Guide de l'utilisateur
Révision 1.0

VirusScan® for Mac

Version 8.6

McAfee®
Protection des systèmes

Une sécurité éprouvée

McAfee®

Publié en novembre 2007 / Logiciel VirusScan for Mac version 8.6

DBN-001-FR

Table des matières

1 Présentation de VirusScan for Mac

Contenu du guide

Ce guide présente VirusScan for Mac 8.6 et fournit les informations suivantes sur la protection de votre ordinateur contre les virus :

- présentation du produit ;
- description des fonctionnalités du produit ;
- description de toutes les nouveautés de cette version du logiciel ;
- instructions détaillées relatives à l'installation du logiciel ;
- instructions détaillées relatives à la configuration et au déploiement du logiciel ;
- procédures d'exécution des tâches ;
- informations relatives au dépannage ;
- intégration de ePolicy Orchestrator versions 3.6 (correctif 2), 3.6.1 et 4.0.

Qu'est-ce que VirusScan ?

L'application VirusScan for Mac est un antivirus qui permet de protéger votre ordinateur Apple contre les virus, les chevaux de Troie et tout autre code malveillant. VirusScan offre les fonctions suivantes : analyse à la demande, analyse des messages Apple Mail, planification eUpdate, aide en ligne, analyse à l'accès et analyse par glisser-déplacer. En outre, vous avez toujours « à portée de clic » une bibliothèque en ligne contenant des informations complètes sur les virus et toutes les nouvelles menaces.

VirusScan protège votre système contre les virus qui peuvent résider sur d'autres ordinateurs Macintosh, Windows et UNIX, ou sur des volumes montés en externe tels que des périphériques USB, Firewire et des CD ou des DVD.

Cette version de VirusScan contient également une protection antivirus pour le système d'exploitation Mac OS X 10.5 (Leopard).

Possibilités offertes par VirusScan

VirusScan détecte et nettoie les virus de programme et de macro, ainsi que les chevaux de Troie, dans tous les types de fichiers Macintosh, Windows et UNIX, y compris les fichiers compressés et les documents composites OLE.

Grâce à VirusScan, vous pouvez analyser un fichier particulier, un répertoire de fichiers, la totalité de votre lecteur ou des volumes montés tels que des CD, des fichiers .DMG, des fichiers montés en réseau, des messages Apple Mail et des périphériques USB (clés USB stylo, iPods et appareils photos). L'analyse heuristique avancée détecte les nouveaux virus de macro et de programme.

Nouveautés de cette version

- Prise en charge de Mac OS X Leopard (10.5)
- Optimisation des performances de l'analyse à l'accès
- Optimisation des performances de l'analyse à la demande
- Prise en charge d'ePolicy Orchestrator 4.0
- Mises à jour des fichiers DAT incrémentiels
- Prise en charge du moteur d'analyse 5200

Fonctionnalités de VirusScan

En plus des puissantes fonctionnalités présentes dans ses versions antérieures, VirusScan propose de nouvelles protections et de nouveaux outils pour la défense de votre système informatique. Par le biais du système d'aide en ligne, vous pouvez en outre obtenir une assistance en matière de dépannage et des procédures de réalisation de tâches.

Console VirusScan

La console VirusScan offre une interface conviviale pour la configuration de VirusScan.

A l'aide de la console, vous pouvez configurer l'analyseur à la demande et également effectuer des analyses à la demande par le biais de la zone de dépôt (zone de la console VirusScan qui vous permet de glisser-déplacer les fichiers que vous souhaitez analyser). Cliquez sur l'option **Déposer éléments ou cliquer ici** pour ouvrir la boîte de dialogue **Sélectionner un fichier ou dossier à analyser et à nettoyer** pour sélectionner le ou les fichiers ou dossiers à analyser et nettoyer à la demande.

Vous pouvez également configurer et activer l'analyseur à l'accès à partir de la console VirusScan, et activer la mise à niveau automatique des définitions de virus à l'aide d'eUpdate.

Pour accéder à la console VirusScan, double-cliquez sur l'icône **VirusScan** dans le dossier **Applications** de l'ordinateur.

Analyseur à la demande

L'analyseur à la demande vous permet de lancer une analyse à tout moment en glissant-déposant le ou les fichiers sélectionnés sur la console. Cliquez sur l'option **Déposer éléments ou cliquer ici** pour ouvrir la boîte de dialogue **Sélectionner un fichier ou dossier à analyser et à nettoyer** pour sélectionner le ou les fichiers ou dossiers à analyser et nettoyer.

L'analyseur à la demande permet de sélectionner plusieurs fichiers, répertoires ou volumes. Les résultats de l'analyse sont récapitulés dans un rapport que vous pouvez enregistrer ou imprimer. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que son action en cas de présence de fichiers infectés. L'analyseur vous avertit lorsqu'il détecte un virus et génère un journal de ses actions.

Pour accéder à l'analyseur à la demande, déposez par glisser-déplacer les fichiers à analyser sur l'icône **VirusScan** ou dans la zone de dépôt de la console.

Analyseur à l'accès

L'analyseur à l'accès fournit une surveillance en continu de tous les fichiers utilisés, qui permet de détecter la présence d'un virus ou de tout code potentiellement malveillant. Une analyse est effectuée automatiquement chaque fois qu'un fichier est lu à partir du disque et/ou écrit sur le disque par l'utilisateur ou par des processus système.

L'analyseur à l'accès applique la stratégie de surveillance en continu pour plusieurs fichiers, répertoires ou volumes, notamment les volumes résidant sur des ordinateurs distants connectés au réseau. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que son action en cas de présence de fichiers infectés. L'analyseur affiche un message dans la fenêtre **Reporter** lorsqu'il détecte un virus ou tout autre code malveillant.

Vous activez l'analyseur à l'accès à partir de la console VirusScan.

VirusScan Schedule Editor

Le composant VirusScan Schedule Editor vous permet de planifier les analyses automatiques et les mises à jour automatiques des fichiers de définitions de virus (DAT) disponibles en ligne. Vous pouvez planifier les analyses et les mises à jour par le biais de la console **VirusScan Schedule Editor**. Il est possible de définir des analyses et des mises à jour automatiques quotidiennes, hebdomadaires ou mensuelles. Pour accéder à VirusScan Schedule Editor, cliquez sur une de ces tâches :

- Cliquez sur **Planificateur**  dans la console VirusScan.
- Sélectionnez **Tâches planifiées** dans **Présentation** dans le menu principal.
- Ouvrez le composant VirusScan Schedule Editor directement à partir du dossier `/Applications/Utilities`.

eUpdate

eUpdate vous permet de mettre à jour les fichiers DAT et le moteur antivirus. eUpdate met continuellement à jour votre logiciel antivirus avec de nouvelles informations sur les virus et les fonctionnalités d'analyse. eUpdate vérifie automatiquement les nouvelles mises à jour et met à jour les définitions de virus lorsque de nouvelles définitions sont disponibles. Vous pouvez également utiliser le composant VirusScan Schedule Editor pour configurer eUpdate de sorte qu'il recherche les mises à jour lorsque vous l'avez planifié.

Pour lancer manuellement une mise à jour eUpdate, cliquez sur l'onglet **eUpdate** sur la console VirusScan, puis sur le bouton **Démarrer**. La prise en charge d'eUpdate est fournie par le biais du protocole FTP.

Gestion d'ePolicy Orchestrator

VirusScan s'intègre à McAfee ePolicy Orchestrator versions 3.6 (patch 2), 3.6.1 et 4.0 vous permettant ainsi d'utiliser ce logiciel dans un environnement géré. Le logiciel ePolicy Orchestrator fournit une plaque tournante pour les solutions de protection de système McAfee. Les administrateurs peuvent ainsi réduire les risques inhérents aux systèmes « voyous » non conformes, maintenir la protection à jour, configurer et appliquer les stratégies de protection et surveiller l'état de sécurité à partir d'une console unique centralisée évolutive en fonction des besoins de l'entreprise. Avec ePolicy Orchestrator, vous pouvez configurer VirusScan for Mac sur les systèmes cibles de votre réseau ; vous n'avez pas besoin de les configurer individuellement à partir de la fenêtre **Préférences**.

L'utilisation d'ePolicy Orchestrator est facultative et vous pouvez utiliser de façon autonome toutes les fonctionnalités de VirusScan.

Vous pourrez utiliser la fonctionnalité ePolicy Orchestrator intégrée uniquement si un serveur ePolicy Orchestrator et l'agent non Windows sont installés et configurés pour gérer VirusScan dans un environnement professionnel.

Public concerné

Ces informations sont destinées aux administrateurs de réseau qui sont responsables du programme de sécurité et de protection antivirus de leur société.

Conventions

Ce guide utilise les conventions suivantes :

Bold Condensed	Tous les mots figurant dans l'interface utilisateur, y compris les noms d'option, de menu, de bouton et de boîte de dialogue. **Exemple :** Entrez le **Nom d'utilisateur** et le **Mot de passe** du compte approprié.

`Courier`	Chemin d'un dossier ou d'un programme, texte que l'utilisateur saisit lui-même (par exemple, une commande à l'invite du système).
	Exemples :
	L'emplacement par défaut du programme est le suivant :
	`/Applications/Utilities`
	Exécutez cette commande sur l'ordinateur client :
	`scan --help`

Italique	Introduction d'un nouveau terme ; emphase ; titres des manuels et des rubriques (têtes de chapitre) dans la documentation des produits. **Exemple :** Pour en savoir plus, consultez le *Guide produit de VirusScan Enterprise*.
Bleu	Adresse Web (URL) et/ou lien actif. **Exemple :** Visitez le site Web McAfee à l'adresse suivante : `http://www.mcafee.com`
<TERME>	Des chevrons encadrent les termes génériques. **Exemple :** Dans l'arborescence de la console, cliquez à l'aide du bouton droit sur le <SERVEUR>.
	**Remarque :** information complémentaire, par exemple, autre méthode pour exécuter la même commande.
	**Astuce :** conseils et recommandations de McAfee en matière de prévention des menaces, de performances et d'efficacité.
	**Attention :** conseils importants destinés à protéger votre système informatique, votre entreprise, votre installation logicielle ou vos données.
	**Avertissement :** conseil important pour mettre en garde un utilisateur contre des blessures corporelles lors de l'utilisation ou de la manipulation d'un produit matériel.

Obtention d'informations sur le produit

Sauf indication contraire, la documentation relative au produit est fournie sous la forme de fichiers .PDF Adobe Acrobat sur le CD du produit ou sur le site de téléchargement de McAfee.

Documentation standard

Guide de l'utilisateur : ce guide présente le produit, décrit ses fonctionnalités et fournit des instructions sur l'installation et la configuration du logiciel, son exploitation et sa maintenance. Il présente également les fonctions de gestion d'ePolicy Orchestrator pour VirusScan et fournit des instructions détaillées pour l'installation, la configuration et la gestion du logiciel dans un environnement professionnel. Le présent guide (*Guide de l'utilisateur de VirusScan*) est disponible en format .PDF dans le dossier **Documentation** du package du produit.

Aide : informations générales et détaillées accessibles depuis l'application.

Notes de version de VirusScan for Mac : ce fichier décrit les fonctionnalités du produit, les ajouts et modifications de dernière minute apportés à la documentation ainsi que tout autre problème lié à la version de produit. Il décrit également le processus d'installation. Ce fichier est disponible dans le dossier **Documentation** du package du produit.

Licence : livret de l'accord de licence McAfee (.PDF) comprenant tous les types de licence disponibles pour le produit concerné. Cet accord définit les conditions générales d'utilisation du logiciel sous licence. Lisez-les attentivement. En installant le produit, vous acceptez les conditions du contrat de licence. L'accord de licence du logiciel McAfee est disponible dans le dossier **Documentation** du package du produit.

Liens internes au produit

Le menu Aide du logiciel contient des liens vers des sources d'informations utiles.

- Aide de VirusScan
- Soumission d'un échantillon
- Support technique
- Bibliothèque d'informations sur les virus

Aide de VirusScan

Ce lien permet d'accéder aux rubriques de l'aide en ligne du logiciel.

Soumission d'un échantillon

Ce lien vous permet d'envoyer des fichiers potentiellement infectés pour les faire analyser par McAfee. Vous recevrez des informations sur vos fichiers, notamment des solutions et des correctifs en temps réel, si nécessaire.

Support technique

Ce lien vous permet d'accéder au site Web de support technique de McAfee pour obtenir de la documentation sur les produits, consulter des foires aux questions ou des conseils et astuces de dépannage.

Bibliothèque d'informations sur les virus

Ce lien permet d'accéder à la bibliothèque d'informations sur les virus de McAfee Avert Labs. Ce site Web rassemble des données détaillées sur l'origine des virus, leurs modes de propagation et les procédures permettant de les éliminer.

Outre les informations sur les véritables virus, cette bibliothèque contient des renseignements utiles sur les programmes canulars, tels que les avertissements de virus envoyés par e-mail, comme par exemple, parmi de nombreux autres, Virtual Card For You et SULFNBK. La prochaine fois que vous recevrez un avertissement bien intentionné signalant l'existence d'un virus, consultez la page de la bibliothèque consacrée aux programmes canulars avant de transmettre le message à vos amis.

Pour accéder à la bibliothèque d'informations sur les virus :

1 Ouvrez VirusScan.

2 Dans le menu **Aide**, sélectionnez **Bibliothèque d'informations sur les virus**.

Coordonnées

Centre de recherche sur les menaces : McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Bibliothèque d'informations sur les menaces d'Avert Labs
http://vil.nai.com

Avert Labs WebImmune et Soumission d'un échantillon *(Informations d'authentification de connexion requises)*
https://www.webimmune.net/default.asp

Service de notification de fichiers DAT Avert Labs
http://vil.nai.com/vil/signup_DAT_notification.aspx

Site de téléchargement http://www.mcafee.com/us/downloads/

Mises à niveau des produits *(numéro de licence valide requis)*

Mises à jour de sécurité (fichiers DAT, moteur)

Versions de correctifs (HotFix) et de patchs

- **Pour les points de vulnérabilité de la sécurité** *(Disponible au public)*
- **Pour les produits** *(compte ServicePortal et numéro de licence valide requis)*

Evaluation des produits

Programme bêta de McAfee

Support technique http://www.mcafee.com/us/support/

Recherche dans la base de connaissances
http://knowledge.mcafee.com/

McAfee Support technique ServicePortal *(Informations d'authentification de connexion requises)*
https://mysupport.mcafee.com/eservice_enu/start.swe

Service clientèle

Web
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

Téléphone : numéro vert pour les États-Unis, le Canada et l'Amérique latine :
+1-888-VIRUS NO ou **+1-888-847-8766** Du lundi au vendredi, de 8h00 à 20h00, Centre

Services professionnels

Enterprise : http://www.mcafee.com/us/enterprise/services/index.html

PME/PMI : http://www.mcafee.com/us/small/services/index.html

2 Installation de VirusScan for Mac

Cette section fournit des instructions sur l'installation du logiciel VirusScan et des informations détaillées dans les domaines suivants :

Configuration système requise

Pour installer le logiciel VirusScan for Mac, vous devez posséder un ordinateur Mac basé PowerPC ou Intel, le système d'exploitation Mac OS X Tiger (10.4.6 ou supérieure) ou Mac OS X Leopard (10.5), 512 Mo (ou plus) de RAM, et au moins 45 Mo d'espace disque libre.

Configuration requise pour ePolicy Orchestrator

VirusScan est compatible avec ePolicy Orchestrator versions 3.6 (correctif 2), 3.6.1 et 4.0. Toutefois, l'utilisation d'ePolicy Orchestrator est facultative et vous pouvez utiliser VirusScan for Mac de façon autonome.

Vous pourrez utiliser la fonctionnalité ePolicy Orchestrator intégrée uniquement si un serveur ePolicy Orchestrator et un agent non Windows sont installés et configurés pour gérer VirusScan dans un environnement professionnel.

Installation de VirusScan

VirusScan for Mac peut être installé selon la méthode standard (par le biais d'une interface graphique) ou selon la méthode silencieuse (par le biais de la ligne de commande). Une fois le produit installé, vous pouvez consulter le fichier ReadMe dans le dossier **Documentation** du package du produit. Ce fichier contient des informations sur les problèmes connus, les ressources en ligne et d'autres informations utiles.

Avec VirusScan, vous pouvez utiliser la fonction eUpdate pour vous connecter à un site Web et télécharger de nouveaux fichiers DAT. Pour en savoir plus sur eUpdate et d'autres fonctions de VirusScan, reportez-vous *Mise en route* , page 17.

Vous devez disposer des privilèges d'administrateur pour installer ce produit.

Installation standard

Vous pouvez installer VirusScan à l'aide du fichier d'installation de VirusScan, situé sur le CD du produit ou dans le fichier .ZIP d'installation téléchargé sur le site Web McAfee et enregistré dans un répertoire temporaire.

