'accès*.

analyse à l'accès

Examen des fichiers à utiliser pour déterminer s'ils contiennent un virus ou tout autre code malveillant. L'analyse à l'accès peut avoir lieu chaque fois qu'un fichier est lu et/ou écrit sur le disque.

Comparer à *Analyse à la demande*.

Arborescence de la console

Côté gauche (*volet*) de la console. Quand il est entièrement développé, il affiche le répertoire de groupes, les ordinateurs et les utilisateurs que gère ePolicy Orchestrator, le contenu du référentiel des logiciels et les composants associés au logiciel Anti-Virus Informant.

Authentifier

Garantir que les transmissions de données numériques sont livrées au destinataire désiré. En outre, l'authentification garantit l'intégrité et la source du message au destinataire. La forme la plus simple d'authentification exige un nom d'utilisateur et un mot de passe pour accéder à un compte particulier. Mais les protocoles d'authentification peuvent aussi être basés sur le chiffrement par clé secrète ou sur des systèmes de clé publique à l'aide de signatures numériques.

Console distante

Console s'exécutant sur un ordinateur sur lequel le serveur ePolicy Orchestrator ne tourne pas. Les consoles distantes permettent à plusieurs personnes d'accéder à la console pour réviser des actions ou pour gérer des sites et des installations.

Console

Un des trois composants du produit ePolicy Orchestrator. La console est l'interface de l'administrateur avec le produit ; elle donne des informations sur le serveur et sur chaque ordinateur hôte sur lequel est installé l'agent. C'est le centre de commande permettant à l'administrateur d'introduire des logiciels dans le référentiel, de déployer et d'administrer des logiciels et de définir des stratégies et des tâches.

Voir aussi *Agent* et *Serveur*.

Déploiement, déployer

Distribution stratégique des logiciels, les stratégies et les tâches des groupes, les ordinateurs et les utilisateurs. Lorsqu'un agent a été déployé sans problèmes, il effectue une communication agent-serveur, faisant état des propriétés du serveur ou demandant des stratégies et des tâches à ce serveur.

Domaine

Sous-réseau composé d'un groupe de clients et de serveurs sous le contrôle d'une seule base de données de sécurité. L'administrateur peut importer un domaine Windows NT entier sous la forme d'un groupe à gérer sous ePolicy Orchestrator.

DUN

Accès réseau à distance (Dial-Up Networking).

Enfant

Côté dépendant d'un lien hiérarchique. Un enfant est un noeud dans une structure hiérarchique qui a un autre noeud au-dessus de lui (plus près de la racine). Les noeuds enfants appartiennent toujours à un groupe parent et par défaut, ils héritent toujours des paramètres de ce groupe. Dans le logiciel ePolicy Orchestrator, un enfant est un élément de l'arborescence de la console dont le nom figure dans l'arborescence du répertoire.

Comparer avec *Parent*.

Evénement

Occurrence importante qui a lieu sur le serveur ou sur l'hôte de l'agent et qui est répertoriée dans un rapport d'événements.

Le rapport d'événements est différent des fichiers journaux créés par le logiciel anti-virus lui-même et stockés en local sur les ordinateurs client.

Voir aussi *Journal.*

Fichier .NAP

Fichier Network Associates Package. Cette extension de fichier désigne les fichiers du programme McAfee que vous installez dans le référentiel de logiciels pour les fonctions de gestion ePolicy Orchestrator.

Fichier EXTRA.DAT

Fichier de définitions de virus créé en réponse à l'apparition d'un nouveau virus ou d'une nouvelle variante d'un virus existant.

Voir aussi *Fichier .DAT, Fichier .DAT incrémentiel* et *SuperDAT*.

Fichiers .DAT

Fichiers de définitions de virus permettant au logiciel anti-virus de reconnaître les virus et leur code imbriqué dans des fichiers. Pour plus d'informations, reportez-vous à la documentation de votre logiciel anti-virus.

Voir aussi *fichier .DAT incrémentiel, fichier EXTRA.DAT* et *SuperDAT*.

Fichiers .DAT incrémentiels

Nouvelles définitions de virus qui viennent compléter les définitions actuellement installées. L'utilitaire de mise à jour peut télécharger uniquement les fichiers .DAT les plus récents plutôt que le jeu complet de fichiers .DAT.

Voir aussi *Fichier .DAT incrémentiel, Fichier EXTRA.DAT* et *SuperDAT*.

