Guide d'installation de McAfee ePolicy Orchestrator 5.10.0

Sommaire

1 Présentation de l'installation

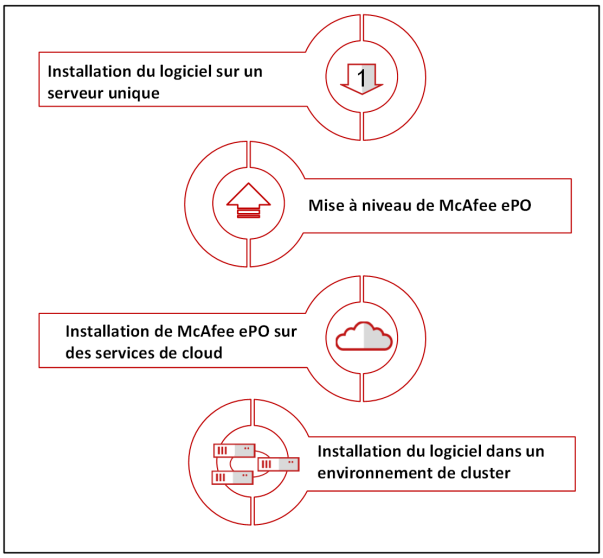
Sommaire

De quel type d'installation avez-vous besoin ?

Installez le logiciel McAfee ePO en tant que serveur unique ou en cluster, dans le cloud ou en tant que mise à niveau.

Chaque scénario d'installation inclut une procédure et un workflow. La planification de l'installation et la vérification de la configuration système requise font également partie du processus d'installation.

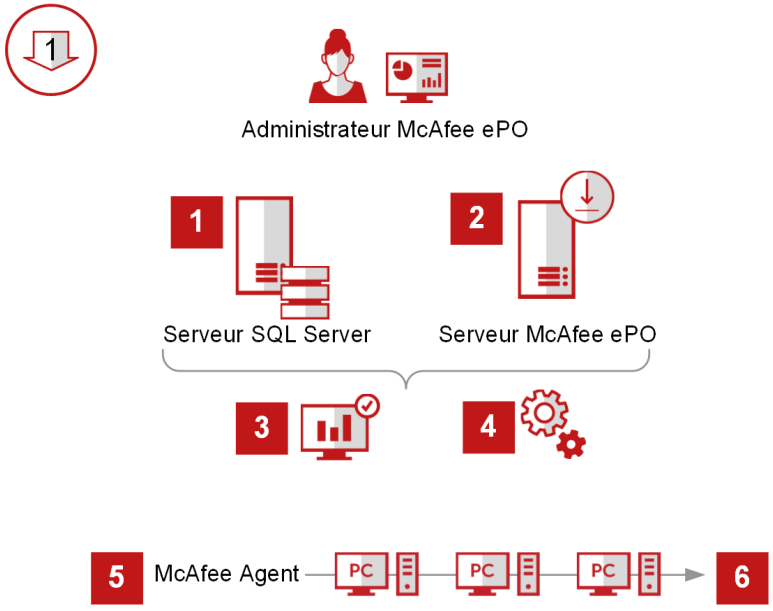
Quel type d'installation voulez-vous utiliser ?



Workflow d'installation sur un serveur unique

Avant de pouvoir installer McAfee ePO pour la première fois, vous devez vous assurer que votre logiciel SQL Server est configuré pour l'accès TCP/IP et installer un système d'exploitation pris en charge sur le serveur McAfee ePO.

1. Vérifiez que votre serveur SQL Server est configuré pour l'accès TCP/IP.
2. Téléchargez et extrayez le logiciel McAfee ePO à partir de https://secure.mcafee.com/enterprise/en-gb/downloads/my-products.html ou du site de téléchargement McAfee à l'aide d'un Grant Number.
3. Vérifiez que les dernières mises à jour de Microsoft sont en cours d'exécution sur le serveur SQL et le serveur McAfee ePO.
4. Exécutez l'utilitaire d'installation sur le serveur McAfee ePO pour installer McAfee ePO. Dans le cadre du processus d'installation, McAfee ePO Pre-Installation Auditor vérifie les problèmes de conformité.
5. Choisissez une méthode pour le déploiement de McAfee Agent.
6. Vérifiez que les systèmes sont managés en vous assurant que McAfee Agent peut se connecter à McAfee ePO.



Workflow d'installation de services de cloud

Configurer un compte de services de cloud ainsi que votre environnement virtuel pour exécuter des services de cloud avec McAfee ePO.

1. Configurez un compte de services de cloud et les éléments suivants :
   - Serveur virtuel à utiliser en tant que serveur McAfee ePO
   - Serveur SQL virtuel
   - Groupe de sécurité

2 Affectez une adresse IP élastique à chaque serveur virtuel.

3 Depuis un ordinateur de gestion, utilisez le Bureau à distance pour vous connecter au serveur McAfee ePO virtuel.

4 Sur la page McAfee.com, copiez le logiciel McAfee ePO vers le serveur McAfee ePO virtuel.

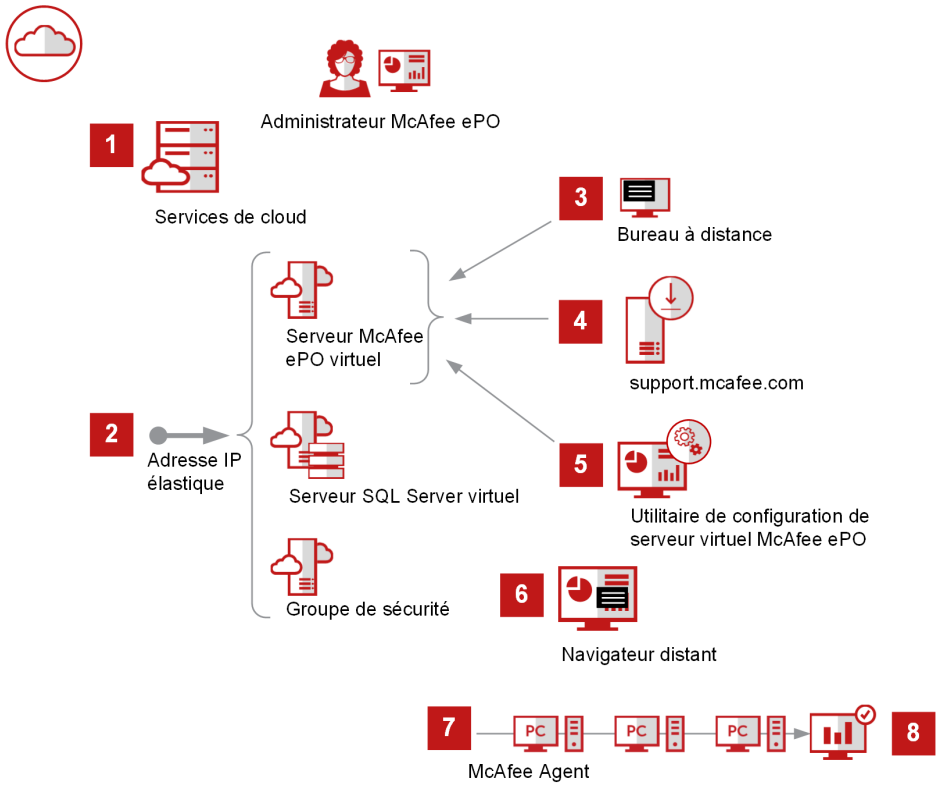
5 Depuis le serveur McAfee ePO, exécutez l'utilitaire d'installation.