Pour installer VirusScan :

1. Double-cliquez sur le fichier **VirusScan.pkg** pour démarrer le programme d'installation.
2. Suivez les instructions pour installer le logiciel.
3. Lisez et acceptez le contrat de licence. Si vous n'acceptez pas ses conditions, vous ne pourrez pas poursuivre l'installation.
4. Cliquez sur **Installer** pour effectuer l'installation. La boîte de dialogue **Authentification** apparaît.
5. Entrez votre nom d'utilisateur et votre mot de passe administrateur, puis cliquez sur **OK**. La fin de l'installation est signalée par un message. Cliquez sur **Fermer**.

Le programme d'installation de VirusScan for Mac place l'application VirusScan dans le dossier `Applications` et l'application VirusScan Schedule Editor dans le dossier `Applications/Utilitaires` de votre ordinateur.

Vous devez redémarrer votre ordinateur après avoir installé VirusScan for Mac 8.6 (contrairement aux versions précédentes).

Installation (silencieuse) par le biais de la ligne de commande

1. Recherchez le fichier **VirusScan.pkg** qui est situé sur le CD du produit ou dans le fichier ZIP d'installation téléchargé à partir du site Web McAfee et enregistrez-le dans un répertoire temporaire.
2. Ouvrez la fenêtre du **terminal** et placez-vous dans le répertoire où est situé le fichier **VirusScan.pkg**.
3. Dans la fenêtre du **terminal**, lancez la commande suivante :
   ```
   sudo installer -pkg VirusScan.pkg -target /
   ```
4. Entrez votre mot de passe système lorsqu'un message vous y invite.
5. La fin de l'installation est signalée par un message. Fermez la fenêtre du **terminal**.

Mise à niveau de l'installation

Vous pouvez mettre à niveau les anciennes versions de VirusScan (8.0 et 8.5) vers VirusScan for Mac v8.6. Après la mise à niveau, les préférences définies pour les versions précédentes sont migrées vers la version actuelle (v8.6).

Test de votre installation

Vous pouvez tester VirusScan à l'aide du fichier de test antivirus standard EICAR (European Institute of Computer Anti-Virus Research). Ce fichier est le résultat des efforts communs de fournisseurs d'antivirus du monde entier qui visent à mettre en place une norme permettant aux clients de vérifier leur logiciel antivirus.

Pour tester votre installation :

1 Accédez au site Web EICAR.ORG à la page `http://www.eicar.org` et téléchargez le fichier de test antivirus Eicar.zip.

2 Lancez une analyse à la demande du fichier ZIP téléchargé. VirusScan indique alors avoir détecté le fichier de test EICAR.

Ce fichier n'est *pas* un virus ; il est conçu pour tester les logiciels antivirus. Il est toutefois conseillé de le supprimer une fois le test du logiciel terminé afin de ne pas inquiéter les utilisateurs non avertis.

Si ce test est réussi, vous pouvez commencer à utiliser le logiciel VirusScan.

Désinstallation de VirusScan

Vous pouvez désinstaller VirusScan à l'aide d'un fichier de désinstallation (**VirusScan Uninstall.command**), situé sur le CD du produit ou dans le fichier .ZIP téléchargé à partir du site Web McAfee et enregistré dans un répertoire temporaire. Vous pouvez également utiliser le programme de désinstallation depuis le terminal.

Pour désinstaller VirusScan :

1 Effectuez l'une des procédures suivantes :

- Double-cliquez sur l'icône **VirusScan Uninstall.command**.°
- Faites glisser l'icône **VirusScan Uninstall.command** et déposez-la dans la fenêtre du **terminal**, puis cliquez sur **Entrée**.
- Dans la fenêtre du **terminal**, sélectionnez le répertoire `/usr/local/vscanx`, puis exécutez **VirusScan Uninstall.command**.

Pour ouvrir l'application **Terminal**, double-cliquez sur l'application située sous `/Applications/Utilities`.

La fenêtre du **terminal** s'ouvre et vous êtes invité à saisir votre mot de passe administrateur.

2 Tapez votre mot de passe administrateur et cliquez sur **Entrée**.

Le mot de passe administrateur ne s'affiche pas dans la fenêtre du **terminal**.

Lorsque le processus de désinstallation est correctement terminé, un message apparaît dans la fenêtre du **terminal** pour indiquer que le logiciel VirusScan a été supprimé de votre ordinateur.

3 Mise en route

Ce chapitre fournit une description de VirusScan et de la manière dont il protège votre ordinateur contre les virus. Il comprend les rubriques suivantes :

Utilisation de la console VirusScan

La console VirusScan vous permet d'utiliser et de configurer l'analyse à la demande et l'analyse à l'accès. Cette console vous permet de vous connecter à la bibliothèque McAfee d'informations sur les virus, d'exécuter des mises à jour via eUpdate, et d'imprimer et d'enregistrer les rapports d'analyse de virus.

La console VirusScan contient également un volet glisser-déplacer pour l'analyse à la demande. Vous pouvez lancer une analyse à la demande à tout moment en faisant glisser les fichiers dans le volet central de la console puis en les déposant dans le volet glisser-déplacer, puis en cliquant sur le bouton **Démarrer**. Si vous ajoutez un autre fichier à la fin de l'analyse, ce nouveau fichier remplace le premier élément analysé.

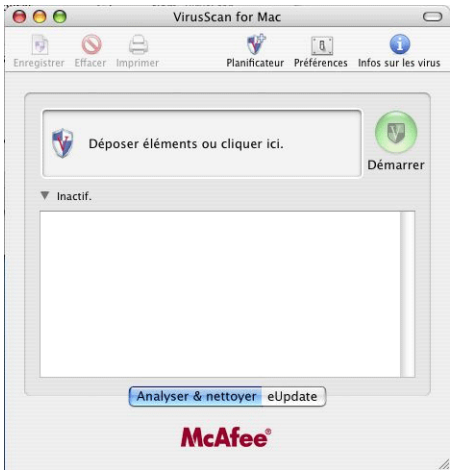
La console VirusScan

La console VirusScan affiche les composants Macintosh standard et antivirus spécialisés, notamment :

- une barre de titre affichant le nom du programme en cours d'exécution ;

- Les boutons de barre d'outils Fermer, Réduire, Agrandir et Masquer, qui permettent de redimensionner ou de masquer l'interface.

Figure 3-1 Console VirusScan



Barre d'outils

La barre d'outils comporte les boutons suivants :

Enregistre le rapport d'analyse virale au format .RTF (Rich Text File).

Supprime le contenu du rapport actuel affiché dans le panneau d'état.

Imprime le rapport actuel.

Permet de planifier une tâche d'analyse et eUpdate.

Ouvre la boîte de dialogue **Préférences** qui vous permet d'effectuer les opérations suivantes :

- définir des préférences pour l'analyseur à la demande ;
- définir des préférences pour l'analyseur à l'accès ;
- définir des préférences pour l'action à exécuter lorsqu'un virus est détecté ;
- consigner les résultats dans un fichier ;
- configurer les paramètres du serveur eUpdate ;
- configurer la liste des exclusions ;
- rechercher automatiquement les mises à jour de définitions de virus.

Ouvre le navigateur par défaut et vous fait accéder à la bibliothèque McAfee d'informations sur les virus.

Barre de menus

La barre de menus propose six menus déroulants standard communs à tous les écrans : **Fichier**, **Modifier**, **Présentation**, **Fenêtre** et **Aide**.

Configuration des analyseurs

La boîte de dialogue **Préférences** est disponible en deux versions, vous permettant de configurer respectivement les paramètres de l'analyseur à la demande et ceux de l'analyseur à l'accès. Les préférences générales sont identiques pour les deux analyseurs, tandis que les options avancées sont spécifiques à chaque type d'analyseur.

Les préférences de l'analyseur sont des paramètres globaux qui s'appliquent à tous les utilisateurs.

Les préférences sont enregistrées automatiquement lorsque vous les sélectionnez.

Vous devez disposer des privilèges d'administrateur pour pouvoir modifier les préférences.

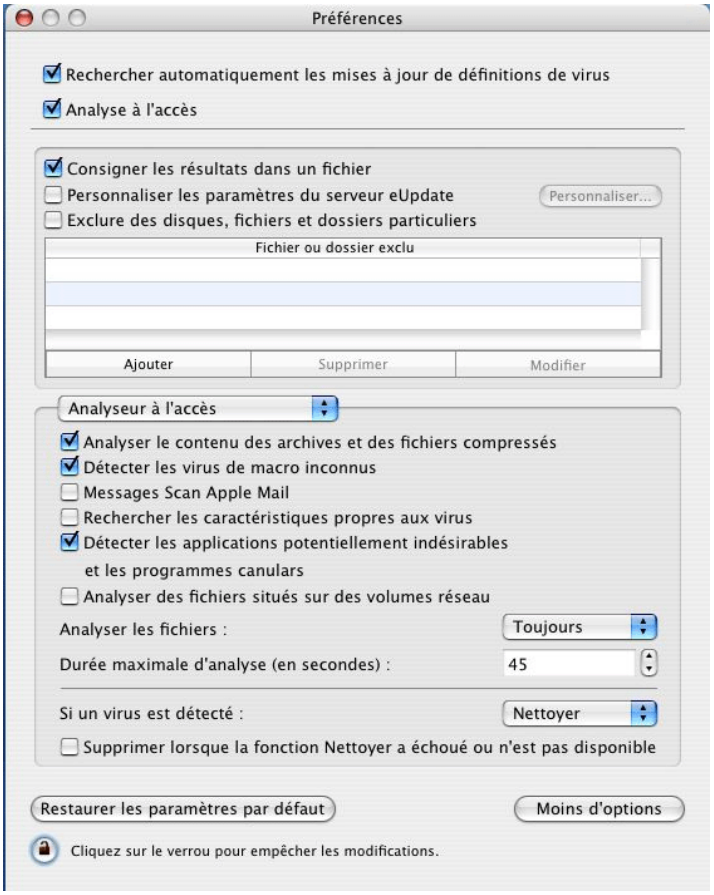
Configuration des préférences générales

Les préférences générales s'appliquent à la fois à l'analyseur à la demande et à l'analyseur à l'accès. Elles sont identiques pour les deux analyseurs.

Pour configurer les préférences générales :

1 Cliquez sur **Préférences**  dans la barre d'outils pour afficher la boîte de dialogue **Préférences**. Le volet supérieur de cette boîte de dialogue contient des options de préférences qui s'appliquent à la fois à l'analyseur à la demande et à l'analyseur à l'accès.

Figure 3-2 Préférences générales



2 Sélectionnez vos préférences générales d'analyse pour les analyseurs à la demande et à l'accès, le Tableau 3-1 indique les préférences générales disponibles.

Tableau 3-1 Préférences générales pour les analyseurs à la demande et à l'accès

Rechercher automatiquement les mises à jour de définitions de virus	Active/désactive la recherche automatique de mises à jour via eUpdate.
Analyse à l'accès	Active/désactive l'analyse à l'accès.
Consigner les résultats dans un fichier	Active/désactive la consignation des résultats dans un fichier.

Tableau 3-1 Préférences générales pour les analyseurs à la demande et à l'accès

Personnaliser les paramètres serveur d'eUpdate	Gère votre serveur de mise à jour avec un nom d'utilisateur et un mot de passe. Cliquez sur **Personnaliser** pour modifier les paramètres FTP pour eUpdate.
Exclure des disques, des fichiers et des dossiers en particulier	Configure les éléments à exclure de l'analyse. Si cette option n'est pas sélectionnée, vous n'obtiendrez pas de liste des exclusions. **Pour ajouter une exclusion :** ■ Cliquez sur **Ajouter** dans la liste **Fichier ou dossier exclu**. Sélectionnez le fichier ou le dossier à partir de la boîte de dialogue **Ouvrir**. **Pour supprimer une exclusion :** ■ Sélectionnez le fichier ou le dossier à partir de la liste **Fichier ou dossier exclu**. Cliquez sur **Supprimer**. **Pour modifier une exclusion :** ■ Sélectionnez le fichier ou le dossier à partir de la liste **Fichier ou dossier exclu**. Cliquez sur **Modifier**. La boîte de dialogue **Ouvrir** s'affiche. Sélectionnez le fichier ou le dossier destiné à remplacer l'exclusion existante.

3 Définissez les préférences avancées selon vos besoins. Celles-ci sont affichées dans le volet inférieur de la boîte de dialogue **Préférences**. Deux ensembles de préférences sont disponibles : l'un pour l'analyseur à la demande et l'autre pour l'analyseur à l'accès. Pour plus d'informations, reportez-vous aux sections *Configuration de l'analyseur à la demande , page 21* et *Configuration de l'analyseur à l'accès , page 23*.

4 Cliquez sur le **Verrou** pour empêcher toute modification des préférences.

5 Cliquez sur **Fermer** dans le coin supérieur gauche pour quitter la boîte de dialogue **Préférences**.

Configuration de l'analyseur à la demande

L'analyseur à la demande vous permet de lancer une analyse à tout moment. Vous configurez les préférences avancées de l'analyseur à la demande à l'aide des options disponibles dans le volet inférieur de la boîte de dialogue Préférences.

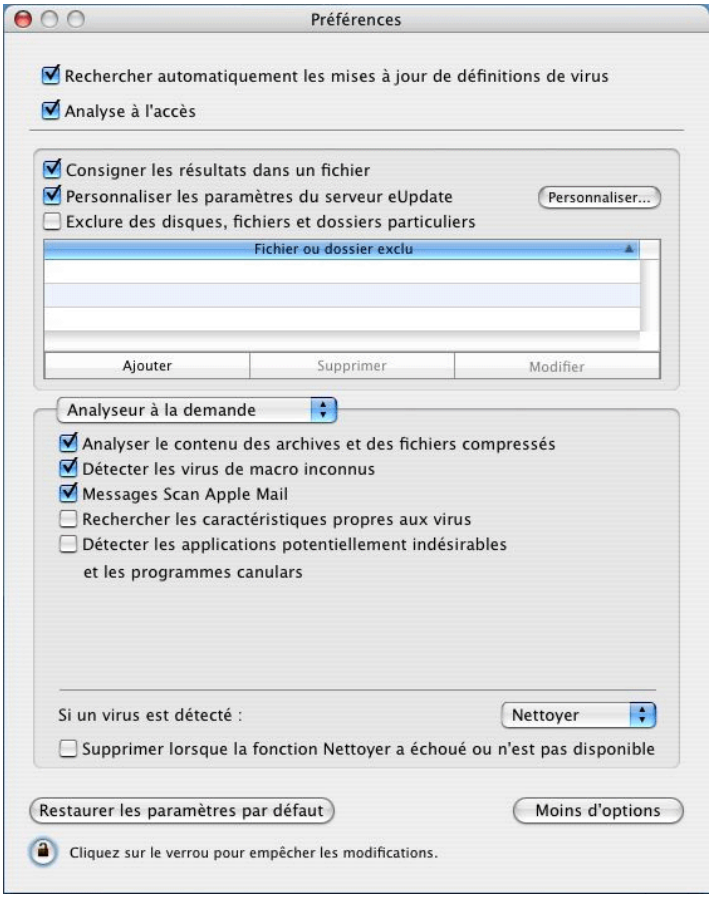
Pour configurer l'analyseur à la demande :

1 Cliquez sur **Préférences** dans la barre d'outils pour afficher la boîte de dialogue **Préférences**.

2 Cliquez sur **Plus d'options** dans l'angle inférieur droit de la boîte de dialogue pour afficher les préférences avancées.

3 Sélectionnez **Analyseur à la demande** dans le menu déroulant (si cette option n'est pas déjà sélectionnée) pour afficher la version Analyse à la demande de cette boîte de dialogue.

Figure 3-3 Préférences de l'analyse à la demande



4 Sélectionnez vos préférences d'analyse avancées pour l'analyseur à la demande. Le Tableau 3-2 indique les préférences disponibles.

Tableau 3-2 Préférences avancées pour l'analyseur à la demande

Analyser le contenu des archives et des fichiers compressés	Définit l'analyseur sélectionné pour analyser des archives et d'autres fichiers compressés. Cette option est activée par défaut pour l'analyseur à la demande.
Détecter les virus de macro inconnus	Si un fichier contient une macro potentiellement infectée (infection inconnue), il sera analysé et nettoyé (ou supprimé) lors du nettoyage.
Analyser les messages Apple Mail	Active/désactive la recherche par l'analyseur à la demande de fichier infecté dans les messages Apple Mail.

Tableau 3-2 Préférences avancées pour l'analyseur à la demande

Rechercher des caractéristiques de virus dans les fichiers	Active/désactive la recherche par l'analyseur à la demande des fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications indésirables et les programmes canulars	Active/désactive la recherche par l'analyseur à la demande des programmes indésirables et des programmes canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action principale de l'analyseur à la demande.
Supprimer lorsque la fonction Nettoyer a échoué ou n'est pas disponible	Sélectionne l'action secondaire de l'analyseur à la demande. Cette option est disponible uniquement lorsque l'action principale est **Nettoyer**.

