F-Secure Policy Manager

Guide de l'administrateur

Sommaire

Chapitre

1

Présentation

Sujets :

Policy Manager offre les fonctionnalités suivantes:

- définir des stratégies de sécurité;
- distribuer des stratégies de sécurité;
- installer des applications sur les systèmes locaux et distants;
- surveiller des activités de tous les systèmes dans l'entreprise afin d'assurer la conformité avec les stratégies de l'entreprise et le contrôle centralisé.

Une fois le système configuré, vous pouvez afficher des informations d'état de l'ensemble du domaine géré en un seul et même endroit. De cette façon, vous pouvez facilement vous assurer que l'ensemble du domaine est protégé et modifier les paramètres de protection lorsqu'il y a lieu. Vous pouvez également empêcher les utilisateurs de modifier les paramètres de sécurité et être sûr que la protection est toujours à jour.

Configuration système requise

Cette section indique la configuration requise pour Serveur Policy Manager et Console Policy Manager.

Serveur Policy Manager

Pour installer Serveur Policy Manager, votre système doit correspondre à la configuration requise suivante.

Système d'exploitation:	Microsoft Windows • Microsoft Windows Server 2003 SP1 ou ultérieur (32 bits); éditions Standard, Enterprise, Web Edition ou Small Business Server • Windows Server 2003 SP1 ou ultérieur (64 bits); éditions Standard ou Enterprise • Windows Server 2008 SP1 (32 bits); éditions Standard, Enterprise ou Web Server • Windows Server 2008 SP1 (64 bits); éditions Standard, Enterprise, Web Server, Small Business Server ou Essential Business Server • Windows Server 2008 R2; éditions Standard, Enterprise ou Web Server Linux: • Red Hat Enterprise Linux 4 and 5 • openSUSE Linux 11.2 • SUSE Linux Enterprise Server 9, 10 and 11 • SUSE Linux Enterprise Desktop 10 and 11 • Debian GNU Linux Lenny 5.0 • Ubuntu 8.04 Hardy
Processeur:	Processeur P4 2GHz ou plus rapide. La gestion de plus de 5000 hôtes ou l'utilisation de Web Reporting exige un processeur P4 à 3GHz ou plus rapide.
Mémoire:	512Mo de RAM, 1Go de RAM recommandé. La gestion de plus de 5000 hôtes ou l'utilisation de Web Reporting exige 1Go de RAM.
Espace disque:	5Go d'espace disque libre; au moins 8Go sont recommandés. La quantité d'espace requis sur le disque dur dépend de la taille de l'installation. Outre la configuration décrite ci-dessus, il est recommandé d'allouer environ 1Mo par hôte pour les alertes et les stratégies. Il est difficile de prévoir la quantité réelle d'espace occupé sur le disque par chaque hôte, puisqu'elle dépend de la manière dont les stratégies sont utilisées ainsi que du nombre de fichiers d'installation stockés.

Réseau:	Réseau 10 Mbits La gestion de plus de 5000 hôtes nécessite un réseau à 100 mégabits.

Console Policy Manager

Pour installer Console Policy Manager, votre système doit correspondre à la configuration requise indiquée ici.

Système d'exploitation:	Microsoft Windows: • Windows XP Professionnel (SP2 ou version ultérieure) • Windows Vista (32 ou 64 bits) avec ou sans SP1; éditions Business, Enterprise ou Intégrale • Windows 7 (32 ou 64 bits) ; éditions Professionnel, Entreprise ou Intégrale • Microsoft Windows Server 2003 SP1 ou ultérieur (32 bits); éditions Standard, Enterprise, Web Edition ou Small Business Server editions • Windows Server 2003 SP1 ou ultérieur (64 bits); éditions Standard ou Enterprise • Windows Server 2008 SP1 (32 bits); éditions Standard, Enterprise ou Web Server • Windows Server 2008 SP1 (64 bits); éditions Standard, Enterprise, Web Server, Small Business Server ou Essential Business Server • Windows Server 2008 R2; éditions Standard, Enterprise ou Web Server Linux • Red Hat Enterprise Linux 4 and 5 • openSUSE Linux 11.2 • SUSE Linux Enterprise Server 9, 10 and 11 • SUSE Linux Enterprise Desktop 10 and 11 • Debian GNU Linux Lenny 5.0 • Ubuntu 8.04 Hardy
Processeur:	Processeur P4 2GHz ou plus rapide. La gestion de plus de 5000 hôtes exige un processeur P4 3GHz ou plus rapide.
Mémoire:	512Mo de RAM. La gestion de plus de 5000 hôtes exige 1Go de mémoire.
Espace disque:	200Mo espace libre sur le disque dur.
Affichage:	Ecran 16 bits minimum d'une résolution de 1024x768: écran 32 bits et résolution de 1280x1024 ou supérieure).

Réseau:	Réseau 10 La gestion de plus de 5000 hôtes exige un réseau 100Mbits.

Principaux composants

La puissance de Policy Manager repose sur l'architecture d'administration F-Secure, qui offre une grande évolutivité pour le personnel disséminé et itinérant.

Console Policy Manager

Console Policy Manager fournit une console de gestion centralisée pour assurer la sécurité des hôtes administrés du réseau. Cette console permet à l'administrateur d'organiser le réseau en unités logiques pour partager les stratégies. Ces stratégies sont définies dans Console Policy Manager puis sont diffusées aux postes de travail via Serveur Policy Manager. Console Policy Manager est une application *Java* qui peut être exécutée sur différentes plates-formes. Elle permet notamment d'installer Management Agent à distance sur d'autres postes de travail sans utiliser de scripts de connexion locaux, sans redémarrer l'ordinateur et sans aucune intervention de l'utilisateur final.

Console Policy Manager comporte deux interfaces utilisateur différentes:

- **Mode antivirus**: interface utilisateur optimisée pour la gestion de Client Security et Anti-virus pour station de travail.
- **Mode avancé**: interface utilisateur qui peut être utilisée pour la gestion d'autres produits F-Secure.

Serveur Policy Manager

Serveur Policy Manager est le référentiel des stratégies et des packages logiciels distribués par l'administrateur, et des informations et alertes d'état envoyées par les hôtes administrés. La communication entre Serveur Policy Manager et les hôtes administrés s'établit via le *protocole HTTP* standard, qui assure un fonctionnement optimal aussi bien sur les réseaux locaux (*LAN*) que sur les réseaux étendus (*WAN*).

Management Agent

Management Agent met en application les stratégies de sécurité définies par l'administrateur sur les hôtes administrés et fournit l'interface utilisateur ainsi que d'autres services. Il gère toutes les fonctions d'administration sur les postes de travail locaux, fournit une interface commune à toutes les applications F-Secure et s'articule autour d'une infrastructure de gestion par stratégies.

Web Reporting

Web Reporting est un système Web de création de rapports graphiques à l'échelle de l'entreprise inclus dans Serveur Policy Manager. Il permet de créer rapidement des rapports graphiques basés sur les tendances passées et d'identifier les ordinateurs qui ne sont pas protégés ou qui sont vulnérables aux attaques de nouveaux virus.

Serveur et agent de mise à jour

Serveur et agent de mise à jour sont utilisés pour la mise à jour des définitions de virus et logiciels espions sur les hôtes administrés et sont inclus à Serveur Policy Manager. Agent de mise à jour automatique permet aux utilisateurs d'obtenir les mises à jour des bases de données de définitions de virus ainsi que des données sans avoir à interrompre leur travail pour télécharger les fichiers à partir d'Internet. Il télécharge les fichiers automatiquement en tâche de fond en utilisant la bande passante non utilisée par les autres applications Internet. Si Agent de mise à jour automatique est connecté en permanence à Internet, il reçoit automatiquement les mises à jour de définitions de virus après leur publication par F-Secure.

Fonctions

Certaines fonctions de Policy Manager sont décrites dans la présente section.

Distribution des logiciels

- Installation des produits F-Secure sur des hôtes à partir d'un emplacement central et mise à jour de fichiers exécutables et fichiers de données, y compris les mises à jour de définitions de virus.
- Les mises à jour peuvent s'effectuer de différentes manières
  - A partir d'un CD F-Secure.
  - Sur le poste client à partir du site Web F-Secure. Ces mises à jour peuvent être automatiquement distribuées par Agent de mise à jour automatique, ou récupérées à la demande sur le site Web de F-Secure.
- Console Policy Manager peut être utilisé pour exporter des packages d'installation préconfigurés, qu'il est également possible de transmettre à l'aide d'un logiciel tiers, tel que SMS, ou des outils similaires.

Gestion de la configuration et des stratégies

- Configuration centralisée des stratégies de sécurité. L'administrateur distribue les stratégies sur le poste de travail de l'utilisateur à partir de Serveur Policy Manager. L'intégrité des stratégies est assurée par l'utilisation de signatures numériques.

Gestion des événements

- Rapports à Visionneuse d'événements (journaux locaux et distants), courrier électronique, fichiers de rapport et création de statistiques des événements.
  .

Gestion des performances

- Création de rapports et gestion des statistiques et des données relatives aux performances.

Gestion des tâches

- Gestion de la détection de virus et autres tâches.

Enregistrement du produit

Vous pouvez fournir à F-Secure des informations relatives à l'utilisation de Policy Manager en enregistrant votre produit.

Les questions et réponses suivantes offrent davantage d'informations sur l'enregistrement de votre installation de Policy Manager. Vous devez également consulter les termes de la licence F-Secure (*http://www.f-secure.com/en_EMEA/estore/license-terms/*) et la politique de confidentialité (*http://www.f-secure.com/en_EMEA/privacy.html*).

Pourquoi F-Secure collecte des données?

Nous collectons des informations statistiques sur l'utilisation des produits F-Secure afin d'améliorer notre service. Pour un meilleur service et support F-Secure, vous pouvez nous autoriser à lier ces informations à vos informations de contact. Pour ce faire, veuillez saisir le numéro de client figurant sur votre certificat de licence lors de l'installation de Policy Manager.

Quelles sont les informations envoyées?

Nous collectons des informations qui ne peuvent pas être liés à l'utilisateur final ou à l'utilisation de l'ordinateur. Les informations collectées incluent les versions du produit F-Secure, les versions du système d'exploitation, le nombre d'hôtes gérés et le nombre d'hôtes déconnectés. Ces informations sont ensuite transférées dans un format sécurisé et crypté.

Quel est l'avantage d'envoyer les informations à F-Secure?

Lorsque vous contactez notre support, celui-ci pourra vous fournir une solution à votre problème plus rapidement grâce aux informations collectées. En outre, elles nous permettent également de développer davantage nos produits et services afin qu'ils répondent encore mieux aux besoins de nos clients.

Où sont stockées les informations et qui peut y accéder?

Le données sont stockées dans un centre de données F-Secure hautement sécurisé. Et seul le personnel F-Secure habilité peut accéder aux données.

Gestion par stratégies

Une stratégie de sécurité peut être définie comme l'ensemble des règles précises édictées dans le but de définir les modalités d'administration, de protection et de distribution des informations confidentielles et autres ressources.

L'architecture d'administration de F-Secure exploite les stratégies configurées de manière centralisée par l'administrateur pour un contrôle total de la sécurité dans un environnement d'entreprise. La gestion par stratégies met en œuvre de nombreuses fonctions:

- contrôle et suivi à distance du comportement des produits;
- analyse des statistiques générées par les produits et par Management Agent;
- lancement à distance d'opérations prédéfinies;
- transmission à l'administrateur système des alertes et des notifications émises par les produits.

L'échange d'informations entre Console Policy Manager et les hôtes s'effectue via le transfert des fichiers de stratégie. Il existe trois types de fichiers de stratégie:

- *fichiers de stratégie par défaut* (`.dpf`);
- *fichiers de stratégie de base* (`.bpf`);
- *fichiers de stratégie incrémentielle* (`.ipf`);

La configuration courante d'un produit inclut ces trois types de fichiers.

Fichiers de stratégie par défaut	Le fichier de stratégie par défaut contient les paramètres par défaut d'un produit qui sont appliqués lors de l'installation. Les stratégies par défaut sont utilisées uniquement sur l'hôte. La valeur d'une variable est extraite du fichier de stratégie par défaut lorsque ni le fichier de stratégie de base ni le fichier de stratégie incrémentielle ne contiennent d'entrée correspondante. Les nouvelles éditions des logiciels intègrent également les nouvelles versions du fichier de stratégie par défaut.
Fichiers de stratégie de base	Les fichiers de stratégie de base contiennent les restrictions et les paramètres administratifs de toutes les variables pour tous les produits F-Secure installés sur un hôte donné (grâce à la définition de stratégies au niveau du domaine, un groupe d'hôtes peut partager le même fichier). Le fichier de stratégie de base est signé par Console Policy Manager, ce qui permet de le protéger contre toute modification lorsqu'il est diffusé sur le réseau et stocké dans le système de fichiers d'un hôte. Ces fichiers sont envoyés à partir de Console Policy Manager vers Serveur Policy Manager. L'hôte récupère à intervalles réguliers les nouvelles stratégies créées par Console Policy Manager.
Fichiers de stratégie incrémentielle	Les fichiers de stratégie incrémentielle permettent de stocker les modifications apportées localement à la stratégie de base. Seules sont autorisées les modifications comprises dans les limites définies dans la stratégie de base. Les fichiers de stratégie incrémentielle sont ainsi envoyés à Console Policy Manager à intervalles réguliers afin que l'administrateur puisse visualiser les paramètres et les statistiques en cours.

Base d'informations de gestion (MIB)

La *Base d'informations de gestion* (*MIB*) est une structure hiérarchique de données de gestion utilisée par le système *SNMP* (*Simple Network Management Protocol*).

Dans Policy Manager, la structure MIB permet de définir le contenu des fichiers de stratégie. Chaque variable est associée à un *Identificateur unique* (*OID*) et à une valeur accessible à partir de l'interface *API Stratégie*. Outre les définitions de la base d'informations de gestion (MIB) du système SNMP, la base d'informations de gestion de F-Secure inclut plusieurs extensions nécessaires à une gestion complète par stratégies.

Les catégories suivantes sont définies dans la base d'informations de gestion (MIB) d'un produit

Paramètres	Cette catégorie permet de gérer la station de travail de la même manière qu'un système SNMP. Les produits gérés fonctionnent dans les limites spécifiées ici.
Statistiques	Cette catégorie fournit à Console Policy Manager les statistiques relatives au produit.
Opérations	Deux variables de stratégie gèrent les opérations: (1) une variable pour transmettre à l'hôte l'identificateur de l'opération et (2) une variable pour informer Console Policy Manager des opérations exécutées. La seconde variable est transmise à l'aide des statistiques habituelles; elle accuse réception de toutes les opérations antérieures simultanément. Un éditeur personnalisé destiné à l'édition des opérations est associé à la sous-arborescence et masque les deux variables.
Privé	Les bases d'informations de gestion peuvent également contenir des variables que le produit stocke en vue d'un usage interne entre les sessions. Cela lui évite de recourir à des services externes, tels que les fichiers du Registre de Windows.
Interruptions	Les interruptions sont des messages (notamment des alertes et des événements) envoyés à la console locale, au fichier journal, au processus d'administration à distance, etc. La plupart des produits F-Secure intègrent les types d'interruptions suivants:
	 Info. Informations de fonctionnement normal émises par un hôte.
	 Avertissement. Avertissement émanant de l'hôte.
	 Erreur. Erreur non fatale survenue sur l'hôte.
	 Erreur fatale. Erreur irrécupérable survenue sur l'hôte.
	 Alerte de sécurité. Incident lié à la sécurité survenu sur l'hôte.

Chapitre
2

Installation du produit

Sujets :

Vous y trouverez des instructions pour installer les principaux composants du produit: Serveur Policy Manager et Console Policy Manager.

Problèmes de sécurité

Serveur Policy Manager emploie la technologie de *serveur Web Apache* et *Jetty*. Bien que nous mettions tout en œuvre pour fournir une technologie sûre et à jour, il est conseillé de consulter régulièrement les sites suivants afin d'obtenir des informations sur les technologies Apache et Jetty et leur sécurité.

Les informations les plus récentes sur les problèmes de sécurité relatifs aux systèmes d'exploitation et au serveur Web Apache sont disponibles sur le site Web de CERT: *http://www.cert.org*.

Vous trouverez un document fournissant des conseils sur la manière de sécuriser l'installation du serveur Web Apache à l'adresse *http://www.apache.org/docs/misc/security_tips.html*, ainsi qu'une liste répertoriant les points vulnérables à l'adresse *http://www.apacheweek.com/features/security-13*.

Vous trouverez une liste des rapports de sécurité Jetty à l'adresse *http://docs.codehaus.org/display/JETTY/Jetty+Security*.

👉 **Remarque:** Vous trouverez des informations importantes sur l'installation et la sécurité dans les notes de publication. Lisez ces notes attentivement.

Installation de Policy Manager dans des environnements à haute sécurité

Policy Manager est essentiellement destiné à la gestion de produits antivirus F-Secure dans des réseaux d'entreprise internes. Il ne doit pas être utilisé sur des réseaux publics, tels qu'Internet.

👉 **Remarque:** Lors de l'installation de Policy Manager dans des environnements à haute sécurité, il convient de s'assurer que le *port d'administration* (par défaut le port 8080) et le *port Hôte* (par défaut le port 80) ne sont pas visibles sur Internet.

Fonctions de sécurité intégrées

Policy Manager possède des fonctions de sécurité intégrées qui garantissent la détection de toute modification de la structure du domaine de stratégie et des données de stratégie. Plus important encore, elles interdisent le déploiement de modifications non autorisées sur les hôtes administrés. Ces deux fonctions reposent sur une paire de clés d'administration qui n'est accessible qu'aux administrateurs. Dans la plupart des cas, ces fonctions, reposant sur de puissantes signatures numériques, fourniront l'équilibre idéal entre facilité d'utilisation et sécurité à la plupart des installations antivirus. Par contre, les fonctions suivantes peuvent exiger une configuration supplémentaire dans des environnements à haute sécurité:

- Par défaut, tous les utilisateurs peuvent accéder en lecture seule à Serveur Policy Manager, mais ils peuvent uniquement consulter les données d'administration. Cette méthode permet de partager aisément les informations avec les utilisateurs ne disposant pas de droits d'administration complets. Plusieurs utilisateurs peuvent ouvrir simultanément une session en lecture seule, afin de surveiller l'état du système sans perturber les autres administrateurs ou les hôtes administrés.
- Pour faciliter la migration vers de nouvelles clés d'administration, il est possible de signer de nouveau la structure du domaine de stratégie et les données de stratégie à l'aide d'une nouvelle paire de clés ou d'une paire de clés existante. Si cette opération est effectuée accidentellement, ou volontairement par un utilisateur non autorisé, l'utilisateur autorisé remarquera la modification lorsqu'il tentera d'ouvrir une nouvelle session dans Policy Manager. Dans le pire des cas, l'utilisateur autorisé devra restaurer des sauvegardes afin d'éliminer les éventuelles modifications apportées par l'utilisateur non autorisé. Dans tous les cas, les modifications de la structure du domaine de stratégie et des données de stratégie seront détectées, et il est impossible de distribuer ces modifications aux hôtes administrés sans la paire de clés d'origine.

Ces deux fonctions peuvent s'avérer indésirables dans un environnement à haute sécurité, où il doit même être interdit de visualiser les données d'administration. Console Policy Manager et Serveur Policy Manager peuvent également être installés sur le même ordinateur, avec un accès illimité à l'hôte local. Un accès administrateur à distance à Console Policy Manager peut être prévu à l'aide d'un produit de connexion de bureau à distance sécurisé.

Web Reporting dans des environnements à haute sécurité

Web Reporting est destiné à la génération de rapports graphiques sur les alertes et l'état de la protection antivirus de Client Security par exemple, dans des réseaux d'entreprise internes. F-Secure ne recommande pas d'employer Web Reporting sur des réseaux publics tels qu'Internet.

L'alternative aux environnements à haute sécurité consiste à limiter l'accès à Web Reporting à l'hôte local au cours de l'installation. Après cela, seule la personne ayant un accès physique à l'hôte local peut utiliser Web Reporting.

Ordre d'installation

Vous devez installer les composants Policy Manager dans un ordre spécifique lorque vous les installez sur des ordinateurs différents.

Pour installer Policy Manager, procédez dans l'ordre indiqué ci-dessous, sauf si vous installez Serveur Policy Manager et Console Policy Manager sur le même ordinateur. Dans ce dernier cas, le programme d'installation installe tous les composants au cours de la même opération:

1. Serveur Policy Manager,
2. Console Policy Manager,
3. applications du points administré.

Installation de Serveur Policy Manager

Cette section contient des instructions pour l'installation de Serveur Policy Manager.

Pour installer Serveur Policy Manager, vous avez besoin d'un accès physique au serveur.

Serveur Policy Manager est le lien entre Console Policy Manager et les hôtes gérés. Il constitue aussi le référentiel pour les stratégies et les logiciels distribués par l'administrateur, et pour les informations de statut et les alertes envoyées par les hôtes gérés.

La communication entre Serveur Policy Manager et d'autres composants peut être établie via le protocole standard HTTP, qui assure un fonctionnement optimal aussi bien sur les réseaux locaux (LAN) que sur les réseaux longue distance.

Les informations stockées par Serveur Policy Manager incluent les fichiers suivants:

- la structure du domaine de stratégie;
- les données de stratégie, c'est-à-dire les informations de stratégie réelles liées à chaque domaine de stratégie ou à chaque hôte;
- les fichiers de stratégie de base créés à partir des données de stratégie;
- les informations d'état, notamment les fichiers de stratégie incrémentielle, les alertes et les rapports;
- les demandes d'auto-enregistrement envoyées par les hôtes;
- les packages d'installation des produits et de mise à jour des bases de données de définitions de virus;
- les données de tendances statistiques et historiques sur les hôtes.

Télécharger et exécuter le package d'installation

La première étape d'installation de Policy Manager consiste à télécharger et à exécuter le package d'installation.

Pour commencer l'installation du produit:

1. Téléchargez le package d'installation sur le site *www.f-secure.com/webclub*.
   Vous trouverez le fichier dans la section **Téléchargement** de la page **Policy Manager**.
2. Cliquez deux fois sur le fichier exécutable pour lancer l'installation.
   L'installation démarre.
3. Sélectionnez la langue d'installation dans le menu déroulant, puis cliquez sur **Suivant** pour continuer.
4. Prenez connaissance du contrat de licence, puis sélectionnez **J'accepte le contrat** et cliquez sur **Suivant** pour poursuivre.

Sélection des composants à installer

La prochaine étape consiste à sélectionner les composants du produit à installer.

Pour continuer l'installation du produit:

1. Sélectionnez les composants à installer et cliquez sur **Suivant** pour poursuivre.
   - Sélectionnez Serveur Policy Manager et Console Policy Manager pour les installer sur le même ordinateur.
   - Sélectionnez Serveur Policy Manager si vous voulez installer Console Policy Manager sur un autre ordinateur.
2. Choisissez le dossier de destination, puis cliquez sur **Suivant**.
   Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Si vous souhaitez installer le produit dans un répertoire différent, utilisez la fonction **Parcourir** et sélectionnez un nouveau répertoire.

> **Remarque:** Si Management Agent est installé sur le même ordinateur, cette fenêtre ne s'affichera pas.

3. Entrez votre numéro de client et cliquez sur **Suivant**.

   Vous trouverez ce numéro sur le certificat de licence fourni avec le produit.

4. Si le programme d'installation ne détecte aucune installation précédente de Policy Manager lors de la configuration, un message vous demande de confirmer qu'une installation précédente du produit existe:

   - Si une version précédente a été installée, sélectionnez **Une installation de F-Secure Policy Manager existe déjà**. Saisissez le chemin du répertoire de communication du programme Policy Manager installé. Le contenu de ce répertoire est copié sous le `<répertoire d'installation du serveur>\commdir\` (répertoire de communication sous le répertoire d'installation de Serveur Policy Manager), et ce répertoire sera utilisé par Serveur Policy Manager comme référentiel. Vous pouvez utiliser le répertoire `commdir` précédent comme sauvegarde, ou vous pouvez le supprimer une fois que vous avez vérifié que Serveur Policy Manager est correctement installé.
   - Si aucune version précédente n'a été installée, sélectionnez **Je n'ai pas déjà installé F-Secure Policy Manager**. Aucun répertoire `commdir` ne sera requis, et un répertoire `commdir` sera créé dans l'emplacement par défaut (sous `<répertoire d'installation de F-Secure Policy Manager 5>\commdir`).

5. Cliquez sur **Suivant** pour poursuivre.
6. Indiquez si vous souhaitez conserver les paramètres existants ou les modifier:

   > **Remarque:** Cette boîte de dialogue s'affiche uniquement si une installation précédente de Serveur Policy Manager a été détectée sur l'ordinateur.