6 A l'aide d'un navigateur distant, connectez-vous à McAfee ePO en saisissant l'adresse `https://<adresse IP élastique/DNS du serveur McAfee EPO virtuel>:<port>`.

- Mettez à jour le **DNS public du serveur McAfee ePO** dans les **Paramètres serveur** avec l'adresse IP élastique ou le DNS du serveur McAfee ePO virtuel.
- Mettez à jour le nom DNS publié ou l'adresse IP du gestionnaire d'agents (le cas échéant) avec l'adresse IP élastique ou le DNS du serveur de gestionnaire d'agents virtuel.
- Créez une URL de déploiement McAfee Agent ou extrayez le package de déploiement McAfee Agent.

7 Choisissez la méthode de déploiement de McAfee Agent.

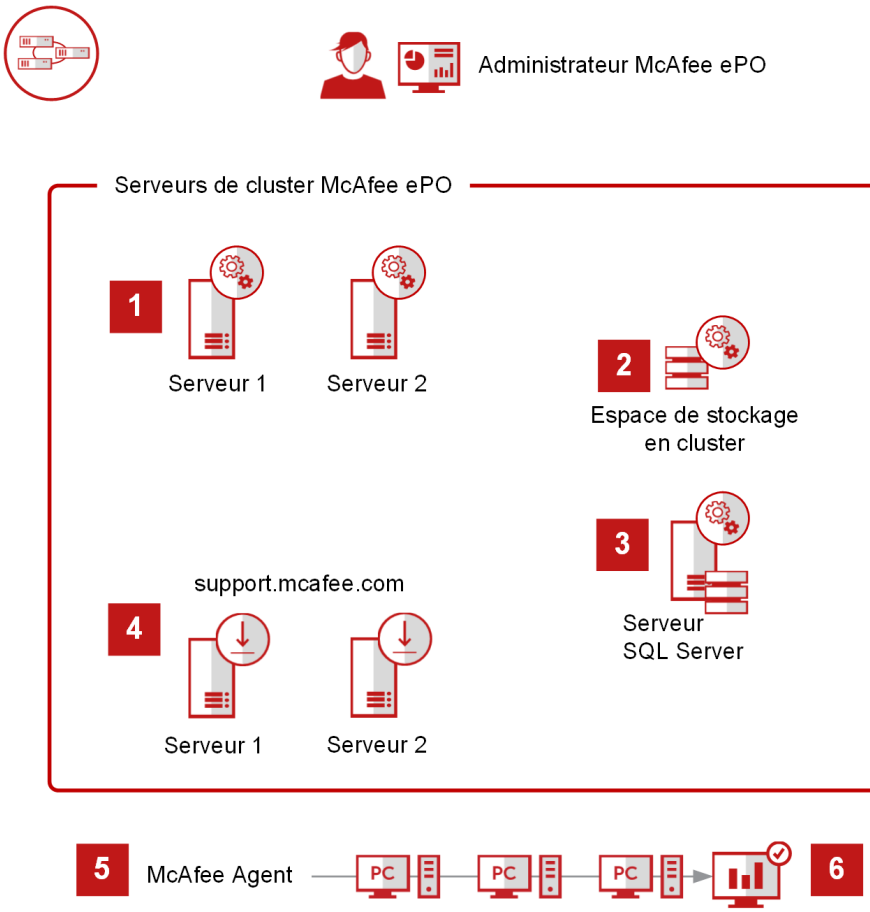
8 Vérifiez que les systèmes sont managés en vous assurant que McAfee Agent peut se connecter à McAfee ePO.



Workflow de l'installation en cluster

McAfee ePO permet d'assurer la haute disponibilité nécessaire aux clusters de serveurs mis en place avec le logiciel Microsoft Cluster Server (MSCS).

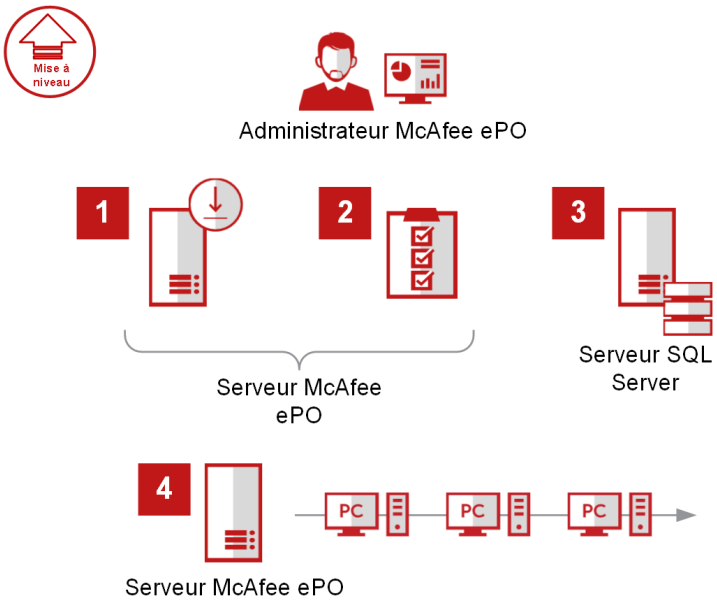
1 Installez le logiciel MSCS sur tous vos serveurs et configurez les éléments suivants :
   - Lecteur de données partagé
   - Lecteur quorum
   - Groupe de basculement
2 Configurez le stockage partagé.
3 Configurez les paramètres de la base de données et du serveur SQL Server.
4 Téléchargez et installez le logiciel McAfee ePO sur tous les serveurs.
5 Choisissez la méthode de déploiement de McAfee Agent.
6 Vérifiez que les systèmes sont managés en vous assurant que McAfee Agent peut se connecter à McAfee ePO.



Workflow de mise à niveau

Mettez à niveau votre logiciel McAfee ePO vers une nouvelle version.

1. Téléchargez et extrayez le logiciel sur votre serveur McAfee ePO.
2. Préparez l'environnement de serveur McAfee ePO.
   McAfee ePO Pre-Installation Auditor s'exécute et vérifie la conformité avec toutes les exigences.
3. Configurez les paramètres de base de données et SQL Server.
4. À partir du serveur McAfee ePO, exécutez l'utilitaire d'installation.



2 Planification de l'installation

Pour utiliser efficacement le serveur McAfee ePO, McAfee conseille de créer un plan complet propre à votre environnement.

L'analyse préalable des besoins uniques de votre environnement vous permet d'être opérationnel plus rapidement.

- Combien de systèmes devez-vous gérer ?
- Vos systèmes sont-ils situés sur un même réseau ou dans plusieurs zones géographiques ?
- Avez-vous des besoins de sécurité spécifiques, par exemple un pare-feu ?
- Utilisez-vous la fonction de traduction des adresses réseau (NAT) dans un réseau externe ?
- Devez-vous respecter des restrictions de bande passante pour les segments de réseau distant ?
- Devez-vous gérer les ordinateurs portables qui sont connectés à Internet et qui se trouvent à l'extérieur du réseau d'entreprise ?
- Plusieurs administrateurs possèdent-ils des autorisations différentes sur différents produits ou groupes de systèmes, ou possèdent-ils différentes fonctions dans la console de gestion ?

Sommaire

Conseils relatifs à l'évolutivité

Votre capacité à gérer la croissance de votre réseau varie selon que vous installez McAfee ePO sur plusieurs serveurs, que vous utilisez plusieurs gestionnaires d'agents, ou les deux.