5 Cliquez sur le **Verrou** pour empêcher toute modification des préférences.

6 Cliquez sur **Fermer** dans le coin supérieur gauche pour quitter la boîte de dialogue **Préférences**.

Configuration de l'analyseur à l'accès

L'analyseur à l'accès surveille en continu tous les fichiers en cours d'utilisation pour détecter la présence éventuelle d'un virus ou de tout autre code malveillant. Une analyse à l'accès est effectuée chaque fois qu'un fichier est lu à partir du disque, écrit sur le disque, ou dans les deux cas, selon les préférences que vous avez définies pour cet analyseur.

Vous configurez les préférences avancées de l'analyseur à l'accès à l'aide des options disponibles dans le volet inférieur de la boîte de dialogue Préférences.

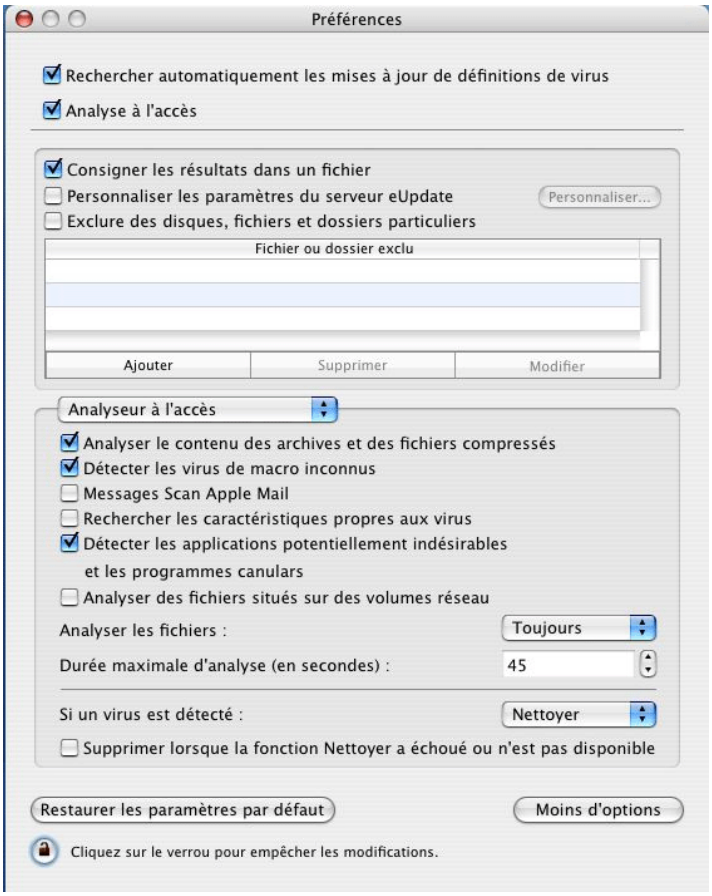
Pour configurer l'analyseur à l'accès :

1 Cliquez sur **Préférences** dans la barre d'outils pour afficher la boîte de dialogue **Préférences**.

2 Cliquez sur **Plus d'options** dans l'angle inférieur droit de la boîte de dialogue pour afficher les préférences avancées.

3 Sélectionnez **Analyseur à l'accès** dans le menu déroulant (si cette option n'est pas déjà sélectionnée) pour afficher la version Analyse à l'accès de cette boîte de dialogue.

Figure 3-4 Préférences de l'analyse lors l'accès



4 Sélectionnez vos préférences pour l'analyseur à l'accès. Le Tableau 3-3 indique les préférences disponibles.

Tableau 3-3 Préférences avancées pour l'analyse à l'accès

Analyser le contenu des archives et des fichiers compressés	Définit l'analyseur sélectionné pour analyser des archives et d'autres fichiers compressés. Cette option est activée par défaut pour l'analyseur à l'accès. Notez que l'analyseur à l'accès n'analyse pas le contenu des archives Stuffit.
Détecter les virus de macro inconnus	Si un fichier contient une macro potentiellement infectée (infection inconnue), il sera analysé et nettoyé (ou supprimé) lors du nettoyage.
Analyser les messages Apple Mail	Active/désactive la recherche par l'analyseur à l'accès de fichier infecté dans les messages Apple Mail.

Tableau 3-3 Préférences avancées pour l'analyse à l'accès

Rechercher des caractéristiques de virus dans les fichiers	Active/désactive la recherche par l'analyseur à l'accès des fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications indésirables et les programmes canulars	Active/désactive la recherche par l'analyseur à l'accès des programmes indésirables et des programmes canulars.
Analyser des fichiers situés sur des volumes réseau	Configure l'analyseur pour analyser les fichiers qui ont fait l'objet d'un accès à partir de volumes réseau.
Analyser les fichiers : ■ Toujours ■ Lors de la lecture ■ Lors de l'écriture	Détermine si l'analyseur à l'accès doit analyser les fichiers lus à partir du disque ou écrits sur le disque, ou les deux.
Durée maximale d'analyse (en secondes)	Durée maximale en secondes d'une analyse, par fichier. (Un fichier compressé n'est pas traité comme un fichier unique ; ce délai maximal s'applique au dernier fichier particulier et non au dernier fichier conteneur de niveau supérieur.)
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action principale de l'analyseur à l'accès.
Supprimer lorsque la fonction Nettoyer a échoué ou n'est pas disponible	Sélectionne l'action secondaire pour l'analyseur sélectionné. Cette option est disponible uniquement lorsque l'action principale est **Nettoyer**.

5 Cliquez sur le **Verrou** pour empêcher toute modification des préférences.

6 Cliquez sur **Fermer** dans le coin supérieur gauche pour quitter la boîte de dialogue **Préférences**.

Utilisation de l'analyseur à la demande

L'analyseur à la demande vous permet de lancer une analyse à tout moment en utilisant l'une des procédures suivantes :

- En déposant par glisser-déplacer les fichiers sur l'icône de **VirusScan** dans le Dock, sur l'icône **VirusScan** dans le Finder ou dans le volet glisser-déplacer de la console.
- Par le biais de la boîte de dialogue **Sélectionner un fichier ou dossier à analyser et à nettoyer**.

Vous pouvez sélectionner plusieurs fichiers ou répertoires. Les résultats sont récapitulés dans la fenêtre des rapports.

Pour exécuter une analyse à la demande :

1 Ouvrez la console VirusScan.

2 Déposez par glisser-déplacer le fichier, le dossier ou le volume à analyser dans le volet de glisser-déplacer de la console principale. Pour sélectionner un groupe de fichiers, effectuez l'une des opérations suivantes :

- Maintenez la touche **Maj** enfoncée et sélectionnez les différents fichiers de votre choix.
- Cliquez sur le volet de glisser-déplacer. Un écran de sélection des fichiers apparaît. Sélectionnez le fichier, le groupe de fichiers, le répertoire ou le volume à analyser, puis cliquez sur **Sélectionner un emplacement**.
- Faites glisser le fichier, le dossier ou le volume vers l'icône de **VirusScan** dans le Dock dans la vue du **Finder**.

3 Cliquez sur **Démarrer** dans la console pour lancer l'analyse.

La **ligne d'état** indique le nom du fichier actuellement analysé, ainsi que l'état de l'analyse. La **flèche** située en regard de la ligne d'état permet de masquer ou d'afficher la fenêtre **des rapports** . La fenêtre **des rapports** est masquée par défaut.

Un rapport d'analyse apparaît dans la fenêtre **des rapports**. Le rapport indique l'heure de l'analyse, le nombre total de fichiers analysés et les actions exécutées. La console affiche l'état de l'analyse sur une ligne située entre le volet de glisser-déplacer et le panneau des rapports. Le panneau d'état indique **Inactif** lorsqu'aucune analyse n'est en cours.

Utilisation de l'analyseur à l'accès

L'analyseur à l'accès applique la stratégie de surveillance automatique en continu pour plusieurs fichiers, répertoires ou volumes, notamment les volumes résidant sur des ordinateurs distants connectés au réseau. Il suffit pour cela d'activer l'analyseur à l'accès.

Pour activer l'analyse à l'accès :

1 Ouvrez la console VirusScan.

2 Cliquez sur **Préférences**  dans la barre d'outils pour afficher la boîte de dialogue **Préférences**.

3 Sélectionnez la case à cocher **Analyse à l'accès** pour activer l'analyse à l'accès.

L'analyseur affiche un message dans la fenêtre **Reporter** lorsqu'il détecte un virus ou tout autre code malveillant.

Mise à jour des fichiers DAT

Par défaut, eUpdate se connecte automatiquement chaque jour au serveur d'eUpdate par l'intermédiaire de votre connexion Internet afin de rechercher de nouveaux fichiers DAT. Les mises à jour peuvent traverser les serveurs proxy. Vous pouvez planifier des mises à jour via eUpdate par l'intermédiaire de **VirusScan Schedule Editor**.

Les analyses à la demande et les mises à jour eUpdate automatiques et planifiées peuvent être exécutées simultanément.

Utilité des mises à jour

Pour garantir la protection de votre système contre les toutes dernières menaces, vous devez maintenir votre logiciel antivirus à jour en mettant régulièrement à jour les fichiers DAT et le moteur.

- De nouveaux virus et vers font fréquemment leur apparition. McAfee propose régulièrement des fichiers DAT mis à jour qui garantissent que VirusScan est en mesure de détecter ces virus et vers.
- Des mises à niveau du moteur d'analyse de virus sont disponibles occasionnellement. Elles permettent à VirusScan d'utiliser les techniques de détection de virus les plus récentes.

Fonctionnement d'eUpdate

eUpdate vous permet d'obtenir et d'appliquer de nouveaux fichiers DAT ou des mises à niveau du logiciel antivirus lorsque vous êtes connecté à Internet. Lorsqu'il existe une mise à jour, VirusScan tente automatiquement de la télécharger et de l'installer. Si l'opération n'a pas été réalisée au bout d'un jour, VirusScan télécharge automatiquement la mise à jour. Votre système est donc toujours mis à jour.

Configuration des paramètres eUpdate

Les fichiers DAT peuvent être mis à jour à partir d'un serveur FTP. McAfee fournit un serveur FTP pour la mise à jour de vos fichiers DAT via eUpdate.

Serveur FTP McAfee

Par défaut, VirusScan est configuré pour accéder au serveur FTP McAfee pour télécharger les derniers fichiers DAT. Une fois installé, VirusScan se connecte automatiquement au serveur FTP pour télécharger et mettre à jour vos fichiers DAT lorsque vous êtes connecté à Internet.

Configuration du serveur FTP interne

Pour utiliser un référentiel FTP eUpdate pour les ordinateurs Macintosh de votre réseau, vous devez configurer un serveur FTP eUpdate. Dans ce cas, vous devez télécharger quotidiennement les fichiers DAT à partir du serveur FTP McAfee (`ftp://ftp.mcafee.com/commonupdater`) sur le serveur FTP interne que vous avez configuré.

Pour configurer le serveur FTP interne :

1. Téléchargez le fichier DAT à partir de `ftp://ftp.mcafee.com/commonupdater`.
2. Copiez le fichier DAT dans un dossier sur le serveur FTP eUpdate.

Pour accéder au serveur FTP à partir des Préférences :

1 Ouvrez la console VirusScan pour modifier les paramètres dans la boîte de dialogue **Paramètres serveur eUpdate**.

2 Cliquez sur **Préférences** dans la barre d'outils. La boîte de dialogue **Préférences** apparaît. Sélectionnez l'option **Personnaliser les paramètres serveur d'eUpdate**.

3 Cliquez sur le bouton **Personnaliser**. La boîte de dialogue **Paramètres serveur d'eUpdate** s'affiche.

4 Tapez l'URL du serveur FTP interne dans la zone **URL du serveur**.

5 Tapez l'emplacement dans lequel vous avez téléchargé le fichier DAT dans la zone **Catalogue**.

6 Cliquez sur **OK**.

Exemple :

1 Créez un répertoire nommé "commonupdater" sous le répertoire supérieur de votre serveur ftp.

2 Ouvrez `ftp://ftp.mcafee.com/commonupdater`.

3 Téléchargez les fichiers suivants de `ftp://ftp.mcafee.com/commonupdater/` vers `<votre serveurftp>/commonupdater/` :

- oem.ini
- Tous les fichiers .gem
- gdeltaavv.ini

4 Téléchargez `ftp://ftp.mcafee.com/commonupdater/current/VSCANDAT1000/DAT/0000/avvdat-xxxx.zip` vers `<votre serveurftp>/commonupdater/current/VSCANDAT1000/DAT/0000/`.

5 Les définitions de virus sont mises à jour quotidiennement. Vous devez donc répéter les étapes 1 à 4 quotidiennement si vous souhaitez conserver votre référentiel de mises à jour local à jour.

Réalisation d'une mise à jour via eUpdate par l'intermédiaire du serveur proxy

Les réglages proxy WebProxy (HTTP) sont pris en charge. Pour plus d'informations sur la configuration de ces réglages proxy sur le système d'exploitation Mac OS X, reportez-vous à la documentation Apple.

Vous devez également vous assurer que l'accès anonyme est activé sur le serveur FTP pour garantir l'exécution correcte des mises à jour via eUpdate.

VirusScan ne prend pas en charge l'authentification de serveur proxy.

Utilisation de VirusScan Schedule Editor

VirusScan Schedule Editor vous permet de créer des analyses se répétant sur une période donnée pour un groupe de fichiers ou de dossiers. Vous pouvez planifier des analyses quotidiennes, hebdomadaires et mensuelles.

Pour planifier une analyse :

1 Cliquez sur **Planificateur** dans la console VirusScan. Vous pouvez également sélectionner **Tâches planifiées** sous **Présentation** dans le menu principal. La boîte de dialogue **VirusScan Schedule Editor** s'affiche.

2 Cliquez sur **Nouvelle tâche d'analyse** . La boîte de dialogue **Sans titre** s'affiche.

Figure 3-5 Boîte de dialogue Nouvelle analyse

3 Attribuez un nom à la tâche. Utilisez un nom décrivant l'analyse planifiée.

4 Cliquez sur **Définir** pour spécifier la **Date et heure** de l'analyse planifiée.

5 Choisissez les éléments à analyser. Pour ce faire, vous pouvez utiliser l'une des méthodes suivantes :

- Déposer par glisser-déplacer les éléments dans le volet **Analyser les éléments**.
- Cliquer sur le volet **Analyser les éléments** . La boîte de dialogue **Sélectionner un élément** apparaît. Cliquez sur **Sélectionner** lorsque vous avez sélectionné les fichiers à analyser.

6 Sélectionnez **Récurrence**. Sélectionnez parmi les options suivantes :

- **Tous les jours** : saisissez la séquence de jours d'exécution de l'analyse.
- **Toutes les semaines** : sélectionnez le ou les jours de la semaine choisis pour l'exécution de l'analyse.
- **Tous les mois** : sélectionnez le ou les jours du mois choisis pour l'exécution de l'analyse, ainsi que la plage de périodicité des mois.
- **Jamais** : sélectionnez cette option si vous ne souhaitez pas recommencer l'analyse.

7 Indiquez la date de fin de la planification, puis cliquez sur **OK**.

Votre nouvelle tâche d'analyse apparaît dans une liste répertoriant toutes les analyses et les mises à jour eUpdate planifiées dans VirusScan Schedule Editor. Pour activer ou désactiver des tâches planifiées, cochez la case en regard de l'élément correspondant.

Si l'ordinateur est éteint au moment d'une tâche planifiée, VirusScan n'exécutera pas cette tâche une fois l'ordinateur démarré.

Planification des mises à jour via eUpdate

VirusScan Schedule Editor vous permet de planifier des mises à jour se répétant sur une période donnée pour les fichiers DAT présents sur vos ordinateurs et pour le moteur d'analyse de virus. Cette prise en charge est fournie par l'intermédiaire de FTP.

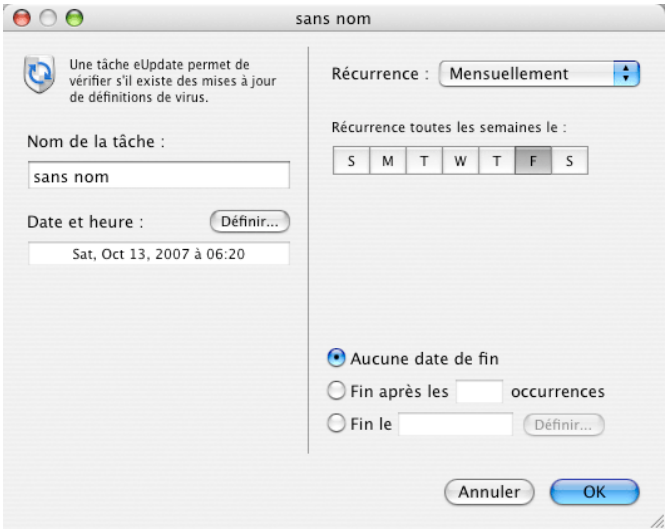
eUpdate est programmé pour rechercher automatiquement toute nouvelle mise à jour. Toutefois, vous pouvez planifier des recherches supplémentaires via eUpdate ou modifier la planification existante.