   - Par défaut, le programme d'installation conserve les paramètres existants. Sélectionnez cette option si vous avez manuellement mis à jour la configuration de Serveur Policy Manager. Cette option conserve automatiquement les ports d'administration, d'hôte et de génération de rapports Web existants.
   - Si vous souhaitez changer les ports d'une installation précédente, sélectionnez l'option **Modifier les paramètres**. Cette option remplace la configuration modifiée et restaure les valeurs par défaut des paramètres.

7. Cliquez sur **Suivant** pour poursuivre.
8. Sélectionnez les modules Serveur Policy Manager à activer:

   - Le module **Hôte** est utilisé pour la communication avec les hôtes. Le port par défaut est 80.
   - Le module **Administration** est utilisé pour la communication avec Console Policy Manager. Le port HTTP par défaut est 8080.

     > **Remarque:** Si vous voulez modifier le port de communication par défaut, vous devez également modifier le paramètre **Numéro de port HTTP** dans Console Policy Manager.

     Par défaut, l'accès au module **Administration** est restreint à l'ordinateur local. C'est le mode d'utilisation du produit le plus sécurisé. En cas de connexion via un réseau, il est conseillé d'envisager de sécuriser la communication à l'aide de F-Secure SSH.
   - Le module **Web Reporting** est utilisé pour la communication avec Web Reporting. Indiquez si vous souhaitez l'activer. Web Reporting se connecte au module **Administration** via un socket local pour rechercher les données du serveur. Le port par défaut est 8081.

     Par défaut, l'accès à Web Reporting est également autorisé depuis les autres ordinateurs. Si vous souhaitez uniquement un accès depuis cet ordinateur, sélectionnez **Restreindre l'accès à l'ordinateur local**.

9. Cliquez sur **Suivant** pour poursuivre.

10. Sélectionnez le(s) module(s) d'installation de produits dans la liste des modules disponibles, puis cliquez sur **Suivant** pour poursuivre.

Réalisation de l'installation du produit

La prochaine étape consiste à effectuer l'installation du produit.

1. Examinez les modifications que le programme d'installation va apporter, puis cliquez sur **Démarrer** pour lancer l'installation des composants sélectionnés.
   Lorsque le programme d'installation est terminé, il indique si tous les composants ont été installés correctement.
2. Cliquez sur **Terminer** pour finaliser l'installation.
3. Redémarrez votre ordinateur si un message vous invite à le faire.

Vérification de la réussite de l'installation

La prochaine étape consiste à vérifier que le produit a bien été installé.

Pour déterminer si l'installation a réussi:

1. Ouvrez un navigateur Web sur l'ordinateur où Serveur Policy Manager a été installé.
2. Entrez l'adresse `http://localhost:8080` (si vous avez utilisé le numéro de port d'administration par défaut lors de l'installation), puis appuyez sur Entrée.
   Si l'installation du serveur a réussi, une page de bienvenue s'affichera.

Remarque: Serveur Policy Manager commence à servir des hôtes uniquement après que Console Policy Manager a initialisé la structure du répertoire de `communication`, ce qui s'effectue automatiquement lors de la première exécution de Console Policy Manager.

Modification du chemin d'accès au répertoire de communication

Si le lecteur réseau sur lequel le répertoire de communication se trouve manque d'espace disponible, vous pouvez changer son emplacement en suivant les instructions ci-dessous.

Pour modifier le chemin d'accès au répertoire de communication:

1. Choisissez un nouveau chemin réseau sur un lecteur offrant plus d'espace.
2. Créez le chemin et vérifiez que l'utilisateur Service local bénéficie de droits d'accès Contrôle total sur tous les répertoires du chemin.
3. Arrêtez le service Serveur Policy Manager.
4. Copiez toute la structure de répertoires de l'ancien chemin `commdir` vers le nouveau chemin.
5. Changez la valeur des directives `CommDir` et `CommDir2` dans `httpd.conf` (situé dans le répertoire `<Répertoire d'installation de Policy Manager Server>\conf\`).

   La configuration par défaut est la suivante:

   ```
   CommDir "C:\Program Files\F-Secure\Management Server 5\CommDir"
   ```

   ```
   CommDir2 "C:\Program Files\F-Secure\Management Server 5\CommDir"
   ```

   Si vous voulez remplacer l'emplacement du répertoire de communication par `E:\CommDir`, modifiez les paramètres de sorte qu'ils reflètent cette configuration. Par exemple:

   ```
   CommDir "E:\CommDir"
   ```

   ```
   CommDir2 "E:\CommDir"
   ```
6. Démarrer le service Serveur Policy Manager.
7. Vérifiez que tout fonctionne encore correctement.
8. Supprimez les anciens fichiers `commdir`.

Installation de Console Policy Manager

Cette section contient des instructions pour l'installation de Console Policy Manager.

Console Policy Manager peut fonctionner dans deux modes:

- Mode administrateur: vous pouvez utiliser toutes les fonctionnalités de Console Policy Manager.
- Mode Lecture seule: permet de visualiser les informations de Console Policy Manager, mais pas d'accomplir des tâches administratives. Ce mode peut par exemple être utile pour les agents d'un service d'assistance.

Les connexions en mode Administrateur et Lecture seule peuvent s'effectuer à l'aide de la même installation de la console. Les sections suivantes expliquent comment exécuter le programme d'installation de Console Policy Manager à partir du package d'installation, ainsi que la manière de choisir le mode d'installation lors de la première exécution de la console. La configuration est identique pour les deux modes et il est possible d'ajouter un nouvel administrateur et des connexions en lecture seule après le premier démarrage.

Télécharger et exécuter le package d'installation

La première étape d'installation de Policy Manager consiste à télécharger et à exécuter le package d'installation.

Pour commencer l'installation du produit:

1. Téléchargez le package d'installation sur le site *www.f-secure.com/webclub*.
   Vous trouverez le fichier dans la section **Téléchargement** de la page **Policy Manager**.
2. Cliquez deux fois sur le fichier exécutable pour lancer l'installation.
   L'installation démarre.
3. Sélectionnez la langue d'installation dans le menu déroulant, puis cliquez sur **Suivant** pour continuer.
4. Prenez connaissance du contrat de licence, puis sélectionnez **J'accepte le contrat** et cliquez sur **Suivant** pour poursuivre.

Sélection des composants à installer

La prochaine étape consiste à sélectionner les composants du produit à installer.

Pour poursuivre l'installation du produit:

1. Sélectionnez les composants à installer (Console Policy Manager) et cliquez sur **Suivant** pour poursuivre.
2. Choisissez le dossier de destination, puis cliquez sur **Suivant**.
   Nous vous recommandons d'utiliser le répertoire d'installation par défaut. Si vous souhaitez installer le produit dans un répertoire différent, vous pouvez cliquer sur **Parcourir** et sélectionnez un autre répertoire.
3. Cliquez sur **Suivant** pour poursuivre.
4. Définissez l'adresse du **serveur F-Secure Policy Manager** et le numéro du **port d'administration**, puis cliquez sur **Suivant** pour poursuivre.

   Remarque: Selon la méthode d'installation choisie, cette fenêtre n'est pas toujours affichée.

Réalisation de l'installation du produit

La prochaine étape consiste à effectuer l'installation du produit.

1. Examinez les modifications que le programme d'installation va apporter, puis cliquez sur **Démarrer** pour lancer l'installation des composants sélectionnés.
   Lorsque le programme d'installation est terminé, il indique si tous les composants ont été installés correctement.

2. Cliquez sur **Terminer** pour finaliser l'installation.
3. Redémarrez votre ordinateur si un message vous invite à le faire.

Exécuter Console Policy Manager

La dernière étape de l'installation du produit consiste à exécuter Console Policy Manager la première fois.

Pour ce faire Console Policy Manager:

1. Exécutez Console Policy Manager en sélectionnant **Démarrer** ➤ **Programmes** ➤ **F-Secure Policy Manager Console** ➤ **F-Secure Policy Manager Console**.

   Lorsque l'application Console Policy Manager est exécutée pour la première fois, l'**Assistant d'installation de la console** collecte les informations requises pour créer une connexion initiale au serveur. La première page de l'Assistant d'installation de Console Policy Manager résume le processus d'installation.
2. Cliquez sur **Suivant** pour poursuivre.
3. Sélectionnez le mode d'utilisation correspondant à vos besoins:
   - **Mode Administrateur**: active toutes les fonctions d'administration.
   - **Mode Lecture seule**: permet de consulter les données d'administration, mais pas d'apporter des modifications. Si vous sélectionnez le **Mode Lecture seule**, vous ne pourrez pas administrer les hôtes. Pour passer en **Mode Administrateur**, vous devrez disposer des clés d'administration `admin.pub` et `admin.prv`.
4. Cliquez sur **Suivant** pour poursuivre.
5. Saisissez l'adresse du serveur Serveur Policy Manager utilisé pour la communication avec les hôtes gérés, puis cliquez sur **Suivant** pour poursuivre.
6. Entrez le chemin d'accès au répertoire où vous souhaitez stocker les fichiers de clé privée et de clé publique de l'administrateur.

   Par défaut, les fichiers de clé sont enregistrés dans le répertoire d'installation de Console Policy Manager: `Program Files\F-Secure\Administrator`.
7. Cliquez sur **Suivant** pour poursuivre.

   👉 **Remarque:** Si la paire de clés n'existe pas encore, elle sera créée plus tard, au cours du processus d'installation.
8. Déplacez votre curseur dans la fenêtre afin d'initialiser le facteur aléatoire utilisé par le générateur du jeu de clés d'administration.

   L'utilisation des déplacements de la souris assure que le facteur de l'algorithme de génération de jeu de clés est suffisamment aléatoire.

   Lorsque l'indicateur de progression atteint 100%, la boîte de dialogue **Phrase de cryptage** s'affiche automatiquement.
9. Entrez une phrase de cryptage qui protège votre clé privée d'administration.
10. Confirmez cette phrase dans la zone **Confirmer la phrase de cryptage** et cliquez sur **Suivant**.
11. Cliquez sur **Terminer** pour terminer le processus de configuration.
    Console Policy Manager génère la paire de clés d'administration. Une fois le jeu de clés créé, Console Policy Manager démarre.

    L'assistant d'installation crée le groupe d'utilisateurs `FSPM users`. L'utilisateur qui avait ouvert une session et qui a procédé à l'installation est automatiquement ajouté à ce groupe. Pour autoriser un autre utilisateur à exécuter Policy Manager, vous devez l'ajouter manuellement au groupe d'utilisateurs `FSPM users`.

Console Policy Managerdémarre en mode **antivirus**, qui constitue une interface utilisateur optimisée pour la gestion de Client Security, de Anti-virus pour station de travail et de Anti-virus pour serveurs Windows. Si vous comptez utiliser Console Policy Manager pour gérer un autre produit F-Secure, vous devez utiliser

l'interface utilisateur en **Mode avancé**. Vous pouvez y accéder en sélectionnant **Affichage** ➤ **Mode avancé** dans le menu.

Lorsque vous configurez les stations de travail, vous devez y installer une copie du fichier de clé `admin.pub` (ou leur donner l'accès à ce fichier). Si vous installez à distance les produits F-Secure sur des postes de travail, à l'aide de Policy Manager, une copie du fichier de clé `admin.pub` y est automatiquement installée. Par contre, si vous effectuez l'installation à partir d'un CD, vous devez transférer manuellement une copie du fichier de clés `admin.pub` sur les postes de travail. La méthode la plus avantageuse et la plus sûre consiste à copier le fichier `admin.pub` sur une disquette, puis à l'installer sur les postes de travail à partir de cette disquette. Vous pouvez également placer le fichier `admin.pub` dans un répertoire accessible à tous les hôtes qui seront configurés avec des produits F-Secure administrés à distance.

Modification du chemin d'accès au navigateur Web

Console Policy Manager obtient le chemin d'accès au navigateur Web par défaut lors du processus d'installation.

Si vous voulez modifier ce chemin d'accès:

1. Sélectionnez **Outils** ➤ **Préférences** dans le menu.
2. Sélectionnez l'onglet **Emplacements** et entrez le nouveau chemin d'accès au fichier.

Désinstallation du produit.

Suivez les étapes ci-dessous pour désinstaller des composants Policy Manager.

Pour désintaller des composants Policy Manager:

1. Ouvrez le menu **Démarrer** Windows et accédez au **Panneau de configuration**.
2. Sélectionnez **Ajout/Suppression de programmes**.
3. Choisissez le composant à désinstaller (Console Policy Manager ou Serveur Policy Manager), puis cliquez sur **Ajouter/Supprimer**.
   La boîte de dialogue **Désinstallation** de F-Secure s'affiche.
4. Cliquez sur **Démarrer** pour lancer la désinstallation.
5. Au terme de la désinstallation, cliquez sur **Fermer**.
6. Recommencez les étapes ci-dessus si vous voulez désinstaller d'autres composants Policy Manager.
7. Une fois que vous avez désinstallé les composants, quittez **Ajout/Suppression de programmes**.
8. Il est recommandé de redémarrer l'ordinateur après la désinstallation.

   Le redémarrage est nécessaire pour nettoyer les fichiers restant sur l'ordinateur après la désinstallation et avant les installations suivantes des mêmes produits F-Secure.

Chapitre
3

Utilisation de Console Policy Manager

Sujets :

Console Policy Manager est une console d'administration à distance destinée aux produits de sécurité les plus courants de F-Secure. Elle fournit une plate-forme commune à toutes les fonctions de gestion de la sécurité requises dans un réseau d'entreprise.

Présentation

Cette section fournit des informations générales sur Console Policy Manager.

L'environnement conceptuel de Console Policy Manager consiste en plusieurs hôtes pouvant être regroupés en domaines de stratégie. Les stratégies sont orientées hôte. Même dans un environnement multi-utilisateurs, tous les utilisateurs d'un hôte donné partagent des paramètres communs.

Un administrateur peut créer différentes stratégies de sécurité pour chaque hôte ou une stratégie unique pour plusieurs hôtes. La stratégie peut être distribuée via un réseau à des stations de travail, des serveurs et des passerelles de sécurité.

Avec Console Policy Manager, vous pouvez:

- configurer les valeurs des attributs des produits gérés;
- configuration des droits des utilisateurs à afficher ou modifier les valeurs des attributs définies à distance par l'administrateur
- regroupement des hôtes administrés sous des domaines de stratégie partageant des valeurs d'attributs communes
- administration simplifiée des hiérarchies de domaines et des hôtes
- création de définitions de stratégie signées, y compris les valeurs d'attributs et les restrictions
- affichage des informations d'état
- gestion des alertes
- gérer les rapports d'analyse de F-Secure Anti-virus.
- gestion des installations distantes
- visualiser des rapports au format HTML ou exporter des rapports vers différents formats.

Console Policy Manager génère la définition de stratégie et affiche l'état et les alertes. Chaque hôte administré dispose d'un module (Management Agent) responsable de l'exécution de la stratégie sur l'hôte.

Console Policy Manager reconnaît deux types d'utilisateurs: les administrateurs et les utilisateurs en mode Lecture seule.

L'administrateur a accès à la clé privée d'administration. Cette clé est stockée dans un fichier que plusieurs utilisateurs peuvent partager en fonction de leurs droits d'administration. L'administrateur utilise Console Policy Manager pour définir les stratégies de différents domaines et hôtes individuels.

En mode Lecture seule, l'utilisateur peut:

- afficher les stratégies, les statistiques, les informations d'état relatives aux opérations, les numéros de version des produits installés, les messages d'alerte et les rapports
- Modifier les propriétés de Console Policy Manager, car son installation est basée sur l'utilisateur et que les modifications ne peuvent être appliquées aux autres utilisateurs.

Dans le mode Lecture seule, l'utilisateur ne peut pas effectuer les tâches suivantes:

- modifier la structure des domaines ou les propriétés des domaines et des hôtes
- modifier les paramètres des produits
- exécuter des opérations
- installer des produits
- enregistrer des données de stratégie
- distribuer des stratégies
- supprimer des messages d'alerte ou des rapports.

Il ne peut y avoir qu'une seule connexion à Serveur Policy Manager en mode Administrateur à la fois. Cependant, il peut y avoir plusieurs connexions en lecture seule simultanées à Serveur Policy Manager.

Informations et tâches de base

Les sections suivantes décrivent la procédure d'ouverture de Console Policy Manager, ses commandes de menu et ses tâches de base.

Ouverture de session

Lorsque vous démarrez Console Policy Manager, la bôite de dialogue **Ouverture de session** s'affiche.

👉 **Astuce:** Vous pouvez cliquer sur **Options** pour agrandir la boîte de dialogue et afficher davantage d'options.

Vous pouvez utiliser la boîte de dialogue **Ouverture de session** pour sélectionner des connexions définies. Chaque connexion s'accompagne de ses propres préférences, ce qui facilite l'administration de plusieurs serveurs avec une seule instance de Console Policy Manager.

Il est également possible de définir plusieurs connexions multiples à un seul serveur. Une fois la connexion sélectionnée, entrez la phrase de cryptage de Console Policy Manager. Il s'agit de la phrase de cryptage définie lors de l'installation du programme, et non de votre mot de passe d'administrateur réseau.

Vous pouvez démarrer le programme en mode Lecture seule, auquel cas vous n'avez pas besoin d'entrer une phrase de cryptage. Le cas échéant, cependant, vous ne pourrez effectuer aucune modification.

L'assistant d'installation crée la connexion initiale, qui figure par défaut dans la zone **Connexions:**. Pour ajouter d'autres connexions, cliquez sur **Ajouter** ou pour modifier une connexion existante, cliquez sur **Modifier**. Ces deux options sont disponibles quand la boîte de dialogue est agrandie.

Notez qu'il est possible de copier des connexions existantes. Vous pouvez ainsi définir aisément plusieurs connexions au même serveur, en employant des paramètres légèrement différents en vue d'utilisations diverses. Par exemple, vous pouvez utiliser une connexion existante comme modèle, puis tester différents paramètres de connexion sur la nouvelle copie, sans influer sur les paramètres d'origine.

Propriétés de connexion

Les propriétés de connexion sont définies lors de l'ajout d'une nouvelle connexion ou de la modification d'une connexion existante.

La liaison au référentiel de données est définie comme l'URL HTTP de Serveur Policy Manager.

Le champ **Nom** permet de définir le nom que portera la connexion dans le champ **Connexion:** de la boîte de dialogue **Connexion**. Si le champ **Nom** reste vide, l'URL ou le chemin d'accès s'affiche.

Les chemins **Fichier de clé publique** et **Fichier de clé privée** indiquent quel jeu de clés d'administration doit être utilisé pour la connexion en question. Si les fichiers de clé spécifiés n'existent pas, Console Policy Manager génère un nouveau jeu de clés.

Modification des préférences de communication

Dans les préférences de communication, vous pouvez définir la fréquence d'interrogation du serveur pour obtenir des informations sur son état, ainsi qu'une limite après laquelle les hôtes sont considérés comme déconnectés.

La boîte de dialogue **Propriétés de connexion** s'ouvre (par exemple en cliquant sur **Options** sur la boîte de dialogue **Ouverture de session**).

Pour modifier les préférences de communication:

1. Sélectionnez l'onglet **Communication**.
2. Modifiez l'**Etat de connexion de l'hôte** si nécessaire.

   Etat de connexion de l'hôte contrôle quand les hôtes sont considérés comme déconnectés de Policy Manager. Tous les hôtes qui n'ont pas contacté Serveur Policy Manager dans l'intervalle défini sont

considérés comme déconnectés. Les hôtes déconnectés sont signalés par une icône de notification dans l'arborescence, et ils sont placés dans la liste **Hôtes déconnectés** de la vue de l'état du **domaine**.

Remarque: Il est possible de définir un intervalle de moins d'un jour en entrant un nombre à décimales dans le champ de saisie. Par exemple, si vous entrez une valeur de `0,5`, tous les hôtes qui n'ont pas contacté le serveur dans les 12 heures sont considérés comme déconnectés. Les valeurs inférieures à un jour ne servent normalement qu'à des fins de dépannage. Dans un environnement traditionnel, certains hôtes sont naturellement déconnectés du serveur de temps à autre. Par exemple, il se peut qu'un ordinateur portable soit incapable d'accéder quotidiennement au serveur, mais dans la plupart des cas, ce comportement est tout à fait acceptable.

3. Cliquez sur **Options d'intervalles d'interrogation** pour modifier les intervalles d'interrogation. La boîte de dialogue **Intervalles d'interrogation** s'affiche.
4. Modifiez les intervalles d'interrogation de sorte qu'ils correspondent à votre environnement.

   Le choix du protocole de communication affecte les intervalles d'interrogation par défaut. Si vous ne souhaitez pas recevoir certaines informations d'administration, désactivez complètement les récupérations inutiles. Pour ce faire, décochez l'élément de récupération que vous souhaitez désactiver. Cependant, l'interrogation automatique ne doit être désactivée qu'en cas de problèmes de performances. L'option **Désactiver toutes les interrogations** permet de désactiver l'ensemble des éléments d'interrogation. Que l'interrogation automatique soit désactivée ou non, les opérations d'actualisation manuelle peuvent servir à actualiser les informations sélectionnées.

Après le démarrage de Console Policy Manager, ces paramètres peuvent être modifiés normalement depuis la vue **Préférences**.

Client Security - Administration

Lorsque vous lancez Console Policy Manager, l'interface utilisateur en mode **antivirus** simplifié s'ouvre.

Ce mode est optimisé pour l'administration de Client Security. En utilisant l'interface utilisateur en mode **antivirus**, vous pouvez réaliser la plupart des tâches de gestion de Client Security ou de Anti-virus pour station de travail.

Vous devriez être en mesure de réaliser la plupart des tâches avec l'interface utilisateur en mode **antivirus**. En revanche, si vous devez administrer des produits autres que Client Security, vous devrez utiliser l'interface utilisateur en **mode avancé**.

Interface utilisateur en mode avancé

Pour utiliser toutes les fonctionnalités disponibles dans Console Policy Manager, vous devez basculer sur l'interface utilisateur en **Mode avancé**.

Pour ouvrir l'interface utilisateur en **mode avancé**, sélectionnez **Affichage** ➤ **Mode avancé**.

Arborescence du domaine de stratégie

Vous pouvez effectuer des actions pour les domaines de stratégie et les hôtes dans l'arborescence du **domaine de stratégie**.

Vous pouvez effectuer les actions suivantes dans l'arborescence du **domaine de stratégie**:

- Ajouter un nouveau domaine de stratégie (cliquez sur l'icône  , située dans la barre d'outils). Pour créer un nouveau domaine de stratégie vous devez avoir sélectionné un domaine parent.
- Ajouter un nouvel hôte (cliquez sur l'icône ).
- Rechercher un hôte.
- Afficher les propriétés d'un domaine ou d'un hôte. Les noms attribués à chaque hôte et domaine doivent être sans ambiguïté.

- Importer des hôtes auto
- Détecter automatiquement des hôtes d'un domaine Windows.
- Supprimer des hôtes ou des domaines.
- Déplacer des hôtes ou des domaines à l'aide des fonctions Couper et Coller.
- Exporter un fichier de stratégie.

Une fois le domaine ou l'hôte sélectionné, vous pouvez accéder à ces commandes depuis le menu **Edition**.

Les domaines désignés dans ces commandes ne sont pas des domaines WindowsNT ni DNS. Les domaines de stratégie sont des groupes d'hôtes ou de sous-domaines disposant d'une stratégie de sécurité similaire.

Contenu de l'interface utilisateur en Mode avancé

La fonction de la zone principale de l'application dans l'interface utilisateur en **Mode avancé** change en fonction de l'onglet ouvert.

- Onglet **Stratégie**: vous permet de définir la valeur d'une variable de stratégie. Toutes les modifications concernent l'hôte ou le domaine de stratégie sélectionné. Un éditeur par défaut est prédéfini pour chaque type de variable de stratégie. L'éditeur s'affiche lorsque vous sélectionnez le type de variable sous l'onglet **Stratégie**. Certains nœuds non terminaux, tables et sous-arborescences peuvent être associés à des éditeurs personnalisés spécifiques. Ces éditeurs personnalisent Console Policy Manager pour chaque produit installé. Vous pouvez également utilisé les **Editeurs de restriction**, qui s'ouvrent dans la zone principale de l'application ou sous la forme d'une boîte de dialogue distincte.
- Onglet **Etat**: vous permet d'afficher les paramètres qui représentent les modifications locales signalées par l'hôte et les statistiques.
- **Alertes**: quand une alerte est sélectionnée dans l'onglet **Alertes**, les détails de l'alerte s'affichent.
- **Rapports**: quand un rapport est sélectionné dans l'onglet **Rapports**, les détails de celui-ci s'affichent.
- Onglet **Installation**: vous pouvez afficher et modifier les informations d'installation.

L'arborescence traditionnelle de la base de données **MIB**Console Policy Manager contient tous les paramètres/activités (stratégie) et les paramètres/statistiques (état) dans une arborescence **MIB** spécifique à un composant du produit.