Vous pouvez faire évoluer votre infrastructure McAfee ePO en déplaçant la base de données SQL McAfee ePO vers un serveur SQL Server plus puissant et plus volumineux, en ajoutant d'autres gestionnaires d'agents, ou encore en augmentant l'UC et la mémoire.

Le logiciel McAfee ePO prendre en charge l'évolutivité verticale ou horizontale de votre réseau.

- ***Evolutivité verticale*** : ajout et mise à niveau de matériel pour augmenter la puissance et la rapidité et gérer des environnements de plus en plus étendus. Pour faire évoluer un serveur verticalement, vous devez mettre à niveau votre matériel serveur et installer McAfee ePO sur plusieurs serveurs dans votre réseau, chacun disposant de sa propre base de données.
- ***Evolutivité horizontale*** : augmentation de la taille de déploiement qu'un serveur McAfee ePO peut gérer. Pour faire évoluer un serveur horizontalement, vous devez installer d'autres gestionnaires d'agents, tous devant partager la même base de données.

Systèmes et serveurs managés

Le nombre de serveurs requis et la taille de ces serveurs est fonction du nombre de systèmes que votre serveur McAfee ePO gère. Le nombre de systèmes managés indique également la taille de serveur recommandée pour la gestion de ces systèmes.

Option	< 1 500 systèmes	De 1 500 à 10 000 systèmes	De 10 000 à 25 000 systèmes	De 25 000 à 75 000 systèmes	> 75 000 systèmes
Serveur McAfee ePO virtuel	Oui	Oui	Oui	Oui	Oui
Serveur de base de données SQL virtuel	Oui	Oui	Oui	Facultative	Facultative
Serveur McAfee ePO et base de données SQL sur le même serveur	Oui	Oui	Facultative	Facultative	
Serveur McAfee ePO et base de données SQL sur un serveur distinct		Facultative	Oui	Oui	Oui
Ajouter des référentiels distribués		Facultative	Facultative	Oui	Oui
Ajouter des gestionnaires d'agents (virtuels)		Facultative	Facultative	Oui	Oui

Il est conseillé d'utiliser un gestionnaire d'agents pour chaque tranche de 50 000 systèmes.

Il n'existe aucune limite maximale quant au nombre de systèmes que McAfee ePO peut gérer. La principale limitation concerne les performances de la base de données SQL, en particulier des performances du disque (IOPS : 10 par seconde). Vous pouvez faire évoluer la base de données SQL ou encore ajouter des référentiels de distribution et des gestionnaires d'agents pour gérer davantage de systèmes.

Taille de l'organisation et composants réseau : exemples

Le nombre de systèmes et de produits managés, ainsi que la période de conservation des données, déterminent les composants serveur nécessaires pour utiliser McAfee ePO.

Ces exemples fournissent des instructions relatives à la détermination des composants serveurs requis en fonction de la taille de l'organisation. Les instructions suivantes indiquent la configuration minimale requise. Afin d'améliorer les performances de votre organisation et de lui permettre d'évoluer, McAfee conseille d'aller au-delà de la configuration minimale requise dès que possible.

Exemple 1 : moins de 10 000 systèmes managés

Dans une organisation comptant moins de 10 000 systèmes managés, vous pouvez réduire le coût matériel en installant le serveur McAfee ePO et une base de données SQL sur le même serveur physique ou sur une machine virtuelle. Vous pouvez utiliser la base de données Microsoft SQL Server Express si vous disposez de

moins de 1 500 systèmes managés. La base de données SQL Express ne peut pas dépasser 10 Go, et la mémoire disponible pour le moteur de base de données SQL Express est limitée à 1 Go. La base de données SQL Server peut être installée sur le même serveur.

Vous pouvez déplacer la base de données McAfee ePO vers un serveur SQL Server dédié pour augmenter la taille de votre environnement.

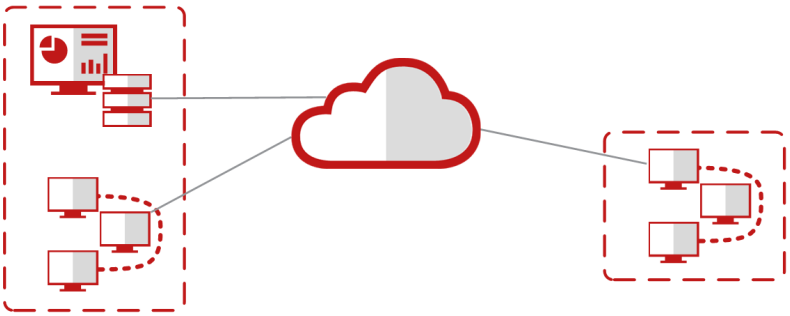


Figure 2-1 Composants réseaux McAfee ePO pour moins de 10 000 systèmes managés

Exemple 2 : de 10 000 à 25 000 systèmes managés

Dans une organisation comptant 10 000 à 25 000 systèmes managés, si Endpoint Security installé, l'ajout de produits à manager peut accroître la capacité recommandée. Il peut être nécessaire d'ajouter des référentiels distribués (comme indiqué dans l'exemple 3) selon le réseau WAN et le nombre de systèmes distribués.

Si votre nombre de systèmes managés dépasse 10 000, envisagez d'installer le serveur McAfee ePO et les serveurs SQL Server sur des serveurs physiques distincts. Pour des performances optimales, confiez l'exploitation et la maintenance du serveur SQL Server à l'administrateur de la base de données.

1 SQL Server

2 Serveur McAfee ePO

Si votre budget vous permet d'acheter des ressources serveur supplémentaires, il est conseillé d'aller au-delà de ces recommandations afin d'améliorer les performances.

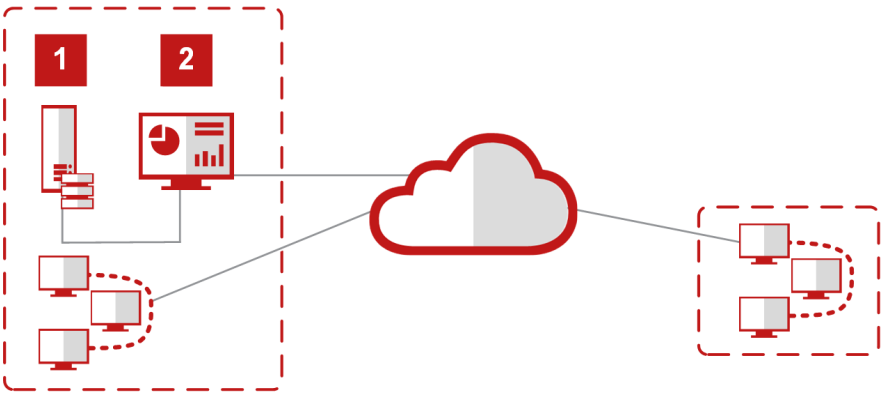


Figure 2-2 Composants réseau McAfee ePO pour 10 000 à 25 000 systèmes managés

Exemple 3 : de 25 000 à 75 000 systèmes managés

Dans une organisation comptant entre 25 000 et 75 000 systèmes managés sur un serveur McAfee ePO, un serveur SQL Server distinct, dotés uniquement du produit Endpoint Security et des référentiels correctement placés pour mettre à jour le contenu et les logiciels.