Forcer la désinstallation

Supprimer un logiciel anti-virus McAfee sur un hôte d'agent. Les écrans de stratégies pour les produits dans le référentiel des logiciels proposent une option pour forcer la désinstallation du logiciel. Vous devez sélectionner cette option pour retirer le logiciel sur un hôte d'agent.

Forcer l'installation

Installer le logiciel anti-virus McAfee sur un hôte d'agent. Les écrans de stratégies pour les produits dans le référentiel des logiciels proposent une option pour forcer l'installation du logiciel. Vous devez sélectionner cette option pour installer le logiciel.

Groupe Perdu & Trouvé

Référentiel pour les données renvoyées d'un agent non identifié. Si les informations sont suffisantes pour placer l'agent dans un groupe Perdu & Trouvé au niveau du site, le noeud y apparaît. Sinon, le noeud apparaît dans le groupe Perdu & Trouvé général.

Groupe

Dans ePolicy Orchestrator, ensemble logique d'entités regroupées pour faciliter la gestion. Un groupe peut contenir des ordinateurs, des utilisateurs ou d'autres groupes.

Hériter

Hériter signifie prendre les propriétés, installations, stratégies et caractéristiques du noeud parent. Les noeuds enfants héritent des caractéristiques ou des actions du parent à moins que l'administrateur ne modifie la stratégie dans la console.

Hôte d'agent

Voir *ordinateur hôte*.

Hôte, ordinateur hôte

Ordinateur client qui héberge l'agent ePolicy Orchestrator. Voir *Hôte d'agent*.

IBM Secureway

Base de données IBM utilisée dans ePolicy Orchestrator.

Interrogation

Technique de communication au cours de laquelle l'agent contacte le serveur à des intervalles prédéfinis pour savoir s'il y a de nouvelles stratégies ou tâches à appliquer ou à exécuter.

Voir aussi *Intervalle des communications d'agent à serveur*.

Intervalle des communications d'agent à serveur (ASCI)

Intervalle entre les requêtes de l'agent au serveur en ce qui concerne les nouvelles stratégies et tâches. Comparer avec *Mise à jour des propriétés*.

La page Options de l'agent ePolicy Orchestrator permet à l'administrateur de définir des valeurs pour deux intervalles :

L'agent demande de nouvelles stratégies et de nouvelles tâches toutes les ___ minutes (ASCI)

L'agent envoie des propriétés au serveur toutes les ___ minutes (Propriétés)

Journal

Fichier stockant les activités d'un composant du logiciel anti-virus McAfee. Les journaux enregistrent les actions effectuées lors d'une installation ou des tâches d'analyse ou de mise à jour.

Voir aussi *Evénement*.

MAPI

Interface MAPI (Messaging Application Programming Interface). C'est l'un des deux protocoles de messagerie utilisés par ePolicy Orchestrator.

Voir aussi *SMTP*.

Masque de sous-réseau

Valeur appliquée à une adresse IP pour différencier l'ID du réseau de l'ID de l'hôte. L'ID du réseau établit le routage correct pour un message TCP/IP.

MDAC

Microsoft Data Access Component. Utilitaire que vous installez sur le serveur ePolicy Orchestrator avant d'installer le logiciel ePolicy Orchestrator si vous avez l'intention d'utiliser Microsoft SQL Server 7 pour la base de données Anti-Virus Informant.

Mise à jour des propriétés

Intervalle entre les rapports de l'agent au serveur en ce qui concerne ses propriétés (configuration en cours et logiciels installés). La page Options de l'agent permet à l'administrateur de définir des valeurs pour deux intervalles :

L'agent envoie des propriétés au serveur toutes les ___ minutes (Propriétés)

L'agent demande de nouvelles stratégies et de nouvelles tâches toutes les ___ minutes (ASCI)

Comparer avec *Intervalle des communications d'agent à serveur.*

MMC

Microsoft Management Console. La console ePolicy Orchestrator est une mise en oeuvre de MMC.

MSDE

Microsoft Data Engine. Base de données Anti-Virus Informant par défaut fournie avec le logiciel ePolicy Orchestrator.

Noeud

Tout élément représenté dans la structure hiérarchique de l'arborescence de la console.

Voir aussi *Enfant* et *Parent*.

Parent

Côté dominant d'un lien hiérarchique. Un parent est un noeud dans l'arborescence de la console qui comporte lui-même des noeuds en dessous. Par défaut, un noeud enfant hérite des stratégies et des tâches du parent. Tous les groupes sont des parents.

Comparer avec *Enfant*.