Utilisation de l'aide

Dans la plupart des cas, les champs de la zone principale de l'application fournissent les mêmes textes d'aide que les nœuds de l'arborescence **MIB**. En outre, chaque onglet possède un texte d'aide spécifique. Ce texte suit les clics de souris (tous les onglets ainsi que les éditeurs de stratégies et d'état) et l'activation des zones (uniquement en cas de sélection de l'onglet **Stratégie**). Vous pouvez cliquer sur l'intitulé d'une zone ou dans la zone de saisie pour activer le texte d'aide correspondant.

Modification des paramètres de stratégie

Vous pouvez modifier les paramètres de stratégie dans la zone principale de l'application.

Sélectionnez un produit (ex. Management Agent) et l'onglet **Stratégie**. Console Policy Manager affichera un volet Affichage produit pour le produit sélectionné et contiendra les paramètres les plus fréquemment utilisés ainsi que les éditeurs de restriction de l'arborescence **MIB**, dans les catégories ci-après:

- **Communication**: paramètres relatifs aux alertes.
- **Alertes**: paramètres relatifs aux alertes.
- **Transmission des alertes**.
- **Certificats**: définition de certificats approuvés.
- **Répertoire des certificats**: définition des paramètres des répertoires où les certificats sont stockés.
- **A propos de**: contient un lien vers F-Secure Web Club.

Vous pouvez modifier les paramètres de stratégie de manière normale et employer le paramètre de restriction (final, masqué) pour définir les droits d'accès des utilisateurs.

Utilisation du menu contextuel pour les paramètres de stratégie

La plupart des zones de saisie de la zone principale de l'application comprennent un menu contextuel (activé par un clic du bouton droit de la souris).

Le menu contextuel contient les commandes suivantes: **Aller à**, **Effacer valeur**, **Forcer valeur** et **Afficher les valeurs du domaine**.

Raccourci vers le nœud de l'arborescence MIB

Il est parfois utile de savoir quel paramètre de l'arborescence **MIB** sera modifié en cas d'édition d'un élément spécifique. Sélectionnez l'élément de menu **Aller à** pour afficher le noeud de l'arborescence **MIB** correspondant.

Notez que, dans la plupart des cas, l'arborescence **MIB** fournit davantage de paramètres. Ceux-ci sont toutefois moins fréquemment utilisés. Par exemple, elle permet d'éditer les restrictions des paramètres de stratégie qui ne contiennent pas directement d'éditeurs de restrictions.

Effacer

La commande **Effacer** fonctionne de la même manière que dans l'arborescence **MIB**. Lorsque la valeur actuelle est effacée, la zone affiche la valeur héritée (de couleur grise) ou est vide. La commande **Effacer** n'est disponible que si une valeur a été définie pour le domaine ou l'hôte actuellement sélectionné.

Forcer la valeur

La commande **Forcer la valeur** n'est disponible que si un domaine de stratégie est sélectionné. Vous pouvez forcer le paramètre du domaine actuel à être également actif dans tous les sous-domaines et sur tous les hôtes. En pratique, cette action efface le paramètre correspondant dans tous les sous-domaines et les hôtes sous le domaine actuel, afin de leur permettre d'hériter de la valeur actuelle. Utilisez cette option avec prudence: toutes les valeurs définies dans le sous-domaine ou les hôtes sous le domaine sélectionné sont effacées et il est impossible de les rétablir.

Afficher les valeurs du domaine

La commande **Afficher les valeurs du domaine** n'est disponible que si un domaine de stratégie est sélectionné. Elle permet d'afficher la liste de tous les domaines de stratégie et des hôtes sous le domaine de stratégie sélectionné, ainsi que la valeur de la zone sélectionnée.

Cliquez sur le nom d'un domaine ou d'un hôte pour le sélectionner. Il est possible d'ouvrir simultanément plusieurs boîtes de dialogue de **valeurs de domaine**.

Affichage de l'état

Vous pouvez afficher les paramètres et les statistiques d'un domaine de stratégie dans l'application principale.

Pour afficher l'état:

1. Ouvrez l'onglet **Etat**.
2. Sélectionnez le produit.
   Console Policy Manager affichera une vue Produit pour le produit sélectionné, dans laquelle vous pourrez afficher les statistiques et paramètres locaux les plus importants.

   > **Remarque:** Il est impossible de modifier les valeurs. Par contre, vous pouvez consulter les textes d'aide **MIB** en cliquant sur une zone ou sur son libellé.

   Pour les domaines de stratégie, l'onglet **Etat** affiche l'état récapitulatif au niveau du domaine: le nombre d'hôtes du domaine et la liste des hôtes déconnectés.
3. Cliquez sur un hôte déconnecté afin de modifier rapidement la sélection de domaine de stratégie pour cet hôte.

Ce faisant, vous pouvez déterminer si l'hôte déconnecté a réussi à envoyer quelques alertes ou des statistiques utiles avant sa déconnexion. Ces informations peuvent vous aider à déterminer pourquoi l'hôte a été déconnecté. Si la raison est évidente (par exemple si le logiciel F-Secure a été désinstallé de l'hôte), vous pouvez supprimer l'hôte normalement.

4. Lorsque vous avez examiné un hôte déconnecté, vous pouvez retourner au niveau précédent de domaine sélectionné en cliquant sur le bouton  de la barre d'outils.
   La vue **Etat du domaine** comprend également deux raccourcis qui permettent de traiter un nombre élevé d'hôtes déconnectés: la sélection de tous les hôtes déconnectés et leur suppression. Ces deux actions sont accessibles via le menu contextuel du nœud **Hôte déconnecté** de l'arborescence.

   Avertissement: La suppression de tous les hôtes déconnectés est une opération potentiellement dangereuse. Certains hôtes existants peuvent, pour l'une ou l'autre raison, être déconnectés temporairement pendant une période supérieure au délai autorisé. Vérifiez toujours la valeur du délai de déconnexion dans la zone **Préférences** avant de supprimer des hôtes. Si un hôte existant est supprimé accidentellement, vous effacerez ses alertes, rapports, états et paramètres de stratégie. Par contre, l'hôte enverra un message d'auto-enregistrement lorsqu'il s'apercevra qu'il a été supprimé de Policy Manager. L'hôte pourra ensuite être réimporté dans l'arborescence du domaine. Toutefois, par rapport à Policy Manager, il sera considéré comme un nouvel hôte.

Volet Messages

Console Policy Manager consigne les messages relatifs aux différents événements dans le volet **Messages**.

Contrairement aux onglets **Alertes** et **Rapports**, les événements du volet **Messages** ne sont générés que par Console Policy Manager.

Il existe trois catégories de messages: **informations**, **avertissements** et **erreurs**. Chaque onglet du volet **Messages** contient des messages de trois niveaux de gravité. Vous pouvez supprimer une catégorie à l'aide du menu contextuel qui s'affiche lorsque vous cliquez sur un onglet avec le bouton droit de la souris. Lorsque vous cliquez sur un message avec le bouton droit de la souris, un menu contextuel s'affiche vous permettant de **couper**, **copier** et **supprimer** le message.

Par défaut, les messages sont répertoriés sous la forme de fichiers dans le sous-répertoire des messages du répertoire d'installation local de Console Policy Manager. Les fichiers journaux des messages sont stockés en anglais et dans la langue que vous avez paramétrée pour Console Policy Manager. Un fichier journal différent est créé pour chaque catégorie de message (noms des onglets dans le volet **Messages**). Utilisez la page **Préférences** ➤ **Emplacements** pour spécifier le répertoire du fichier journal et activer ou désactiver la tenue du journal. Les fonctions de la page **Messages** ne sont pas affectées lorsque vous activez ou que vous désactivez l'enregistrement de messages.

Barre d'outils

La barre d'outils contient des boutons pour les tâches de Console Policy Manager

	Enregistre les données de stratégie.
	Distribue la stratégie.
	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.
	Accède au domaine parent.
	Coupe un hôte ou un domaine.

	Colle un hôte ou un domaine.
	Ajoute un domaine au domaine actuellement sélectionné.
	Ajoute un hôte au domaine actuellement sélectionné.
	Affiche la boîte de dialogue **Propriétés** d'un domaine ou d'un hôte.
	Démarre l'outil **Autodécouvrir hôtes Windows**. De nouveaux hôtes vont être ajoutés au domaine de stratégie actuellement sélectionné.
	Démarre l'installation distante sur les hôtes Windows.
	Importe des hôtes auto-enregistrés dans le domaine actuellement sélectionné. Si cette icône est verte, cela signifie que l'hôte a envoyé une demande d'auto-enregistrement.
	Affiche les packages d'installation disponibles.
 ou 	Affiche toutes les alertes. L'icône est mise en surbrillance s'il existe de nouvelles alertes. Lorsque vous démarrez Console Policy Manager, l'icône est toujours mise en surbrillance.

Options des menus

Cette section fournit une référence pour les options de menus disponibles dans Console Policy Manager.

Menu	Commande	Action
Fichier	Nouvelle stratégie	Crée une instance de données de stratégie à l'aide des paramètres par défaut de la base d'informations de gestion (MIB). Cette option est rarement utilisée car les données de stratégie existantes sont généralement modifiées, puis enregistrées à l'aide de l'option **Enregistrer sous**.
	Ouvrir une stratégie	Ouvre les données d'une stratégie précédemment enregistrée.
	Enregistrer les modifications de stratégie	Enregistre les données de stratégie actuelles.
	Enregistrer la stratégie sous	Enregistre les données de stratégie sous le nom spécifié.
	Distribuer des stratégies	Distribue les fichiers de stratégie.
	Exporter le fichier de stratégie de l'hôte	Exporte les fichiers de stratégie.
	Quitter	Ferme Console Policy Manager.
Edition	Couper	Coupe l'élément sélectionné.
	Coller	Colle l'élément à l'emplacement sélectionné.
	Supprimer	Supprime l'élément sélectionné.
	Nouveau domaine de stratégie	Ajoute un nouveau domaine.
	Nouvel hôte	Ajoute un nouvel hôte.

Menu	Commande	Action
	Importer des hôtes auto-enregistrés	Importe les hôtes qui ont envoyé une demande d'auto
	Autodécouvrir hôtes Windows	Importe des hôtes à partir de la structure de domaine Windows.
	Distribuer l'installation aux hôtes Windows	Installe le logiciel à distance et importe les hôtes définis par l'adresse IP ou le nom WINS.
	Rechercher	Recherche une chaîne dans les propriétés de l'hôte. La recherche est effectuée sur tous les hôtes du domaine sélectionné.
	Propriétés de domaine/d'hôte	Affiche la page des **propriétés** de l'hôte ou du domaine de stratégie sélectionné.
Affichage	Editeurs de restriction intégrés	Bascule entre l'éditeur de restriction intégré et la boîte de dialogue des restrictions.
	Volet Messages	Affiche ou masque le volet **Message** en bas de l'écran.
	Ouvrir pour un nouveau message	S'il est sélectionné, le volet **Message** s'ouvre automatiquement quand un nouveau message est reçu.
	Retour	Accède au domaine ou à l'hôte précédent dans l'historique de sélection de l'arborescence.
	Suivant	Accède au domaine ou à l'hôte suivant dans l'historique de sélection de l'arborescence.
	Domaine parent	Accède au domaine parent.
	Toutes les alertes	Ouvre la page **Alertes** pour afficher toutes les alertes.
	Mode avancé	Active l'interface utilisateur en **Mode avancé**.
	Mode antivirus	Active l'interface utilisateur en **Mode antivirus**, qui est optimisée pour une gestion centralisée de Client Security.
	Actualiser <Elément>	Permet d'actualiser manuellement l'affichage du rapport, de l'état ou de l'alerte. L'élément de menu varie en fonction de l'onglet ou de la page sélectionné.
	Actualiser tout	Permet d'actualiser manuellement toutes les données concernant l'interface: stratégie, état, alertes, rapports, packages d'installation et demandes d'auto-enregistrement.
Outils	Packages d'installation	Affiche dans une boîte de dialogue les informations relatives aux packages d'installation.
	Modifier la phrase de cryptage	Change la phrase de cryptage de connexion (la phrase de cryptage protégeant la clé privée de Console Policy Manager.
	Transmission des rapports	Vous permet de sélectionner les méthodes de transmission de rapports, les domaines/hôtes et les produits inclus dans les rapports.
	Préférences	Définit les propriétés locales de Console Policy Manager. Ces propriétés concernent uniquement l'installation locale de Console Policy Manager.
Aide	Sommaire	Affiche l'index de l'**Aide**.

Menu	Commande	Action
	Enregistrer	Ouvre une boîte de dialogue qui vous permet d'enregistrer le produit.
	Contacts	Affiche les coordonnées des contacts de la société F-Secure.
	A propos de F-Secure Policy Manager Console	Affiche les informations de version.

Administration des domaines et des hôtes

Si vous souhaitez utiliser des stratégies de sécurité différentes pour différents types d'hôtes (portables, ordinateurs de bureau, serveurs), pour différents services de l'entreprise ou pour des utilisateurs ayant des connaissances différentes en informatique, il est judicieux de planifier la structure du domaine en fonction de ces critères.

Cela facilitera la gestion des hôtes. Si vous avez conçu au préalable la structure du domaine de stratégie, vous pouvez importer les hôtes directement dans cette structure. Si vous souhaitez démarrer rapidement, vous pouvez également commencer par importer tous les hôtes dans le domaine racine et créer la structure du domaine plus tard, lorsque le besoin s'en fait sentir. Les hôtes peuvent alors êtres coupés et collés dans leur nouveau domaine.

Chaque domaine ou hôte de cette structure doit disposer d'un nom unique.

Il est également possible de créer les différents bureaux nationaux en tant que sous-domaines.

Ajout de domaines de stratégie

Cette rubrique décrit comment ajouter des nouveaux domaines de stratégie.

Pour ajouter un nouveau domaine de stratégie:

1. Sélectionnez **Edition** ➤ **Nouveau domaine de stratégie** dans le menu.
   Alternativement:
   - Cliquez sur  dans la barre d'outils.
   - Appuyez sur Ctrl + Insert.

   Le nouveau domaine de stratégie est un sous
2. Entrez un nom pour le domaine de stratégie.
   Une icône représentant le domaine est créée.

Ajout d'hôtes

Cette section décrit les différentes méthodes d'ajout d'hôtes à un domaine de stratégie.

Les principales méthodes d'ajout d'hôtes dans votre domaine de stratégie, selon le système d'exploitation utilisé, sont les suivantes:

- Importer des hôtes directement à partir de votre domaine Windows.
- Importer des hôtes par auto-enregistrement (nécessite que Management Agent soit installé sur les hôtes importés). Vous pouvez également utiliser d'autres critères pour importer les hôtes auto-enregistrés dans différents sous-domaines.
- Créez des hôtes manuellement à l'aide de la commande **Nouvel hôte**.

Ajout d'hôtes à des domaines Windows

Dans un domaine Windows, la méthode la plus pratique pour ajouter des hôtes dans votre domaine de stratégie consiste à importer ceux-ci à l'aide du composant d'installation intelligente.

Notez que cela installe également Management Agent sur les hôtes importés. Pour importer des hôtes depuis un domaine Windows:

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Autodécouvrir hôtes Windows** dans le menu.

Au terme de l'opération de découverte automatique, le nouvel hôte est automatiquement ajouté à l'arborescence du **Domaine de stratégie**.

Importation d'hôtes auto-enregistrés

Il est également possible d'importer les hôtes dans Console Policy Manager en utilisant la fonction d'*auto-enregistrement*.

Cette opération n'est réalisable qu'une fois Management Agent installé sur les hôtes et après l'envoi d'une demande d'auto-enregistrement par les hôtes. Management Agent devra être installé à partir d'un CD-ROM, d'un script de connexion ou d'une autre manière.

Pour importer des hôtes auto-enregistrés:

1. Cliquez sur  dans la barre d'outils.

   Autre possibilité:

   - Sélectionnez **Edition** ➤ **Importer des hôtes auto-enregistrés** dans le menu.
   - Sélectionnez **Importer des hôtes auto-enregistrés** dans la vue **Installation**.

   Une fois l'opération terminée, l'hôte est ajouté à l'arborescence du domaine. Les hôtes auto-enregistrés peuvent être importés dans différents domaines en fonction de différents critères, tels que l'IP ou l'adresse DNS de l'hôte. La vue **Auto-enregistrement** présente les données envoyées par l'hôte dans le message d'auto-enregistrement sous forme de tableau. Ces données comprennent les propriétés d'auto-enregistrement personnalisées éventuellement incluses dans le package d'installation distante lors de l'installation.
2. Vous pouvez effectuer les opérations suivantes dans la vue **Auto-enregistrement**:

   - Vous pouvez trier les messages d'auto-enregistrement selon les valeurs de n'importe quelle colonne. Pour ce faire, cliquez sur son en-tête dans le tableau.
   - Vous pouvez modifier l'ordre des colonnes en les faisant glisser à l'emplacement souhaité. La largeur des colonnes peut également être modifiée.
   - Vous pouvez utiliser le menu contextuel de la table (cliquez avec le bouton droit de la souris sur la barre d'en-tête de la table) pour spécifier les propriétés d'auto-enregistrement à afficher dans la table.

Utilisation des règles d'importation de l'auto-enregistrement

Vous pouvez définir les règles d'importation des hôtes auto-enregistrés dans l'onglet **Règles d'importation** de la boîte de dialogue **Importer les hôtes auto-enregistrés**.

Les critères d'importation suivants peuvent être utilisés dans les règles :

- Nom WINS, nom DNS, nom DNS dynamique, propriétés personnalisées
  - L'astérisque (`*`) peut être utilisé comme caractère générique. Le caractère `*` peut remplacer n'importe quel nombre de caractères. Par exemple: `test_hôte*` ou `*.exemple.com`.
  - La correspondance n'est pas sensible à la casse: les caractères en majuscule et en minuscule sont donc traités de la même façon.
- Adresse IP, adresse IP dynamique
  - Ces critères prennent en charge la correspondance exacte d'adresse IP (par exemple: `192.1.2.3`) et la correspondance de sous-domaines IP (par exemple: `10.15.0.0/16`).

1. Vous pouvez masquer et afficher des colonnes de la table à l'aide du menu contextuel qui apparaît lorsque vous cliquez avec le bouton droit de la souris sur n'importe quel en-tête de colonne de la fenêtre **Importer des règles**.

Seules les valeurs contenues dans les colonnes actuellement visibles sont utilisées comme critères de correspondance lors de l'importation des hôtes dans le domaine de stratégie. Les valeurs contenues dans les colonnes masquées sont ignorées.

2. Il est également possible d'ajouter de nouvelles propriétés personnalisées à utiliser comme critères lors de l'importation des hôtes.

   Les propriétés personnalisées peuvent également être utilisées pour créer des packages d'installation indépendants pour différents services devant être regroupés dans des domaines de stratégie spécifiques. Dans ce cas, il est possible d'utiliser le nom du service comme propriété personnalisée, puis de créer des règles d'importation qui utilisent le nom des services comme critère d'importation. Notez que les noms de propriété personnalisée masqués ne sont conservés en mémoire que jusqu'à la fermeture de Console Policy Manager. Pour ajouter une nouvelle propriété personnalisée:

   a) Cliquez avec le bouton droit sur un en-tête de colonne et sélectionnez **Ajouter une propriété personnalisée**.
   La boîte de dialogue **Nouvelle propriété personnalisé** s'ouvre.
   b) Saisissez le nom de la propriété personnalisée (par exemple, le nom du service), puis cliquez sur **OK**.
   La nouvelle propriété personnalisée apparaît dans le tableau. Elle peut désormais être utilisée comme critère d'importation dans de nouvelles règles d'importation d'auto-enregistrement.

3. Créer une nouvelle règle d'importation d'auto-enregistrement:

   a) Cliquez sur **Ajouter** dans l'onglet **Règles d'importation**.
   La boîte de dialogue **Sélectionner le domaine de stratégie de destination pour la règle** s'ouvre et affiche les domaines et sous-domaines existants.
   b) Sélectionnez le domaine pour lequel vous créez la règle et cliquez sur **OK**.
   c) Sélectionnez la ligne que vous venez de créer, cliquez dans la cellule à renseigner, puis cliquez sur **Modifier**.
   d) Saisissez la valeur dans la cellule.
   Le critère d'importation est défini.

   - Lors de l'importation d'hôtes auto-enregistrés, les règles sont vérifiées de haut en bas. La première règle correspondante est appliquée. Il est possible de changer l'ordre des règles en cliquant sur **Déplacer vers le bas** ou **Déplacer vers le haut**.
   - Si vous souhaitez créer plusieurs règles pour un domaine, vous pouvez utiliser l'option **Cloner**. Commencez par créer une règle pour le domaine. Sélectionnez ensuite la ligne et cliquez sur **Cloner**. Vous pouvez désormais modifier les critères dans la ligne dupliquée.

4. Lorsque vous voulez débuter l'importation, sélectionnez l'onglet **Hôtes auto-enregistrés** et cliquez sur **Importer**.

   Les règles d'importation définies seront validées avant le début de l'importation.

   Une fois les hôtes importés, une boîte de dialogue récapitulative s'ouvre et affiche le nombre d'hôtes importés avec succès et le nombre d'importations échouées. Notez qu'un ensemble de conditions vide est traité comme une correspondance absolue.

Création manuelle d'hôtes

Cette rubrique décrit comment créer des hôtes manuellement.

Pour créer un hôte manuellement:

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Nouvel hôte** dans le menu.

   Autre possibilité:

   - Cliquez sur  dans la barre d'outils.
   - Appuyez sur Insérer.

   Cette opération est utile dans les cas suivants :

- Apprentissage et test: vous pouvez essayer un sous-ensemble des fonctions de Console Policy Manager sans installer de logiciel en complément de Console Policy Manager.
- Définition des stratégies en avance: vous pouvez définir et générer une stratégie pour un hôte avant d'installer le logiciel sur l'hôte.
- Cas particuliers: vous pouvez générer des stratégies pour des hôtes qui n'accèderont jamais directement au serveur (c'est-à-dire lorsqu'il est impossible d'importer l'hôte). Il est, par exemple, possible de générer des fichiers de stratégie de base pour un ordinateur n'ayant pas accès à F-Secure Policy Manager Server. Vous devez transférer le fichier de stratégie de base soit manuellement, soit en utilisant un autre mode de transport externe. Pour ce faire, choisissez la commande **Edition** ➤ **Exporter le fichier de stratégie** dans le menu.

Remarque: Les hôtes non équipés de Management Agent ne peuvent pas être administrés par Console Policy Manager, car ils n'ont aucun moyen de rechercher les stratégies. De plus, ils ne disposent d'aucune information d'état. Toutes les modifications apportées à la structure du domaine sont appliquées, même si vous fermez Console Policy Manager sans les enregistrer dans les données de stratégies en cours.

Propriétés d'hôte

Cette section fournit une présentation des propriétés d'hôte pouvant être affichées et modifiées dans Console Policy Manager.

Les noms d'hôte du réseau peuvent être des adresses IP, des noms de domaine ou des noms WINS. Pour afficher les propriétés de l'hôte, cliquez avec le bouton droit de la souris sur l'hôte et, dans le menu qui s'affiche, sélectionnez **Propriétés** (ou appuyez sur alt + entrée). Pour modifier les propriétés de l'hôte, décochez la case **Propriétés de mise à jour automatique** dans l'onglet **Identités** de la boîte de dialogue **Propriétés de l'hôte**. Vous pouvez ouvrir la boîte de dialogue **Propriétés de l'hôte** en sélectionnant **Propriétés** dans le menu **Édition**, ou en cliquant sur  dans la barre d'outils.

Le nom réseau de l'hôte est le nom que celui-ci utilise en interne sur le réseau pour accéder aux stratégies.

Chaque hôte possède un identifiant utilisateur (UID). Il s'agit d'un identifiant unique: une chaîne de caractères et de nombres utilisée pour identifier de façon unique chaque hôte du système.

Dans l'onglet **Plate-forme**, il est possible d'ajouter le système d'exploitation de l'hôte dans les propriétés. Le **nom de plate-forme** désigne le nom du système d'exploitation. Les numéros de version des systèmes d'exploitation sont les suivants:

Windows XP	5.1/5.10
Windows Vista	6.0

Vous pouvez définir un alias pour l'hôte dans l'onglet **Divers**. Si un alias est défini, celui-ci remplace l'identité réelle de l'hôte dans l'arborescence du domaine affichée à l'écran.

Distribution des logiciels

Policy Manager propose plusieurs méthodes d'installation et de mise à jour des applications gérées.