1 SQL Server

2 Serveur McAfee ePO

3 Référentiels distribués permettant de stocker et de distribuer du contenu de sécurité pour vos systèmes managés

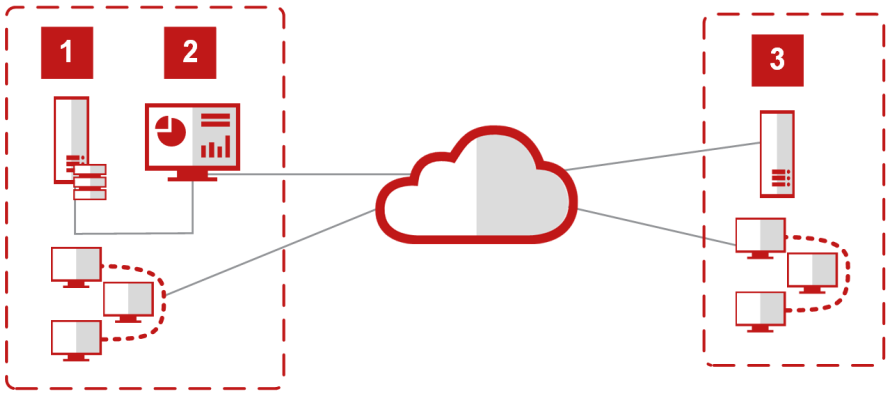


Figure 2-3 Composants réseau McAfee ePO pour 25 000 à 75 000 systèmes managés

Exemple 4 : de 75 000 à plus de 150 000 systèmes managés

Dans une organisation comptant entre 75 000 et plus de 150 000 systèmes managés sur un serveur McAfee ePO, un serveur SQL Server distinct, des Gestionnaires d'agents distincts et des référentiels correctement placés pour mettre à jour le contenu et les logiciels.

1 Les Gestionnaires d'agents distincts coordonnent les demandes McAfee Agent entre eux-mêmes et McAfee ePO. Les Gestionnaires d'agents requièrent une communication constante avec la base de données SQL. Ils vérifient la file de travail du serveur toutes les dix secondes afin de déterminer la tâche à exécuter. Les Gestionnaires d'agents ont besoin d'une connexion haut débit à faible latence avec la base de données et ne doivent pas être distribués. Il est conseillé d'utiliser un Gestionnaire d'agents pour 50 000 systèmes managés.

Dans les organisations comptant entre 75 000 et plus de 150 000 systèmes managés, installez un Gestionnaire d'agents sur le même sous-réseau que le serveur McAfee ePO à des fins de redondance, pour permettre au serveur McAfee ePO de gérer les communications agent-serveur en cas de défaillance de de la connexion au Gestionnaire d'agents.

2 SQL Server

3 Serveur McAfee ePO

4 Les référentiels distribués McAfee ePO stockent et distribuent du contenu de sécurité important pour vos systèmes clients managés.

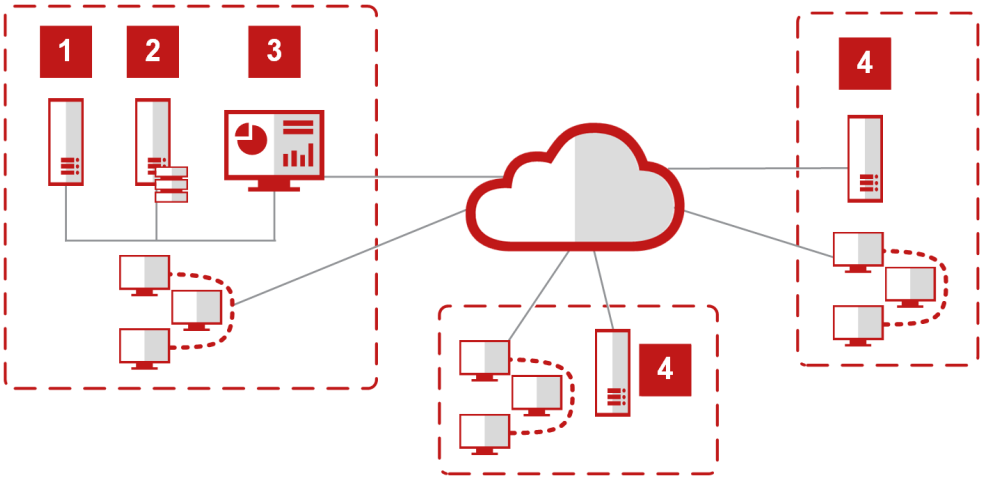


Figure 2-4 Composants réseau McAfee ePO pour 75 000 à plus de 150 000 systèmes managés

Facteurs ayant un impact sur les performances de McAfee ePO

Il est important de connaître les facteurs qui ont un impact sur les performances de votre serveur et de la base de données SQL associée.

Par exemple, un serveur et une base de données McAfee ePO peuvent gérer jusqu'à 200 000 systèmes client en installant seulement le logiciel Endpoint Security. A mesure que vous ajoutez des produits logiciels et des clients, toutefois, le même serveur ne peut plus fournir les performances que vous attendez.

Tenez compte des facteurs ci-dessous au fur et à mesure de la croissance de votre réseau managé et de l'évolution de vos besoins en matière de sécurité.

- Matériel du serveur **McAfee ePO**
- **Serveur SQL Server** : ce serveur, moteur de l'infrastructure McAfee ePO, a un impact sur les performances du serveur McAfee ePO des requêtes, des tableaux de bord et de la console McAfee ePO.
- **Nombre de logiciels installés** : chaque logiciel que vous installez ajoute à la charge de traitement du serveur McAfee ePO et de la base de données SQL.
- **Nombre de clients managés et de Gestionnaires d'agents** : ces nombres sont proportionnels aux performances du serveur McAfee ePO et de la base de données. Chaque Gestionnaire d'agents ajoute des charges fixes sur le serveur de base de données :
  - Surveillance de la pulsation (toutes les minutes)
  - Vérifications de la file d'attente des travaux (toutes les 10 secondes)
  - Pool de connexions à la base de données maintenues ouvertes (deux connexions par processeur au service de l'analyseur d'événements et quatre connexions par processeur au service Apache)

Protocole IP dans un environnement managé

Le logiciel McAfee ePO est compatible avec les versions IPv4 et IPv6 du protocole IP.

Le serveur McAfee ePO fonctionne dans trois modes différents :

- **IPv4 uniquement** : seul le format d'adresse IPv4 est pris en charge.
- **IPv6 uniquement** : seul le format d'adresse IPv6 est pris en charge.
- **Mode mixte** : les formats d'adresse IPv4 et IPv6 sont pris en charge.

Le mode de fonctionnement de votre serveur McAfee ePO dépend de la configuration de votre réseau. Si votre réseau est configuré pour n'utiliser que les adresses IPv4, votre serveur fonctionnera en mode IPv4 uniquement. Si votre réseau est configuré pour utiliser des adresses IPv4 et IPv6, votre serveur fonctionnera en mode mixte.

Tant que IPv6 n'est pas installé et activé, votre serveur McAfee ePO écoute uniquement les adresses IPv4. Une fois IPv6 activé, il fonctionne dans le mode dans lequel il est configuré.

Lorsque le serveur McAfee ePO communique avec un **Gestionnaire d'agents** via IPv6, les propriétés liées aux adresses (telles que l'adresse IP, l'adresse de sous-réseau ou le masque de sous-réseau) sont indiquées au format IPv6. Les propriétés liées à IPv6 sont affichées sous la forme étendue et sont mises entre crochets lorsqu'elles sont transmises entre le client et le serveur McAfee ePO ou affichées dans l'interface utilisateur ou dans un fichier journal.