POAGINST.EXE

Fichier exécutable pour l'installation de l'agent. Lors de son exécution, ce fichier installe l'agent ePolicy Orchestrator sur un ordinateur hôte.

Pull

Action par laquelle un agent extrait des informations du serveur. L'agent *extrait* de cette manière des stratégies et des tâches du serveur.

Push

Action par laquelle le serveur transmet des logiciels, des stratégies ou des tâches à l'agent pour qu'il les installe ou les applique.

Racine de la console

Noeud au sommet de l'arborescence de la console dans ePolicy Orchestrator. Il comporte deux noeuds, chacun contenant un des deux composants installables du programme :

- **ePolicy Orchestrator**
- **Anti-Virus Informant**

Référentiel

Voir *Référentiel de logiciels*.

Référentiel de logiciels

Emplacement où sont stockés les progiciels anti-virus et apparentés que le programme ePolicy Orchestrator peut déployer et gérer. Dans l'arborescence de la console, c'est le noeud logiciel situé sous ePolicy Orchestrator. Voir *Référentiel*.

Réviseur de site

Type de compte permettant de voir un seul site de l'arborescence de la console. Le réviseur de site ne peut pas exécuter de fonction à part les rapports prédéfinis Anti-Virus Informant pour ce site uniquement.

Comparer à *Réviseur général* et *Administrateur de site*.

Réviseur général

Type de compte permettant de voir l'intégralité de l'installation du logiciel ePolicy Orchestrator mais pas d'exécuter les fonctions, hormis les rapports préréglés du logiciel Anti-Virus Informant.

Comparer à *Réviseur de site* et *Administrateur général*.

Serveur

Un des trois composants du produit ePolicy Orchestrator. Le serveur héberge l'application ePolicy Orchestrator, sa base de données et le référentiel des logiciels.

Voir aussi *Agent* et *Console*.

Site

Site de premier niveau sous le répertoire de l'arborescence de la console. Un site possède des propriétés spéciales qui facilitent sa gestion, par exemple l'affectation d'une adresse IP.

SMTP

Protocole de transfert de courrier simple (Simple Mail Transfer Protocol). C'est l'un des deux protocoles de messagerie utilisés par ePolicy Orchestrator.

Voir aussi *MAPI*.

SPIPE

PIPE sécurisé, processus de communications sécurisées qui sert à passer des informations entre les composants du produit ePolicy Orchestrator.

SSL

Secured Sockets Layer.

Stratégie

Paramètres de configuration des activités routinières, telles que l'analyse à l'accès. Il ne peut y avoir qu'un seul jeu de stratégies par ordinateur pour chaque produit logiciel installé.

Comparer avec *Tâche.*

Stratégie anti-virus

Voir *Stratégie.*

SuperDAT

Utilitaire qui installe des fichiers de définitions de virus à jour (.DAT) et, lorsque c'est nécessaire, met à jour le moteur d'analyse.

Voir aussi *Fichier .DAT, Fichier EXTRA.DAT* et *Fichier .DAT incrémentiel.*

Tâche

Activité non routinière, telle que l'analyse à la demande ou la mise à jour, qui est programmée pour se produire à un moment particulier ou à des intervalles spécifiques.

Comparer à *Stratégie.*

Volet de portée

Terminologie Microsoft désignant le côté gauche de la console. Sur la console ePolicy Orchestrator, il s'agit de *l'arborescence* de la console.

Volet de résultats

Terminologie Microsoft désignant le côté droit de la console. Sur la console ePolicy Orchestrator, il s'agit du *volet des détails.*

Volet Détails

Côté droit de la console d'ePolicy Orchestrator, qui comporte trois onglets : Stratégies, Propriétés et Tâches. Les informations affichées dans le volet des détails varient selon l'onglet sélectionné.

Voir aussi *Volet supérieur des détails* et *Volet inférieur des détails.*

Volet inférieur des détails

Sur la console, partie inférieure du volet des détails, qui affiche les stratégies configurables pour un progiciel. Il n'apparaît que si vous avez sélectionné un élément dans le répertoire et cliqué sur l'onglet Stratégies.

Voir aussi *Volet des détails* et *Volet supérieur des détails.*

Volet supérieur des détails

Sur la console, partie supérieure du volet des détails qui affiche les logiciels installés et les fonctions pouvant être configurées. Le volet des détails ne se fractionne que si vous avez sélectionné un élément dans le répertoire et cliqué sur l'onglet Stratégies.

Volet

Sous-section de la console.

Voir *Volet des détails* et *Arborescence de la console.*

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V