Installations distantes	Policy Manager peut installer des logiciels sur de nouveaux hôtes qui ne sont pas encore administrés de manière centralisée. Les hôtes peuvent être recherchés à partir de domaines Windows à l'aide de la fonction **Autodécouvrir hôtes Windows** ou l'hôte cible peut être défini directement à l'aide de son nom WINS ou de son adresse IP via la fonction **Distribuer l'installation aux hôtes Windows**. Les fonctions d'installation à distance sont utiles pour les nouvelles installations, mais aussi pour mettre à jour ou réparer des installations si les procédures par stratégies ne conviennent pas.
Installation par stratégies	Policy Manager peut démarrer les opérations d'installation et de mise à jour à l'aide de stratégies. Pour ce faire, les hôtes doivent déjà être administrés de manière centralisée, c'est-à-dire qu'ils doivent figurer dans un domaine de stratégie de Console Policy Manager.
Installations et mises à jour locales depuis un CD-ROM	Vous pouvez également effectuer l'installation séparément sur l'hôte en exécutant le programme d'installation directement à partir du CD-ROM. Au terme de l'installation, Management Agent envoie un message d'enregistrement à Policy Manager. L'administrateur peut alors visualiser et accepter le nouvel hôte en sélectionnant la commande **Importer les hôtes enregistrés automatiquement** dans le menu **Edition** de Console Policy Manager.
Installations et mises à jour locales à l'aide de packages préconfigurés	Au lieu d'utiliser le programme d'installation standard du CD-ROM, vous pouvez vous servir de Policy Manager pour préparer un fichier d'installation personnalisé (JAR ou MSI) comportant les informations relatives aux paramètres définis pour l'installation. L'installation peut être réalisée de façon automatique sur l'ordinateur de l'utilisateur final car le fichier préconfiguré contient tous les paramètres habituellement demandés à l'utilisateur.
Mises à jour de la base de données de définitions de virus F-Secure	Policy Manager peut mettre à jour les dernières bases de données antivirus en les téléchargeant automatiquement à partir du site de mise à jour automatique de F-Secure. Les hôtes administrés chargent les mises à jour depuis Policy Manager en fonction de leur stratégie, en procédant automatiquement ou à l'aide d'actions déclenchées à distance.

Les raccourcis vers toutes les fonctions d'installation sont regroupés dans l'onglet **Installation**.

Installations distantes

Cette section décrit comment effectuer une installation distante sur les hôtes.

La seule différence entre les fonctions **Autodécouvrir hôtes Windows** et **Distribuer l'installation aux hôtes Windows** réside dans la manière dont les hôtes de destination sont sélectionnés. La fonction de découverte automatique examine les domaines Windows, et l'utilisateur peut sélectionner les hôtes de destination dans une liste. La fonction de distribution de l'installation permet pour sa part de définir directement les hôtes de destination à l'aide d'adresses IP ou de noms d'hôte. Une fois les hôtes de destination sélectionnés, les deux opérations d'installation distante se déroulent de la même manière.

👉 **Remarque:** Avant de commencer l'installation de produits F-Secure sur les hôtes, vous devez vous assurer qu'aucun programme antivirus ou de pare-feu n'entre en conflit avec les programmes installés.

Autodécouvrir hôtes Windows

Les hôtes cibles peuvent être sélectionnés avec la fonction *Autodécouvrir*.

Pour sélectionner des hôtes cibles:

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Autodécouvrir hôtes Windows** dans le menu.

   Vous pouvez également cliquer sur le bouton  .
3. Dans la liste des **Domaines NT**, sélectionnez l'un des domaines et cliquez sur **Actualiser**.

   La liste des hôtes est actualisée lorsque vous cliquez sur le bouton **Actualiser**. Afin d'optimiser les performances, seules les informations stockées en mémoire cache apparaissent à l'écran. Avant de cliquer sur **Actualiser**, vous pouvez modifier les options suivantes:

   - **Masquer les hôtes déjà administrés**. Cochez cette case afin d'afficher uniquement les hôtes ne disposant pas d'applications F-Secure.
   - **Identifier les hôtes en détail (plus lent)**. Cette option affiche tous les détails relatifs aux hôtes, comme les versions du système d'exploitation et de Management Agent.
   - **Identifier les noms d'hôtes et les commentaires uniquement (plus rapide)**. Cette option peut être utilisée lorsque tous les hôtes n'apparaissent pas de façon détaillée ou que la récupération de la liste prend trop de temps. Notez qu'il peut parfois s'écouler un petit moment avant que le **Navigateur principal** affiche un hôte récemment installé sur le réseau.
4. Sélectionnez les hôtes sur lesquels effectuer l'installation.

   Appuyez sur la barre d'espace pour vérifier les hôtes sélectionnés. Plusieurs hôtes peuvent être facilement sélectionnés en maintenant appuyée la touche Maj. et en effectuant l'une des tâches suivantes:

   - cliquer sur plusieurs lignes d'hôtes;
   - faire glisser la souris au-dessus de plusieurs lignes d'hôtes;
   - utiliser les touches portant une flèche vers le haut ou vers le bas.

   Vous pouvez également cliquer à l'aide du bouton droit de la souris. Dans le menu contextuel de la liste des hôtes, utilisez l'une des commandes suivantes:

   - **Activer**: active la case à cocher de l'hôte sélectionné (équivaut à appuyer sur la barre d'espacement).
   - **Désactiver**: désactive la case à cocher de l'hôte sélectionné (équivaut à appuyer sur la barre d'espacement).
   - **Tout activer**: active les cases à cocher de tous les hôtes du domaine Windows sélectionné.
   - **Désactiver tout**: désactive les cases à cocher de tous les hôtes du domaine Windows sélectionné.
5. Cliquez sur **Installer** pour continuer.

Lorsque vous avez sélectionné les hôtes cibles, vous devez tout de même installer à distance les applications sur les hôtes.

Distribuer l'installation aux hôtes Windows

Vous pouvez également sélectionner les hôtes cibles à l'aide de la fonction **Distribuer l'installation aux hôtes Windows**.

Pour sélectionner des hôtes cibles:

1. Sélectionnez le domaine cible.
2. Sélectionnez **Edition** ➤ **Distribuer l'installation aux hôtes Windows** dans le menu.

   Vous pouvez également cliquer sur le bouton  .
3. Entrez le nom des hôtes de destination sur lesquels démarrer l'installation, puis cliquez sur **Suivant** pour continuer.

   Vous pouvez cliquer sur **Parcourir** pour vérifier les versions de Management Agent sur les hôtes.

Lorsque vous avez sélectionné les hôtes cibles, vous devez installer à distance les applications sur les hôtes.

Installation distante après la sélection de l'hôte cible

Lorsque vous avez sélectionné les hôtes cibles, vous devez exécuter à distance les packages d'installation.

Pour exécuter à distance des packages d'installation sur les hôtes cibles sélectionnés:

1. Sélectionnez le package d'installation de votre choix, puis cliquez sur **Suivant** pour continuer.
2. Sélectionnez les produits à installer et cliquez sur **Suivant** pour continuer.

   Vous pouvez forcer la réinstallation s'il existe déjà des applications portant le même numéro de version.
3. Acceptez la stratégie par défaut ou choisissez la stratégie d'hôte ou de domaine à employer comme stratégie anonyme, puis cliquez sur **Suivant**.
4. Choisissez le compte d'utilisateur et le mot de passe pour l'installation à distance en sélectionnant soit **Ce compte** (le compte actuel) ou **Un autre utilisateur**.

   Remarque: Durant l'installation, la fonction d'installation distante doit disposer des droits d'accès administrateur sur le poste de destination. Si le compte que vous avez sélectionné ne dispose pas de droits d'accès administrateur sur l'un des hôtes distants, le message d'erreur **Accès refusé** apparaît pour l'hôte concerné, tandis que l'installation se poursuit pour les autres hôtes.

   Lorsque vous sélectionnez **Ce compte**, vous disposez des droits de sécurité du compte auquel vous êtes connecté. Utilisez cette option dans les cas suivants:

   - Vous êtes déjà connecté en tant qu'administrateur de domaine.
   - Vous êtes connecté en tant qu'administrateur local avec un mot de passe qui correspond à celui de l'administrateur local sur l'hôte de destination.

   Un autre utilisateur: entrez le compte et le mot de passe. L'administrateur peut saisir n'importe quels compte et mot de passe corrects d'administrateur de domaine afin d'effectuer l'installation distante sur les hôtes sélectionnés.

   - En cas d'installation sur des domaines approuvés et non approuvés à l'aide d'un compte de domaine, veillez à entrer le compte avec le format`DOMAINE\\COMPTE`.
   - Lorsque vous utilisez un compte d'administrateur local, utilisez le format `COMPTE`. N'ajoutez pas le nom d'hôte à celui du compte, faute de quoi ce compte ne sera accepté que par l'hôte en question.

   Remarque: Lors de l'installation, si l'ordinateur de l'administrateur a ouvert des connexions réseau avec l'ordinateur de destination à l'aide d'un autre compte d'utilisateur, le message d'erreur NT **1219** (conflit d'identification) s'affiche. Dans ce cas, interrompez les connexions actives avant de lancer l'**installation distante**.
5. Prenez connaissance du résumé de l'installation.
6. Pour démarrer l'**Assistant d'installation distante**, cliquez sur **Démarrer**.

   L'**Assistant d'installation distante** affiche une série de boîtes de dialogue dans lesquelles vous devez répondre à des questions pour permettre la réalisation de l'installation. Dans la dernière boîte de dialogue, cliquez sur **Terminer** puis passez à l'étape suivante.

   Policy Manager installe Management Agent et les produits sélectionnés sur les hôtes. Durant cette opération, la ligne d'**état** affiche l'avancement de la procédure. Vous pouvez cliquer à tout moment sur **Annuler** pour interrompre l'installation.
7. Quand la ligne d'**état** affiche terminé, le processus est terminé et vous pouvez sélectionner le domaine dans lequel inclure les nouveaux hôtes à l'aide des paramètres d'importation.
8. Cliquez sur **Terminer**.

   Console Policy Manager place les nouveaux hôtes dans le domaine sélectionné, sauf si vous avez entré un domaine différent dans cette boîte de dialogue. Vous pouvez également décider de ne pas placer automatiquement les hôtes dans un domaine. Les nouveaux hôtes enverront des demandes d'enregistrement automatique qui permettront de les importer.

Après quelques minutes, la liste des produits installés s'affiche.

9. Afin de visualiser cette liste, sélectionnez l'onglet **Installation**. Vous pouvez également sélectionner le domaine principal sur l'arborescence du **Domaine de stratégie**).

Installation par stratégies

Des fichiers de stratégie de base sont utilisés pour démarrer des installations sur les hôtes où Management Agent est installé.

Console Policy Manager crée un package d'installation spécifique d'une opération, qu'il stocke sur Serveur Policy Manager, puis écrit une tâche d'installation dans les fichiers de stratégie de base (une distribution de stratégie est donc nécessaire pour démarrer les installations). Les fichiers de stratégie de base et le package d'installation sont signés par la paire de clés d'administration, si bien que les hôtes n'accepteront que des informations authentiques.

Management Agent charge les nouvelles stratégies à partir de Serveur Policy Manager et recherche la tâche d'installation. Management Agent récupère, à partir du serveur, le package d'installation indiqué dans les paramètres de la tâche, puis démarre le programme d'installation.

Au terme de l'installation, Management Agent envoie le résultat de l'opération au serveur, dans un fichier de stratégie incrémentiel. Console Policy Manager recherche les nouvelles informations d'état et présente le résultat.

La désinstallation s'effectue à l'aide des mêmes mécanismes de remise. Les résultats de la désinstallation ne seront pas signalés.

Utilisation de l'éditeur d'installation

L'éditeur d'installation doit être utilisé sur les hôtes équipés de Management Agent.

Pour utiliser l'éditeur d'installation:

1. Ouvrez l'onglet **Stratégie** et sélectionnez le nœud racine (l'arborescence secondaire **F-Secure**).

   Vous pouvez également ouvrir l'onglet **Installer**.

   L'**Editeur d'installation** s'affiche.
2. Dans l'**Editeur d'installation**, sélectionnez les produits à installer sur l'hôte ou le domaine de stratégie actuellement sélectionné.

   L'**Editeur d'installation** contient les informations suivantes relatives aux produits installés sur l'hôte ou un domaine de stratégie de destination:

Nom de produit	Nom du produit déjà installé sur un hôte ou un domaine ou qui peut être installé à l'aide d'un package d'installation disponible.
Version installée	Numéro de version du produit. Si plusieurs versions du produit sont installées, tous les numéros de version correspondants s'affichent. Pour les hôtes, il s'agit toujours d'un numéro de version unique.
Version à installer	Numéros de version des packages d'installation disponibles pour le produit.
Version actuelle	Version actuelle, en cours d'installation sur un hôte ou un domaine.
En cours	Progression de l'installation. Le champ **En cours** affiche des informations différentes pour les hôtes et pour les domaines.

- Lorsqu'un hôte est sélectionné, le champ **En cours** affiche l'un des messages suivants:

En cours	L'installation a démarré (et a été ajoutée aux données de stratégie), mais l'hôte n'a pas encore signalé le succès ou l'échec de l'opération.
Échec	L'installation ou la désinstallation a échoué. Cliquez sur le bouton du champ **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée. Ce message disparaît lorsque vous fermez l'**Editeur d'installation**.
(Zone vide)	Aucune opération n'est en cours. Le champ **Version installée** affiche le numéro de version des produits actuellement installés.

- Lorsqu'un domaine est sélectionné, la zone **En cours** contient l'une des informations suivantes:

<nombre> hôtes restants - **<nombre> installations ayant échoué**	Nombre d'hôtes restants et nombre d'installations qui ont échoué. Cliquez sur le bouton de la zone **En cours** pour afficher des informations d'état détaillées.
Terminé	L'installation ou la désinstallation est achevée sur tous les hôtes.
(Zone vide)	Aucune opération n'est en cours. La **version installée** affiche le numéro de version des produits actuellement installés.

3. Lorsque tous les numéros de version requis sont sélectionnés, cliquez sur **Démarrer**. L'**Editeur d'installation** lance l'**Assistant d'installation**, qui invite l'utilisateur à configurer les paramètres de l'installation. L'**Editeur d'installation** prépare ensuite un package personnalisé de distribution de l'installation pour chaque opération d'installation. Ce package est sauvegardé sur Serveur Policy Manager.

   Remarque: Le bouton **Démarrer** permet à l'administrateur de démarrer les opérations d'installation sélectionnées dans la zone **Version à installer**. Si vous fermez l'**Editeur d'installation** sans cliquer sur le bouton **Démarrer**, toutes les modifications sont annulées.

4. L'installation étant déclenchée par une stratégie, vous devez distribuer les nouveaux fichiers de stratégie.

   Le fichier de stratégie contient une entrée qui invite l'hôte à rechercher le package d'installation et à démarrer l'installation.

   Notez qu'une installation peut prendre énormément de temps, notamment lorsqu'un hôte concerné n'est pas connecté au réseau lors de l'installation ou si l'opération activée requiert que l'utilisateur redémarre son poste de travail avant que l'installation soit terminée. Si les hôtes sont connectés au réseau et qu'ils n'envoient ou ne reçoivent pas correctement les fichiers de stratégie, cela signifie qu'il peut y avoir un problème important. Il est possible que l'hôte ne confirme pas correctement la réception de l'installation. Dans tous les cas, vous pouvez supprimer l'opération d'installation de la stratégie en cliquant sur le bouton **Tout arrêter**. Toutes les opérations d'installation définies pour le domaine de stratégie ou l'hôte sélectionné seront alors annulées. Vous pouvez arrêter toutes les tâches d'installation dans le domaine sélectionné et tous ses sous-domaines en choisissant l'option **Annuler de façon récurrente les installations pour les sous-domaines et les hôte** dans la boîte de dialogue de confirmation.

   Le bouton **Tout arrêter** est activé uniquement si une opération d'installation est définie pour l'hôte ou le domaine actuel. Les opérations définies pour les sous-domaines ne modifient pas son état. **Tout arrêter** supprime uniquement l'opération de la stratégie. Si un hôte a déjà récupéré le fichier de stratégie précédent, il est possible qu'il tente d'exécuter l'installation même si elle n'est plus visible dans l'**Editeur d'installation**.

Désinstallation à distance:

La désinstallation d'un produit peut s'exécuter aussi facilement qu'une mise à jour. Le système crée un fichier de diffusion contenant uniquement le logiciel nécessaire à la désinstallation du produit. Si ce dernier ne prend pas en charge la désinstallation à distance, l'**Editeur d'installation** n'affiche aucune option de désinstallation.

Si vous sélectionnez **Réinstaller**, la version actuelle sera à nouveau installée. Utilisez cette option uniquement pour résoudre certains problèmes. En règle générale, il n'est pas nécessaire de réinstaller un produit.

Lors de la désinstallation de Management Agent, aucune information statistique indiquant que la désinstallation a réussi n'est envoyée car Management Agent a été supprimé et ne peut pas envoyer d'informations. Si vous désinstallez par exemple F-Secure Anti-Virus et Management Agent:

1. Désinstaller F-Secure Anti-Virus
2. Attendez que Console Policy Manager signale le succès ou l'échec de la désinstallation.
3. Si F-Secure Anti-Virus a été désinstallé correctement, désinstallez Management Agent.
4. Si la désinstallation de Management Agent a échoué, Console Policy Manager affiche un rapport statistique de l'échec. La réussite ne peut pas être signalée, mais elle se remarque à la coupure des communications, le rapport final de Management Agent contenant la mention «`en cours`»..

Installations et mises à jour locales à l'aide de packages préconfigurés

Vous pouvez exporter des packages pré-configurés dans un format JAR ou MSI (programme d'installation Microsoft).

Les packages MSI peuvent être distribués, par exemple, en utilisant la stratégie de groupe Windows dans l'environnement Active Directory.

La procédure d'exportation dans les deux formats est la même (voir ci-dessous). Vous pouvez sélectionner le format de fichier pour le package personnalisé dans la boîte de dialogue **Exporter le package d'installation**.

Utilisation du package d'installation à distance personnalisé

L'utilisation du script de connexion peut se faire de deux façons sur les plates-formes Windows: à l'aide d'un fichier d'installation distante personnalisé ou à l'aide d'un fichier MSI personnalisé.

Pour utiliser le fichier JAR d'installation distante personnalisé:

1. Exécutez Console Policy Manager.
2. Sélectionnez **Outils** ➤ **Packages d'installation**.
   La boîte de dialogue **Packages d'installation** s'ouvre.
3. Sélectionnez le package d'installation contenant les produits que vous souhaitez installer, puis cliquez sur **Exporter**.
4. Indiquez le format, JAR ou MSI, et l'emplacement où vous souhaitez enregistrer le package d'installation, puis cliquez sur **Exporter**.
5. Indiquez l'emplacement où vous souhaitez enregistrer le package d'installation JAR personnalisé, puis cliquez sur **Enregistrer**.
6. Sélectionnez les composants à installer et cliquez sur **Suivant** pour continuer.
7. Acceptez la stratégie par défaut ou choisissez la stratégie d'hôte ou de domaine à employer comme stratégie anonyme, puis cliquez sur **Suivant** pour continuer.
8. Sélectionnez le type d'installation.

   Le choix par défaut, **Installation avec administration centralisée**, est recommandé. Vous pouvez également préparer un package pour un hôte autonome.

   Une page récapitulative présente les options choisies pour l'installation.
9. Consultez le récapitulatif, puis cliquez sur **Démarrer** pour continuer l'installation de l'assistant.

   Console Policy Manager affiche les **Assistants d'installation à distance** qui collectent toutes les informations nécessaires à l'installation des produits sélectionnés. Vous pouvez inclure autant de propriétés d'auto-enregistrement personnalisées que vous le voulez dans le fichier d'installation. Les hôtes ajouteront

ces propriétés personnalisées au message d'auto-enregistrement qu'ils envoient à Policy Manager après l'installation locale. Les propriétés spécifiques des clients s'affichent avec les propriétés standard d'identification d'hôte de la vue d'**auto-enregistrement**. Le nom de la propriété personnalisée est utilisé comme nom de colonne, et sa valeur comme valeur de cellule.

Vous pouvez par exemple utiliser des propriétés personnalisées pour créer un fichier d'installation distinct destiné à des unités d'exploitation différentes qui doivent être regroupées dans des domaines de stratégie spécifiques. Le nom de la propriété peut être `Unité`, sa valeur différant pour chaque fichier d'installation. Il est désormais possible de distinguer les hôtes de chaque unité dans la vue d'auto-enregistrement. Vous pouvez importer tous les hôtes d'une unité dans leur domaine de destination à l'aide des fonctions de tri des colonnes et de sélection multiple. Notez que le domaine de destination peut être modifié directement depuis la vue d'**auto-enregistrement**. Après quoi, les hôtes d'une autre unité peuvent être importés dans le domaine de destination approprié.

10. Lorsque vous atteignez la dernière page de l'assistant, cliquez sur **Terminer** pour continuer.
11. Vous pouvez installer le package JAR exporté sur les hôtes en exécutant l'outil `ilaunchr.exe`.

    L'outil `ilaunchr.exe` se trouve dans le répertoire d'installation de Console Policy Manager sous `...\Administrator\Bin`. Pour ce faire:

    a) Copiez `ilaunchr.exe` et le package JAR exporté à un emplacement où le script de connexion peut accéder à ceux-ci.
    b) Entrez la commande:`ilaunchr <nom de package>.jar` où `<nom de package>` est remplacé par le nom réel du package JAR installé.

    Lors de l'installation, l'utilisateur voit une boîte de dialogue affichant l'avancement de l'installation. Si un redémarrage s'impose après l'installation, un message invite l'utilisateur à redémarrer l'ordinateur de la manière définie lors de l'exportation du package d'installation. Si vous souhaitez que l'installation s'exécute en mode silencieux, utilisez la commande suivante:`ilaunchr <nom de package>.jar /Q`. Dans ce cas, l'utilisateur peut être invité à redémarrer l'ordinateur après l'installation, et si une erreur fatale se produit pendant l'installation, un message s'affiche.

    ILAUNCHR comporte les paramètres de ligne de commande suivants:

    `/U` — Aucune assistance. Aucun message ne s'affiche, même lorsqu'une erreur fatale se produit.

    `/F` — Installation forcée. Complète l'installation même si Management Agent est déjà installé.

    Tapez `ILAUNCHR /?` à l'invite de commande afin d'afficher la totalité de l'aide.

    Lorsque vous effectuez une installation sur XP (ou version plus récente), vous pouvez également utiliser les paramètres suivants:

    - `/user:domaine\nom_utilisateur` (variation: `/user:nom_utilisateur`): spécifie le compte utilisateur et le nom de domaine. Le nom de domaine est facultatif.
    - `/password:secret` (variation: `/password:"secret avec espaces"`): spécifie le mot de passe du compte utilisateur.

    La fonctionnalité de l'utilitaire ilaunchr reste la même si aucun de ces deux paramètres n'est fourni. Si un seul des paramètres est fourni, ilaunchr renvoie un code d'erreur. Si les deux paramètres sont fournis, llaunchr démarre le programme**d'installation**. Exemple de la commande:

    ```
    ILaunchr <fichier jar> /user:domaine\nom_utilisateur /password:mot_secret
    ```

Transmission des informations

Toutes les informations d'installation sont fournies sous forme de fichiers via Serveur Policy Manager.

Les packages d'installation consistent en des archives JAR que vous pouvez visualiser (avec WinZip, par exemple), tandis que les autres types de fichiers, comme les fichiers de stratégie et les fichiers `INI`, permettent de lancer le processus d'installation proprement dit. .

Avant que Console Policy Manager puisse commencer l'installation, le package d'installation initial doit être transféré vers Serveur Policy Manager. Les packages d'installation sont disponibles auprès de deux sources:

- le CD-ROM d'installation;
- Le site Web F-Secure.

Normalement, les nouveaux fichiers d'installation distante sont installés à partir du CD-ROM, et le programme d'installation de Policy Manager les déplace automatiquement sur le serveur. Si un package d'installation distante est obtenu d'une autre manière, vous pouvez l'importer en cliquant sur le bouton **Importer** de la vue **Packages d'installation**, ou utiliser à cette fin la boîte de dialogue **Packages d'installation**. Autrement, le fichier d'installation peut être copié manuellement vers le sous-répertoire `/Install/Entry` du répertoire racine du serveur.

Console Policy Manager vérifie que le nouveau package d'installation est signé avec la clé privée de F-Secure avant d'en autoriser l'utilisation.

Gestion des stratégies

Cette section décrit la façon de configurer et distribuer les stratégies.

Paramètres

Pour configurer les paramètres d'une stratégie, parcourez l'arborescence de celle-ci et modifiez les valeurs des variables de stratégie.

Il existe deux types de variables de stratégie:

- les nœuds non terminaux dépendant d'une arborescence,
- les cellules de tableau.