Par exemple, `3FFE:85B:1F1F::A9:1234` s'affiche comme suit :

```
[3FFE:085B:1F1F:0000:0000:0000:00A9:1234]
```

Aucune modification des adresses IPv6 n'est requise lorsqu'elles sont configurées pour des sources FTP ou HTTP. Cependant, lors de la configuration d'une adresse littérale IPv6 pour une source UNC, vous devez utiliser le format littéral IPv6 de Microsoft. Pour plus d'informations, consultez la documentation Microsoft.

TLS 1.0 est désactivé par défaut pour la communication avec les serveurs externes, dont SQL Server. Pour plus d'informations sur la prise en charge de TLS, consultez l'article KB90222. Cette version de McAfee ePO requiert l'activation de la prise en charge du protocole TLS 1.2 par votre navigateur.

Procédures à exécuter avant l'installation

Avant de démarrer l'installation de McAfee ePO, vérifiez que vous disposez de toutes les informations nécessaires et que vous connaissez les étapes à suivre. Exécutez McAfee ePO Pre-Installation Auditor pour limiter ou éviter les problèmes liés à l'installation ou à la mise à niveau.

- Clé de licence de produit McAfee (non requise pour les versions d'évaluation)
- L'authentification Microsoft SQL nécessite l'une des informations d'identification suivantes :
  - Informations d'identification pour l'authentification Windows : informations d'identification du domaine incluant des droits de propriétaire de base de données sur le serveur SQL Server
  - Informations d'identification pour l'authentification SQL
- Dossier de destination pour l'installation du logiciel McAfee ePO (requis pour les installations Personnalisée et en Cluster)
- Serveur SQL Server installé : indiquez les informations suivantes (selon votre configuration) dans la page Informations de base de données :
  - Nom du serveur SQL Server ou nom du serveur SQL Server *incluant* le nom de l'instance.
  - Numéro de port dynamique utilisé par le serveur SQL Server.

- Si vous souhaitez restaurer le serveur McAfee ePO à partir d'une capture instantanée de la base de données, vous devez :
  - Avoir préalablement restauré la base de données SQL de McAfee ePO via l'un des processus de restauration de Microsoft SQL.
  - Connaître la phrase secrète de chiffrement de la banque de clés utilisée pour les enregistrements de Capture instantanée pour la reprise sur sinistre. Vous en aurez besoin pour déchiffrer les informations confidentielles stockées dans les enregistrements de capture instantanée SQL.

3 Configuration requise

Sommaire

Configuration requise et recommandations concernant le système

Avant d'installer le logiciel McAfee ePO, vérifiez que votre environnement respecte la configuration requise et les recommandations.

Exécutez Pre-Installation Auditor afin de vous assurer que votre environnement respecte la configuration requise pour l'installation. Pour plus d'informations sur le téléchargement et l'utilisation de Pre-Installation Auditor, consultez les notes de publication de l'outil.

Composant	Configuration requise et recommandations
Serveur dédié	Si votre réseau compte moins de 250 systèmes managés, vous pouvez installer McAfee ePO sur un serveur pré-existant, tel qu'un serveur de fichiers. Si votre réseau compte plus de 250 systèmes managés, utilisez un serveur dédié pour McAfee ePO.
Contrôleurs de domaine	(Recommandé) Une relation d'approbation est nécessaire entre le serveur et le contrôleur de domaine du réseau. Pour plus d'informations, consultez la documentation produit de Microsoft. L'installation du logiciel sur un contrôleur de domaine est prise en charge, mais elle n'est pas recommandée.
Système de fichiers	Partition NTFS (NT File System) recommandée.
Espace disque disponible	20 Go minimum.

Composant	Configuration requise et recommandations
Adresse IP	Utilisez des adresses IP statiques pour McAfee ePO. Les adresses IP statiques sont recommandées pour McAfee ePO et les Gestionnaires d'agents. McAfee ePO prend en charge les réseaux IPv4 et IPv6.
Mémoire	8 Go de mémoire RAM disponible minimum.
Carte d'interface réseau	100 Mo minimum. Si vous utilisez un serveur ayant plusieurs adresses IP, le logiciel McAfee ePO utilise la première adresse IP identifiée. Pour utiliser d'autres adresses IP pour les communications agent-serveur, créez des groupes de Gestionnaires d'agents supplémentaires pour chaque adresse IP. Pour plus d'informations, reportez-vous à l'article KB56281.
Ports	• Vérifiez que les ports que vous choisissez ne sont pas déjà utilisés sur le système serveur. • Signalez au personnel responsable du réseau les ports que vous allez utiliser pour la communication avec McAfee ePO et McAfee Agent.
Processeur	• Compatible Intel 64 bits • (Recommandé) 4 cœurs minimum

Configuration logicielle requise et recommandations

Vérifiez que les logiciels requis et recommandés sont installés sur votre système serveur avant d'installer McAfee ePO.

Logiciels	Configuration requise et recommandations
Mises à jour Microsoft	Recommandées. Vérifiez que votre logiciel et vos applications Microsoft incluent les dernières mises à jour. Désactivez les mises à jour Windows avant de lancer l'installation ou la mise à niveau du logiciel.
Microsoft Visual C++ 2010 Redistributable Package (x64 et x86)	Requis. Installé automatiquement.
Microsoft Visual C++ 2015 Redistributable Package (x64 et x86)	Requis. Installé automatiquement.
MSXML 3.0 et 6.0	Requis. Installé automatiquement.
Logiciels de sécurité	Recommandés. • Installez et mettez à jour le logiciel antivirus sur le serveur et lancez une analyse antivirus avant toute installation. • Installez et mettez à jour le logiciel pare-feu sur le serveur.
Navigateur pris en charge	Recommandé. Ce n'est pas indispensable pour l'installation, mais McAfee ePO nécessite l'utilisation d'un navigateur pris en charge.
Versions de SQL Server prises en charge	Requis. Vous devez disposer d'une version de SQL Server ou SQL Server Express prise en charge pour installer McAfee ePO.
Client natif SQL Server 2012 (ou version ultérieure)	Requis. Installé automatiquement.

Systèmes d'exploitation pris en charge

Vous pouvez installer McAfee ePO sur tout système d'exploitation serveur Microsoft Windows pris en charge.

Systèmes d'exploitation serveur pris en charge

Ce logiciel requiert l'un des systèmes d'exploitation serveur 64 bits pris en charge, répertoriés ci-dessous.

- Windows Server 2008 R2 Service Pack 1
- Windows Server 2012
- Windows Server 2012 Service Pack 1
- Windows Server 2012 R2
- Windows Server 2016

Si vous utilisez Windows Server 2012 ou une version supérieure, vous devrez également installer la mise à jour 2919355 de Microsoft.

Systèmes d'exploitation destinés à l'évaluation

Vous pouvez utiliser ces systèmes d'exploitation pour évaluer le logiciel McAfee ePO, mais aucun support n'est fourni les concernant.

- Windows 7 (x64 uniquement)
- Windows 8 et 8.1 (x64 uniquement)
- Windows 10 (x64 uniquement)

Langue du système d'exploitation

Le logiciel McAfee ePO est exécuté sur tout système d'exploitation pris en charge, quelle que soit la langue dans laquelle il est configuré.