Pour planifier une mise à jour via eUpdate :

1 Dans le menu **Présentation** , sélectionnez **Tâches planifiées**. La boîte de dialogue **VirusScan Schedule Editor** s'affiche.

2 Cliquez sur **Nouvelle tâche eUpdate**. La fenêtre **Sans titre** s'affiche.

Figure 3-6 Boîte de dialogue Nouvelle eUpdate



3 Entrez un nom pour la tâche. Il est conseillé d'utiliser un nom décrivant la tâche planifiée.

4 Cliquez sur **Définir** pour spécifier la **Date et heure** de la mise à jour planifiée.

5 Sélectionnez **Récurrence**. Sélectionnez parmi les options suivantes :

- **Tous les jours** : saisissez la série de jours auxquels le composant eUpdate doit se connecter.
- **Toutes les semaines** : sélectionnez le(s) jour(s) de la semaine choisis pour l'exécution du composant eUpdate.
- **Tous les mois** : sélectionnez le ou les jours du mois choisis pour la mise à jour automatique, ainsi que la séquence de mois.
- **Jamais** : sélectionnez cette option si vous ne souhaitez pas que la mise à jour automatique s'exécute à nouveau.

6 Sélectionnez une date de fin et cliquez sur **OK**.

Votre nouvelle tâche eUpdate apparaît dans une liste répertoriant toutes les analyses et mises à jour eUpdate planifiées dans VirusScan Schedule Editor. Pour activer ou désactiver des tâches eUpdate, sélectionnez la case à cocher en regard de la tâche appropriée. eUpdate démarre automatiquement lorsqu'une mise à jour est disponible.

Pour lancer une mise à jour eUpdate non planifiée :

1 Ouvrez la console VirusScan.

2 Cliquez sur l'onglet **eUpdate** pour afficher le volet eUpdate.

3 Cliquez sur **Démarrer** pour vérifier s'il y a de nouvelles définitions de virus à télécharger.

4 Intégration à ePolicy Orchestrator 3.6

Introduction

Cette section explique comment configurer VirusScan for Mac avec les versions 3.6 et 3.6.1 du logiciel de gestion McAfee ePolicy Orchestrator . Pour utiliser efficacement ce guide, vous devez déjà être familiarisé avec le logiciel ePolicy Orchestrator. Pour plus d'informations, consultez les *Guides produit d'ePolicy Orchestrator*. Le logiciel ePolicy Orchestrator fournit un point de contrôle unique pour tous vos produits antivirus McAfee, vous permettant de gérer toutes les stratégies antivirus et d'afficher les rapports sur les événements antivirus et l'activité des virus dans un environnement d'entreprise. Avec ePolicy Orchestrator, vous pouvez configurer VirusScan for Mac sur les ordinateurs cibles de votre réseau ; vous n'avez pas besoin de les configurer individuellement.

Cette section contient les informations suivantes :

- Ajout d'une configuration d'agent ePolicy Orchestrator au serveur ePolicy Orchestrator
- Définition des stratégies antivirus sur les systèmes cibles, en vue de configurer les fonctions suivantes de VirusScan for Mac :
  - Stratégies générales de contrôle des fonctions globales de VirusScan for Mac
  - Stratégies du serveur eUpdate
  - Stratégies de l'analyseur à la demande
  - Stratégies de l'analyseur à l'accès
- Configuration des fonctions de l'agent ePolicy Orchestrator pour les ordinateurs Macintosh :
  - Intervalles de communication de l'agent
  - Intervalles d'application des stratégies
  - Transmission des événements
  - Consignation.

Ce guide ne fournit pas d'informations détaillées sur l'installation et l'utilisation du logiciel ePolicy Orchestrator. Reportez-vous aux *Guides produit d'ePolicy Orchestrator*.

Conditions préalables pour gérer VirusScan for Mac avec ePolicy Orchestrator

Avant d'utiliser le logiciel ePolicy Orchestrator pour gérer VirusScan for Mac :

- Enregistrez les fichiers Network Associate Package (.NAP) appropriés pour VirusScan for Mac dans le référentiel du logiciel ePolicy Orchestrator.
- Enregistrez le fichier de l'agent non-Windows (NWA) dans le référentiel d'ePolicy Orchestrator.

> L'agent non-Windows (NWA, Non Windows Agent) est également connu sous le nom d'Agent ePolicy Orchestrator sous Mac OS X.

- Installez l'agent ePolicy Orchestrator sur votre ordinateur Macintosh.

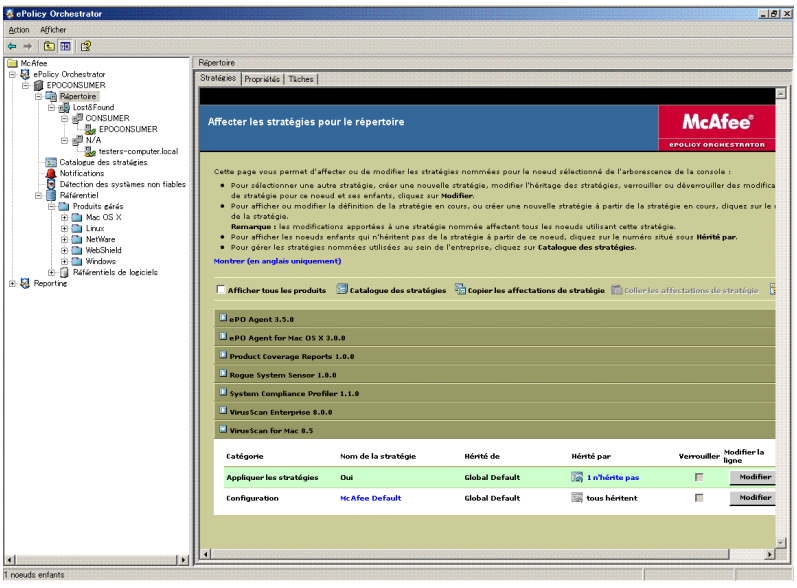
Présentation de la console ePolicy Orchestrator

La console de gestion Microsoft (MMC) est l'interface utilisée pour exploiter ePolicy Orchestrator et ses différentes fonctions. Elle permet d'enregistrer et de configurer le produit antivirus VirusScan for Mac géré via ePolicy Orchestrator. La console utilise les fonctionnalités standard de la console MMC.

Cette console se compose de deux parties ou volets :

- L'arborescence de la console constitue son volet de navigation. Elle affiche les serveurs, les postes de travail et les périphériques que vous pouvez administrer avec ePolicy Orchestrator.
- Le volet de détails occupe la partie droite de la console. Selon l'élément de l'arborescence de la console sélectionné, le volet de détails peut être divisé en volets supérieur et inférieur.

Figure 4-1 Console ePolicy Orchestrator



Lorsque vous vous connectez pour la première fois au serveur, la console s'affiche et sa **racine** apparaît en surbrillance dans le volet gauche.

L'apparence de la console change en fonction des éléments sélectionnés dans l'arborescence de la console ou le volet des détails.

Pour obtenir des informations détaillées sur l'utilisation d'ePolicy Orchestrator, reportez-vous aux *Guides produit d'ePolicy Orchestrator*.

Installation

Introduction

L'agent non-Windows est un composant distribué d'ePolicy Orchestrator à installer sur chaque ordinateur Macintosh du réseau. Il collecte et envoie des informations entre le serveur ePolicy Orchestrator et les référentiels, et gère les installations VirusScan sur tout le réseau. La configuration de l'agent et de ses paramètres de stratégie détermine la façon dont il simplifie la communication et les mises à jour au sein de votre environnement.

Configuration système requise

L'agent peut être installé sur un système d'exploitation Apple Macintosh OS X, version 10.4.6 (ou ultérieure), sur n'importe laquelle des plates-formes Macintosh suivantes :

- G3
- G4
- G5
- SMP (biprocesseur)
- Ordinateur Macintosh Intel

Enregistrement des fichiers .NAP pour la gestion de VirusScan

Pour gérer VirusScan à l'aide d'ePolicy Orchestrator, vous devez commencer par ajouter les fichiers .NAP du produit au référentiel du logiciel sur le serveur ePolicy Orchestrator. Les fichiers .NAP contiennent les pages de stratégie VirusScan, grâce auxquelles vous pouvez contrôler les paramètres du produit déployés via l'agent ePolicy Orchestrator sur les ordinateurs clients.

McAfee distribue des fichiers .NAP pour tous les antivirus et produits de sécurité pris en charge par ePolicy Orchestrator. Le fichier .NAP d'un produit donné se situe, à l'instar des autres fichiers d'installation, sur le CD du produit ou dans le fichier ZIP du produit, téléchargé depuis le site Web de McAfee. Les fichiers .NAP correspondant à VirusScan sont disponibles dans le sous-dossier **ePolicy Orchestrator Server Components** du CD du produit ou du fichier ZIP téléchargé. Le fichier .NAP possède toujours l'extension .NAP. Son nom correspond au code du nom du produit suivi du numéro de version, par exemple NWA-MAC300.NAP.

Les pages de stratégie ne sont pas ajoutées au référentiel maître, mais stockées sur le serveur ePolicy Orchestrator. Par conséquent, les fichiers NAP ne sont ni répliqués sur les référentiels distribués, ni mis à jour sur les ordinateurs Macintosh.

Ajout du fichier .NAP de l'agent Macintosh non-Windows (NWA-MAC300.NAP)

Pour enregistrer le fichier .NAP d'un agent Macintosh non-Windows sur le serveur ePolicy Orchestrator :

1. Localisez le fichier **NWA-MAC300.NAP** sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
2. Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
3. Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit sur **Référentiel** et sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.

Vous avez également la possibilité d'ouvrir l'Assistant en double-cliquant sur **Référentiel** dans l'arborescence de la console ePolicy Orchestrator, puis en cliquant sur **Archiver NAP** dans le volet de détails.

4. Sélectionnez **Ajouter de nouveaux logiciels à gérer** et cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, recherchez et sélectionnez le fichier **NWA-MAC300.NAP** que vous avez enregistré dans un dossier temporaire à l' Étape 1, page 36.
6. Cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP sélectionné.

Ajout du fichier .NAP de VirusScan for Mac (Virex.nap)

Pour ajouter le fichier Virex.nap au serveur ePolicy Orchestrator :

1. Localisez le fichier **Virex.nap** sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
2. Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
3. Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit de la souris sur le **Référentiel** puis sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.
4. Sélectionnez **Ajouter de nouveaux logiciels à gérer** et cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, recherchez et sélectionnez le fichier **Virex.nap** que vous avez enregistré dans un dossier temporaire à l' Étape 1, page 36.
6. Cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP sélectionné.

Ajout du fichier .NAP de rapports de VirusScan for Mac (virexExt.nap)

Pour ajouter le fichier virexExt.nap au serveur ePolicy Orchestrator :

1. Localisez le fichier **virexExt.nap** sur le CD du produit ou dans le fichier ZIP téléchargé depuis le site Web de McAfee, puis enregistrez-le dans un dossier temporaire accessible à partir du serveur ePolicy Orchestrator.
2. Connectez-vous au serveur ePolicy Orchestrator avec des droits d'administrateur.
3. Dans l'arborescence de la console ePolicy Orchestrator, cliquez avec le bouton droit sur **Référentiel** et sélectionnez **Configurer le référentiel**. L'Assistant **Configuration du Référentiel de logiciels** s'affiche.
4. Sélectionnez **Ajouter de nouveaux rapports** et cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Sélectionner un ensemble de logiciels**, recherchez et sélectionnez le fichier **virexExt.nap** que vous avez enregistré dans un dossier temporaire à l' Étape 1 de la section *Ajout du fichier .NAP de rapports de VirusScan for Mac (virexExt.nap)*, puis cliquez sur **Ouvrir** pour permettre à ePolicy Orchestrator de charger le fichier .NAP de rapports dans le référentiel.

Lorsque ePolicy Orchestrator a terminé de charger les fichiers .NAP, l'agent s'affiche dans la liste des stratégies dans le volet de détails.

Installation de l'agent ePolicy Orchestrator pour Macintosh

Vous pouvez installer l'agent ePolicy Orchestrator pour Macintosh via une installation standard (interface graphique) ou une ligne de commande (installation silencieuse). L'agent est installé dans le répertoire `/Library/NETAepoagt` et utilise le répertoire `/Library/NETASSOC` pour toutes les informations relatives à la configuration.

Il est impossible de modifier le répertoire d'installation de l'agent ePolicy Orchestrator.

Installation standard

1. Recherchez le fichier **nwa.dmg** qui figure sur le CD du produit ou dans le fichier ZIP d'installation téléchargé depuis le site Web McAfee, et enregistrez-le dans un dossier temporaire.

   Le fichier **nwa.dmg** se trouve dans le dossier **ePO Agent** du fichier **ePO Components.ZIP** sur le CD du produit.

2. Double-cliquez sur le fichier **nwa.dmg**. Les fichiers suivants s'affichent.
   - NWA.pkg
   - cmdinstall

3 Double-cliquez sur le fichier **NWA.pkg**. La fenêtre **Bienvenue dans le programme d'installation du logiciel ePO Agent for Mac OS X** apparaît.

4 Cliquez sur **Continuer**. La fenêtre **ReadMe** apparaît. Elle décrit les fonctions de l'agent, et répertorie tous les comportements et problèmes connus avec la présente version du produit.

5 Cliquez sur **Continuer**. La fenêtre **Accord de licence du logiciel** apparaît.

Lisez et acceptez le contrat de licence. Si vous n'acceptez pas ses conditions, vous ne pourrez pas poursuivre l'installation.

6 Cliquez sur **Continuer**. La fenêtre **Sélectionner le répertoire de destination** apparaît. Sélectionnez le répertoire dans lequel vous souhaitez installer l'agent ePolicy Orchestrator, puis cliquez sur **Continuer**.

7 La fenêtre **Installation simple** apparaît.

Cette fenêtre présente des options différentes, selon que vous installez/réinstallez l'agent ou que vous le mettez à niveau. Si vous installez l'agent pour la première fois ou si vous le réinstallez après avoir désinstallé l'installation précédente de l'agent ePolicy Orchestrator, cette fenêtre contient un bouton **Installer**. Si vous mettez à niveau une version précédente de l'agent ePolicy Orchestrator, cette fenêtre contient un bouton **Mettre à niveau**.

8 Cliquez sur **Installer/Mettre à niveau** pour continuer.

9 Vous êtes invité à entrer vos informations d'identification. Tapez votre mot de passe et cliquez sur **OK**. La fenêtre **Installation du logiciel** apparaît.

Au cours de ce processus, le programme d'installation vous demande d'authentifier le **configurateur de l'agent ePO**. Tapez votre mot de passe et cliquez sur **OK**. La boîte de dialogue **Configurateur de l'agent ePO** apparaît.

10 Indiquez l'**adresse IP du serveur ePO** et le numéro du **port du serveur ePO**. Cliquez sur **Appliquer**. La fenêtre **Installation du logiciel** s'affiche.

11 Cliquez sur **Redémarrer** pour terminer le processus d'installation.

Installation silencieuse (ligne de commande)

1 Recherchez le fichier **nwa.dmg** qui figure sur le CD du produit ou dans le fichier ZIP d'installation téléchargé depuis le site Web McAfee, et enregistrez-le dans un dossier temporaire.

Le fichier **nwa.dmg** se trouve dans le dossier **ePO Agent** du fichier **ePO Components.ZIP** sur le CD du produit.

2 Double-cliquez sur le fichier **nwa.dmg.** Les fichiers suivants s'affichent.

- NWA.pkg
- cmdinstall

3 Ouvrez la fenêtre du **terminal** et sélectionnez le répertoire de travail `/Volumes/NAINWA`.

Vous devez posséder des droits administrateur pour exécuter cette commande.

4 Dans la fenêtre du **terminal**, exécutez la commande suivante :
`sudo ./cmdinstall <Adresse IP du serveur ePO>:<Port du serveur ePO>`

5 Lorsque l'installation silencieuse est terminée, la fenêtre du **terminal** affiche les informations suivantes :

Figure 4-2 Fenêtre du terminal - Installation/Mise à niveau terminée

```
installer[661]:                        It took 3.385372 seconds to run preupgrade script for ePO Agent for Mac OS X
installer[661]:                        It took 0.445282 seconds to Write files
installer[661]:                        It took 3.174604 seconds to run postupgrade script for ePO Agent for Mac OS X
installer[661]:                        It took 0.098582 seconds to Assembling receipt
installer[661]:
installer[661]: Summary Information
installer[661]: Type           Elapsed time (sec)
installer[661]:          patch           0.000117
installer[661]:           zero           0.010520
installer[661]:         script           6.559976
installer[661]:        extract           0.445282
installer[661]:         config           0.065356
installer[661]:        receipt           0.433727
installer[661]:           disk           1.006918
installer[661]:        install           7.509475
installer[661]:
installer[661]: Starting installation:
installer[661]: Finalizing installation.
#
installer:     Finishing Installation
installer[661]: Registering applications
installer[661]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
#
installer:
#
installer: The software was successfully installed.....
installer: The upgrade was successful.
installer: The install recommends restarting now.
Cleaning /tmp/NAINWA.mpnlThby
iMac-Mactel-2:/Volumes/NAINWA shreyas$
```

Vous avez correctement installé/mis à niveau votre agent ePolicy Orchestrator pour Mac OS X.