Toutes les variables de stratégie sont associées à un type. Vous pouvez définir leurs valeurs dans la zone principale de l'application. Le type d'une variable de stratégie peut être l'un des suivants:

- Entier: nombre entier normal.
- Chaîne d'affichage: chaîne de texte ASCII 7 bits.
- Adresse IP: adresse IP sur quatre octets.
- Compteur: entier incrémenté.
- Indicateur: entier non bouclé.
- Cycles d'horloge: unités de temps écoulées (mesurées en centièmes de seconde).
- Chaîne d'octets: données binaires (ce type est également utilisé dans les chaînes de texte UNICODE)
- OID: identificateur unique.
- Opaque: données binaires qui peuvent représenter d'autres types de données.

La valeur d'une variable de stratégie peut être prédéfinie. Les valeurs par défaut agissent comme si elles étaient héritées du domaine racine supérieur. Elles apparaissent ainsi comme des valeurs héritées même si le domaine supérieur (racine) est sélectionné. Les valeurs par défaut peuvent être remplacées comme n'importe quelles autres valeurs.

Les valeurs correspondant au domaine de stratégie sélectionné font l'objet d'un codage couleur

- Noir: valeurs modifiées au niveau du domaine de stratégie ou de l'hôte sélection.
- Gris: valeurs héritées.
- Rouge: valeurs invalides.
- Rouge atténué: valeurs non valables héritées.

Restrictions

Grâce aux restrictions de valeurs, un administrateur peut limiter les valeurs d'une variable de stratégie à une liste de valeurs acceptables dans laquelle l'utilisateur peut faire son choix.

On distingue deux types de restrictions: les restrictions d'accès et les restrictions de valeurs. Les restrictions d'accès sont **Final** et **Masqué**. **Final** impose toujours la stratégie: la variable de stratégie remplace toute valeur de l'hôte local et l'utilisateur final ne peut pas modifier cette valeur tant que la restriction est de type **Final**. Le type **Masqué** cache simplement la valeur à l'utilisateur final. Contrairement à la restriction de type **Final**, une restriction de type **masqué** n'est pas forcément prise en compte par l'application administrée.

Il a également la possibilité de restreindre les variables de type entier (**Entier**, **Compteur** et **Indicateur**) à une plage de valeurs acceptables. Une restriction supplémentaire, la restriction de type **TAILLE_FIXE**, peut être appliquée aux tables. Grâce à cette restriction, l'utilisateur final n'est pas en mesure d'ajouter ou de supprimer des lignes dans des tables de taille fixe. Comme la restriction **Final** ne peut pas être utilisée pour une table vide, la restriction **TAILLE_FIXE** doit être employée à cette fin (afin d'empêcher les utilisateurs finaux de modifier les valeurs de la table).

Si une variable de la base de données MIB du produit contient déjà une définition de plage ou de choix, l'administrateur peut restreindre celle-ci davantage, mais pas l'étendre. Si aucune restriction de valeurs n'est définie, l'administrateur peut spécifier n'importe quelle restriction de plage ou de choix.

Les restrictions peuvent être modifiées dans la zone principale de l'application ou dans une boîte de dialogue distincte. Pour passer d'une possibilité à l'autre, sélectionnez **Editeurs de restriction intégrés** dans le menu **Affichage**. Si les éditeurs intégrés sont désactivés, la zone principale de l'application affiche les boutons de lancement des éditeurs de dialogue.

Configuration des paramètres

La modification des paramètres s'effectue en modifiant les variables de stratégie.

Pour configurer les paramètres:

1. Parcourez l'arborescence de la stratégie.
2. Modifiez les variables de stratégie.
3. Modifiez les restrictions des variables de stratégie si nécessaire.

   Les restrictions peuvent être modifiées dans la zone principale de l'application ou dans une boîte de dialogue séparée. Pour passer d'une possibilité à l'autre:

   a) Sélectionnez **Affichage** ➤ **Editeurs de restriction intégrés** dans le menu.

      Si les éditeurs intégrés sont désactivés, la zone principale de l'application affiche les boutons de lancement des éditeurs de dialogue.

4. Enregistrer la stratégie:

   - Sélectionnez **Fichier** ➤ **Enregistrer** dans le menu.
   - Sélectionnez **Fichier** ➤ **Enregistrer sous** dans le menu.

   Il est conseillé d'opter pour **Enregistrer sous**, qui permet d'enregistrer les données de stratégie sous un nouveau nom. Vous pouvez ainsi réutiliser une ancienne configuration de stratégie si nécessaire

5. Distribuer les fichiers de stratégie:

   Une fois la configuration des domaines et des hôtes terminée, vous devez diffuser celle-ci sur les hôtes. Pour ce faire:

   - Cliquez sur dans la barre d'outils.
   - Sélectionnez **Fichier** ➤ **Distribuer** dans le menu.
   - Appuyez sur CTRL + D.

   Console Policy Manager enregistre les données de stratégie en cours, puis génère la stratégie de base. Les fichiers de stratégie sont copiés dans le répertoire de `Communication`, où ils sont récupérés à intervalles réguliers par le logiciel F-Secure des hôtes.

   Remarque: Aucune modification ne sera prise en compte tant que la stratégie n'aura pas été diffusée et que l'hôte n'aura pas récupéré le fichier correspondant. Cela vaut également pour les opérations car elles sont implémentées à l'aide d'un mécanisme par stratégie.

Transmission des stratégies

Dans Console Policy Manager, chaque domaine de stratégie hérite automatiquement des paramètres de son domaine parent, ce qui permet une administration aisée et efficace des réseaux de grande taille.

Vous pouvez modifier ces paramètres pour des hôtes ou des domaines individuels. Lorsque vous modifiez les paramètres hérités d'un domaine, ces modifications sont transmises à tous les hôtes et sous-domaines contenus dans ce domaine. Tout paramètre remplacé peut être de nouveau hérité à l'aide de l'opération **Effacer**. Le paramètre étant supprimé dans l'hôte ou le domaine de stratégie actuellement sélectionné, il est remplacé par le paramètre du domaine parent.

La transmission des stratégies simplifie la définition d'une stratégie commune. La stratégie peut être davantage affinée pour des sous-domaines, voire des hôtes individuels. La granularité de définitions de stratégie peut varier considérablement d'une installation à l'autre. Certains administrateurs peuvent ne vouloir définir que quelques stratégies différentes pour des domaines étendus, tandis que d'autres préféreront associer les stratégies directement à chaque hôte, obtenant ainsi la granularité la plus fine.

La combinaison de ces stratégies permet de tirer le meilleur parti des deux méthodes. Certains produits peuvent hériter leurs stratégies de domaines étendus, tandis que d'autres produits peuvent hériter leurs stratégies de sous-domaines, voire disposer de stratégies propres aux hôtes.

Si les modifications de stratégies sont déployées à plusieurs niveaux de la hiérarchie du domaine de stratégie, le suivi des modifications peut devenir complexe. Une méthode pratique consiste à employer la fonction **Afficher les valeurs du domaine** pour voir quelles modifications ont été apportées à un paramètre de stratégie précis.

S'il est nécessaire de rétablir les valeurs actuelles du domaine pour le sous-domaine ou l'hôte, vous pouvez utiliser la fonction **Forcer valeur** afin d'écraser les valeurs du sous-domaine et de l'hôte en question.

👉 **Astuce:** Vous pouvez également utiliser l'**Outil de transmission de rapports** pour créer des **Rapports d'héritage** qui montrent les endroits où les paramètres hérités ont été remplacés.

Héritage des index des tables

Lorsque vous effacez une ligne d'une table à l'aide du bouton **Effacer une ligne**, le contenu de la ligne sélectionnée est effacé; le résultat de cette opération dépend des types de lignes par défaut définis dans les domaines parents et dans la base de données MIB.

- S'il existe une ligne qui possède les mêmes valeurs d'index que la ligne effacée, elle sera de nouveau héritée.
- S'il n'existe pas de ligne possédant les mêmes valeurs d'index que la ligne effacée, cette dernière restera vide après l'emploi de la fonction Effacer la ligne.

👉 **Remarque:** La ligne peut être héritée d'un domaine parent ou, en tant que ligne par défaut, d'une base MIB (définition des paramètres et contenant les valeurs par défaut pour tous les paramètres. La base de données MIB peut être considérée comme un «domaine au-dessus du domaine racine» en matière d'héritage des valeurs de nœuds non terminaux ou des lignes. Les valeurs par défaut de la base de données MIB sont transmises aux sous-domaines, sauf si elles sont supplantées au niveau du domaine. Pour écraser une ligne héritée, définissez une ligne possédant les mêmes valeurs de colonne d'index. Les valeurs par défaut de la base de données MIB sont obtenues en fonction de la version du produit installée sur les hôtes. Pour un domaine, les valeurs provenant de la version la plus récente du produit sont utilisées.

Certains produits F-Secure écrasent le déploiement des tables par défaut, si bien qu'ils n'utilisent pas le mode normal d'héritage de tables décrit ci-dessus.

Par exemple, les tables suivantes utilisent leur propre mécanisme sans héritage de base:

- Table des **règles de protection Internet**
- Table des **services de protection Internet**
- Table des **niveaux de sécurité de protection Internet**

Reportez-vous à la documentation du produit concerné pour obtenir plus d'informations sur le comportement des tables dans de tels cas.

👉 **Remarque:** Les lignes héritées et dérivées localement se distinguent par leur couleur: les lignes héritées sont de couleur grise et les lignes dérivées localement de couleur noire.

Gestion des opérations et des tâches

Vous pouvez effectuer de nombreuses opérations spécifiques au produit via Console Policy Manager.

Pour lancer une opération à partir de Console Policy Manager:

1. Sélectionnez l'une des actions dans la branche **Opérations** du produit sélectionné, sous l'onglet **Stratégie**.
2. Cliquez sur **Démarrer** pour lancer l'opération sélectionnée.
3. L'opération est lancée sur l'hôte dès que vous avez diffusé la nouvelle stratégie et que l'hôte a récupéré le fichier de stratégie.

   Vous pouvez cliquer à tout moment sur **Annuler** pour interrompre l'opération.

Alertes

Cette section décrit la façon d'afficher les alertes et les rapports et de configurer la transmission d'alertes.

Affichage des alertes et des rapports

Les hôtes peuvent émettre des alertes et des rapports en cas de problème avec un programme ou une opération.

En cas d'alerte, le bouton  s'illumine. Pour afficher les alertes :

1. Cliquez sur  .
   L'onglet **Alertes** s'affiche. Toutes les alertes reçues s'affichent au format suivant:

Accep.	Cliquez sur le bouton **Accep.** pour accuser réception d'une alerte. Si vous avez accusé réception de toutes les alertes, ce bouton est grisé.		
Gravité	La gravité du problème. Une icône est associée à chaque niveau de gravité:		
		Info	Informations de fonctionnement normal émises par un hôte.
		Avertissement	Avertissement émanant de l'hôte.
		Erreur	Erreur non fatale survenue sur l'hôte.
		Erreur fatale	Erreur fatale survenue sur l'hôte.
		Alerte de sécurité	Incident lié à la sécurité survenu sur l'hôte.
Date/Heure	Date et heure de l'alerte.		
Description	Description du problème.		
Hôte/Utilisateur	Nom de l'hôte/utilisateur.		
Produit	Le produit F-Secure qui a envoyé l'alerte.		

   Lorsque vous sélectionnez une alerte dans la liste, des informations détaillées sur celle-ci s'affichent. F-Secure les alertes d'analyse antivirus peuvent être associées à un rapport, qui s'affichera également.
2. Pour afficher les rapports, cliquez sur l'onglet **Rapports** ou sélectionnez **Vue du produit** ➤ **Messages** dans le menu.
   La structure de l'onglet **Rapports** est identique à celle de l'onglet **Alertes**. Vous pouvez trier les tables**Alertes** et les tables **Rapports** en cliquant sur l'en-tête de la colonne.

Configuration de la transmission des alertes

Vous pouvez configurer les alertes en modifiant la table **Transmission des alertes**, située sous **F-Secure Management Agent** ➤ **Paramètres** ➤ **Alertes** ➤ **Transmission des alertes**.

La même table se trouve dans la vue Produit de Management Agent sous l'onglet **Transmission des alertes**.

Pour configurer la transmission des alertes:

1. Sélectionnez **F-Secure Management Agent** ➤ **Paramètres** ➤ **Alertes** ➤ **Transmission des alertes** dans le menu.
2. Spécifiez la destination des alertes en fonction de leur niveau de gravité.

Il peut s'agir de Console Policy Manager, de l'interface utilisateur locale, d'un agent d'avertissement (comme l'**Observateur d'événements**, un fichier journal ou SMTP) ou d'une extension d'administration.

La table **Transmission des alertes** dispose de son propre jeu de valeurs par défaut.

Par défaut, les alertes d'information et d'avertissement ne sont ni envoyées à Console Policy Manager ni affichées sur l'interface utilisateur. Ces alertes et notifications de faible priorité peuvent fournir des informations très utiles pour la résolution des problèmes; toutefois, lorsqu'elles sont activées, le nombre des alertes émises augmente de façon substantielle. Si la structure de votre domaine est très étendue, la définition de règles strictes de transfert d'alertes au niveau du domaine racine peut entraîner un afflux massif d'alertes vers Console Policy Manager.

3. Si nécessaire, configurez davantage la destination des alertes en définissant les variables de stratégie dans les zones spécifiques de cette cible.
   Par exemple **Paramètres** ➤ **Alertes** ➤ **F-Secure Policy Manager Console** ➤ **Intervalle avant nouvelle tentative d'envoi** détermine à quelle fréquence un hôte tente d'envoyer des alertes à Console Policy Manager si les tentatives précédentes ont échoué.

Outil de transmission de rapports

L'**Outil de transmission de rapports** permet aux utilisateurs d'afficher et d'explorer des rapports sur les données gérées par Console Policy Manager.

Les fonctions de visualisation et d'exportation sont un moyen efficace d'examiner simultanément les données de plusieurs hôtes/domaines.

Volet Domaine de stratégie/Sélecteur d'hôte

Dans le volet **Sélecteur de domaine de stratégie**, vous pouvez sélectionner les domaines et/ou les hôtes dont les rapports vous intéressent.

Le domaine sélectionné dans l'arborescence du domaine de stratégie de la zone principale de l'application est sélectionné par défaut dans l'**Outil de transmission des rapports**.

Si vous activez la case à cocher **Récurrent**, tous les hôtes qui sont placés, de façon récurrente, sous les domaines sélectionnés de la hiérarchie de domaines sont également inclus dans le rapport.

Volet Sélecteur de type de rapport

Vous pouvez sélectionner le type de rapport que vous voulez exécuter dans ce volet.

Dans le volet **Sélecteur de type de rapport**, vous pouvez effectuer les opérations suivantes:

- sélectionner le type de rapport à établir
- sélectionner le filtrage par produits (seules les informations relatives aux produits sélectionnés sont incluses dans le rapport).

Les types de rapports suivants sont actuellement disponibles

Type de rapport	Description
Stratégie	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables de stratégie des produits sélectionnés dans les domaines sélectionnés. Vous pouvez également cocher la case **Héritage**, si vous voulez que les informations de ce type soit incluses dans le rapport.
Héritage	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables de stratégie des produits sélectionnés dans les domaines et qui ne sont pas héritées d'un domaine supérieur, c'est-à-dire toutes les variables de stratégie remplacées dans les domaines sélectionnés.
Statut	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de toutes les variables locales de paramètres et d'état des produits sélectionnés dans les domaines.
Propriétés	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les valeurs de tous les champs de propriétés des composants de domaine. Vous pouvez également utiliser le **Sélecteur de propriété** pour sélectionner les champs de propriété à inclure dans le rapport.

Type de rapport	Description
Alerte	Ce type de rapport vous permet d'exporter/de visualiser les rapports contenant les informations relatives à toutes les alertes des domaines. Vous pouvez également utiliser le Sélecteur de l'ordre du tri pour définir le tri parmi les champs de description d'alertes. Vous pouvez utiliser le Sélecteur de gravité pour sélectionner la gravité des alertes à inclure dans le rapport.
Configuration	Ce type de rapport vous permet d'exporter et de visualiser les rapports contenant les informations relatives aux produits installés parmi les produits sélectionnés dans les domaines.
Antivirus	Ce type de rapport permet d'exporter et de visualiser les rapports contenant les valeurs de l'état du domaine des versions des produits et des mises à jour des bases de données des définitions de virus.

Volet Rapport

Après avoir sélectionné un type de rapport, vous pouvez sélectionner les configurations en fonction du type dans ce volet.

Le volet Rapports permet d'effectuer les opérations suivantes:

- Sélectionner des configurations en fonction du type du rapport actuellement sélectionné. Grâce à ces configurations, l'utilisateur peut mieux adapter le filtrage en fonction du rapport à établir.
- Rechercher la description du type de rapport actuellement sélectionné.

Les configurations des types de rapports actuellement disponibles sont les suivantes

- Les configurations correspondant aux rapports de stratégie vous permettent de sélectionner les informations relatives aux valeurs de stratégie que vous souhaitez inclure dans le rapport à établir.
- Les configurations correspondant aux rapports de propriétés vous permettent de sélectionner, parmi les propriétés d'identités, de plates-formes et les propriétés diverses et d'interrogation, les informations que vous souhaitez inclure dans le rapport à établir.
- Les configurations correspondant aux rapports d'alertes vous permettent de trier les alertes par champs de description d'alerte et de sélectionner par gravité les alertes que vous souhaitez inclure dans le rapport à établir.

Volet inférieur

Après la configuration d'un rapport, vous pouvez sélectionner l'action à exécuter dans le volet inférieur de l'Outil de transmission de rapports.

Le volet inférieur vous permet d'effectuer les opérations suivantes:

- réinitialisation de tous les paramètres par défaut des composants de l'interface utilisateur
- démarrage du processus d'exportation de rapports
- démarrage du processus de visualisation de rapports
- arrêt du processus de génération de rapports
- Fermez l'interface utilisateur de l'Outil de transmission de rapports. Cela ne met pas fin à la génération d'un rapport; ce dernier est exécuté en tâche de fond. Vous pouvez mettre fin à la génération du rapport à l'aide de la boîte de dialogue qui s'affiche.

Affichage et exportation d'un rapport

Vous pouvez et afficher des rapports à l'aide de l'**Outil de transmission des rapports**.

Pour utiliser l'**Outil de transmission des rapports**:

1. Sélectionnez **Outils** ➤ **Rapports...** dans le menu.
   Autre possibilité:
   - Lancez l'**Outil de transmission des rapports** à partir du menu contextuel de la zone principale de l'application.

   L'**Outil de transmission de rapports** s'ouvre.
2. Sélectionnez les domaines et/ou les hôtes que vous voulez inclure dans le rapport.
   - Sélectionnez **Récurrent**, si vous voulez que tous les hôtes se trouvant dans les domaines sélectionnés soient inclus au rapport.
3. Sélectionnez le type de rapport.
4. Sélectionnez les produits à inclure dans le rapport, si nécessaire.
5. Sélectionnez des configurations en fonction du rapport actuellement sélectionné, si nécessaire.
6. Afficher ou exporter le rapport:
   - Cliquez sur **Afficher** dans le volet inférieur pour générer le rapport et l'afficher au format HTML sur votre navigateur Web par défaut. Si vous n'avez défini aucun navigateur Web par défaut, une boîte de dialogue s'ouvre et vous invite à définir votre navigateur Web.
   - Cliquez sur **Exporter** dans le volet inférieur pour générer le rapport et l'enregistrer sous forme de fichier. Le chemin d'accès au fichier et le format du rapport sont définis dans la boîte de dialogue **Enregistrer le fichier** qui s'affiche après avoir cliqué sur **Exporter**.

Préférences

Les paramètres de préférences sont soit partagés, soit appliqués à une connexion donnée.

Préférences spécifiques à une connexion

Pour modifier ces préférences, choisissez la commande **Préférences** dans le menu **Outils**; seule la connexion actuelle est affectée.

Onglet	Paramètre	Signification
Communication	**Intervalles d'interrogation**	Intervalles d'interrogation de différents types de fichiers. Vous pouvez sélectionner ou désélectionner les cases afin d'activer ou de désactiver l'interrogation d'un type de fichier donné. Cochez la case **Désactiver toutes les interrogations**, si vous souhaitez toujours utiliser les opérations d'actualisation manuelle au lieu de l'interrogation automatique.
	Etat de connexion de l'hôte	Détermine quand les hôtes sont considérés comme déconnectés de Policy Manager. Tous les hôtes qui n'ont pas contacté Serveur Policy Manager dans l'intervalle défini sont considérés comme déconnectés. Les hôtes déconnectés sont signalés par une icône de notification dans l'arborescence, et ils sont placés dans la liste **Hôtes déconnectés** de la vue **Etat du domaine**. Les icônes de notification de l'arborescence des domaines peuvent être désactivées à l'aide de la section **Aspect** ➤ **Options du domaine de stratégie**. Notez qu'il est possible de définir un intervalle de moins d'un jour en entrant un nombre à décimales dans la zone de saisie. Par exemple, si vous entrez une valeur de `0,5`, tous les hôtes qui n'ont pas contacté le serveur dans les 12 heures sont considérés comme déconnectés. Les valeurs inférieures à un jour ne servent normalement qu'à des fins de dépannage. Dans un environnement traditionnel, certains hôtes sont naturellement déconnectés du serveur de temps à autre. Par exemple, il se peut qu'un ordinateur portable soit incapable d'accéder quotidiennement au serveur, mais dans la plupart des cas, ce comportement est tout à fait acceptable.
	Options des alertes et des rapports	Ces options contrôlent: • la suppression automatique des alertes et des rapports anciens, • le chargement en arrière-plan des alertes et des rapports.
Options de communication avancées	**Cache d'état**	Permet de définir le nombre d'hôtes pour lesquels Console Policy Manager place les informations d'état en mémoire cache.
	Désactivation du chargement de l'état initial	Vous pouvez désactiver le chargement de l'état initial si vous voulez réduire le temps nécessaire au démarrage de Console Policy Manager dans un environnement de grande taille. Il s'agit d'une option avancée qui doit être utilisée avec prudence, car elle provoque les différences fonctionnelles suivantes par rapport au traitement normal des états: • Aucun logiciel ne semble installé sur les hôtes. Cela affecte l'**Editeur d'installation**.

Onglet	Paramètre	Signification
		• Les éléments d'état ne sont pas disponibles dans un premier temps. Cela affecte les affichages de produits, quand l'onglet **Etat** est sélectionné. • Tous les hôtes reçoivent des stratégies générées à partir de la version la plus récente de la base de données MIB, car les informations de version de cette dernière ne sont pas disponibles. La désactivation de l'option de chargement de l'état initial n'influe pas sur l'actualisation d'état manuelle ni sur la recherche d'état périodique. Si nécessaire, vous pouvez désactiver la recherche d'état automatique. Pour ce faire: **1.** Sélectionnez **Outils** ➤ **Préférences** dans le menu. **2.** Sélectionnez l'onglet **Communications** et cliquez sur **Options de période d'interrogation**. **3.** Sélectionnez **Désactiver toutes les interrogations**.
Fichiers de stratégie	**Optimisations des fichiers de stratégie**	La Mise en retrait détermine si des caractères de séparation seront ajoutés au fichier lors de sa création, ce qui facilite sa lecture par un opérateur. Si vous désactivez la **Mise en retrait**, aucun caractère de séparation n'est ajouté aux fichiers. Ceux-ci sont moins lisibles pour un opérateur, mais ils restent tout à fait corrects et peuvent toujours être lus par un ordinateur. Les séparateurs peuvent être des espaces ou des tabulations. Il est conseillé d'employer des tabulations, le fichier produit étant de taille plus réduite qu'en cas d'emploi d'espaces. L'option **Inclure des commentaires** influe sur la taille des fichiers de stratégie produits par Console Policy Manager. Ces commentaires servent à rendre le fichier plus compréhensible par l'utilisateur s'il veut directement lire les valeurs dans le fichier. Ces paramètres ne sont employés qu'à des fins de débogage et doivent être désactivés pour une utilisation normale en environnement de production.
	Numéro de série du fichier de stratégie	Numéro de série des fichiers de stratégie de base générés. Le numéro de série s'incrémente automatiquement. Normalement, il n'est pas nécessaire de l'ajuster manuellement. Vous avez uniquement besoin d'augmenter cette valeur si des hôtes n'acceptent pas des fichiers de stratégie à cause de numéros de série trop petits (qu'ils signalent comme des erreurs). Dans ce cas, vous devez augmenter le numéro de série de façon à ce qu'il soit supérieur au numéro de série du dernier fichier de stratégie de base récupéré par les hôtes.
Installation distante	**Délai d'installation**	Délai maximal pendant lequel Console Policy Manager attend les résultats d'une opération d'installation.
	Délai de navigation	Ce paramètre est important uniquement si l'option **Masquer les hôtes déjà administrés** est activée. Il s'agit de la durée maximale accordée pour accéder au Registre de l'hôte.