L'interface de McAfee ePO a été traduite dans les langues indiquées ci-dessous. Si vous installez le logiciel sur un système d'exploitation dont la langue ne figure pas dans cette liste, l'interface s'affiche en anglais.

- Anglais
- Italien
- Anglais (Royaume-Uni)
- Chinois (simplifié)
- Chinois (traditionnel)
- Français
- Allemand
- Japonais
- Coréen
- Portugais (Brésil)
- Russe
- Espagnol
- Turc

Logiciels d'infrastructure virtuelle pris en charge

Le logiciel McAfee ePO prend en charge l'utilisation de plusieurs types de logiciels d'infrastructure virtuelle.

Les logiciels d'infrastructure virtuelle pris en charge sont :

- Microsoft Hyper-V Server 2016
- Microsoft Hyper-V Server 2012 R2
- VMware ESXi 5.5
- VMware ESXi 5.1

- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2008 R2
- VMware ESXi 6
- XenServer 6.2
- XenServer 6

Pour plus d'informations sur les dernières plates-formes, environnements et systèmes d'exploitation pris en charge pour McAfee ePO, consultez l'article KB51569.

Serveurs SQL pris en charge

Le logiciel McAfee ePO nécessite l'utilisation d'un serveur SQL Server pris en charge.

L'Assistant d'installation détecte si un serveur SQL pris en charge est installé sur le système serveur où vous installez le logiciel.

McAfee ePO prend en charge toutes les éditions des serveurs Microsoft SQL Server indiqués ci-dessous.

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017

Configuration requise des paramètres de SQL Server

Le logiciel McAfee ePO nécessite une configuration spécifique des paramètres de SQL Server. Pour plus d'informations sur ces paramètres, consultez la documentation de SQL Server.

Configuration	Détails
Déclencheurs imbriqués	L'option **Déclencheurs imbriqués de SQL Server** doit être activée.
Classement de base de données	Le logiciel McAfee ePO prend en charge tous les classements Microsoft SQL Server à l'aide des deux propriétés de classement SQL suivantes : • Non-respect de la casse • Prise en charge du jeu de caractères ASCII complet (ces caractères sont inclus à tous les jeux de caractères Unicode) Pour connaître les types de classement Microsoft SQL Server pris en charge, consultez l'article KB73717.
Paramètres de maintenance	Il est conseillé de définir des paramètres de maintenance spécifiques pour les bases de données McAfee ePO. Pour plus d'instructions, consultez le Guide produit de McAfee ePO.

Configuration de l'accès TCP/IP au serveur SQL Server

McAfee ePO ne peut communiquer avec le serveur SQL Server qu'à l'aide d'une connexion TCP/IP. Avant d'installer McAfee ePO, vérifiez que le protocole TCP/IP a été activé sur le serveur SQL Server qui hébergera la base de données McAfee ePO.

Notez le numéro de port que le serveur SQL Server utilise.

Procédure

1 Pour configurer le protocole TCP/IP pour le serveur SQL Server :

   a Démarrez le **gestionnaire de configuration SQL Server**.

   b Dans le volet de la console, développez **Configuration du réseau SQL Server**, puis sélectionnez l'élément Protocoles correspondant à votre instance SQL Server. Par exemple, si vous utilisez l'instance MSSQLSERVER par défaut, sélectionnez **Protocoles pour MSSQLSERVER**.

   c Dans le volet de détails, recherchez l'entrée **TCP/IP** et vérifiez la valeur de la colonne **Statut**. Si elle est définie sur **Activé**, accédez à l'étape 2 pour déterminer le port utilisé.

   d Si le paramètre TCP/IP est défini sur **Désactivé**, double-cliquez sur **TCP/IP** pour ouvrir la fenêtre **Propriétés TCP/IP**.

   e Sélectionnez l'onglet **Protocole**, cliquez sur **Activé**, puis sélectionnez **Oui**.

   f Cliquez sur **Appliquer**, puis sur **OK** pour fermer la boîte de dialogue **Avertissement**.

   Le protocole TCP/IP est activé. Vous pouvez maintenant redémarrer le service afin de vous assurer que les modifications prennent effet.

   g Dans le volet de la console, cliquez sur **Services SQL Server**.

   h Dans le volet de détails, cliquez avec le bouton droit de la souris sur le service SQL Server, puis cliquez sur **Redémarrer**.

2 Pour déterminer le port utilisé par le serveur SQL Server :

   a Le cas échéant, démarrez le **gestionnaire de configuration SQL Server**, développez **Configuration du réseau SQL Server**, puis sélectionnez l'élément Protocoles correspondant à votre instance SQL Server.

   b Double-cliquez sur **TCP/IP** pour ouvrir la fenêtre **Propriétés TCP/IP**.

   c Cliquez sur l'onglet **Adresses IP**.

   Vérifiez que l'option **Activé** est définie sur **Oui** pour chaque adresse IP active.

   d Sous **IPAll**, notez la valeur du paramètre **Ports TCP dynamiques**.

   Si une valeur est spécifiée, `57482` par exemple, cela signifie que votre serveur SQL Server utilise des ports dynamiques. Notez cette valeur, car elle vous sera demandée plus loin dans l'installation.

   Si vous utilisez des ports dynamiques, le service SQL Browser doit être en cours d'exécution sur le serveur SQL Server. Si le champ **Ports TCP dynamiques** est vide, cela signifie que votre serveur SQL Server utilise un port statique. La valeur de ce port sera indiquée dans le champ **Port TCP**.

3 Si vous utilisez des ports dynamiques, notez le nom de l'instance SQL qui hébergera la base de données McAfee ePO. Si vous utilisez l'instance SQL par défaut, son nom est MSSQLSERVER.

Navigateurs Internet pris en charge

Le logiciel McAfee ePO nécessite l'utilisation de l'un des navigateurs pris en charge suivants.

- Internet Explorer 11 ou version supérieure
- Firefox 4.5 ou version supérieure
- Chrome 5.1 ou version supérieure
- Safari 10 ou version supérieure (sur Mac OS uniquement, non pris en charge par Windows)
- Microsoft Edge

Exigence relative à TLS

Si vous utilisez un navigateur plus ancien, vérifiez que le protocole TLS 1.2 est activé.

Utilisation de la sécurité renforcée d'Internet Explorer

Si vous utilisez Internet Explorer avec l'option de sécurité renforcée activée, vous devez ajouter l'adresse du serveur McAfee ePO à la liste des sites de confiance Internet Explorer (au format `https://<nomduserveur>`). Si ce n'est pas le cas, Internet Explorer affiche un message d'erreur lorsque vous tentez de vous connecter au serveur McAfee ePO.

Configuration serveur requise pour le gestionnaire d'agents

Vous pouvez installer le logiciel du gestionnaire d'agents McAfee ePO sur tout système d'exploitation serveur Microsoft Windows pris en charge.

Le gestionnaire d'agents peut s'authentifier auprès de la base de données SQL McAfee ePO à l'aide des informations d'identification de domaine. En cas d'échec de l'authentification Windows, le compte utilisé par le gestionnaire d'agents pour s'authentifier auprès de la base de données doit utiliser l'authentification SQL. Pour plus d'informations sur l'authentification Windows et SQL, consultez la documentation Microsoft SQL Server.

Le logiciel du gestionnaire d'agents nécessite l'un des systèmes d'exploitation serveur suivants :

- Windows Server 2008 R2 Service Pack 1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Si vous utilisez Windows Server 2012 ou une version supérieure, vous devrez également installer la mise à jour 2919355 de Microsoft.