Installation de VirusScan for Mac

Reportez-vous à la section *Installation de VirusScan for Mac* , page 13 pour plus d'informations sur l'installation du logiciel sur les ordinateurs Macintosh.

Désinstallation

Suppression de VirusScan for Mac du serveur ePolicy Orchestrator

Vous pouvez désinstaller les fichiers .NAP de VirusScan for Mac du serveur ePolicy Orchestrator.

Pour supprimer le fichier .NAP de VirusScan for Mac :

1. Connectez-vous au serveur de base de données ePolicy Orchestrator.
2. Sélectionnez **VirusScan for Mac** sous **Référentiel** | **Produits gérés** | **MAC OS X** | dans l'arborescence de la console.
3. Cliquez avec le bouton droit sur **VirusScan for Mac** et sélectionnez **Supprimer** pour désinstaller le fichier .NAP de VirusScan du serveur ePolicy Orchestrator.

Suppression de l'agent ePolicy Orchestrator pour Mac OS X du serveur ePolicy Orchestrator

Vous ne pouvez pas supprimer l'**agent ePolicy Orchestrator pour MAC OS X** du serveur ePolicy Orchestrator une fois qu'il y a été enregistré.

Suppression de l'agent ePolicy Orchestrator de VirusScan for Mac

Vous pouvez supprimer l'agent ePolicy Orchestrator d'un ordinateur Macintosh.

Pour désinstaller l'agent ePolicy Orchestrator à partir de la ligne de commande :

1. Connectez-vous avec des droits d'administrateur.
2. Placez-vous dans le répertoire `/Library/NETAepoagt`.
3. Exécutez `cmduninst`.

Définition des stratégies dans ePolicy Orchestrator

La console ePolicy Orchestrator vous permet d'appliquer des stratégies à un ordinateur ou à un groupe d'ordinateurs. Elles prennent le pas sur les configurations définies pour chaque ordinateur.

Avant de configurer des stratégies, sélectionnez le groupe d'ordinateurs pour lequel vous souhaitez modifier les stratégies VirusScan for Mac. Vous pouvez modifier les stratégies VirusScan for Mac depuis les pages et onglets VirusScan for Mac du volet de détails de la console ePolicy Orchestrator. Ces pages sont presque identiques à celles auxquelles vous pouvez accéder à partir de l'interface utilisateur de VirusScan for Mac.

Après avoir modifié les stratégies appropriées et enregistré les modifications sur l'ordinateur ou le groupe d'ordinateurs concerné, vous êtes prêt à déployer les nouveaux paramètres par le biais de l'agent ePolicy Orchestrator.

Pour modifier les stratégies VirusScan for Mac dans ePolicy Orchestrator :

1 Connectez-vous au serveur ePolicy Orchestrator.

2 Dans l'arborescence de la console sous **ePolicy Orchestrator** | <**SERVEUR**> | **Répertoire**, sélectionnez le site, le groupe, l'ordinateur particulier ou le répertoire complet auquel vous souhaitez appliquer ces stratégies. Les onglets **Stratégies**, **Propriétés** et **Tâches** s'affichent dans la partie supérieure du volet de détails.

3 Sélectionnez l'onglet **Stratégies** dans le volet de détails, puis développez **VirusScan for Mac 8.6**. Les options **Appliquer les stratégies** et **Stratégies VirusScan** apparaissent sous l'entrée **VirusScan for Mac 8.6**.

4 Sous **Nom de la stratégie**, cliquez sur **Paramètres McAfee par défaut** pour une **catégorie** pour afficher les paramètres de stratégie par défaut.

Vous ne pouvez pas configurer les paramètres de stratégie **Paramètres McAfee par défaut** pour une **catégorie** sélectionnée. Pour configurer une catégorie sélectionnée, vous *devez* créer une stratégie pour cette **catégorie**.

Pour créer une stratégie pour une catégorie :

1 Cliquez sur **Modifier** pour une **catégorie** dans l'entrée **VirusScan for Mac 8.6** du volet de détails d'ePolicy Orchestrator.

2 Cliquez sur la liste déroulante **Nom de la stratégie** et sélectionnez **Nouvelle stratégie**. La boîte de dialogue **Créer une stratégie** apparaît.

Options de création d'une stratégie

Dupliquer la stratégie suivante	Crée une stratégie dupliquée pour la **catégorie** sélectionnée. Sélectionnez la stratégie dans la liste déroulante.
Créer une stratégie où l'héritage est appliqué à tous les onglets	Crée une stratégie dans laquelle tous les paramètres des onglets de stratégie sont hérités.
Nom de la nouvelle stratégie	Saisissez le nom de la nouvelle stratégie pour la **catégorie** que vous souhaitez créer.

3 Configurez les options requises à partir de la stratégie d'origine, puis cliquez sur **OK** pour créer la stratégie.

4 Cliquez sur **Appliquer** pour enregistrer ces paramètres.

Pour modifier une stratégie existante :

1 Cliquez sur pour la **catégorie** sélectionnée dans l'entrée **VirusScan for Mac 8.6** du volet de détails d'ePolicy Orchestrator.

2 Configurez les options requises, puis cliquez sur **Appliquer** pour enregistrer la stratégie.

Pour appliquer les stratégies :

1 Cliquez sur **Modifier** pour l'option **Appliquer les stratégies** dans l'entrée VirusScan for Mac dans ePolicy Orchestrator.

2 Cliquez sur la liste déroulante **Nom de la stratégie** et sélectionnez **Oui**.

3 Cliquez sur **Appliquer** pour appliquer les stratégies que vous venez de configurer.

Onglet Général

L'onglet **Général** vous permet d'appliquer des stratégies générales qui contrôlent le fonctionnement général de VirusScan for Mac, telle que la vérification des mises à jour de définition de virus, la réalisation d'analyses lors de l'accès, la consignation des résultats de l'analyse et la création de liste d'exclusions pour des disques, des fichiers ou des dossiers déterminés.

Vous pouvez appliquer les stratégies générales suivantes ::

Rechercher automatiquement les mises à jour de définitions de virus	Active/désactive la recherche automatique de mises à jour via eUpdate.
Analyse lors de l'accès	Active/désactive l'analyse à l'accès.
Consigner les résultats dans un fichier	Active/désactive la consignation des résultats dans un fichier.
Exclure des disques, des fichiers et des dossiers en particulier	Exclut de l'analyse les éléments listés ici. Si cette option n'est pas sélectionnée, l'analyseur ignore la liste des exclusions. Pour ajouter une exclusion : ■ Cliquez sur **Ajouter**, la boîte de dialogue **Ajouter un élément à analyser -- Page Web** apparaît. Saisissez le chemin complet d'accès au fichier, au répertoire ou au disque à exclure, puis cliquez sur **OK**. Les éléments à exclure figureront dans la liste **Exclusions.** Pour supprimer une exclusion : ■ Sélectionnez l'élément à supprimer dans la liste **Exclusions**, puis cliquez sur **Supprimer**. Pour modifier une exclusion : ■ Sélectionnez l'élément à supprimer dans la liste **Exclusions**, puis cliquez sur **Modifier**.

Onglet eUpdate

L'onglet **eUpdate** vous permet de personnaliser les paramètres de mise à jour des fichiers .DAT et du moteur d'analyse antivirus. Cette fonction maintient à jour en permanence votre logiciel antivirus en intégrant les dernières informations sur les virus et les capacités d'analyse les plus récentes. Vous pouvez mettre à jour vos fichiers .DAT et vos fichiers de moteur via FTP.

Personnalisation des paramètres eUpdate

Lorsque vous mettez à jour vos fichiers DAT et vos fichiers de moteur, vous devez indiquer les informations détaillées relatives au serveur à partir de l'emplacement où les fichiers de mises à jour doivent être transférés.

URL du serveur	URL du serveur depuis lequel vous souhaitez télécharger les mises à jour des fichiers DAT et du moteur.
Port	Numéro de port à utiliser pour la communication FTP.
Nom d'utilisateur	Votre nom d'utilisateur.
Mot de passe	Votre mot de passe.
Compte	Votre compte FTP.
Répertoire	Chemin d'accès à vos fichiers DAT et de moteur.

Onglet Analyseur à l'accès

L'onglet Analyse lors de l'accès permet l'analyse automatique de tous les fichiers en cours d'utilisation afin de détecter la présence éventuelle d'un virus ou de tout autre code malveillant. Une analyse est effectuée chaque fois qu'un fichier est lu à partir du disque et/ou écrit sur le disque par l'utilisateur ou par des processus système. Grâce à l'analyseur à l'accès, il est possible de mettre en œuvre une application en continu des stratégies pour plusieurs fichiers, répertoires et/ou volumes, y compris les volumes résidant sur des ordinateurs distants connectés au réseau. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que son action en cas de présence de fichiers infectés. L'analyseur vous avertit, dans la fenêtre contextuelle **Reporter** de l'ordinateur Macintosh, si un virus ou tout autre code malveillant est détecté.

Vous pouvez appliquer les stratégies suivantes de l'analyseur à l'accès :

Analyser le contenu des archives et des fichiers compressés	Définit l'analyseur pour analyser le contenu des archives et autres fichiers compressés. Cette option est **désactivée** par défaut pour l'analyseur à l'accès. Notez que l'analyseur à l'accès n'analyse pas le contenu des archives Stuffit.
Détecter les virus de macro inconnus	Si un fichier contient une macro potentiellement infectée (infection inconnue), il sera analysé et nettoyé (ou supprimé) lors du nettoyage.
Messages Scan Apple Mail	Définit l'analyseur pour analyser les messages Apple Mail.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications potentiellement indésirables et les programmes canulars	Active/désactive la recherche de programmes indésirables et de programmes canulars.
Analyser des fichiers situés sur des volumes réseau	Configure l'analyseur pour analyser les fichiers qui ont fait l'objet d'un accès à partir de volumes réseau.
Analyser les fichiers : ■ Toujours ■ Lors de la lecture ■ Lors de l'écriture	Détermine si l'analyseur examine les fichiers lus à partir du disque ou écrits sur le disque, ou les deux. Par défaut, cette option est définie sur **Toujours**. De cette manière, les fichiers écrits sur le disque et lus à partir du disque sont analysés.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action principale de l'analyseur à l'accès en cas de détection de virus.
Supprimer lorsque la fonction Nettoyer a échoué ou n'est pas disponible	Sélectionne l'action secondaire de l'analyseur en cas de détection de virus. Cette option est disponible uniquement lorsque l'action principale est **Nettoyer**.
Durée maximale d'analyse (en secondes)	Durée maximale, en secondes, d'une analyse pour un seul fichier. (Un fichier compressé n'est pas traité comme un fichier unique, ce délai maximal s'applique au dernier fichier particulier et non au dernier fichier conteneur de niveau supérieur.)

Onglet Analyseur à la demande

L'analyseur à la demande permet de lancer une analyse à tout moment en déposant par glisser-déplacer les fichiers sélectionnés dans la console ou en utilisant une boîte de dialogue d'**ouverture** des **fichiers**. L'analyseur à la demande permet de sélectionner plusieurs fichiers, répertoires ou volumes. Les résultats de l'analyse sont récapitulés dans un rapport que vous pouvez enregistrer ou imprimer. Vous pouvez configurer l'objet de la recherche de l'analyseur, ainsi que son action en cas de présence de fichiers infectés. L'analyseur vous avertit lorsqu'il détecte un virus et génère un journal répertoriant ses actions.

L'analyseur à la demande prend en charge les stratégies suivantes :

Analyser le contenu des archives et des fichiers compressés	Définit l'analyseur pour analyser le contenu des archives et autres fichiers compressés. Cette option est **activée** par défaut pour l'analyseur à la demande.
Détecter les virus de macro inconnus	Si un fichier contient une macro potentiellement infectée (infection inconnue), il sera analysé et nettoyé (ou supprimé) lors du nettoyage.
Messages Scan Apple Mail	Définit l'analyseur pour analyser les messages Apple Mail.
Rechercher les caractéristiques propres aux virus	Active/désactive l'analyse heuristique, qui recherche les fichiers présentant des caractéristiques propres aux virus ou aux vers et susceptibles de contenir des infections encore inconnues.
Rechercher les applications potentiellement indésirables et les programmes canulars	Active/désactive la recherche de programmes indésirables et de programmes canulars.
Si un virus est détecté : ■ Nettoyer ■ Supprimer ■ Avertir	Sélectionne l'action principale de l'analyseur en cas de détection de virus.
Supprimer lorsque la fonction Nettoyer a échoué ou n'est pas disponible	Sélectionne l'action secondaire de l'analyseur sélectionné en cas de détection de virus. Cette option est disponible uniquement lorsque l'action principale est **Nettoyer**.

Planification des analyses et des mises à jour automatiques via eUpdate

Lors des recherches antivirus, VirusScan utilise les informations contenues dans les fichiers .DAT pour trouver et supprimer les virus. De nombreux virus sont découverts chaque jour et McAfee publie régulièrement de nouveaux fichiers DAT pour assurer une protection contre ces nouvelles menaces. Pour bénéficier de la meilleure protection antivirus possible, vous pouvez configurer ePolicy Orchestrator de sorte qu'il indique à VirusScan for Mac où trouver les derniers fichiers .DAT, créer des planifications pour le remplacement des fichiers .DAT antérieurs et réaliser des analyses à la demande.

Avec ePolicy Orchestrator, vous pouvez planifier les tâches suivantes pour VirusScan for Mac :

- Analyse à la demande
- eUpdate

Les tâches planifiées d'un ordinateur peuvent être définies pour s'exécuter en fonction de l'heure locale ou GMT (heure du méridien Greenwich). Toutefois, ePolicy Orchestrator ne pouvant pas surveiller la progression d'une tâche planifiée, nous vous recommandons de consulter régulièrement le fichier journal sur le serveur pour vérifier si la tâche planifiée a été exécutée correctement.

Analyses à la demande

VirusScan for Mac peut effectuer l'analyse à la demande de vos fichiers, afin de rechercher dans tous les fichiers de votre ordinateur la présence éventuelle de virus, de chevaux de Troie ou de tout autre code malveillant. Vous pouvez planifier un nombre illimité d'analyses à la demande ; ces analyses seront exécutées à intervalles définis ou au moment choisi par l'utilisateur. Si vous souhaitez que certaines planifications ne soient pas exécutées automatiquement, vous pouvez également les désactiver.

Création d'une tâche

1. Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Tâches**. Cliquez avec le bouton droit dans le volet et sélectionnez l'option **Planifier les tâches**.
2. Dans le champ **Nom de la nouvelle tâche**, attribuez un nom à la tâche, puis sélectionnez le type de tâche à créer.
3. Dans la liste déroulante **Type de tâche**, sélectionnez **Analyse à la demande**. Cliquez sur **OK**.

   La tâche créée s'affiche dans l'onglet **Tâches**.

Modification d'une tâche

1 Cliquez avec le bouton droit de la souris sur la tâche et sélectionnez l'option **Modifier la tâche**.

2 Cliquez sur **Paramètres**. La page **Emplacement** vous permettant d'inclure les fichiers et les répertoires dans l'analyse planifiée s'affiche.

Inclure ces fichiers et répertoires à l'analyse	Configure les éléments à inclure dans l'analyse. Pour inclure un élément : ■ Cliquez sur **Ajouter**, la boîte de dialogue **Ajouter un élément à analyser -- Page Web** apparaît. Saisissez le chemin complet d'accès au fichier, au répertoire ou au disque à inclure dans l'analyse, puis cliquez sur **OK**. L'élément à inclure figurera dans la **liste des inclusions.** Pour supprimer un élément inclus : ■ Sélectionnez l'élément à supprimer dans la **Liste** des **inclusions**, puis cliquez sur **Supprimer**. Pour modifier un élément inclus : ■ Sélectionnez l'élément voulu dans la **liste des éléments à inclure**, puis cliquez sur **Modifier**. La boîte de dialogue **Ajouter un élément à analyser -- Page Web** s'affiche. Elle vous permet de modifier le chemin complet d'accès au fichier ou au répertoire correspondant. Cliquez sur **OK**.

Paramètres de planification

3 Désélectionnez **Hériter** pour activer les paramètres du volet **Paramètres de planification**.

Activer (la tâche planifiée est exécutée à une heure précise)	Sélectionnez cette option pour exécuter la tâche à l'horaire indiqué.
Arrêter la tâche si elle s'exécute depuis :	Indique le nombre maximal d'heures et de minutes durant lequel la tâche peut s'exécuter avant d'être annulée.