Onglet	Paramètre	Signification
	Nombre maximal d'opérations réseau simultanées	Vous pouvez régler le nombre d'opérations sur le réseau. Il est conseillé de conserver la valeur par défaut, mais si vous employez une connexion réseau lente qui pose des problèmes lors d'installations distantes, diminuez le nombre de connexions réseau simultanées en conséquence.
	Indicateur d'avancement	Vous pouvez choisir si l'indicateur d'avancement doit être affiché pour l'utilisateur final au cours d'une installation distante.

Préférences partagées

Elles s'appliquent à toutes les connexions définies dans une installation spécifique de Console Policy Manager.

Onglet	Paramètre	Signification
Aspect ➤ Options générales	Langue	Il s'agit du choix de la langue. Vous pouvez sélectionner la langue utilisée par votre système d'exploitation ou le paramètre Anglais par défaut. Tous les objets ne prenant pas en charge la langue utilisée par votre système d'exploitation seront affichés en anglais. Vous devez redémarrer Console Policy Manager pour que les modifications entrent en vigueur.
Aspect ➤ Domaines de stratégie	Surbrillance des hôtes déconnectés	Vous pouvez mettre en surbrillance les hôtes déconnectés dans l'arborescence d'un domaine de stratégie.
	Police	Police employée dans Console Policy Manager. Le changement de police entre en vigueur après le redémarrage du programme.
	Style	Définit l'aspect et le comportement des composants de l'interface utilisateur. Le changement entre en vigueur après le redémarrage du programme.
Fichiers de stratégie	Produits	Permet de désactiver des MIB pour des produits que vous n'avez pas installés, et de les exclure des fichiers de stratégie distribués. La désactivation des MIB réduit la taille des fichiers de stratégie envoyés aux hôtes administrés. ⚠ **Avertissement:** Ne désactivez les MIB que si vous êtes invité à le faire par F-Secure. Leur désactivation pour des produits qui sont installés sur certains hôtes administrés entraînera un dysfonctionnement du système.
Installation distante	Effacer le cache	Pour libérer de l'espace sur le disque, vous pouvez effacer toutes les informations placées en mémoire cache et relatives aux hôtes examinés et aux logiciels installés.
Emplacement	Chemin du navigateur HTML	Il s'agit du chemin d'accès complet du fichier exécutable du navigateur HTML. Utilisez le navigateur pour visualiser les pages d'aide en ligne et les rapports relatifs aux virus.
	Chemin des journaux de messages	Entrez un chemin vers un répertoire où seront créés les fichiers journaux pour chaque onglet de la vue Messages. Chaque fichier journal contient le titre de l'onglet correspondant et un message par ligne comprenant sa gravité et l'heure de création.

Onglet	Paramètre	Signification
	Enregistrer les messages	Permet d'activer ou de désactiver l'enregistrement de messages. Nous vous recommandons vivement de conserver la consignation, car les informations du journal peuvent s'avérer très utiles pour le dépannage.
Antivirus	**Définitions de virus**	Cette valeur vous permet de définir le moment où les définitions de virus sont considérées comme obsolètes en mode **Antivirus**.

Chapitre

4

Maintenance de Serveur Policy Manager

Sujets :

Vous y trouverez toutes les instructions relatives à la sauvegarde et à la restauration des données de la console dans Serveur Policy Manager.

Sauvegarde et restauration des données de Console Policy Manager

Serveur Policy Manager peut être maintenu en exécutant des opérations routinières de sauvegarde des données de la console sur le serveur, s'il doit être restauré.

Nous vous recommandons vivement de sauvegarder régulièrement les informations d'administration les plus importantes. Sauvegardez au moins la totalité du sous-répertoire `fsa\domains` du répertoire de communication. Le répertoire de communication, nommé `commdir\` se trouve généralement dans le répertoire d'installation de Serveur Policy Manager. Ce répertoire contient la structure du domaine de stratégie, ainsi que toutes les données de stratégie enregistrées.

👉 **Remarque:** Avant de sauvegarder le répertoire `fsa\domains`, assurez-vous qu'aucune session Console Policy Manager n'est ouverte.

Il est également possible de sauvegarder tout le référentiel. Cela vous permet de récupérer non seulement la structure du domaine de stratégie mais aussi les alertes, les statistiques des hôtes et les opérations d'installation. Vous pouvez également récupérer rapidement les fichiers de stratégie. Lorsque vous ne sauvegardez que le sous-répertoire `fsa\domains`, vous devez distribuer les stratégies par la suite. La sauvegarde de la totalité du référentiel présente l'inconvénient que ce dernier peut contenir plus de données que le répertoire `fsa\domains`. De plus, vous devez arrêter Serveur Policy Manager avant d'effectuer la sauvegarde complète.

Pour sauvegarder le jeu de clés d'administration, copiez les fichiers `admin.prv` et `admin.pub` qui se trouve à la racine du répertoire d'installation local de Console Policy Manager. Stockez le fichier `admin.prv` dans un emplacement sûr. Il est très important d'enregistrer une copie de sauvegarde du fichier de clés `admin.prv`.

👉 **Remarque:** Si vous perdez une clé d'administration (`admin.pub` ou `admin.prv`), vous devrez créer une nouvelle paire et distribuer la clé `admin.pub` respective sur tous les hôtes administrés en réinstallant chacun d'eux manuellement, les opérations par stratégie n'étant plus utilisables. La relation d'approbation entre Console Policy Manager et les hôtes administrés repose sur une signature numérique. Sans clé privée valide, il n'est pas possible de créer une signature valable que les hôtes acceptent.

Si vous voulez enregistrer les préférences de Console Policy Manager, sauvegardez le fichier `lib\Administrator.properties` à partir du répertoire d'installation local.

👉 **Remarque:** Le fichier `Administrator.properties` est créé lors de la première exécution de Console Policy Manager et contient des informations associées à la session, telles que la taille de la fenêtre ou l'URL du serveur.

Création de la sauvegarde

Vous pouvez créer une sauvegarde complète ou uniquement une sauvegarde des données de la stratégie et de la structure du domaine.

- La sauvegarde complète inclut la structure des domaines de stratégie, les alertes, les statistiques des hôtes et les opérations d'installation.
- La sauvegarde des données de la stratégie et de la structure du domaine inclut le sous-répertoire `fsa\domains` du répertoire Serveur Policy Manager (`Commdir`).

1. Pour créer une sauvegarde complète:
   a) Fermez toutes les sessions de gestion de Console Policy Manager.
   b) Arrêtez le service Serveur Policy Manager.
   c) Sauvegardez le `répertoire de communication`.
   d) Sauvegardez le répertoire `<Dossier d'installation de F-Secure>\Management Server 5\data\db`.
   e) Sauvegardez les fichiers `admin.prv` et `admin.pub` placés à la racine du répertoire d'installation local de Console Policy Manager.
   f) Sauvegardez le fichier `lib\Administrator.properties` dans le répertoire d'installation local Console Policy Manager.
   g) Redémarrez le service Serveur Policy Manager.
   h) Ouvrez à nouveau les sessions de gestion de Console Policy Manager.
2. Pour créer une sauvegarde des données de stratégie et de la structure de domaine:
   a) Fermez toutes les sessions de gestion Console Policy Manager.
   b) Sauvegardez le répertoire `fsa\domains` et conservez la sauvegarde dans un endroit sûr.
   c) Rouvrez les sessions d'administration de Console Policy Manager.

Restauration de la sauvegarde

En cas de perte des données Policy Manager, vous pouvez restaurer les données récemment sauvegardées.

Pour restaurer des données Policy Manager sauvegardées:

1. Si vous avez sauvegardé tout le contenu du répertoire de communication et les informations de la console (sauvegarde complète), procédez comme suit pour les restaurer:
   a) Fermez toutes les sessions de gestion Console Policy Manager et arrêtez le service Serveur Policy Manager.
   b) Supprimez le répertoire de communication.
   c) Copiez la sauvegarde du répertoire de communication à son emplacement correct.
   d) Copiez la sauvegarde du répertoire `<Dossier d'installation de F-Secure>\Management Server 5\data\db` à l'emplacement qui convient.
   e) Copiez la clé `admin.pub` à la racine du répertoire d'installation de Console Policy Manager.
   f) Copiez la clé `admin.prv` à la racine du répertoire d'installation de Console Policy Manager.
   g) Copiez les préférences de la console (`Administrator.properties`) dans le répertoire `<répertoire d'installation de la console>\lib`.
   h) Redémarrez le service Serveur Policy Manager.
   i) Ouvrez à nouveau les sessions de gestion de Console Policy Manager.
   j) distribuer des stratégies
2. Si vous n'avez sauvegardé que la structure du domaine de stratégie, procédez comme suit pour la restaurer:
   a) Fermez toutes les sessions de gestion de Console Policy Manager et arrêtez le service Serveur Policy Manager.
   b) Supprimez le contenu du répertoire `<répertoire de communication>\fsa\domains`.
   c) Copiez les données sauvegardées dans le répertoire indiqué ci
   d) Redémarrez le service Serveur Policy Manager.
   e) Ouvrez à nouveau toutes les sessions de gestion de Console Policy Manager.
   f) distribuer des stratégies

Duplication de logiciels à l'aide de fichiers image

Si vous utilisez des fichiers d'image pour distribuer des installations de produit, vous devez vous assurer que les identifiants uniques n'entrent pas en conflit.

Anti-virus peut être inclus lors de la duplication de logiciels à l'aide de fichiers image de disque. Cependant, chaque installation d'un produit comprend un code d'identification unique (ID unique) utilisé par Policy Manager. Si vous employez une image de disque pour installer des logiciels sur de nouveaux ordinateurs, il se peut que plusieurs ordinateurs tentent d'utiliser le même ID unique. Une telle situation empêche Policy Manager de fonctionner correctement.

Procédez comme suit pour vous assurer que chaque ordinateur emploiera un ID unique personnalisé, même en cas d'emploi d'images de disque:

1. Installez le système et tous les logiciels à inclure dans le fichier image, avec entre autres Anti-virus.
2. Configurez Anti-virus pour qu'il utilise le bon serveur Serveur Policy Manager.

   Remarque: N'importez pas l'hôte dans Console Policy Manager s'il a envoyé une demande d'auto-enregistrement à Serveur Policy Manager. Vous ne devez importer que les hôtes sur lesquels le fichier image sera installé.

3. Exécutez la commande `fsmautil resetuid` à partir de l'invite de commande.

   Cet utilitaire se trouve généralement dans le répertoire `C:\Program Files\F-Secure\Common`. Ce répertoire peut être différent si vous employez une version localisée de Windows ou si vous avez choisi un chemin d'installation différent du chemin par défaut.

4. Arrêtez l'ordinateur.

   Remarque: Ne redémarrez pas l'ordinateur à cette étape.

5. Créez le fichier d'image de disque.
   L'utilitaire réinitialise l'ID unique dans l'installation de Anti-virus. Un nouvel ID unique est créé automatiquement lors du redémarrage du système. L'opération s'effectue individuellement sur chaque ordinateur où le fichier image est installé. Ces ordinateurs enverront des demandes d'auto-enregistrement à Policy Manager et les demandes seront traitées normalement.

Chapitre

5

Mise à jour des bases de données de définition de virus

Sujets :

Les bases de données de définition des virus doivent être maintenues à jour afin de garantir une protection optimale contre les nouvelles menaces.

Mises à jour automatiques avec Agent de mise à jour automatique

Avec Agent de mise à jour automatique, vous pouvez obtenir les mises à jour des bases de données de définitions de virus ainsi que des informations sans avoir à interrompre leur travail pour télécharger les fichiers à partir d'Internet.

Agent de mise à jour automatique télécharge automatiquement les fichiers en tâche de fond en utilisant la bande passante inutilisée par d'autres applications Internet. Ainsi, l'utilisateur est sûr de disposer des mises à jour les plus récentes et ce, sans avoir à effectuer de recherches sur Internet.

Si Agent de mise à jour automatique est connecté en permanence à Internet, il reçoit automatiquement les mises à jour dans les deux heures qui suivent leur publication par F-Secure. Les éventuels retards dépendent de la disponibilité de la connexion à Internet.

Agent de mise à jour automatique sert à mettre à jour les produits F-Secure qu'il soit géré de manière centralisée ou installé sur un ordinateur autonome. Par défaut, l'agent télécharge aussi les informations sur les virus. Si vous le souhaitez, vous pouvez désactiver le téléchargement de ces informations. Vous pouvez installer et utiliser Agent de mise à jour automatique avec des produits de sécurité Anti-virus.

Fonctionnement de Agent de mise à jour automatique

Agent de mise à jour automatique interroge régulièrement le serveur pour savoir si de nouvelles données sont disponibles, qu'il téléchargera automatiquement par la suite.

Quand le service Agent de mise à jour automatique est démarré, il se connecte au serveur de mise à jour F-Secure. L'agent interroge régulièrement le serveur pour savoir si de nouvelles données sont disponibles. Les nouvelles données sont automatiquement téléchargées. L'intervalle de récupération est défini par le serveur et ne peut être ajusté à partir du client.

Dans Policy Manager 6.0 et versions ultérieures, Agent de mise à jour automatique installé avec F-Secure tente de télécharger les mises à jour automatiques à partir des sources de mises à jour configurées dans l'ordre suivant:

1. Si des proxies Policy Manager sont utilisés dans le réseau de l'entreprise, le client tente de se connecter à Serveur Policy Manager par l'intermédiaire de chaque proxy Policy Manager à tour de rôle.
2. Si le client est configuré pour utiliser le proxy HTTP, il tente de télécharger les mises à jour par le biais du proxy HTTP à partir du serveur de mise à jour Serveur Policy Manager.
3. Ensuite, le client tente de télécharger les mises à jour directement depuis Serveur Policy Manager.
4. Si des proxies Policy Manager sont utilisés dans le réseau de l'entreprise, le client tente de se connecter au serveur de mise à jour F-Secure par l'intermédiaire de chaque proxy Policy Manager à tour de rôle.
5. Si le client est configuré pour utiliser le proxy HTTP, il tente de télécharger les mises à jour par le biais du proxy HTTP à partir du serveur de mise à jour de F-Secure.
6. Le client tente ensuite de télécharger les mises à jour directement depuis le serveur de mise à jour de F-Secure.

Avantages de Agent de mise à jour automatique

Agent de mise à jour automatique télécharge automatiquement les mises à jour et économise la bande passante.

Téléchargements optimisés des mises à jour de définitions de virus

Agent de mise à jour automatique détecte la date à laquelle la base de données des définitions de virus a été modifiée. Il s'appuie sur des algorithmes de quelques octets pour télécharger uniquement les modifications et non pas l'ensemble des fichiers ou de la base de données. Les modifications ne représentent généralement qu'une petite fraction de la mise à jour complète, ce qui permet aux utilisateurs distants disposant de modems

lents d'obtenir aisément les mises à jour quotidiennes. Cela permet également aux utilisateurs disposant d'une liaison permanente d'économiser une part non négligeable de la bande passante.

Possibilité de reprendre un transfert de données interrompu

Agent de mise à jour automatique peut télécharger ses données en plusieurs sessions. Si le téléchargement est interrompu, Agent de mise à jour automatique enregistre ce qui a été téléchargé et poursuit le téléchargement des fichiers restants lors de la connexion suivante.

Mises à jour automatiques

Vous n'avez pas à rechercher les dernières mises à jour et à les télécharger manuellement. Grâce à Agent de mise à jour automatique, vous obtenez automatiquement les dernières mises à jour des définitions de virus publiées par F-Secure.

Utilisation de Agent de mise à jour automatique

Vous pouvez configurer le logiciel Agent de mise à jour automatique en modifiant le fichier de configuration `fsaua.cfg`.

Configuration de Agent de mise à jour automatique

Avec Policy Manager 7.0 et versions ultérieures, Agent de mise à jour automatique installé avec Policy Manager est configuré en modifiant le fichier de configuration `fsaua.cfg`.

👉 **Important:** Ces instructions de configuration s'appliquent uniquement à Agent de mise à jour automatique installé avec Serveur Policy Manager. Vous ne devez modifier que les paramètres mentionnées ci-dessous. Ne modifiez pas les autres paramètres dans le fichier de configuration.

Pour configurer Agent de mise à jour automatique:

1. Ouvrez le fichier de configuration `fsaua.cfg` qui se trouve à l'emplacement suivant: `C:\Program Files\F-Secure\FSAUA\program\fsaua.cfg`.
2. Spécifiez les proxies HTTP:

   La directive `http_proxies` contrôle les proxies HTTP utilisés par Agent de mise à jour automatique. Utilisez le format suivant:

   ```
   http_proxies=[http://][[domain\]user[:passwd]@]<address>[:port]
   [,[http://][[domain\]user[:passwd]@]<address>[:port]]
   ```

   Exemples:

   ```
   http_proxies=http://proxy1:8080/,http://backup_proxy:8880/,
   http://domain\username:usernamespassword@ntlmproxy.domain.com:80
   ```

3. Spécifiez l'intervalle d'interrogation:

   La directive `poll_interval` spécifie la fréquence à laquelle Agent de mise à jour automatique recherche de nouvelles mises à jour. Le paramètre par défaut est de 1800 secondes, soit une demi heure.

   ```
   poll_interval=1800
   ```

   👉 **Remarque:** Si l'intervalle d'interrogation minimum défini sur le serveur de mise à jour F-Secure est de 2 heures par exemple, les paramètres du fichier de configuration Agent de mise à jour automatique ne peuvent pas écraser cette limite.

4. Enregistrez le fichier et fermez-le.
5. Vous devez arrêter le service **fsaua** et le redémarrer pour que les modifications soient prises en compte.

   Pour ce faire, saisissez les commandes suivantes sur la ligne de commande:

   ```
   net stop fsaua
   ```

   ```
   net start fsaua
   ```

Lire le fichier journal

Le fichier `fsaua.log` est utilisé pour stocker les messages générés par Agent de mise à jour automatique.

Certains des messages fournissent des informations sur les opérations normales, tels que le démarrage et la fermeture. D'autres messages indiquent des erreurs.

Le fichier `fsaua.log` se trouve à l'emplacement `C:\Program Files\F-Secure\FSAUA\program`.

Chaque message du journal comporte les informations suivantes:

- Date et heure de génération de l'alerte.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

- Explication rapide de ce qui s'est passé. Lorsqu'une mise à jour est téléchargée, le nom et la version de la mise à jour sont indiqués.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

- Pour les mises à jour, le message indique également la source de la mise à jour et la taille du téléchargement.

```
[ 3988]Thu Oct 26 12:40:39 2006(3): Downloaded 'F-Secure Anti-Virus Update
2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com,
 12445450 bytes (download size 3853577)
```

Messages dans fsaua.log

Des exemples de messages apparaissant dans le fichier journal sont présentés ci-dessous.

Message	Signification
`Update check completed successfully`	La connexion à la source des mises à jour a réussi.
`Update check completed successfully. Aucune mise à jour n'est disponible.`	La connexion à la source des mises à jour a réussi, mais il n'y avait rien à télécharger.
`Downloaded 'F-Secure Anti-Virus Update 2006-10-26_04' - 'DFUpdates' version '1161851933' from fsbwserver.f-secure.com, 12445450 bytes (download size 3853577)`	La connexion a réussi et des fichiers ont été téléchargés.
`Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success`	Les fichiers ont été correctement placés dans le répertoire de destination (et les fichiers existants ont été supprimés). Ce résultat est celui de la mise à jour du répertoire de communication. Notez que Agent de mise à jour automatique ne peut pas indiquer si les nouveaux fichiers ont été utilisés par les hôtes ou non.
`Update check failed. Erreur de connexion de fsbwserver.f-secure.com (échec de la consultation DNS)`	Message d'erreur indiquant que la vérification des mises à jour a échoué.

Comment vérifier que tout fonctionne à partir du journal?

Quand tout fonctionne normalement, le résultat de la dernière installation pour chaque mise à jour téléchargée doit être indiqué comme `Success`. Par exemple:

```
Installation of 'F-Secure Anti-Virus Update 2006-10-26_04' : Success
```

Vous pouvez également voir un résumé des statuts de mises à jour DeepGuard, des logiciels espions et virus sur le server sous l'onglet **Résumé** de Console Policy Manager.

Pour vérifier le statut de la mise à jour sur un hôte géré de façon centralisée, allez à la page **Etat** ➤ **Protection globale** dans Console Policy Manager.

Activation forcée de Agent de mise à jour automatique pour vérifier immédiatement les nouvelles mises à jour

Si vous devez forcer l'activation de Agent de mise à jour automatique pour rechercher immédiatement de nouvelles mises à jour, vous devez utiliser l'interface de Agent de mise à jour automatique.

Pour cela :

1. Sélectionnez **Démarrer** ➤ **Programmes** ➤ **F-Secure Policy Manager** ➤ **F-Secure Automatic Update Agent** pour ouvrir l'interface de l'application Agent de mise à jour automatique.
2. Cliquez sur **Vérifier maintenant** pour vérifier l'existence de nouvelles mises à jour.
   La ligne **Communication** indiquera l'état actuel de la mise à jour.

Mise à jour manuelle des bases de données

Si votre ordinateur n’est pas connecté à Internet, vous pouvez mettre à jour manuellement les bases de données.

1. Connectez-vous à http://support.f-secure.com/ à partir d'un autre ordinateur.
2. Téléchargez l'outil `fsdbupdate.exe`.
3. Transférez l'outil `fsdbupdate.exe` sur votre ordinateur, par exemple, en utilisant un support amovible et exécutez-le.

Dépannage

Vous trouverez ci-dessous des exemples de problèmes qui peuvent être consignés comme messages d'erreur dans le fichier `fsaua.log`.

Problème	**Raison**	**Solution**
Un échec de consultation DNS a eu lieu ou la connexion a échoué, a été perdue ou refusée.	Problèmes de réseau	Vérifiez que le réseau est correctement configuré.
Échec de l'authentification du proxy.	Le mot de passe saisi pour le proxy HTTP est incorrect.	Vérifiez et corrigez le mot de passe du proxy HTTP dans la directive `http_proxies` du fichier `fsaua.cfg`.
Le disque est plein ou une erreur d'E/S s'est produite.	Il n'y a pas assez d'espace disque libre sur le lecteur sur lequel le répertoire de destination est situé.	Libérez de l'espace disque afin que la mise à jour puisse s'effectuer
Une erreur serveur ou une erreur non spécifiée s'est produite.	Inconnu	-

Chapitre
6

Utilisation du produit sous Linux

Sujets :

Policy Manager fonctionne sous Linux comme sous Windows, même si certaines fonctions ne sont pas disponibles et si la procédure d'installation est différente.

Présentation

Vous trouverez ici des informations générales sur l'utilisation et l'installation du produit sous Linux.

Différences entre Windows et Linux

Services non disponibles lorsque la Console Policy Manager est exécutée sous Linux :

- Fonctions d'installation poussée,
- l'exportation de paquet d'installation Windows (MSI),
- découverte automatique de postes de travail sur le réseau.

Distributions prises en charge

Policy Manager prend en charge de nombreuses distributions Linux basées sur le système de paquet de gestion Debian (DEB) et sur le système de gestion de paquet Redhat (RPM). Les deux versions, 32-bit et 64-bit, des distributions sont prises en charge.

Distribution prise en charge	Système d'empaquetage
Red Hat Enterprise Linux 4, 5	RPM
SUSE Linux Enterprise Server 9, 10, 11	RPM
SUSE Linux Enterprise Desktop 10, 11	RPM
openSUSE 11.2	RPM
Debian GNU Linux Lenny 5.0	DEB
Ubuntu 8.04 Hardy	DEB

Installation

Policy Manager s'installe en trois parties.

Vous devez installer les composants du produit dans l'ordre suivant :

1. Agent de mise à jour automatique
2. Serveur Policy Manager
3. Console Policy Manager

Vous devez installer le Serveur Policy Manager et l'Agent de mise à jour automatique sur le même ordinateur.

Vous pouvez installer la Console Policy Manager sur le même ordinateur ou sur un autre ordinateur.

👉 **Remarque:** Lorsque vous effectuez une mise à niveau de version de Policy Manager où Web Reporting a été installé, vous devez d'abord désinstaller Web Reporting avant de mettre à niveau le Serveur Policy Manager.

👉 **Remarque:** Pour plus d'informations sur le processus d'installation et de mise à niveau de Policy Manager, reportez-vous aux notes de version.

Notes d'installation

Distributions Red Hat et Suse :

- Certaines plateformes nécessitent la bibliothèque de compatibilité `libstdc++`. Installez les paquets suivants avant d'installer le Serveur Policy Manager :
  - Pour Red Hat Enterprise Linux 4 and 5, installez le paquet `compat-libstdc++-33`.
  - Pour 32-bit openSuse 11.2, installez le paquet `libstdc++33`.
  - Pour 64-bit openSuse 11.2, installez le paquet `libstdc++33-32bit`.
- Lorsque vous installez le Serveur Policy Manager et la Console Policy Manager sur une plateforme 64-bit, vous devez utiliser la version 64-bit des paquets d'installation.