Installation SQL Server décrite dans ce guide

Le logiciel McAfee ePO nécessite l'utilisation d'un serveur SQL Server pris en charge. Le scénario d'installation décrit en détail dans ce guide implique que vous ayez déjà installé une version prise en charge de SQL Server ou SQL Server Express.

Dans ce scénario, vous installez manuellement le serveur SQL Server et le programme d'installation installe le logiciel McAfee ePO. Pour plus d'informations sur l'installation d'un serveur SQL Server, consultez la documentation du logiciel SQL Server.

Si McAfee ePO est installé dans un environnement de cluster, le serveur SQL Server doit être distinct de McAfee ePO : il ne doit pas être installé dans le même cluster que McAfee ePO.

Autres installations et mises à niveau SQL Server pertinentes

Consultez la documentation fournie par Microsoft pour plus d'informations sur les exemples d'installation suivants :

- Installation de SQL Server 2012, 2014, 2016 ou 2017
- Mise à niveau à partir de SQL Server 2005 ou 2008 vers des versions de SQL Server prises en charge
- Mise à niveau à partir de SQL Server 2005 Express ou 2008 Express vers des versions de SQL Server prises en charge

Autorisations SQL requises

Des rôles SQL Server spécifiques sont nécessaires pour le compte utilisé par McAfee ePO.

Pour une nouvelle installation de McAfee ePO...	Utilisez ces rôles serveur
Pendant l'installation	Que ce soit pour l'authentification Windows ou SQL, les informations d'identification du compte utilisateur doivent inclure les **Rôles serveur** suivants sur le serveur SQL Server cible : • publics • dbcreator Le rôle serveur dbcreator est requis pour que le programme d'installation puisse créer et ajouter les objets de la base de données McAfee ePO principale nécessaires au serveur SQL Server cible pendant l'installation. Ce compte utilisateur SQL McAfee ePO comporte l'autorisation **rôle de base de données** db_owner pour la base de données McAfee ePO.
Une fois la base de données créée	Le rôle serveur dbcreator peut être retiré à l'utilisateur SQL McAfee ePO. Cette révocation limite le compte utilisateur aux seules autorisations octroyées au rôle de base de données db_owner sur la base de données McAfee ePO.

Pour une mise à niveau ou une installation de patch...	Utilisez ces rôles
Pendant l'installation	Les informations d'identification de compte pour l'authentification Windows ou SQL doivent inclure les **rôles serveur** suivants sur le serveur SQL Server cible : • publics • dbcreator

Formats pris en charge pour le nom utilisateur et le mot de passe de base de données SQL

Consultez les formats pris en charge lorsque vous créez des noms d'utilisateur et des mots de passe de base de données McAfee ePO et SQL.

Tous les caractères imprimables du jeu de caractères ISO 8859-1 sont pris en charge à l'exception des suivants :

Plate-forme	Caractères non pris en charge pour les mots de passe et les noms d'utilisateur
Base de données SQL	• Espaces au début ou à la fin du mot de passe, ou mots de passe composés d'espaces uniquement • Apostrophes (') • Guillemets (") • Barre oblique inverse (\) placée au début • Deux-points dans les noms d'utilisateur (:) • Points-virgules dans les noms d'utilisateur (;)

Pour plus d'informations sur les formats de mots de passe et de noms d'utilisateur pris en charge par McAfee ePO, consultez l'article KB66286.

Options de port

Les ports utilisés par McAfee ePO sont prédéfinis et renseignés par défaut.

Consultez le tableau suivant pour savoir quelles affectations de port vous pouvez modifier.

Port	Valeur par défaut	Modifiable pendant l'installation	Modifiable après l'installation
Port de communication agent-serveur	80	X	
Port sécurisé de communication agent-serveur	443	X	
Port de communication de réactivation de l'agent	8081	X	X
Port de communication de diffusion de l'agent	8082	X	X
Port de communication console-serveur d'applications	8443	X	
Port de communication authentifiée client-serveur	8444	X	
Port TCP du serveur SQL	1433	X	

Installation automatique des produits

Lors d'une installation automatique, McAfee ePO télécharge et installe tous les produits McAfee qui vous sont concédés en vertu de votre clé de licence McAfee ePO.

L'option Installation automatique des produits télécharge tous les produits disponibles dans le catalogue de logiciels.

En règle générale, l'exécution du processus Installation automatique des produits n'est pas visible au cours d'une installation automatique. Elle démarre à l'issue de l'installation de McAfee ePO et avant que vous vous connectiez.

Si la page Installation automatique des produits s'affiche lorsque vous vous connectez pour la première fois à McAfee ePO, cela signifie qu'une erreur s'est produite lors du téléchargement ou de l'installation de vos produits. Par exemple, votre connexion Internet s'est interrompue. Notez le produit pour lequel l'installation a échoué et cliquez sur **Réessayer** pour retenter l'installation du produit.

Pour arrêter l'installation automatique de produits, cliquez sur **Arrêter**. Une boîte de dialogue s'affiche dans laquelle vous devez confirmer que vous souhaitez utiliser le Catalogue de logiciels pour installer vos produits.

Après avoir cliqué sur **OK** dans la boîte de dialogue de confirmation Arrêter la configuration automatique des produits, vous devez utiliser le Catalogue de logiciels pour installer vos produits ou installer manuellement ces derniers dans le référentiel maître. L'option Installation automatique des produits est disponible une seule fois au cours de l'installation initiale.

Si l'installation d'un produit continue d'échouer lors de l'Installation automatique des produits, contactez le support technique, ou cliquez sur **OK** pour quitter la page Installation automatique des produits et pour commencer à configurer le serveur McAfee ePO.

Pour obtenir des informations sur l'état des installations futures de produits, ouvrez le Catalogue de logiciels : **Menu** | **Logiciels** | **Catalogue de logiciels**.

Configuration requise pour les référentiels distribués

Les référentiels distribués de votre environnement permettent l'accès au contenu utilisé par le serveur McAfee ePO. Vos référentiels distribués doivent respecter la configuration minimale requise.

Composant	Configuration minimale requise
Espace disque disponible	Au moins 1 Go (4 Go recommandés) sur le lecteur où est stocké le référentiel. L'espace requis varie en fonction de la taille des packages logiciels faisant l'objet d'une réplication à partir du Référentiel maître. L'espace disque requis pour les référentiels distribués sur les systèmes où les agents sont désignés comme des SuperAgents correspond à l'espace disque disponible pour le Référentiel maître.
Mémoire	Au moins 512 Mo.
Hôtes de référentiel	• Serveurs HTTP fonctionnant sous Microsoft Windows ou Linux • Serveurs FTP Windows, Linux ou Open Enterprise • Partages UNC Windows, Linux ou UNIX Samba • Systèmes sur lesquels un SuperAgent est installé

Produits pris en charge et problèmes connus

Avant d'effectuer l'installation, consultez la liste des produits pris en charge par McAfee ePO ainsi que les problèmes connus.

- Produits pris en charge — KB90383
- Problèmes connus — KB90382

4 Installation de McAfee ePO sur un serveur unique

Installation de McAfee ePO sur un serveur unique

La première installation de McAfee ePO suppose également le téléchargement et le lancement de l'installation. Terminez l'installation en sélectionnant et en configurant votre base de données, votre port de communication et vos options de licence.

Procédure

1. Connectez-vous au système Windows Server qui servira de serveur McAfee ePO.

   Utiliser un compte disposant des autorisations d'administrateur local.