4 L'onglet **Planifier** comporte ces options :

Planifier la tâche	Sélectionnez l'un des types de tâche disponibles dans la liste déroulante : ■ Quotidiennement ■ Hebdomadairement ■ Mensuellement ■ Une fois ■ Au démarrage du système ■ Exécuter immédiatement
Heure de début ■ Heure UTC ■ Heure locale	Spécifiez l'heure de début de la tâche planifiée. Sélectionnez l'option Heure locale pour lancer la tâche d'après l'intervalle planifié à l'heure système de l'ordinateur client. Cette option permet de planifier pendant les heures creuses l'exécution des tâches qui utilisent un pourcentage élevé des ressources système, comme les analyses à la demande. L'option Heure UTC utilise l'heure en temps universel coordonné (également appelée heure GMT) pour exécuter la tâche. Lorsque cette option est sélectionnée, la tâche s'exécute au même moment sur tous les clients Macintosh, quelle que soit leur heure système locale.

Activer la sélection aléatoire	La tâche ne démarrera pas exactement à l'heure de début définie, mais après une durée aléatoire définie. Pour activer la sélection aléatoire, vous devez définir l'heure et les minutes.
Exécuter la tâche manquée	Permet de lancer la tâche même si l'ordinateur Macintosh est arrêté ou indisponible à l'heure de début planifiée. La tâche sera alors exécutée aussitôt l'ordinateur Macintosh redevenu disponible.
Décaler la tâche manquée de	Cliquez sur **Avancé** dans la boîte de dialogue **Options de planification avancées**. Cette option définit le délai au terme duquel une tâche omise sera exécutée à nouveau une fois l'ordinateur Macintosh redevenu disponible.
Date de début/Date de fin	Cliquez sur **Avancé** dans la boîte de dialogue **Options de planification avancées**. Tapez les dates de début et de fin uniquement si vous souhaitez que la tâche s'exécute sur une période spécifiée, par exemple, quelques jours ou quelques semaines.
Répéter la tâche	Cliquez sur **Avancé** dans la boîte de dialogue **Options de planification avancées**. Utilisez cette option si vous voulez exécuter une tâche plusieurs fois au cours de la même journée. Pour cela, cochez la case **Répéter la tâche** et définissez l'intervalle de répétition souhaité. En général, cette option est utile pour exécuter une tâche d'actualisation du client plusieurs fois par jour, notamment en cas d'apparition d'un grand nombre de nouveaux virus. Elle vous permet également de planifier une tâche pour qu'elle se répète selon d'autres intervalles, de façon hebdomadaire ou mensuelle par exemple.
Planifier tous les X jours	Indiquez l'intervalle choisi pour l'exécution de la tâche planifiée. Il peut s'agir d'un intervalle d'1 ou plusieurs jours. Si vous sélectionnez 1, la tâche planifiée est exécutée une fois tous les deux jours.

Suppression d'une tâche

- Cliquez avec le bouton droit de la souris sur la tâche dans le volet **Tâches**, puis sélectionnez **Supprimer**.

eUpdate

Pour que votre logiciel antivirus vous protège de façon optimale, vous devez l'actualiser avec les derniers fichiers DAT et moteur d'analyse antivirus disponibles. Nous vous recommandons de mettre à jour quotidiennement les fichiers DAT et de consulter régulièrement le site Web McAfee Avert pour en rechercher des nouveaux. Si vous possédez plusieurs serveurs sur un même domaine (tous exécutant VirusScan for Mac), vous pouvez utiliser l'un de ces serveurs pour télécharger les derniers fichiers DAT, puis configurer les autres pour qu'ils copient les fichiers depuis ce serveur. Vos serveurs peuvent télécharger des fichiers destinés à plusieurs systèmes d'exploitation, et ce, quel que soit leur système d'exploitation.

Spécification de l'emplacement des fichiers DAT

Vous pouvez spécifier l'emplacement source des fichiers DAT à l'aide de l'onglet **eUpdate**.

Création d'une tâche eUpdate

1 Dans l'arborescence de la console, sous **ePolicy Orchestrator**, cliquez avec le bouton droit de la souris sur le **répertoire** ou le site, le groupe ou l'hôte, puis sélectionnez **Planifier la tâche**. La boîte de dialogue **Planifier la tâche** s'affiche.

2 Entrez un nom dans le champ **Nom de la nouvelle tâche**.

3 Dans la liste **Logiciel/Type de tâche**, sélectionnez **VirusScan for Mac 8.6 - Mise à jour**.

4 Cliquez sur **OK** pour créer la tâche.

Configuration d'une tâche eUpdate

Après avoir créé une nouvelle tâche eUpdate, vous pouvez la configurer comme vous le souhaitez.

1 Dans l'onglet **Tâches** de la partie supérieure du volet de détails, cliquez avec le bouton droit de la souris sur une tâche, puis sélectionnez **Modifier la tâche**. La boîte de dialogue **Planificateur ePolicy Orchestrator** s'affiche.

2 Cliquez sur **Paramètres**, modifiez les options requises dans les onglets **Tâche** et **Planifier**.

3 Désélectionnez **Hériter**.

4 Sélectionnez **Exécuter eUpdate**, puis sélectionnez **Hériter**.

5 Cliquez sur **OK** pour revenir à la boîte de dialogue **Planificateur ePolicy Orchestrator**.

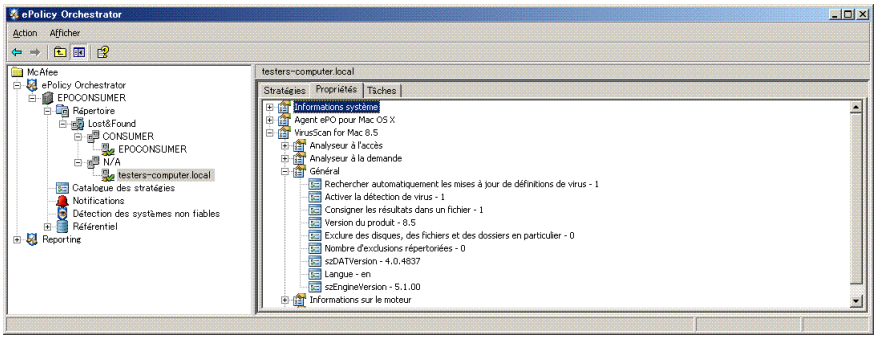
Affichage des propriétés d'ePolicy Orchestrator

Le serveur ePolicy Orchestrator vous permet d'afficher différentes propriétés du système.

Pour afficher les propriétés :

1 Dans l'arborescence de la console, sélectionnez le serveur dont vous souhaitez afficher les paramètres.

Figure 4-3 Propriétés du système



2 Dans la partie supérieure du volet de détails, cliquez sur l'onglet **Propriétés**.

3 Dans le volet **Propriétés**, développez l'arborescence de l'élément **VirusScan for Mac 8.5** pour afficher toutes ses propriétés.

4 Cliquez sur le signe **+** en regard d'une propriété pour en afficher les détails.

Rapports

A partir de la console ePolicy Orchestrator, vous pouvez afficher des rapports indiquant la façon dont les hôtes VirusScan for Mac gèrent les infections, et vérifier la configuration définie sur ces hôtes. Vous pouvez également créer des rapports en utilisant les données envoyées par l'agent non-Windows dans la base de données ePolicy Orchestrator sélectionnée. Vous pouvez aussi enregistrer les sélections effectuées dans les boîtes de dialogue **Saisir les entrées de rapport** et **Filtre de données pour les rapports** pour une utilisation ultérieure.

Tous les rapports VirusScan for Mac sont classés sous l'en-tête **Antivirus**.

Les rapports ePolicy Orchestrator offrent diverses possibilités :

- Filtrage du répertoire pour collecter uniquement les informations que vous souhaitez visualiser. Lors de la définition du filtre, vous pouvez choisir la partie de l'arborescence de la console ePolicy Orchestrator incluse dans le rapport.
- Filtrage des données, en utilisant des opérateurs logiques, afin de filtrer avec précision les données renvoyées par le rapport.
- Génération de rapports graphiques à partir des informations de la base de données et filtrage des rapports en fonction de vos besoins. Vous pouvez imprimer les rapports et les exporter pour les utiliser dans d'autres logiciels.
- Exécution de requêtes sur des ordinateurs, des événements et des installations.

Pour exécuter un rapport :

1 Connectez-vous au serveur de base de données ePolicy Orchestrator.

2 Sélectionnez le rapport VirusScan for Mac souhaité sous **Rapports** | **Bases de données ePO** | <**serveur de base de données**> | **Rapports** | <**groupe de rapports**> dans l'arborescence de la console.

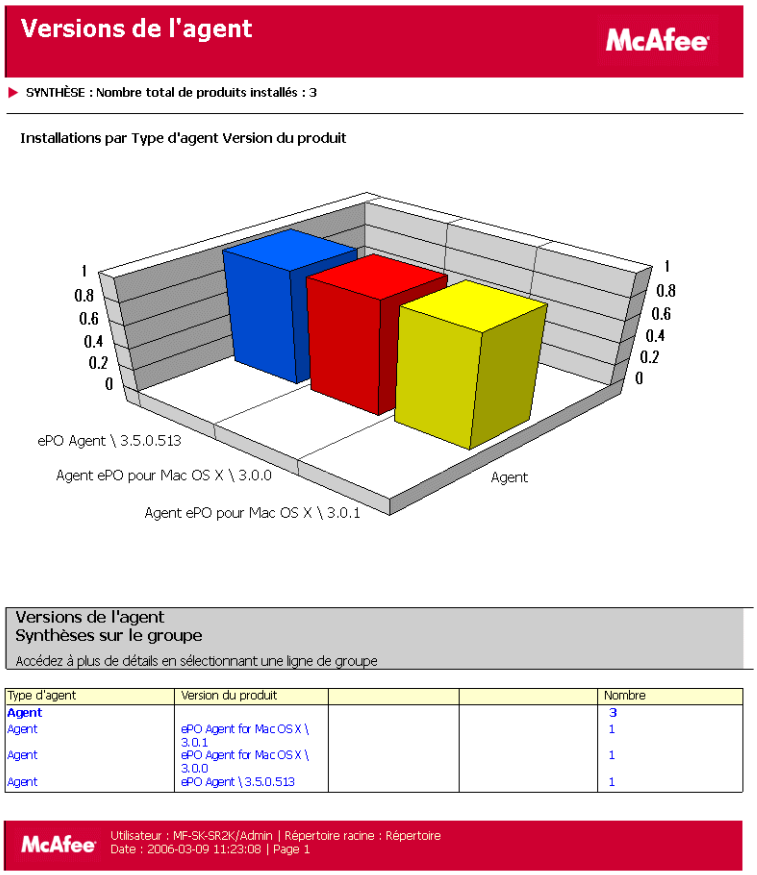
- Si la boîte de dialogue **Normes actuelles en matière de protection** s'affiche, spécifiez les numéros de version des fichiers de définition de virus ou le moteur d'analyse des virus sur lesquels vous souhaitez des rapports.
- Si la boîte de dialogue **Saisir les entrées de rapport** s'affiche, effectuez vos choix dans les onglets correspondants : **Règles, Mise en page, Groupements de données, Intervalle, Paramètres enregistrés**.

Ces onglets peuvent différer en fonction du rapport sélectionné. Pour plus d'informations sur tous les onglets de paramètres, reportez-vous aux *Guides produit d'ePolicy Orchestrator.*

3 Sélectionnez le rapport (**Versions de l'agent**) que vous souhaitez générer, puis définissez le filtre de données dans la boîte de dialogue **Filtre de données pour les rapports**. Cliquez sur **OK**.

4 Un rapport relatif aux **versions de l'agent** est alors généré.

Figure 4-4 Exemple de rapport - Versions de l'agent



Configuration des rapports

Vous pouvez contrôler les données qui s'affichent dans les rapports de diverses manières. Vous pouvez définir le numéro de version des fichiers de signatures de virus, des moteurs d'analyse antivirus et des produits pris en charge qui doivent être installés sur les ordinateurs clients Macintosh afin de les rendre conformes aux stratégies de sécurité et antivirus définies pour votre entreprise. Vous pouvez également filtrer les résultats des rapports en fonction de critères liés aux produits sélectionnés (par exemple, par nom d'ordinateur, système d'exploitation, nom de virus ou action entreprise sur les fichiers infectés).

Une fois les résultats d'un rapport affichés, vous pouvez effectuer un certain nombre de tâches sur les données. Vous pouvez afficher des informations détaillées sur les données de rapport requises (par exemple, pour déterminer les ordinateurs client Macintosh non dotés d'une version conforme de VirusScan for Mac). Certains rapports proposent même des liens vers d'autres rapports, appelés sous-rapports, qui fournissent des données sur le rapport actuel. Vous pouvez également imprimer les rapports ou exporter les données des rapports dans différents formats de fichiers, y compris HTML et Microsoft Excel.

5 Intégration à ePolicy Orchestrator 4.0

Introduction

Ce chapitre indique comment configurer VirusScan en utilisant le logiciel de gestion McAfee ePolicy Orchestrator version 4.0. Pour bien comprendre ce chapitre, vous devez être familiarisé avec le logiciel ePolicy Orchestrator 4.0.

ePolicy Orchestrator 4.0 est une plate-forme évolutive destinée à la gestion et à l'application centralisées de stratégies pour vos produits de sécurité et les systèmes sur lesquels elle se trouve. Le logiciel permet également de créer des rapports complets et de déployer des produits à l'aide d'un point de contrôle unique.

Ce guide ne fournit pas d'informations détaillées sur l'installation et l'utilisation du logiciel ePolicy Orchestrator. Reportez-vous au *Guide produit d'ePolicy Orchestrator v4.0*.

Extensions

Les extensions de VirusScan sont préinstallées avec ePolicy Orchestrator 4.0. Vous pouvez installer, supprimer et gérer les fichiers d'extension VirusScan. Les fichiers d'extension sont au format .ZIP. Ils doivent être installés pour que ePolicy Orchestrator 4.0 puisse gérer le produit ou le composant.

Si vous souhaitez désinstaller des extensions VirusScan, vous pourrez les trouver sous **Program Files** | **McAfee** | **ePolicyOrchestrator** | **Extensions**.

Les deux fichiers d'extension pour VirusScan sont :

- **VSCANMAC8600.ZIP**
- **VIREXREPORTS.ZIP**

Pour installer les fichiers d'extension de stratégie VirusScan :

1. Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.
2. Cliquez sur **Configuration** | **Extensions** | **Installer une extension**. La boîte de dialogue **Installer une extension** apparaît.
3. Cliquez sur **Parcourir**, sélectionnez le fichier d'extension **VSCANMAC8600.ZIP** et cliquez sur **OK**.

Pour installer les fichiers d'extension de rapport VirusScan :

1 Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.

2 Cliquez sur **Configuration** | **Extensions** | **Installer une extension**. La boîte de dialogue **Installer une extension** apparaît.

3 Cliquez sur **Parcourir**, sélectionnez le fichier d'extension **VIREXREPORTS.ZIP** et cliquez sur **OK**.

Présentation du tableau de bord ePolicy Orchestrator 4.0

Les tableaux de bord regroupent un ensemble de moniteurs pré-configurés et/ou sélectionnés par l'utilisateur et affichent les données actuelles de vos détections.

Le tableau de bord ePolicy Orchestrator est constitué de plusieurs moniteurs désignés. Selon les droits dont vous disposez avec votre compte, vous pouvez créer des tableaux de bord, les gérer, les sélectionner ou éditer les préférences.

Création d'un tableau de bord

1 Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.

2 Cliquez sur **Tableaux de bord** | **Options** | **Nouveau tableau de bord**. La page **Nouveau tableau de bord** apparaît.

3 Entrez un **nom de tableau de bord** et définissez sa **taille** à l'aide de la liste déroulante.

4 Cliquez sur **Nouveau moniteur**.

5 Sélectionnez la **catégorie Requêtes**, ainsi qu'une requête associée au VirusScan souhaité à partir du menu déroulant **Moniteur**.

6 Cliquez sur **OK**.

7 Répétez les étapes 4 et 5 pour les autres moniteurs.

8 Cliquez sur **Enregistrer**. La boîte de dialogue **Activer** s'affiche.

9 Cliquez sur **Oui** pour ajouter le nouveau tableau de bord à votre ensemble actif.

Tableau 5-1 Options du tableau de bord

Options	Description
Nom du tableau de bord	Indique le nom du tableau de bord sélectionné.
Taille du tableau de bord	Indique les dimensions (par nombre de moniteurs par tableau de bord) du tableau de bord sélectionné.
Créé par	Indique le nom de l'utilisateur qui a créé le tableau de bord sélectionné.
Dernière modification effectuée par	Indique le nom de l'utilisateur, la date et l'heure de la dernière modification effectuée sur le tableau de bord sélectionné.
Modifier	Vous redirige vers la page **Modifier un tableau de bord** où vous pourrez changer le nom et la taille du tableau de bord.
Supprimer	Supprime le tableau de bord sélectionné.