Distributions Debian et Ubuntu :

- Le Serveur Policy Manager nécessite la bibliothèque de compatibilité `libstdc++`. Installez le paquet `libstdc++5` avant d'installer le Serveur Policy Manager. Si l'installation n'a pas été acheté faut de bibliothèque de compatibilité, installez la bibliothèque puis utilisez la commande `apt-get install -f` pour terminer l'installation du produit.
- Lorsque vous installez le Serveur Policy Manager et la Console Policy Manager sur une plateforme 64-bit, vous devez utiliser la version 64-bit du paquet d'installation. En outre :
  - Installez le paquet `ia32-libs` avec les bibliothèques Runtime pour l'architecture ia32/i386 avant d'installer le Serveur Policy Manager.
  - Installez le paquet Agent de mise à jour automatique en choisissant l'option `--force-architecture`.

Installez l'Agent de mise à jour automatique et le Serveur Policy Manager

La première étape consiste à installer l'Agent de mise à jour automatique F-Secure et le Serveur Policy Manager.

1. Connectez-vous en tant que `root`.

   Si vous installez le produit sur une distribution Ubuntu, connectez-vous en tant qu'utilisateur normal ajouté à `/etc/sudoers`.

2. Ouvrez un terminal.
3. Pour l'installer, saisissez les commandes suivantes :

Type de distribution	Commande
Distributions basées Debian	`dpkg -i f-secure-automatic-update-agent_<version_number>.<build number>_i386.deb` `dpkg -i f-secure-policy-manager-server_<version_number>.<build number>_i386.deb`
Distributions basées RPM	`rpm -i f-secure-automatic-update-agent-<version_number>.<build number>-1.i386.rpm` `rpm -i f-secure-policy-manager-server-<version_number>.<build number>-1.i386.rpm`
Distributions Ubuntu	`sudo dpkg -i f-secure-automatic-update-agent_<version_number>.<build number>_i386.deb` `sudo dpkg -i f-secure-policy-manager-server_<version_number>.<build number>_i386.deb`

4. Pour le configurer, saisissez `/opt/f-secure/fsaua/bin/fspms-config` et répondez aux questions.
   Pour les distributions Ubuntu, saisissez `sudo /opt/f-secure/fsaua/bin/fspms-config`.
   Appuyez sur Entrée pour sélectionner la configuration par défaut (entre crochets).
5. Connectez-vous en tant qu'utilisateur normal et saisissez les commandes suivantes pour vérifier le statut des compotants :
   - `/etc/init.d/fsaua status`
   - `/etc/init.d/fspms status`

   Vous pouvez également ouvrir votre navigateur et aller aux URL suivantes :
   - `http://localhost` - statut du Serveur Policy Manager
   - `http://localhost/B` - statut du serveur de mise à jout automatique
   - `http://localhost:8081` - statut de Web Reporting

Une fois le script de configuration terminé, l'Agent de mise à jour automatique et le Serveur Policy Manager sont exécutés et démarreront automatiquement dès que l'ordinateur aura été relancé.

Installez la Console Policy Manager

Ensuite, installez la Console Policy Manager.

1. Connectez-vous en tant que `root`.
   Si vous installez le produit sur une distribution Ubuntu, connectez-vous en tant qu'utilisateur normal ayant été ajouté à `/etc/sudoers`.
2. Ouvrez un terminal.

3. Pour installer le type :

Type de distribution	Commande
Distributions basées Debian	`dpkg -i f-secure-policy-manager-console_<version_number>.<build number>_i386.deb`
Distributions RPM	`rpm -i f-secure-policy-manager-console-<version_number>.<build number>-1.i386.rpm`
Distributions Ubuntu	`sudo dpkg -i f-secure-policy-manager-console_<version_number>.<build number>_i386.deb`

   La Console Policy Manager est installée sous `/opt/f-secure/fspmc/`. Un nouveau groupe d'utilisateurs nommé `fspmc` est automatiquement créé.

4. Ajoutez ces utilisateurs au groupe `fspmc`.

   Vous devez procéder ainsi avant qu'ils ne puissent exécuter la Console Policy Manager:

   a) Vérifiez à quels groupes l'utilisateur appartient :

      `groups <user id>`

      Ainsi, si l'utilisateur estTom :

      `groups Tom`

   b) Ajoutez cet utilisateur au groupe `fspmc` :

      `/usr/sbin/usermod -G fspmc,<groupes auxquels l'utilisateur appartient (sous forme de liste séparée par des virgules)> <user id>`

      Ainsi, si Tom appartient aux groupes `normal_users` et `administrators` la commande est :

      `/usr/sbin/usermod -G fspmc,normal_users,administrators Tom`

      Remarque: La liste de groupes séparés par des virgules remplace les groupes auxquels l'utilisateur a appartenu.

5. Sélectionnez la Console Policy Manager dans le sous-menu F-Secure du menu **Programmes**.

   Vous pouvez également démarrer la Console Policy Manager depuis la ligne de commande en saisissant `sg fspmc -c /opt/f-secure/fspmc/fspmc`.

   Remarque: Sous Red Hat Enterprise Linux 4, vous devez vous déconnecter puis vous reconnecter avant d'utiliser l'élément de menu **Programmes**. De même, étant donné que la commande `sg` n'accepte pas l'argument `<command>`, vous pouvez utiliser `newgrp` dans la ligne de commande :

   - `newgrp fspmc`
   - `/opt/f-secure/fspmc/fspmc`

Lors du premier démarrage de la Console Policy Manager, vous serez invité à répondre à quelques questions pour compléter la configuration. Ces questions sont les mêmes que dans la version Windows.

Désinstallation du produit.

Pour désinstaller Policy Manager sous Linux, vous devez désinstaller les composants dans un ordre donné.

Vous devez désinstaller les 3 composants dans l'ordre suivant :

1. Serveur Policy Manager
2. Agent de mise à jour automatique
3. Console Policy Manager

1. Connectez-vous en tant que `root`.

   Si le produit est installé sur une distribution Ubuntu, connectez-vous en tant qu'utilisateur normal ayant été ajouté à `/etc/sudoers`.
2. Ouvrez un terminal.
3. Saisissez les commandes suivantes dans l'ordre indiqué :

Type de distribution	Commande
Distributions basées Debian	1. `dpkg -r f-secure-policy-manager-server` 2. `dpkg -r f-secure-automatic-update-agent` 3. `dpkg -r f-secure-policy-manager-console`
Distributions basées RPM	1. `rpm -e f-secure-policy-manager-server` 2. `rpm -e f-secure-automatic-update-agent` 3. `rpm -e f-secure-policy-manager-console`
Distributions Ubuntu	1. `sudo dpkg -r f-secure-policy-manager-server` 2. `sudo dpkg -r f-secure-automatic-update-agent` 3. `sudo dpkg -r f-secure-policy-manager-console`

Remarque: Afin d'éviter la suppression accidentelle de données impossibles à reproduire créées par les composants de Policy Manager, telles que les fichiers journaux, les fichiers MIB, l'arborescence du domaine, les stratégies, les fichiers de configuration et les préférences, le processus de désinstallation ne supprime pas les répertoires listés ci-dessous. Ne supprimez pas des clés dont vous pourriez avoir besoin. Pour supprimer complètement ce produit, connectez-vous en tant que `root` et saisissez les commandes suivantes :

```
rm -rf /var/opt/f-secure/fspms
rm -rf /var/opt/f-secure/fsaus
rm -rf /etc/opt/f-secure/fspms
rm -rf /etc/opt/f-secure/fsaus
rm -rf /opt/f-secure/fspmc
```

Foire aux questions

Vous trouverez ici la solution aux problèmes courants.

Question	Réponse
Où se trouvent les fichiers journaux, les fichiers de configuration et le répertoire de communication dans la version Linux ?	Le répertoire de communicatin du Serveur Policy Manager contenant les données se trouve sous `/var/opt/f-secure/fspms/commdir` Vous pouvez établir une liste de tous les fichiers et de leur emplacement en saisissant la commande suivante, en tant qu'utilisateur normal : • Distributions basées RPM : `rpm -ql f-secure-<component_name>`. • Distributions basées Debian : `dpkg -L f-secure-<component_name>`. Vous trouverez les fichiers journaux aux emplacements suivants : • Console Policy Manager : `/opt/f-secure/fspmc/lib/Administrator.error.log`. • L'Agent de mise à jour automatique consigne les erreurs d'exécution, les alertes et les autres informations dans le `syslog`, qui se trouve en règle générale sous `/var/log/messages` • Serveur Policy Manager : `/var/opt/f-secure/fspms/logs` et `/var/opt/f-secure/fsaus/log`. Vous trouverez les fichiers de configuration aux emplacements suivants : • Console Policy Manager : `/opt/f-secure/fspmc/lib/Administrator.properties`. • Agent de mise à jour automatique : `/etc/opt/f-secure/fsaua/fsaua_config` • Serveur Policy Manager : `/etc/opt/f-secure/fspms/fspms.conf`.
Pourquoi ces fichiers se trouvent à des emplacements si inhabituels ?	Tous les fichiers de Policy Manager ont leur propre emplacement, conformément à la norme de hiérarchie du système de fichiers (FHS). Pour plus d'informations sur la FHS, allez à *http://www.pathname.com/fhs/*.
Pourquoi le Serveur Policy Manager ne démarre-t-il pas ?	Vérifiez que vous avez exécuté le script de configuration `/opt/f-secure/fspms/bin/fspms-config`. Vous pouvez également vérifié que tous les ports configurés pour le Serveur Policy Manager sont actifs en vous connectant en tant qu'utilisateur `root` pour exécuter la commande `netstat -lnpt`.

Question	Réponse
Comment puis-je démarrer, arrêter et redémarrer ou vérifier le statut des composants de Policy Manager ?	Agent de mise à jour automatique : `/etc/init.d/fsaua {start|stop|restart|status}` Serveur Policy Manager : `/etc/init.d/fspms {start|stop|restart|status}`
Comment puis-je spécifier un proxy HTTP :	Vous pouvez exécuter le script de configuration `/opt/f-secure/fsaua/bin/fsaua-config` ou éditer manuellement le fichier de configuration. La directive est `http_proxies=http://address:port/`. Pensez à redémarrer l'Agent de mise à jour automatique pour activer les nouveaux paramètres.
Comment puis-je modifier les ports par défaut (80 et 8080) desquels le Serveur Policy Manager reçoit les requêtes ?	Ces ports sont configurés à l'aide du script de configuration `/opt/f-secure/fspms/bin/fspms-config`.
Comment puis-je modifier le port par défaut (8081) duquel Web Reporting reçoit les requêtes ?	Le port Web Reporting est configuré avec le script de configuration du Serveur Policy Manager : `/opt/f-secure/fspms/bin/fspms-config`.
Comment puis-je modifier le port par défaut (3050) utilisé par Web Reporting pour accéder à la base de données Firebird ?	Par exemple, pour passer du port 3050 à 3051 : **1.** Changez la ligne contenant `RemoteServicePort = 3050` en `RemoteServicePort = 3051` dans la catégorie `# TCP Protocol Settings` du fichier `/opt/f-secure/fspms/firebird/firebird.conf`. **2.** Changez la ligne `firebird_port=3050` en `firebird_port=3051` dans le `/opt/f-secure/fspms/firebird/tools/fspmwr-db-cleanup.sh`. Vous devez redémarrer votre ordinateur après avoir modifié les fichiers de configuration.Serveur Policy Managerpour que la nouvelle configuration prenne effet.
Puis-je définir ma propre planification pour la mise à jour des définitions de virus F-Secure ?	Oui. Les mises à jour automatiques sont effectuées à l'aide du démon de planification du système d'exploitation `cron`. Modifiez ou ajoutez votre entrée de planification au fichier `/etc/crontab`. Ainsi, pour planifier des mises à jour de définition de virus toutes les dix minutes, ajoutez cette ligne dans `/etc/crontab` : `*/10 * * * * fspms /opt/f-secure/fspms/bin/fsavupd` Pour en savoir plus sur la configuration des mises à jour automatiques à l'aide de `cron`, reportez-vous à `man cron` et `man 5 crontab`. En général, vous pourrez configurer la mise à jour planifiée des

Question	Réponse
	définitions de virus F-Secure à l'aide de la commande `/opt/f-secure/fspms/bin/fspms-config`.
Comment puis-je mettre à jour manuellement les définitions de virus F-Secure ?	Connectez-vous en tant qu'utilisateur `fspms` et exécutez l'outil de mise à jour en saisissant : `sudo -u fspms /opt/f-secure/fspms/bin/fsavupd --debug` Le drapeau facultatif `--debug` force plus de messages commentés de diagnostics.

Comment puis-je publier manuellement les définitions de virus F-Secure depuis le dernier paquet `fsdbupdate` ?	Téléchargez le dernier outil `fsdbupdate.run` sur *http://download.f-secure.com/latest/fsdbupdate.run*. Connectez-vous en tant qu'utilisateur `root` et exécutez cet outil :
	`./fsdbupdate.run`
	Cela permet de mettre à jour la base de données dans l'Agent de mise à jour automatique. Ensuite, publiez ces mises à jourdans le serveur de mise à jour et le Serveur Policy Manager en planifiant `fsavupd` dans `crontab` ou en exécutant manuellement la commande `fsavupd` :
	`sudo -u fspms /opt/f-secure/fspms/bin/fsavupd`

Existe-t-il un outil de diagnostic que je peux utiliser ?	Oui. Utilisez `fsdiag` pour collecter des informations sur votre système et les paquets correspondant. Lorsque vous êtes connecté en tant que root, exécutez : `/opt/f-secure/fspms/bin/fsdiag` Toutes les informations pertinentes seront stockées dans l'archive `fsdiag.tar.gz` situé dans le répertoire actuel. Vous pouvez ensuite envoyer le fichier à l'assistance client F-Secure sur demande.
Je reçois l'alerte `...Un autre serveur de mise à jour automatique a été détecté...` lors du démarrage. Que dois-je faire ?	**1.** Vérifiez si un autre serveur de mise à jour est exécuté et utilise les sockets TCP : `netstat -anp | grep bwserver` `ps axuww | grep bwserver` **2.** Stop the other Automatic Update Server by running: `kill `pidof bwserver`` `kill -9 `pidof bwserver`` **3.** Redémarrez le Serveur Policy Manager : `/etc/init.d/fspms stop` `rm -f /var/lock/subsys/fsaus /var/opt/f-secure/fsaus/log/fsaus.pid`

Question	Réponse
	`/etc/init.d/fspms start`
Comment vérifier et réparer une base de données Firebird utilisée par Web Reporting lorsque la vitesse de génération des rapports ralentit considérablement ?	Dans ce cas, utilisez le script `fspmwr-db-cleanup.sh`, fourni avec Policy Manager. Ce script vérifie l'intégrité de la base de données, crée une sauvegarde de la base de données et tente de réparer tout problème de base de données qu'il détecte. Pour entretenir la base de données Firebird, connectez-vous en tant que `root` et exécutez le script : `/opt/f-secure/fspms/firebird/tools/fspmwr-db-cleanup.sh` Lorsque vous exécutez le script, le Serveur Policy Manager sera automatiquement arrêté et redémarrera une fois la maintenance terminée.

Comment puis-je réinitialiser une base de données corrompue utilisée par Web Reporting ?	**1.** Arrêtez le Serveur Policy Manager comme suit :
	`/etc/init.d/fspms stop`
	2. Remplacez le fichier de base de données Firebird corrompu avec le fichier de base de données vide fourni en utilisant les commandes suivantes :
	`cd /var/opt/f-secure/fspms/firebird/data`
	`cp /opt/f-secure/fspms/firebird/data/fspmwr.fdb.empty fspmwr.fdb`
	`chown firebird:firebird fspmwr.fdb`
	3. Démarrez le Serveur Policy Manager comme suit :
	`/etc/init.d/fspms start`

Comment puis-je installer un logiciel sur les hôtes distants depuis la Console Policy Manager sous Linux ?	Vous pouvez exporter les paquets d'installation vers les fichiers JAR et utiliser l'outil `ilaunchr.exe` pour installer le logiciel sur les hôtes, en utilisant par exemple les scripts de connexion. Suivez la procédure décrite dans le manuel. Vous trouverez l'outil `ilaunchr.exe` dans le répertoire `/opt/f-secure/fspmc/bin`.
Comment puis-je configurer Policy Manager pour l'utiliser dans de grands environnements ?	• Augmentez les valeurs de l'`intervalle d'interrogation des paquets entrants` et de l'`intervalle d'interrogation des paquets sortants` de 30 à 60 minutes dans la Console Policy Manager. • Utilisez l'installation ou les installations du Proxy Policy Manager pour réduire la charge sur le Serveur Policy Manager dues aux mises à jour de base de données envoyées aux clients.

Question	Réponse
	• Si un fichier système `ext3` est utilisé sur la partition contenant `/var/opt/f-secure/fspms/commdir`, activez l'indexation de répertoire (`dir_index` ext2/ext3feature), si elle n'est pas déjà activée. Vous pouvez également désactiver `atime` sur cette partition. Pour une description détaillée, allez dans *http://en.opensuse.org/Speeding_up_Ext3*.

Chapitre

7

Web Reporting

Sujets :

Les rapports graphiques détaillés dans Web Reporting vous permettent d'identifier des ordinateurs qui ne sont pas protégés ou qui sont vulnérables aux attaques de virus. Web Reporting vous permet de créer rapidement des rapports graphiques basés sur des données de tendances historiques à l'aide d'une interface basée sur le web. Vous pouvez générer différents rapports et requêtes utiles à partir des alertes Client Security et des informations de statut envoyées par l'Management Agent au Serveur Policy Manager. Vous pouvez exporter les rapports en format HTML.

Web Reporting est intégré à une base de données Firebird garantissant son fonctionnement dans toute entreprise, quelle que soit la taille. La base de données Web Reporting collecte toutes les données actuellement stockées dans le Serveur Policy Manager et ajoute les nouvelles données au fur et à mesure. Les données collectées comprennent la plupart des données contenues dans les alertes et certaines données des fichiers incrémentiels de stratégie (`.ipf`).

Pour afficher les rapports générés par Web Reporting, vous devez disposer d'un navigateur Internet tel qu'Internet Explorer ou Mozilla Firefox.

Génération et affichage des rapports

Les types généraux de rapports qu'il est possible de créer incluent, par exemple, des graphiques à barres et des graphiques à secteurs sur la sécurité actuelle, des rapports de tendance et des listes détaillées.

Pour afficher les types et les modèles de rapports disponibles, sélectionnez l'une des pages (**Synthèse de la protection antivirus**, **Synthèse de la protection Internet**, **Alertes**, **Logiciels installés** et **Propriétés de l'hôte**) présentes dans l'interface utilisateur de Web Reporting.

Génération d'un rapport

Avec Web Reporting, vous pouvez rapidement créer des rapports graphiques en fonction des tendances passées.

Vous pouvez générer un rapport Web comme suit:

1. Ouvrez la page principale de Web Reporting.
2. Dans votre navigateur, entrez le nom ou l'adresse IP de Serveur Policy Manager suivie du port utilisé par Web Reporting (séparé par deux points).
   Par exemple, `fspms.example.com:8081`.

   Si vous accédez à Web Reporting de manière locale, ouvrez Web Reporting à partir du menu **Démarrer**: **Démarrer** ➤ **F-Secure Policy Manager Server** ➤ **Web Reporting**.
3. Attendez l'ouverture de la page de Web Reporting.

   Cette opération peut être longue dans des environnements de grande taille.

   Quand la page de Web Reporting s'ouvre, elle affiche un rapport par défaut pour la catégorie de rapport sélectionnée. **Racine** est sélectionné par défaut dans l'arborescence **Domaines de stratégie**.
4. Pour afficher un nouveau rapport, sélectionnez d'abord le domaine, le sous-domaine ou l'hôte pour lequel vous souhaitez générer le rapport
5. Sélectionnez ensuite une catégorie de rapports (**Synthèse de la protection antivirus**, **Synthèse de la protection Internet**, **Alertes**, **Logiciels installés** et **Propriétés de l'hôte**) et le rapport à générer.
6. Patientez pendant l'affichage du rapport dans la partie inférieure de la fenêtre principale.

Création d'un rapport imprimable

Vous pouvez également imprimer un rapport généré.

Pour obtenir une version imprimable de la page:

1. Cliquez sur le lien **Version imprimable** dans le coin supérieur droit de la page.
   Cette action ouvre une nouvelle fenêtre dans le navigateur avec le contenu du cadre principal sous un format imprimable.
2. Imprimez la page via la fonction d'impression de votre navigateur.

Vous avez également la possibilité d'enregistrer le rapport pour une utilisation ultérieure. Pour cela, utilisez les options **Enregistrer sous** ou **Enregistrer la page sous**. Assurez-vous que l'option **Enregistrer** permet bien l'enregistrement de la page Web complète, images incluses:

- Si vous utilisez Microsoft Internet Explorer, sélectionnez **Fichier** ➤ **Enregistrer** dans le menu. Dans la fenêtre **Enregistrer la page Web** qui s'ouvre, sélectionnez **Page Web complète** dans le menu déroulant **Type**.
- Si vous utilisez Mozilla, sélectionnez **Fichier** ➤ **Enregistrer la page sous** dans le menu.

Génération de rapports automatisés

Vous pouvez enregistrer l'URL d'un rapport imprimable pour générer des rapports automatisés.

Si vous générez automatiquement des rapports, vous n'aurez plus à sélectionner la catégorie du rapport, son type ni le domaine de stratégie à surveiller la prochaine fois que vous voulez générer le même rapport, car ces informations seront déjà incluses dans l'adresse URL spécifique au rapport.

Deux possibilités se présentent:

- Générez un rapport comportant les éléments à surveiller, puis ajoutez un lien vers ce rapport sur votre ordinateur (bureau, signets ou tout autre emplacement). La prochaine fois que vous ouvrirez Web Reporting via ce lien, le rapport sera à nouveau généré et contiendra les toute dernières données.
- Vous pouvez également enregistrer le rapport que vous avez généré de manière à pouvoir comparer la situation présente avec les rapports ultérieurs. Créez tout d'abord une version imprimable de la page avant de l'enregistrer dans son intégralité dans le navigateur. Vous pourrez, de cette manière, conserver le rapport tel qu'il était lors de l'enregistrement.

Maintenance de Web Reporting

Cette section traite des tâches de maintenance de Web Reporting.

> **Remarque:** Web Reporting est activé et désactivé pendant l'installation de Serveur Policy Manager. Pour activer ou désactiver Web Reporting, vous devez réinstaller Serveur Policy Manager. La restriction de l'accès à la machine locale est également configurée lors de l'installation.

Pour assurer la maintenance de Web Reporting, un fichier de commandes est fourni. Ce fichier se trouve à l'emplacement suivant: `<Dossier F-Secure Installation>\Management Server 5\Web Reporting\firebird\tools` et peut être utilisé dès qu'une dégradation remarquable de la vitesse de génération des rapports se produit. Sous Windows Vista et Server 2008, le fichier de commandes doit être exécuté avec des privilèges d'administration

Création d'une copie de sauvegarde de la base de données de Web Reporting

Nous vous conseillons d'effectuer des mises à jour régulières pour empêcher la perte de données de rapports utiles.

Il est possible de sauvegarder la base de données de Web Reporting sur un support de sauvegarde, comme suit:

1. Arrêtez le service Serveur Policy Manager.
2. Copiez le fichier `C:\Program Files\F-Secure\Management Server 5\Web Reporting\firebird\data\fspmwr.fdb` sur le support de sauvegarde.

   Vous pouvez également recourir à un utilitaire de compression des données pour compresser le fichier. Son utilisation vous permet par ailleurs de vérifier que la base de données sauvegardée est restée intacte.
3. Redémarrez le service Serveur Policy Manager.

> **Remarque:** Une copie de sauvegarde permet de protéger les historiques de toute corruption. Elle permet également de conserver les données plus anciennes qui auraient pu être supprimées lors d'une modification de la durée de stockage maximale appliquée à la base de données de Web Reporting.

Restauration de la base de données de Web Reporting à partir d'une copie de sauvegarde

Vous pouvez restaurer des données sauvegardées qui ont été perdues à cause d'une corruption ou de la modification de la capacité maximale de stockage des données dans la base de données de Web Reporting.

Il est possible de restaurer la base de données de Web Reporting à partir d'une copie de sauvegarde de la façon suivante:

1. Arrêtez le service Serveur Policy Manager.
2. Copiez et décompressez le fichier `fspmwr.fdb` situé sur le support de sauvegarde dans le répertoire suivant: `C:\Program Files\F-Secure\Management Server 5\Web Reporting\firebird\data`.
3. Redémarrez le service Serveur Policy Manager.

Web Reporting - Messages d'erreur et dépannage

Cette section traite des messages d'erreur Web Reporting et du dépannage de la base de données Web Reporting.