Tableau 5-1 Options du tableau de bord

Options	Description
Dupliquer	Crée et enregistre une copie du tableau de bord sélectionné. Vous pouvez ainsi copier et modifier des tableaux de bord similaires sans devoir en créer un tout nouveau.
Publier	Ajoute le tableau de bord privé sélectionné à la liste des tableaux de bord publics. Ils seront ainsi disponibles pour tous les utilisateurs dotés des autorisations adéquates.
Activer	Ajoute le tableau de bord sélectionné à l'onglet Tableaux de bord pour faciliter son accès.

Systèmes

Tous les éléments du réseau sont gérés à partir de l'onglet **Systèmes**. L'**arborescence des systèmes** contient tous les systèmes gérés par ePolicy Orchestrator. C'est l'interface principale pour la gestion des stratégies et des tâches sur ces systèmes. Vous pouvez organiser ou trier ces systèmes en groupes logiques dans l'**arborescence des systèmes**.

La racine de l'**arborescence des systèmes** se nomme **Mon organisation**. La racine comprend un groupe **Collecteur** qui stocke les systèmes dont l'emplacement n'a pas été déterminé par le serveur. Selon vos méthodes de création et de gestion des segments de l'**arborescence des systèmes** (des systèmes), le serveur utilise différentes caractéristiques pour répartir les systèmes dans l'**arborescence**.

Pour obtenir des informations sur l'ajout d'un nouveau système, reportez-vous au *Guide produit d'ePolicy Orchestrator 4.0*.

Envoi d'un appel de réactivation de l'agent

1. Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.
2. Cliquez sur **Systèmes**.
3. Sélectionnez un groupe dans l'**arborescence des systèmes**.
4. Sélectionnez le ou les **noms d'ordinateurs** souhaités pour ce groupe.
5. Cliquez sur **Plus d'actions** | **Réactiver un agent**. La page **Réactiver des agents** apparaît.
6. Sélectionnez un **type d'appel de réactivation** et une période de **sélection aléatoire** (de 0 à 60 minutes) pendant laquelle le ou les systèmes réagissent à l'appel de réactivation envoyé par le serveur ePolicy Orchestrator.
7. Sélectionnez **Obtenir les propriétés complètes du produits** pour le ou les agents. Cette option vous permet d'envoyer toutes les propriétés au lieu de n'envoyer que celles qui ont été modifiées depuis la dernière communication agent-serveur.
8. Cliquez sur **OK**.

L'option **Journal des tâches serveur** vous permet de connaître l'état de l'appel de réactivation de l'agent.

Stratégies

Vous pouvez créer, modifier, supprimer ou attribuer une stratégie à un système/groupe spécifique dans l'**arborescence des systèmes**.

Création d'une stratégie

1 Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.

2 Cliquez sur **Systèmes** | **Arborescence des systèmes** et sélectionnez le groupe de votre choix.

3 Dans **Stratégies**, sélectionnez le **produit** souhaité dans la liste déroulante. Une liste de stratégies gérées par le produit sélectionné s'affiche dans la partie inférieure du volet.

4 Recherchez la catégorie de stratégies souhaitée, puis cliquez sur **Modifier l'attribution**. La page **Attribution de stratégie pour: Mon organisation| Collecteur | (groupe sélectionné)** s'affiche.

5 Cliquez sur **Créer une stratégie**. La boîte de dialogue **Créer une stratégie** apparaît.

6 Sélectionnez **Valeur McAfee par défaut** ou **Ma valeur par défaut**.

Les stratégies **par défaut McAfee** sont en lecture seule et ne peuvent être modifiées, renommées ou supprimées.

7 Entrez un **nouveau nom de stratégie**.

8 Cliquez sur **OK**, puis sur **Enregistrer**.

Application des stratégies

Vous pouvez appliquer une stratégie à plusieurs systèmes gérés au sein d'un groupe.

1 Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.

2 Cliquez sur **Systèmes** | **Arborescence des systèmes** et sélectionnez le groupe de votre choix.

3 Sélectionnez le ou les systèmes souhaités.

4 Cliquez sur **Attribuer une stratégie**. La page **Attribution d'une stratégie pour <n> système(s)** s'affiche.

5 Sélectionnez le **produit**, la **catégorie** et la **stratégie** souhaités dans la liste déroulante, puis cliquez sur **Enregistrer**.

6 Sélectionnez une nouvelle fois les systèmes.

7 Envoyez un appel de réactivation de l'agent.

Pour connaître les instructions d'envoi d'un appel de réactivation d'agent, reportez-vous à *Envoi d'un appel de réactivation de l'agent* , page 53.

Vous pouvez seulement créer et appliquer les stratégies VirusScan et consulter les rapports après avoir ajouté les fichiers d'extension VirusScan.

Tâches du client

ePolicy Orchestrator vous permet de créer, de planifier et de gérer les tâches d'un client opérant sur des systèmes gérés. Vous pouvez définir les tâches d'un client pour l'intégralité de l'**arborescence des systèmes**, pour un groupe spécifique ou un seul système.

Avec ePolicy Orchestrator 4.0, vous pouvez planifier les tâches suivantes pour VirusScan :

- Tâche eUpdate
- Tâche d'analyse à la demande

Les tâches client disponibles dans la liste déroulante dépendent des fichiers d'extension installés.

Tâche eUpdate

Pour que votre logiciel vous protège de façon optimale, vous devez l'actualiser avec les dernières définitions de virus (DAT) et le plus récent moteur d'analyse antivirus disponibles. Nous vous recommandons de mettre à jour quotidiennement les fichiers DAT et de consulter régulièrement le site Web McAfee AVERT (Anti-Virus Emergency Response Team) pour rechercher les nouveaux fichiers DAT.

Création d'une tâche eUpdate

1. Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.
2. Cliquez sur **Systèmes** | **Arborescence des systèmes** et sélectionnez le groupe de votre choix.
3. Dans **Tâches du client**, sélectionnez le groupe dans l'**arborescence des systèmes** pour lequel vous souhaitez créer la tâche eUpdate.
4. Cliquez sur **Créer une tâche**. La page **Générateur de tâches client** apparaît.
5. Dans **Description**, saisissez un **nom** et vos **remarques** (le cas échéant) pour la tâche eUpdate.
6. Sélectionnez **Tâche eUpdate (VirusScan 8.6)** comme **Type** de tâche et cliquez sur **Suivant**.
7. Planifiez la tâche comme vous le souhaitez et cliquez sur **Suivant** pour consulter la **synthèse** de la tâche eUpdate. La synthèse contient le **nom**, les **remarques**, le **produit**, le **type** de la tâche et les informations concernant la **planification**.
8. Cliquez sur **Enregistrer**.
9. Envoyez un appel de réactivation de l'agent.

Pour connaître les instructions d'envoi d'un appel de réactivation d'agent, reportez-vous à *Envoi d'un appel de réactivation de l'agent* , page 53.

Cliquez sur **Modifier** pour changer la description ou la planification d'une tâche eUpdate ou sur **Supprimer** pour l'effacer.

Tâche d'analyse à la demande

Vous pouvez planifier un nombre illimité d'analyses à la demande ; ces analyses seront exécutées à intervalles définis ou au moment choisi par l'utilisateur.

Création d'une tâche d'analyse à la demande

1 Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.

2 Cliquez sur **Systèmes** | **Arborescence des systèmes** | **Tâches du client**.

3 Dans l'**arborescence des systèmes**, sélectionnez le groupe pour lequel vous souhaitez créer la tâche d'analyse à la demande.

4 Cliquez sur **Créer une tâche**. La page **Générateur de tâches client** apparaît.

5 Dans **Description**, saisissez un **nom** et vos **remarques** (le cas échéant) pour la tâche d'analyse à la demande.

6 Sélectionnez **Analyse à la demande (VirusScan 8.6)** comme **Type** de tâche et cliquez sur **Suivant**.

7 Dans **Configuration**, sélectionnez une stratégie dans la liste déroulante.

8 Cliquez sur **Suivant** et procédez à la planification de la tâche.

9 Cliquez sur **Suivant** pour consulter la **synthèse** de la tâche d'analyse à la demande. Cette synthèse contient le **nom**, les **remarques**, le **produit**, le **type** de la tâche et les informations concernant la **planification**.

10 Cliquez sur **Enregistrer**.

11 Envoyez un appel de réactivation de l'agent.

Pour connaître les instructions d'envoi d'un appel de réactivation d'agent, reportez-vous à *Envoi d'un appel de réactivation de l'agent* , page 53.

Cliquez sur **Modifier** pour changer la description ou la planification d'une tâche d'analyse à la demande ou sur **Supprimer** pour l'effacer.

Désinstallation

Suppression de l'extension du produit

1. Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.
2. Cliquez sur **Configuration** | **Extensions**.
3. Cliquez sur le fichier d'extension **VirusScan**, puis sur **Supprimer**.
4. Sélectionnez l'option **Forcer la suppression en ignorant les recherches et les erreurs**.
5. Cliquez sur **OK**.

Suppression de l'extension du rapport

1. Connectez-vous au serveur ePolicy Orchestrator avec un compte d'administrateur.
2. Cliquez sur **Configuration** | **Extensions**.
3. Cliquez sur le fichier d'extension **Rapports VirusScan**, cliquez sur **Supprimer**.
4. Sélectionnez l'option **Forcer la suppression en ignorant les recherches et les erreurs**.
5. Cliquez sur **OK**.

6 Dépannage

Ce chapitre apporte des solutions à des situations que vous risquez de rencontrer lors de l'installation ou de l'utilisation du logiciel VirusScan.

Les rubriques suivantes sont incluses :

Foire aux questions

Installation

Pourquoi le programme d'installation ne fonctionne-t-il pas ?
Vérifiez la plate-forme sur laquelle vous tentez d'installer VirusScan : il doit s'agir de Mac OS X version 10.4.6 (ou ultérieure) ou de Mac OS X Leopard version 10.5, sur un ordinateur Mac basé PowerPC ou Intel. L'ordinateur doit être doté d'au moins 512 Mo de mémoire RAM et 45 Mo d'espace disque disponible. Il est aussi possible qu'un autre programme antivirus ait été détecté pendant l'installation et qu'il doive être supprimé pour que l'installation de VirusScan réussisse. Pour fonctionner correctement, VirusScan requiert le sous-système BSD.

Quels sont les fichiers VirusScan et où sont-ils installés ?
VirusScan est installé dans le dossier `/Applications`, VirusScan Schedule Editor est installé dans le dossier `/Applications/Utilities` et VirusScan Reporter est installé dans le dossier `/Library/Application Support`. Les fichiers DAT, les bibliothèques dynamiques et les démons se trouvent dans le dossier `/usr/local/vscanx`.

Analyse

Pourquoi VirusScan n'a-t-il pas analysé certains fichiers ?
Vérifiez que les fichiers ignorés ne figurent pas dans la liste des exclusions. De plus, VirusScan n'analyse pas les archives ni les fichiers compressés, sauf si le programme a été configuré pour les analyser.

Pendant que VirusScan analysait un fichier, j'en ai déposé un autre pour analyse. Qu'est-il arrivé à ce fichier ?
Il est impossible d'ajouter des fichiers à la file d'attente d'analyse. Le fait de faire glisser plusieurs éléments simultanément augmente la file d'attente. Ainsi, si vous faites glisser trois dossiers ou fichiers, l'analyseur procède à trois analyses. Si vous faites glisser un dossier contenant plusieurs fichiers, l'analyseur ne réalise qu'une seule analyse.

Pourquoi VirusScan n'analyse-t-il pas régulièrement mon ordinateur ?
Vérifiez que vous avez bien planifié une analyse à la demande de votre ordinateur, qu'elle est activée et configurée pour un lancement à intervalles réguliers.

Virus et détection

VirusScan peut-il détecter à la fois les virus Macintosh et les virus Windows ?
VirusScan détecte tous les virus et vers Macintosh et Windows connus.

Pourquoi VirusScan a-t-il cessé d'afficher les éléments analysés ?
VirusScan affiche uniquement les 200 000 premiers éléments analysés et identifiés comme infectés.

Pourquoi le contenu de mon fichier journal est-il tronqué ?
La taille d'un fichier journal est limitée à 512 Ko. Lorsque la taille d'un fichier journal excède 512 Ko, il est renommé en **VirusScan.log.0** et un nouveau fichier **VirusScan.log** est créé. Deux fichiers journaux de sauvegarde au maximum sont conservés. Si vous voulez spécifiquement conserver une copie du fichier journal existant, nous vous recommandons d'enregistrer tous les anciens fichiers journaux avant de démarrer une nouvelle analyse. Pour afficher le fichier journal, sélectionnez **Fichier** | **Afficher le journal**.

Informations générales

Puis-je annuler les modifications que j'ai apportées aux paramètres de préférences ?
Si les préférences que vous avez enregistrées sont incorrectes, vous pouvez réinitialiser les paramètres en cliquant sur **Restaurer les paramètres par défaut** dans le coin inférieur gauche de la fenêtre **Préférences**. Il n'est pas possible d'annuler des modifications apportées aux préférences une fois qu'elles sont réalisées, leurs paramètres étant enregistrés dès la modification effectuée. Nous vous conseillons de prendre note de vos paramètres de préférences avant de les modifier.

L'annulation des mises à jour avec eUpdate est-elle prise en charge ?
eUpdate ne prend en charge que les mises à jour actuelles ou nouvelles. L'annulation n'est pas prise en charge.

Les définitions de virus Macintosh sont-elles incluses dans les mises à jour ?

Les mises à jour eUpdate incluent les définitions de virus Macintosh et Windows.

Comment trouver la date et le numéro de version des fichiers de définitions de virus (DAT) ?

Sélectionnez **À propos de VirusScan** dans le menu VirusScan dans la barre de menus de l'application. Les dates des versions DAT indiquent uniquement le jour de création des fichiers DAT.

Quelle est la fréquence de mise à jour automatique des fichiers DAT dans VirusScan ?

eUpdate vérifie automatiquement les nouvelles mises à jour via Internet chaque jour. Vous pouvez également télécharger manuellement les mises à jour quotidiennes depuis le site Web de la bibliothèque MacAfee d'informations sur les virus.

Pourquoi ne puis-je pas me connecter au serveur eUpdate pour réaliser une mise à jour non programmée ?

Vérifiez que vous êtes bien connecté à Internet. Le serveur eUpdate est peut-être occupé.

Dépannage avancé

Une fois VirusScan installé, puis-je voir l'exécution des processus ?

Les processus qui s'exécutent sont VShieldScanManager et VShieldScanner.

Puis-je télécharger manuellement des définitions de virus sans utiliser eUpdate ?

À partir de la barre d'outils de la console VirusScan, cliquez sur **Infos Virus**. Votre navigateur par défaut est lancé et accède à la bibliothèque McAfee d'informations sur les virus. Cliquez sur le lien **Downloads** à gauche de l'écran pour télécharger les fichiers DAT.

Comment personnaliser les paramètres serveur d'eUpdate ?

1. Cliquez sur **Préférences** dans la barre d'outils pour afficher la boîte de dialogue Préférences.
2. Cliquez sur **Plus d'options**.
3. Sélectionnez l'option **Personnaliser les paramètres serveur d'eUpdate**, puis cliquez sur **Personnaliser**.
4. Configurez les paramètres du serveur FTP eUpdate, puis cliquez sur **OK**.
5. Cliquez sur **Fermer**.

Emplacement des fichiers journaux

Le Tableau 6-1 répertorie les fichiers journaux.

Tableau 6-1 Fichiers journaux

Fichier journal	Description	Emplacement
VirusScan.log	Contient des entrées VirusScan.	Vous pouvez accéder à ce fichier journal à partir de `/var/log/VirusScan.log`
log	Contient des entrées liées à l'agent ePolicy Orchestrator.	Vous pouvez accéder à ce fichier journal à partir de `/Library/NETAepoagt/scratch /etc/log`

Messages d'erreur

Le Tableau 6-2 répertorie tous les messages d'erreur possibles susceptibles de s'afficher lors de l'exécution de l'application VirusScan et les raisons possibles de leur apparition.

Tableau 6-2 Messages d'erreur - Application VirusScan

Numéro	Message	Raison possible
1	L'initialisation du moteur VirusScan a échoué (erreur %d).	Le moteur ou les fichiers DAT sont altérés ou ont été déplacés/supprimés. Réinstallez l'application.
2	Le rapport n'a pas pu être enregistré. Il est possible que le disque soit saturé ou que le rapport ne contienne aucune donnée.	Votre disque ne dispose peut-être pas de suffisamment d'espace pour enregistrer le rapport. Libérez de l'espace et réessayez d'enregistrer.
3	Impossible d'ouvrir l'URL de la bibliothèque d'informations sur les virus. Votre navigateur n'est peut-être pas installé correctement.	Assurez-vous que votre navigateur est correctement installé.
4	Une erreur s'est produite lors de l'installation de la mise à jour. eUpdate ne s'est pas terminé.	Une erreur s'est produite lors de la tentative d'installation de la mise à jour. Relancez la procédure eUpdate et réessayez.
5	Une erreur s'est produite lors de la décompression du programme de mise à jour. eUpdate ne s'est pas terminé.	Une erreur s'est produite lors de la tentative de décompression du programme de mise à jour en vue de l'installation. Relancez la procédure eUpdate et réessayez.
6	Une erreur s'est produite lors du téléchargement de la mise à jour. eUpdate ne s'est pas terminé.	Une erreur s'est produite lors de la tentative de téléchargement de la mise à jour. Le serveur est peut-être occupé actuellement. Patientez quelques minutes, puis relancez la procédure eUpdate et réessayez.
7	Ce produit est sur le point d'expirer. Afin que l'antivirus reste efficace, il est conseillé de mettre à jour le produit le plus rapidement possible.	Votre version de VirusScan a expiré. Nous vous conseillons de mettre à niveau votre version de VirusScan en choisissant la toute dernière version afin de garantir la meilleure protection antivirus possible.
8	Ce produit logiciel arrive en fin de vie. Son utilisation n'est plus prise en charge. Afin que l'antivirus reste efficace, il est désormais essentiel que vous mettiez à jour le produit le plus rapidement possible.	Votre version de VirusScan a expiré. Nous vous conseillons de mettre à niveau votre version de VirusScan en choisissant la toute dernière version afin de garantir la meilleure protection antivirus possible.
9	Ce logiciel ne peut désormais plus assurer une protection antivirus satisfaisante. Afin que l'antivirus reste efficace, il est désormais indispensable que vous mettiez à jour le produit.	Votre version de VirusScan a expiré. Nous vous conseillons de mettre à niveau votre version de VirusScan en choisissant la toute dernière version afin de garantir la meilleure protection antivirus possible.
10	Le moteur d'analyse de ce produit arrive en fin de vie. Afin que l'antivirus reste efficace, il est conseillé de mettre à jour le moteur d'analyse le plus rapidement possible.	Le moteur fourni avec VirusScan est devenu obsolète. Nous vous conseillons de lancer une tâche eUpdate dès que possible pour optimiser votre protection antivirus.

Tableau 6-2 Messages d'erreur - Application VirusScan

Numéro	Message	Raison possible
11	Le moteur d'analyse de ce produit arrive en fin de vie. Son utilisation n'est plus prise en charge. Afin que l'antivirus reste efficace, il est désormais essentiel que vous mettiez à jour le moteur d'analyse le plus rapidement possible.	Le moteur fourni avec VirusScan est devenu obsolète. Nous vous conseillons de lancer une tâche eUpdate dès que possible pour optimiser votre protection antivirus.
12	Le moteur d'analyse installé pour ce produit ne constitue plus une protection antivirus satisfaisante. Afin que l'antivirus soit efficace, il est désormais indispensable que vous mettiez à jour le moteur d'analyse.	Le moteur fourni avec VirusScan est devenu obsolète. Nous vous conseillons de lancer une tâche eUpdate dès que possible pour optimiser votre protection antivirus.

Glossaire

Administrateur général	Compte utilisateur possédant des droits de lecture, d'écriture et de suppression, ainsi que des droits pour exécuter toutes les opérations. Les opérations qui affectent la totalité de l'installation sont réservées à l'usage exclusif des comptes utilisateur d'administrateur général.
Agent ePolicy Orchestrator	Programme qui effectue des tâches en arrière-plan sur des ordinateurs gérés, sert d'intermédiaire pour toutes les requêtes entre le serveur ePolicy Orchestrator et les produits de sécurité ou antivirus installés sur ces ordinateurs et signale en retour au serveur l'état de ces tâches.
Agent inactif	Tout agent n'ayant pas communiqué avec le serveur ePolicy Orchestrator pendant une période spécifiée.
Alerte	Message ou notification concernant l'activité de l'ordinateur telle que la détection d'un virus. Elle peut être envoyée automatiquement selon une configuration prédéfinie, aux administrateurs système et aux utilisateurs par courrier électronique, pager ou téléphone.
Analyse à la demande	Examen planifié de fichiers sélectionnés visant à déterminer s'ils contiennent un virus ou un autre code potentiellement indésirable. Cet examen peut s'effectuer immédiatement, à une prochaine date planifiée ou à des intervalles planifiés régulièrement.
Analyse à l'accès	Examen en continu des fichiers utilisés afin de détecter la présence éventuelle d'un virus ou de tout autre code malveillant. Cet examen peut être effectué chaque fois qu'un fichier est lu à partir du disque, et/ou écrit sur le disque. L'analyse peut porter sur plusieurs répertoires et volumes.
Analyse, analyser	Examen de fichiers pour détecter la présence d'un virus ou d'autre code potentiellement dangereux.
Analyseur à la demande	L'analyseur à la demande vous permet de lancer une analyse à tout moment en déposant par glisser-déplacer les fichiers sélectionnés dans la console ou en utilisant une boîte de dialogue d'ouverture de fichiers. Vous pouvez analyser plusieurs fichiers, répertoires et volumes.
Analyseur à l'accès	L'analyseur à l'accès surveille de manière continue tous les fichiers utilisés afin de détecter la présence d'un virus ou de tout code potentiellement malveillant. Il s'exécute chaque fois qu'un fichier est lu à partir du disque et/ou écrit sur le disque. L'analyse peut porter sur plusieurs répertoires et volumes.
Appel de réactivation de l'agent	Processus permettant d'établir la communication agent-serveur à partir du serveur.
Application	Mise en vigueur de paramètres prédéfinis sur des ordinateurs clients à intervalles prédéterminés.

Arborescence de la console — Contenu de l'onglet **Arborescence**, dans le volet gauche de la console ePolicy Orchestrator. L'arborescence affiche les éléments disponibles dans la console.

Archivage — Ajout de fichiers au référentiel maître.

Autres fichiers DAT — Fichiers de définition de virus supplémentaires créés en réaction à l'apparition d'un nouveau virus ou d'une nouvelle variante d'un virus connu.

Base de données ePolicy Orchestrator — Base de données qui stocke toutes les données reçues par le serveur ePolicy Orchestrator de l'agent ePolicy Orchestrator, ainsi que tous les paramètres configurés sur le serveur lui-même.

Bibliothèque McAfee d'informations sur les virus — La bibliothèque d'informations sur les virus (http://vil.nai.com/vil/default.aspx) propose des informations détaillées sur l'origine des virus, la manière dont ils infectent un ordinateur et la façon de les supprimer. Ce site contient également des informations sur les programmes canulars.

Branche — Emplacement du référentiel maître qui permet de stocker et de distribuer différentes versions de mises à jour sélectionnées.

Cheval de Troie — Programme prétendant posséder ou décrit comme possédant un ensemble de fonctionnalités utiles mais qui, en fait, contient un élément destructeur. Les chevaux de Troie ne sont techniquement pas des virus, dans la mesure où ils ne se répliquent pas.

Communication agent-serveur — Toute communication ayant lieu entre l'agent ePolicy Orchestrator et le serveur ePolicy Orchestrator et au cours de laquelle ceux-ci échangent des données. En règle générale, c'est l'agent qui établit toutes les communications avec le serveur.

Console distante ePolicy Orchestrator — Interface utilisateur ePolicy Orchestrator, lorsqu'elle est installée sur un ordinateur distinct du serveur ePolicy Orchestrator.

Console ePolicy Orchestrator — Interface utilisateur du logiciel ePolicy Orchestrator utilisée pour contrôler et surveiller à distance des ordinateurs gérés.

Console VirusScan — Interface utilisateur la plus courante de VirusScan. Cette console vous permet de configurer l'analyseur à la demande et l'analyseur à l'accès, d'exécuter des analyses à la demande et de démarrer des mises à jour eUpdate.

Contrôleur de l'agent — Interface utilisateur de l'agent que vous pouvez choisir d'afficher sur les ordinateurs gérés. Elle vous permet d'exécuter des tâches immédiatement alors qu'elles sont normalement déclenchées par l'agent selon des intervalles prédéfinis.

Démon — Programme qui fonctionne en permanence et dont le rôle est de traiter les demandes de services reçues par le système. Il transmet ensuite ces requêtes à d'autres programmes ou processus.

Déployer, déploiement — Action consistant à distribuer et à installer les programmes d'installation sur des ordinateurs clients depuis un emplacement centralisé.

EICAR — European Institute of Computer Anti-Virus Research (Institut européen pour la recherche antivirus informatique). L'institut EICAR a mis au point des fichiers permettant de tester l'installation et le fonctionnement corrects des logiciels antivirus.

Élément de l'arborescence de la console	Chacune des icônes de l'arborescence de la console ePolicy Orchestrator.
eUpdate	eUpdate vous permet de mettre à jour les fichiers DAT et le moteur d'analyse des virus. Ce composant recherche automatiquement chaque jour les nouvelles mises à jour lorsque la connexion à Internet est établie.
Événements	Données échangées durant une communication agent-serveur et comprenant des informations au sujet de chaque ordinateur géré (par exemple, matériel et logiciels) et de ses produits gérés (par exemple, paramètres de stratégie spécifiques et numéros de version du produit).
Événements du serveur	Activité ayant lieu sur le serveur ePolicy Orchestrator et enregistrée par l'Observateur d'événements Windows. Ces informations ne sont pas enregistrées dans la base de données ePolicy Orchestrator et ne sont donc pas disponibles pour la création de rapports.
Fichier journal/journal	Enregistrement des activités d'un composant de logiciel antivirus McAfee. Les fichiers journaux enregistrent les actions exécutées pendant une installation ou pendant l'analyse ou les tâches de mise à jour.
Fichiers (d'installation) binaires	Programme d'installation et tous les autres fichiers requis pour installer des produits.
Fichiers DAT	Fichiers de définition de virus qui permettent au logiciel antivirus d'identifier les virus et le code indésirable éventuellement incorporé dans les fichiers.
FTP	File Transfer Protocol (Protocole de transfert de fichiers). Méthode répandue permettant de déplacer des fichiers entre deux sites Internet.
Groupe	Dans l'arborescence de la console, ensemble logique d'entités regroupées pour en faciliter la gestion. Les groupes peuvent contenir d'autres groupes ou des ordinateurs, et vous pouvez leur assigner des intervalles d'adresses IP ou des masques de sous-réseau IP de façon à classer les ordinateurs en fonction de leur adresse IP. Si vous avez créé un groupe en important un domaine Windows NT, vous pouvez envoyer automatiquement le package d'installation de l'agent à l'ensemble des ordinateurs importés du domaine.
Groupe Perdu&Trouvé	Groupe où sont stockés temporairement les ordinateurs dont il n'est pas possible de déterminer l'emplacement approprié dans le **Répertoire**.
Hériter, héritage	Application d'un élément des paramètres définis pour l'élément situé juste au-dessus de lui au sein de la hiérarchie.
Heure-UTC	Coordinated Universal Time (Temps Universel Coordonné). Fait référence à l'heure du méridien zéro ou méridien de Greenwich.
HTTP	HyperText Transfer Protocol (Protocole de transfert hypertexte). Protocole permettant de transférer des fichiers sur Internet. Il nécessite la présence d'un programme client HTTP à une extrémité et d'un programme serveur HTTP à l'autre extrémité.
Installation silencieuse	Méthode d'installation transparente d'un package logiciel sur un ordinateur, sans qu'aucune intervention de l'utilisateur ne soit requise.
Intervalle d'application des stratégies	Période durant laquelle l'agent applique les paramètres qu'il a reçus du serveur ePolicy Orchestrator. Ces paramètres s'appliquant localement, cet intervalle ne requiert pas de bande passante.

Intervalle de communication agent-serveur (ASCI)	Délai entre deux communications agent-serveur prédéfinies.
Macro	Dans certains programmes, comme les logiciels de traitement de texte, une macro est une série de commandes enregistrées qui peut être stockée, puis rappelée à l'aide d'une simple commande ou en appuyant sur une touche.
Mise à niveau automatique (AutoUpgrade) de l'agent	Processus par lequel l'agent est mis à niveau automatiquement dès qu'une nouvelle version est disponible sur le serveur ePolicy Orchestrator.
Nettoyer, nettoyage	Mesure prise par l'analyseur lorsqu'un *virus*, un *cheval de Troie* ou un *ver* est détecté. L'action de nettoyage peut inclure la suppression du virus d'un fichier et la remise en état fonctionnelle du fichier, la suppression des références au virus des fichiers système, des fichiers système .INI et du registre, l'interruption des processus générés par le virus, la suppression d'une macro ou d'un script Microsoft Visual Basic qui infecte un fichier, la suppression d'un fichier s'il s'agit d'un cheval de Troie ou d'un ver et le changement de nom d'un fichier qui ne peut être nettoyé.
Package d'installation de l'agent	Programme d'installation et tous les autres fichiers requis pour installer l'agent.
Packages de langue de l'agent	Ensemble de fichiers devant être distribués sur les ordinateurs clients pour y afficher l'interface utilisateur de l'agent dans des langues autres que l'anglais.
Pare-feu	Programme qui joue le rôle de filtre entre l'ordinateur et le réseau ou Internet. Il peut analyser tout le trafic qui arrive sur votre ordinateur (trafic entrant) et tout le trafic envoyé par votre ordinateur (trafic sortant). Il analyse le trafic au niveau des paquets et le bloque ou l'autorise en fonction de règles que vous paramétrez.
Priorité d'avertissement	Valeur que vous attribuez à chaque message d'alerte, à titre informatif. Vous disposez des options de priorité : **Critique**, **Majeur**, **Mineur**, **Avertissement** et **Informationnel**.
Programme canular	Programme ne se répliquant pas, susceptible d'inquiéter ou d'importuner les utilisateurs, mais qui n'endommage pas en fait les fichiers ou les données.
Propriétés	Données échangées durant une communication agent-serveur et comprenant des informations au sujet de chaque ordinateur géré (par exemple, matériel et logiciels) et de ses produits gérés (par exemple, paramètres de stratégie spécifiques et numéro de version du produit).
Référentiel	Emplacement où sont stockées les pages de stratégie utilisées pour gérer les produits.
Référentiels de logiciels distribués	Ensemble de sites Web ou d'ordinateurs placés sur le réseau de façon à fournir l'accès aux ordinateurs clients en optimisant la bande passante. Les référentiels distribués stockent les fichiers dont les ordinateurs clients ont besoin pour installer des produits pris en charge et leurs mises à jour.
Répertoire	Dans l'arborescence de la console, liste de tous les ordinateurs à gérer par ePolicy Orchestrator ; lien vers les interfaces principales de gestion de ces ordinateurs.
Serveur de base de données ePolicy Orchestrator	Ordinateur hébergeant la base de données ePolicy Orchestrator. Il peut s'agir de l'ordinateur même sur lequel est installé le serveur ePolicy Orchestrator ou d'un ordinateur distinct.

Serveur ePolicy Orchestrator	Composant principal du logiciel ePolicy Orchestrator.
Site	Dans l'arborescence de la console, ensemble logique d'entités regroupées pour en faciliter la gestion. Les sites peuvent contenir des groupes d'ordinateurs et peuvent être organisés par intervalle d'adresses IP, masque de sous-réseau IP, emplacement, service et autres.
Stratégie	Paramètres de configuration de produits gérés qui sont définis et administrés à partir d'ePolicy Orchestrator.
Tâche	Activité ponctuelle (*analyse à la demande*) ou récurrente (*mise à jour*) qui est planifiée pour s'exécuter aux heures ou aux intervalles spécifiés. Comparer à *Stratégie*.
Tâche d'analyse	Événement d'analyse unique.
Transmission immédiate des événements	Envoi immédiat vers le serveur ePolicy Orchestrator d'événements présentant un degré de gravité minimal spécifié dès qu'un nombre prédéfini d'événements sont disponibles. Cette communication est établie séparément des autres communications agent-serveur.
Utilitaire de rapport d'erreur	Utilitaire spécialement conçu pour suivre et enregistrer dans un fichier journal les défaillances du logiciel McAfee installé sur votre système. Les informations ainsi obtenues peuvent faciliter l'analyse des problèmes.
Ver	Virus qui se propage en créant des copies de lui-même sur d'autres lecteurs, systèmes ou réseaux. Il ne se lie pas à d'autres programmes mais peut modifier, installer ou détruire des fichiers et des programmes.
Virus	Programme contenant du code malveillant pouvant altérer ou détruire des fichiers ou des programmes, capable de se répliquer avec une intervention nulle ou minime de l'utilisateur. Le ou les programmes répliqués se répliqueront à leur tour.
VirusScan Schedule Editor	Vous permet de planifier d'autres mises à jour de définitions de virus et mises à jour logicielles.
Volet de détails supérieur	Dans la console, le volet supérieur droit qui contient les onglets **Stratégies**, **Propriétés** et **Tâches**.

Index

McAfee®

mcafee.com