Messages d'erreur

Les messages d'erreur courants que vous risquez de rencontrer lors de l'utilisation de Web Reporting sont répertoriés dans cette section.

- Message d'erreur du navigateur: **La connexion a été refusée lors de la tentative pour joindre <emplacement>**

  Votre navigateur n'a pas pu entrer en contact avec Serveur Policy Manager. Votre lien renvoie peut-être vers un ordinateur ou un port incorrect, Serveur Policy Manager n'est pas installé sur cet ordinateur ou le service Serveur Policy Manager n'est pas en cours d'exécution. Vérifiez chacun de ces points dans l'ordre indiqué. Il se peut également qu'un pare-feu empêche la connexion.
- Message d'erreur: **Web Reporting a perdu sa connexion à la base de données, il vous faut redémarrer le service Policy Manager Server.**

  Si Web Reporting ne peut pas entrer en contact avec la base de données, redémarrez le service Serveur Policy Manager. Si le problème persiste, vous pouvez réinstaller Serveur Policy Manager, en conservant la base de données existante.

Dépannage

En général, si Web Reporting ne fonctionne pas, vous devez essayer les étapes indiquées dans la présente section.

Effectuez ces étapes dans l'ordre suivant:

1. Rechargez la page.
2. Si le problème est dû au fait que les processus sont en cours de démarrage, patientez quelques instants, puis réessayez de recharger la page.

   Pour réduire le temps nécessaire au démarrage, supprimez les alertes inutiles du répertoire `CommDir`.
3. Redémarrez le service Web Reporting.
4. Redémarrez Serveur Policy Manager.
5. Redémarrez l'ordinateur.
6. Réinstallez Serveur Policy Manager tout en conservant la configuration existante.
7. Si toutes ces solutions échouent, réinitialisez la base de données de Web Reporting ou restaurez-la à partir d'une copie de sauvegarde.

Réinitialisation de la base de données de Web Reporting

Si la base de données de Web Reporting se révèle être endommagée, vous pouvez la remplacer par un fichier de base de données vide.

Normalement, le serveur Web Reporting efface automatiquement les données obsolètes de la base de données, en fonction du délai maximum configuré pour le stockage de celles-ci. Toutefois, si la base de données se révèle être endommagée, vous pouvez la remplacer par un fichier de base de données vide. La procédure est la suivante:

1. Arrêtez le service Serveur Policy Manager.
2. Copiez le fichier `fspmwr.fdb.empty` sur le fichier `fspmwr.fdb` pour le remplacer.

Ils se trouvent tous deux dans le même répertoire. Si, par inadvertance, vous avez perdu le fichier `fspmwr.fdb.empty`, réinstallez Serveur Policy Manager.

3. Démarrez le service Serveur Policy Manager.

Modification du port de Web Reporting

La méthode recommandée pour modifier le port de Web Reporting consiste à réexécuter le programme d'installation de Policy Manager, et à y modifier le port de Web Reporting.

Vous pouvez également changer le port de Web Reporting en modifiant la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`:

1. Arrêtez Serveur Policy Manager.
2. Ouvrez la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`.
3. Modifiez la valeur `WRPortNum` et saisissez le nouveau numéro de port.

   Assurez-vous que **Décimal** est sélectionné comme option de **Base** lors de la saisie du nouveau numéro de port.
4. Démarrez Serveur Policy Manager.

   S'il existe un conflit entre les ports, Serveur Policy Manager ne démarre pas et génère un message d'erreur dans le fichier journal. Dans ce cas, essayez un autre port qui ne soit pas déjà utilisé.

Chapitre

8

Proxy Policy Manager

Sujets :

Dans cette section, vous trouverez des informations de base sur Proxy Policy Manager.

Présentation

Proxy Policy Manager offre une solution aux problèmes de bande passante rencontrés dans les installations distribuées de Client Security en réduisant sensiblement la charge sur les réseaux utilisant des connexions lentes.

Proxy Policy Manager met en cache les mises à jour de base de données de définitions de virus récupérées à partir de Serveur Policy Manager ou du serveur de mise à jour F-Secure. Il se trouve sur le même réseau distant que les hôtes qui l'emploient comme point de distribution des bases de données. Chaque réseau lent devrait idéalement comporter une installation de Proxy Policy Manager. Proxy Policy Manager charge les mises à jour de bases de données de définitions de virus directement depuis le serveur de distribution de F-Secure. Les hôtes exécutant Anti-virus récupèrent ces mises à jour localement à partir de Proxy Policy Manager. Les postes de travail des bureaux distants communiquent eux aussi avec Serveur Policy Manager du siège central, mais cette communication est limitée à l'administration des stratégies distantes, à la surveillance d'état et aux alertes.

Chapitre

9

Dépannage

Sujets :

Si vous rencontrez des problèmes lors de l'utilisation du produit, vous pourrez trouver des solutions dans cette section.

Serveur Policy Manager et Console Policy Manager

Le problèmes liés à Serveur Policy Manager et Console Policy Manager sont décrits dans la présente section.

Question	Réponse
Serveur Policy Manager ne démarre pas. Pourquoi?	Vous trouverez des erreurs d'exécution, des avertissements et d'autres informations dans le fichier: `<F-Secure>\Management Server 5\logs\error.log` Si le **journal Application** dans l'**Observateur d'événements** (**Outils d'administration** dans NT/2000/2003) indique «`ServerRoot must be a valid director`» ou «`Syntax error on line 6`» en provenance du service Apache, procédez comme suit: Vérifiez d'abord la validité de la ligne`ServerRoot` qui est définie dans le fichier `httpd.conf` (ligne 6 par défaut). Si cette ligne est correcte, vérifiez que les droits d'accès au répertoire de communication (`properties/security/permissions`) incluent le compte d'utilisateur Service local. Si Service local n'est pas indiqué comme utilisateur autorisé, ajoutez l'utilisateur manuellement et définissez les droits d'accès avec la valeur **Contrôle total**. Propagez les droits d'accès au répertoire `Management Server 5` (par défaut à l'emplacement `C:\Program Files\F-Secure\Management Server 5`) et à tous ses sous-répertoires. Après avoir effectué ces modifications, redémarrez le service Serveur Policy Manager ou redémarrez l'ordinateur. Le compte Service local est le compte système Windows, et le service Serveur Policy Manager est démarré sous ce compte d'utilisateur. Lors d'une installation normale, les droits d'accès pour le répertoire `Management Server 5` sont automatiquement définis de façon appropriée. Si le répertoire est copié manuellement ou, par exemple, s'il est restauré à partir d'une sauvegarde, les droits d'accès risquent d'être supprimés. Dans ce cas, procédez de la manière indiquée dans le paragraphe précédent.

Où les fichiers journaux, les fichiers de configuration et le répertoire de communication sont-ils situés pour Serveur Policy Manager?	Les fichiers journaux se trouvent dans
	`<F-Secure>\Management Server 5\logs`
	Les fichiers de configuration se trouvent dans
	`<F-Secure>\Management Server 5\conf`
	Le répertoire de communication Serveur Policy Manager se trouve dans:

Question	Réponse
	`<F-Secure>\\Management Server 5\commdir`
Où les fichiers journaux de Console Policy Manager sont-ils situés?	Le fichier journal est le suivant `<F-Secure>\Administrator\lib\administrator.error.log`
Comment la modification du rôle du serveur arrête le fonctionnement de Serveur Policy Manager?	Le serveur Contrôleur de domaine et le serveur Membre/autonome utilisent différents types de comptes: comptes de domaine sur un contrôleur de domaine et comptes locaux sur un serveur membre. Comme Serveur Policy Manager utilise son propre compte pour s'exécuter, ce compte devient non valide lors du changement de rôle. La façon la plus facile de restaurer Serveur Policy Manager après le changement de rôle du serveur est de réinstaller Serveur Policy Manager avec l'option **Conserver les paramètres actuels** sélectionnée. Cette opération recréera le compte Serveur Policy Manager et réinitialisera les droits d'accès à leur valeur correcte. 👉 **Remarque:** Si vous avez déplacé le répertoire `commdir` manuellement, vous devrez éventuellement rajouter un contrôle total pour le nouveau compte dans cette arborescence.

Comment un renforcement de sécurité de Windows peut-il empêcher la bonne exécution de Serveur Policy Manager?	Les restrictions de droits d'accès, surtout les restrictions sous le répertoire `%SystemRoot%` (`c:\windows` ou `c:\winnt`) peuvent empêcher Serveur Policy Manager de démarrer, puisque son propre compte (Service local) doit pouvoir lire les fichiers DLL et SYS associés au réseau.
	Vous devez permettre au compte Service local de «lire» les répertoires suivants:
	`%SystemRoot%`
	`%SystemRoot%\system32`
	`%SystemRoot%\system32\drivers`
	Certaines restrictions de service peuvent également empêcher le service Serveur Policy Manager de démarrer. Pour plus d'informations à ce sujet, consultez la documentation de Microsoft Windows Server.

Pourquoi m'est-il impossible de me connecter à Serveur Policy Manager?	Si vous obtenez l'erreur «`Impossible de se connecter au serveur d'administration. Un autre administrateur doit être connecté`, vérifiez que personne d'autre n'est connecté à Serveur Policy Manageravec Console Policy Manager. Cette erreur peut également être provoquée par un arrêt incorrect de Console Policy Manager. Pour régler le problème, vois pouvez soit

Question	Réponse
	attendre que Serveur Policy Manager s'éteigne seul (<=5 minutes) soit supprimer le fichier `admin.lck` dans `commdir`, puis redémarrer le service Serveur Policy Manager.
Pourquoi la connexion entre Console Policy Manager et Serveur Policy Manager est-elle interrompue?	Si Console Policy Manager est exécuté sur un ordinateur différent de celui où est exécuté Serveur Policy Manager, la connexion peut être altérée par les problèmes de réseau. Il a été souvent observé, par exemple, qu'un changement de commutateur réseau peut entraîner des problèmes de perte de connexion entre Console Policy Manager et Serveur Policy Manager. Généralement, ces problèmes sont corrigés par la mise à jour des pilotes réseau à la dernière version sur les ordinateurs concernés ou en reconfigurant les ordinateurs Console Policy Manager et Serveur Policy Manager. Si Console Policy Manager est installé sur le même ordinateur que Serveur Policy Manager, il existe un risque que Serveur Policy Manager pâtisse d'une charge réseau telle qu'il ne dispose plus d'une seule connexion disponible. Console Policy Manager et tous les hôtes sont en concurrence pour l'obtention des mêmes ressources réseau. Avec les paramètres par défaut, Serveur Policy Manager ne peut gérer que 150 connexions simultanées. Vous pouvez accroître le nombre de connexions simultanées en augmentant la valeur `ThreadsPerChild` dans le fichier `httpd.conf` et en redémarrant ensuite Serveur Policy Manager. Autres solutions possibles: augmenter les intervalles d'interrogation des hôtes, écourter les délais d'attente réseau de Windows ou encore augmenter le nombre de ports réseau Windows. Paramètres réseau Windows pratiques `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort` (nombre maximal de ports réseau, valeur par défaut = 5000) `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpTimedWaitDelay` (délai d'attente avant fermeture d'une connexion réseau inactive, valeur par défaut = 240 secondes). La commande `netstat -an` permet de vérifier si un trop grand nombre de connexions sont ouvertes sur le serveur.
Comment modifier les ports sur lesquels le serveur écoute les requêtes?	Par défaut, le module d'administration de Serveur Policy Manager (le composant qui traite les demandes provenant de Console Policy Manager) surveille le port 8080. Le module hôte de Serveur Policy Manager (le composant qui traite les demandes des postes de

Question	Réponse
	travail) surveille pour sa part le port 80. Ces paramètres peuvent être modifiés lors de l'installation. Si vous devez modifier les numéros de port après l'installation: **1.** Arrêtez Serveur Policy Manager. **2.** Ouvrez la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`. **3.** Modifiez les valeurs `AdminPortNum` (module d'administration) et `HttpPortNum` (module hôte) et saisissez les nouveaux numéros de port. Assurez-vous que **Décimal** est l'option de **base** sélectionnée lors de la saisie du nouveau numéro de port. **4.** Démarrez Serveur Policy Manager. ⚠ **Avertissement:** Si certaines de vos stations de travail sont déjà configurées pour accéder à Serveur Policy Manager (via le module hôte de Serveur Policy Manager), vous ne devez pas modifier le port hôte de Serveur Policy Manager via lequel les agents communiquent, puisque vous risquez d'être dans un état où les stations de travail ne pourront pas contacter le serveur.

Policy ManagerWeb Reporting

L'emplacement des fichiers de configuration et journaux est indiqué ici.

Question	Réponse

Où se trouvent les fichiers journaux et les fichiers de configuration pour Web Reporting ?	Les fichiers journaux se trouvent dans
	`<F-Secure>\Management Server 5\Web Reporting\logs`
	Les fichiers de configuration se trouvent dans
	La clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\Data Fellows\F-Secure\Management Server 5`
	`<F-Secure>\Management Server 5\Web Reporting\firebird\aliases.conf`
	`<F-Secure>\Management Server 5\Web Reporting\firebird\firebird.conf`
	Consultez également les fichiers de configuration du Serveur Policy Manager :
	`<F-Secure>\Management Server 5\conf\httpd.conf`

Distribution des stratégies

Dans cette section, vous trouverez des informations sur les messages d'erreur communs relatifs à la distribution de stratégies.

Question	Réponse
Lors de la distribution d'une stratégie, Console Policy Manager affiche un message d'erreur relatif à une valeur de stratégie incorrecte. Que dois-je faire?	Voir ci-dessous pour des informations sur les messages d'erreur susceptibles de s'afficher pendant la distribution des stratégies, leurs causes et des solutions éventuelles.

Message d'erreur	Raison	Solution

`«nom du paramètre» a une valeur en dehors de la restriction`
`«<nom du paramètre>» a une restriction incorrecte`
`«<nom du paramètre>» possède une valeur incorrecte: «<valeur>»`
	Raison 1:
	La valeur sélectionnée dans une liste de choix ne fait pas partie des choix d'un sous-domaine ou d'un hôte, les limites de restriction spécifiées sont trop hautes ou trop basses, ou une liste de choix vide a été spécifiée.
	Lorsqu'un domaine comprend des hôtes sur lesquels différentes versions de produits sont installées, les paramètres de la base de données MIB de la version la plus récente sont utilisés pour modifier les valeurs de stratégie. De ce fait, la distribution de la stratégie peut échouer sur les hôtes dotés de versions antérieures du logiciel car ces dernières ne prennent pas en charge les nouveaux paramètres ou nouvelles valeurs de la stratégie.
	.
	Raison 2 :
	Vous avez saisi une valeur entière non compris dans les restrictions de plage.
		Divisez les hôtes en sous-domaines de façon à pouvoir définir la nouvelle valeur pour les hôtes bénéficiant de la version la plus récente du logiciel et à utiliser des valeurs de stratégie plus anciennes pour les autres hôtes. Pour ce faire:
		1. Regroupez les hôtes en sous-domaines basés sur la version du produit installé. Vous pouvez, par exemple, grouper les hôtes qui ont installé Client Security 6.x dans un sous-domaine et les hôtes qui ont installé Client Security7.x dans un autre domaine.
		2. Définissez la plupart des paramètres sur le domaine racine, puis créez des sous-domaines pour les exceptions. C'est une bonne solution si vous ne disposez que de quelques hôtes avec une ancienne version du logiciel.

`«<nom du paramètre>» est requis mais n'est pas défini`	Le paramètre est requis, mais il est vide.	Saisissez une valeur ou appliquez l'opération **Effacer** pour rétablir l'héritage de la valeur à partir du domaine ou MIB parent. Si la valeur est vide à plusieurs niveaux du domaine, vous devrez peut-être effectuer l'opération **Effacer** plusieurs fois.

Chapitre
10

Codes d'erreur llaunchr

Sujets :

Cette section fournit des informations sur les codes d'erreur relatifs au composant **llaunchr**.

Codes d'erreur

Après l'exécution de la commande `Ilaunchr.exe`, les résultats d'installation s'affichent à l'aide des codes standard.

Le script de connexion vous permet de rechercher la cause du problème. Voici un exemple que vous pouvez insérer dans votre script de connexion:

```
Start /Wait ILaunchr.exe \\server\share\mysuite.jar /U if errorlevel 100 Go to
Some_Setup_Error_occurred if errorlevel 5 Go to Some_Ilaunchr_Error_occurred if
 errorlevel 3 Go to Problem_with_JAR_package if errorlevel 2 Go to
User_does_not_have_admin_rights if errorlevel 1 Go to FSMA_was_already_installed
 if errorlevel 0 Echo Installation was OK!
```

Codes d'erreur:

Code d'erreur	Description
0	Installation OK.
1	FSMA déjà installé.
2	L'utilisateur ne dispose pas des droits d'administrateur.
3	Fichier JAR introuvable.
4	Fichier JAR endommagé.
6	Erreur survenue lors de la décompression d'un fichier d'installation.
7	Espace insuffisant sur le disque de destination pour l'installation.
8	Le fichier `package.ini` est introuvable dans le fichier JAR.
9	Le fichier `package.ini` ne contient aucune instruction de fonctionnement.
10	Paramètres incorrects sur la ligne de commande ou dans le fichier `.ini`.
11	Erreur d'initialisation d'un nouveau processus de travail.
12	Erreur de création du processus destiné au programme d'installation.
13	Impossible de créer un répertoire `temporaire`.
14	Erreur indéfinie.
100	Données nécessaires à l'installation silencieuse introuvables. Fichier JAR incorrect.
101	Mise à jour désactivée (tentative de mise à jour de l'installation lors de l'exécution du programme d'installation).
102	Le programme d'installation n'a pas pu lire le fichier `product.ini`.
103	Données incorrectes rencontrées dans `prodsett.ini`.

Code d'erreur	Description
104	Management Agent a interrompu l'installation ou un conflit de logiciel a été détecté. L'installation a été interrompue.
105	La clé d'abonnement est erronée ou introuvable. L'installation a été interrompue.
110	Espace disque insuffisant.
111	Le lecteur de destination n'est pas local.
120	L'utilisateur ne dispose pas des droits d'accès administrateur au poste.
130	Le programme d'installation n'a pas pu copier les fichiers non compressés dans le répertoire de destination.
131	Le programme d'installation n'a pas pu copier le plugin de désinstallation du produit dans le répertoire de destination.
132	Le programme d'installation n'a pas pu copier le fichier `product.ini` dans le répertoire `temporaire`.
133	Erreur survenue lors de la sauvegarde du fichier du produit dans le répertoire de destination.
134	Impossible de copier `prodsett.ini`.
140	Une version plus récente de la suite a été détectée.
150	Le programme d'installation n'a pas pu charger la DLL du plugin du produit.
151	Le programme d'installation n'a pas pu charger la DLL de prise en charge de l'installation.
152	Le programme d'installation n'a pas pu charger la DLL wrapper.
160	Le programme d'installation n'a pas pu initialiser le fichier Cab.
170	Le plugin d'installation de Management Agent a retourné une erreur.
171	Le plugin a retourné un code inattendu.
172	Le plugin a retourné un code wrapper.
173	L'une des opérations d'installation ou de désinstallation précédentes n'a pas été terminée. Un redémarrage est nécessaire pour la terminer.
174	L'ordinateur de destination a été redémarré afin de terminer une des opérations d'installation ou de désinstallation précédentes. Veuillez relancer l'installation.
200	Réussite partielle. L'installation de certains produits a échoué.

Chapitre
11

Codes d'erreur de l'installation distante avec FSII

Sujets :

- *Codes d'erreur*

Cette section décrit les codes d'erreur les plus courants et les messages qui apparaissent durant l'opération **Autodécouvrir hôtes Windows**.

Codes d'erreur

Vous trouverez dans cette section des descriptions pour les codes et messages d'erreur les plus répandus qui s'affichent lors d'opérations d'installation à distance.

Codes d'erreur Windows

Code d'erreur	Description
1057	Le nom du compte utilisateur est incorrect ou n'existe pas.
5	Accès refusé. Si vous utilisez l'option **Ce compte**, il est important que l'administrateur soit connecté à l'ordinateur Console Policy Manager avec des droits d'administrateur du domaine. En ce qui concerne les **domaines sécurisés**, veillez à vous connecter à Console Policy Manager avec le compte associé au domaine.
1069	Echec de connexion. Dans la plupart des cas, le mot de passe saisi est incorrect.
1722	Le serveur RPC n'est pas disponible. Ce message d'erreur apparaît lorsque vous redémarrez l'hôte immédiatement après l'installation alors que Console Policy Manager n'a pas terminé la vérification de l'installation.
1219	Console Policy Manager a des connexions réseau ouvertes sur le poste de travail cible. Fermez ces connexions avant de tenter d'en ouvrir avec un autre compte d'utilisateur.

Messages d'erreur

Message d'erreur	Description
Le droit requis n'est pas attribué au compte actuel. Il doit être ajouté manuellement.	Par défaut, même l'administrateur ne dispose pas du droit requis **Acteur dans un système d'exploitation** sur l'ordinateur Console Policy Manager. Si vous ne disposez pas de ce droit, WindowsNT empêche l'authentification par FSII des comptes utilisateur saisis. Afin d'ajouter ce droit au compte de l'administrateur sur Console Policy Manager, ouvrez **Gestionnaire des utilisateurs WindowsNT** ➤ **Stratégies** ➤ **Droits utilisateur**.
Management Agent a interrompu l'installation ou un conflit de logiciel a été détecté. Installation interrompue.	Le programme d'installation de Management Agent annule l'ensemble de l'installation dans les cas suivants: • Un conflit avec un logiciel tiers est détecté. • Il existe de nombreuses autres possibilités, notamment: l'adresse URL de Serveur Policy Manager n'est pas correcte.

Message d'erreur	Description
La clé du CD est erronée ou introuvable. Installation interrompue.	L'installation sur l'hôte distant ne démarre pas en raison d'une saisie incorrecte de la clé d'abonnement. Vérifiez la syntaxe.
Espace disque insuffisant sur l'hôte de destination	L'hôte de destination ne dispose pas d'un espace disque suffisant. Généralement, au moins 20Mo sont nécessaires.
L'installation de Management Agent a échoué en raison d'une erreur FSMAINST fatale. Reportez	Une erreur d'installation fatale est survenue lors de l'installation de Management Agent. Il est recommandé de l'installer manuellement sur l'hôte. Vous pouvez également rechercher le mot clé ERREUR dans le`fswssdbg.log` fichier situé dans le répertoire Windows de l'hôte de destination.
Produit F-Secure plus récent détecté, installation interrompue	Si une version plus récente d'un produit est installée sur l'hôte de destination, l'installation ne peut démarrer que lorsque celle-ci est désinstallée.
Données incorrectes rencontrées dans prodsett.ini.	Le fichier de configuration `prodsett.ini` comporte des informations incorrectes. Si vous l'avez modifié manuellement, vérifiez que la syntaxe est correcte. Pour l'installation, il est plutôt recommandé d'exporter les fichiers JAR à l'aide de la commande **ILAUNCHR** que de modifier directement `prodsett.ini`.

Chapitre
12

Notation NSC pour masques de réseau

Sujets :

- *Détails de la notation NSC*

Vous trouverez des informations sur l'association d'une adresse réseau avec son sous-réseau associé.

Détails de la notation NSC

La notation NSC est une norme de notation abrégée qui associe une adresse réseau au masque de réseau correspondant.

La notation NSC définit le nombre de bits uniques contigus dans le masque de réseau en ajoutant après l'adresse réseau une barre oblique suivie d'un nombre. Voici un exemple simple:

Adresse réseau	Masque de réseau	Notation NSC
192.168.0.0	255.255.0.0	192.168.0.0/16
192.168.1.0	255.255.255.0	192.168.1.0/24
192.168.1.255	255.255.255.255	192.168.1.255/32

La notation NSC est incompatible avec les réseaux utilisant des masques de réseau de type «peigne» dans lesquels les bits uniques ne sont pas tous contigus. Le tableau suivant indique le nombre de bits pour chaque masque de réseau autorisé.

.0.0.0/0 est une définition de réseau spéciale réservée à l'itinéraire par défaut.

Masque de réseau	Bits
128.0.0.0	1
192.0.0.0	2
224.0.0.0	3
240.0.0.0	4
248.0.0.0	5
252.0.0.0	6
254.0.0.0	7
255.0.0.0	8
255.128.0.0	9
255.192.0.0	10
255.224.0.0	11
255.240.0.0	12
255.248.0.0	13
255.252.0.0	14
255.254.0.0	15
255.255.0.0	16
255.255.128.0	17
255.255.192.0	18
255.255.224.0	19
255.255.240.0	20
255.255.248.0	21
255.255.252.0	22
255.255.254.0	23
255.255.255.0	24
255.255.255.128	25

Masque de réseau	Bits
255.255.255.192	26
255.255.255.224	27
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30
255.255.255.254	31
255.255.255.255	32