2. Recherchez le logiciel téléchargé à partir du site web McAfee et extrayez les fichiers dans un emplacement temporaire. Cliquez avec le bouton droit sur **Setup.exe** et sélectionnez **Exécuter en tant qu'administrateur**.

   L'exécutable se trouve dans le dossier d'installation McAfee ePO téléchargé.

   > Si vous lancez `Setup.exe` sans extraire au préalable le contenu du fichier .zip, l'installation échoue.

   Le programme **McAfee ePolicy Orchestrator - Assistant InstallShield** démarre.

3. Cliquez sur **Suivant** pour poursuivre l'installation.

   Surveillez le processus d'installation lors de l'utilisation de l'Assistant InstallShield. Vous devrez peut-être redémarrer le système.

4. A l'étape Dossier de destination, cliquez sur :

   - **Suivant** pour installer le logiciel McAfee ePO à l'emplacement par défaut (C:\Program Files (x86)\McAfee \ePolicy Orchestrator\).
   - **Modifier** pour indiquer un emplacement de destination personnalisé pour le logiciel McAfee ePO. Lorsque la fenêtre Modifier le dossier de destination actuel s'ouvre, accédez au dossier de destination et si nécessaire créez des dossiers, puis cliquez sur **OK**.

5. Le programme d'installation recherche des serveurs SQL Server. Si le programme d'installation détecte des serveurs SQL Server, il passe automatiquement à l'étape suivante et vous pouvez sélectionner les serveurs détectés dans la liste déroulante. Si le programme d'installation ne détecte aucun serveur, une boîte de dialogue vous demande si vous souhaitez effectuer la recherche à nouveau. Cliquez sur **Non** pour passer à l'étape suivante, qui vous permet d'entrer manuellement les informations du serveur SQL Server.

6 A l'étape Informations de base de données, indiquez les informations de votre base de données et cliquez sur **Suivant**.

a Spécifiez le **Serveur de base de données** et le **Nom de la base de données**.

Serveur de base de données	Si le programme d'installation a détecté le serveur SQL Server à l'étape précédente, sélectionnez votre serveur dans la liste déroulante. Si le serveur n'est pas répertorié, entrez les informations manuellement en entrant le nom du serveur SQL Server. Si vous utilisez des ports SQL dynamiques, entrez le nom du serveur SQL et le nom de l'instance SQL séparés par une barre oblique inverse. Par exemple, si votre serveur SQL Server est nommé **SQLServer** et si vous utilisez le nom d'instance par défaut **MSSQLSERVER**, entrez `SQLServer\MSSQLSERVER`.
Nom de la base de données	Cette valeur est automatiquement remplie avec le nom de la base de données. Entrez un nouveau nom de base de données pour modifier la valeur.

b Indiquez le type d'**Informations d'identification pour le serveur de base de données** à utiliser.

Authentification Windows	Dans le menu **Domaine**, sélectionnez le domaine du compte d'utilisateur permettant d'accéder au serveur SQL Server dans la liste déroulante. Si le domaine requis n'est pas répertorié, entrez le nom de domaine, le nom utilisateur et le mot de passe.
Authentification SQL	Entrez le nom utilisateur et le mot de passe de votre serveur SQL Server. Les informations d'identification que vous fournissez doivent correspondre à un utilisateur existant sur le serveur SQL Server muni de droits d'accès appropriés. Le menu **Domaine** est grisé si vous utilisez l'authentification SQL.

c Cliquez sur **Suivant**.

Le programme d'installation tente de se connecter au serveur SQL Server avec les informations d'identification données. Si le programme d'installation ne peut pas déterminer automatiquement le port, le message suivant s'affiche : **Le programme d'installation n'a pas pu accéder au port SQL UDP 1434**. Cliquez sur **OK** pour revenir à la page **Informations de base de données**. Toutefois, le champ Port TCP SQL Server est désormais disponible. Entrez le port, puis cliquez sur **Suivant**.

7 Pre-Installation Auditor démarre automatiquement. Passez en revue les résultats et corrigez les défaillances, puis cliquez sur **Réexécuter**. Une fois que tous les contrôles sont positifs, cliquez sur **Terminer**.

8 À l'étape Informations de port HTTP, examinez l'affectation de port par défaut, puis cliquez sur **Suivant** pour vérifier que les ports ne sont pas déjà utilisés sur ce système.

Vous pouvez modifier certains de ces ports maintenant. Une fois l'installation terminée, vous pouvez uniquement modifier le **Port de communication de réactivation de l'agent** et le **Port de communication de diffusion de l'agent**.

9 A l'étape Informations sur l'administrateur, entrez ces informations, puis cliquez sur **Suivant**.

a Entrez le nom utilisateur et le mot de passe que vous souhaitez utiliser pour le compte de l'administrateur principal.

b Entrez la phrase secrète de récupération du serveur.

La phrase secrète comprend 14 à 200 caractères, ne doit pas contenir de barres obliques inverses au début ou à la fin (\), d'espaces, de guillemets doubles (") ou de caractères non compris entre ASCII 32 et ASCII 65535.

Conservez cette phrase secrète, car vous en aurez besoin pour déchiffrer les enregistrements d'instantanés de reprise sur sinistre et McAfee ne peut pas la récupérer.

10 A l'étape Entrer la clé de licence, indiquez votre clé de licence, puis cliquez sur **Suivant**.

Si vous ne possédez pas de clé de licence, sélectionnez **Evaluation** pour poursuivre l'installation du logiciel en mode d'évaluation. La période d'évaluation est limitée à 90 jours. Vous pouvez entrer une clé de licence après l'installation, à partir des paramètres ou du catalogue de logiciels de McAfee ePO. Si vous souhaitez que McAfee ePO télécharge automatiquement les produits pour lesquels vous disposez d'une licence après l'installation, vous pouvez également sélectionner **Autoriser l'installation automatique du produit**. Pour plus d'informations, consultez *Installation automatique du produit*.

L'option **Autoriser l'installation automatique du produit** est activée par défaut et uniquement disponible si vous disposez d'une clé de licence.

11 Acceptez l'Accord de licence utilisateur final McAfee et cliquez sur **OK**.

12 Dans la boîte de dialogue Prêt pour l'installation du programme, choisissez si vous souhaitez autoriser McAfee à collecter des données télémétriques sur le système et le logiciel, puis cliquez sur **Installer** pour commencer l'installation du logiciel.

13 Lorsque l'installation est terminée, cliquez sur **Terminer** pour quitter le programme d'installation.

Le logiciel McAfee ePO est à présent installé. Double-cliquez sur l'icône **Lancer ePolicy Orchestrator** de votre bureau pour commencer à utiliser votre serveur McAfee ePO, ou accédez au serveur à partir d'une console web à distance (`https://nomduserveur:port`).

Un avertissement de certificat s'affiche lorsque vous accédez à un site HTTPS avec un certificat autosigné.

Si vous utilisez Internet Explorer avec l'option de sécurité renforcée activée, vous devez ajouter l'adresse du serveur McAfee ePO à la liste des sites de confiance Internet Explorer (au format https://<nomduserveur>). Si ce n'est pas le cas, Internet Explorer affiche un message d'erreur lorsque vous tentez de vous connecter au serveur McAfee ePO.

5 Installation de McAfee ePO sur un serveur cloud

Sommaire

Utilisation d'un serveur AWS avec McAfee ePO

Vous pouvez utiliser Amazon Web Services pour installer McAfee ePO.

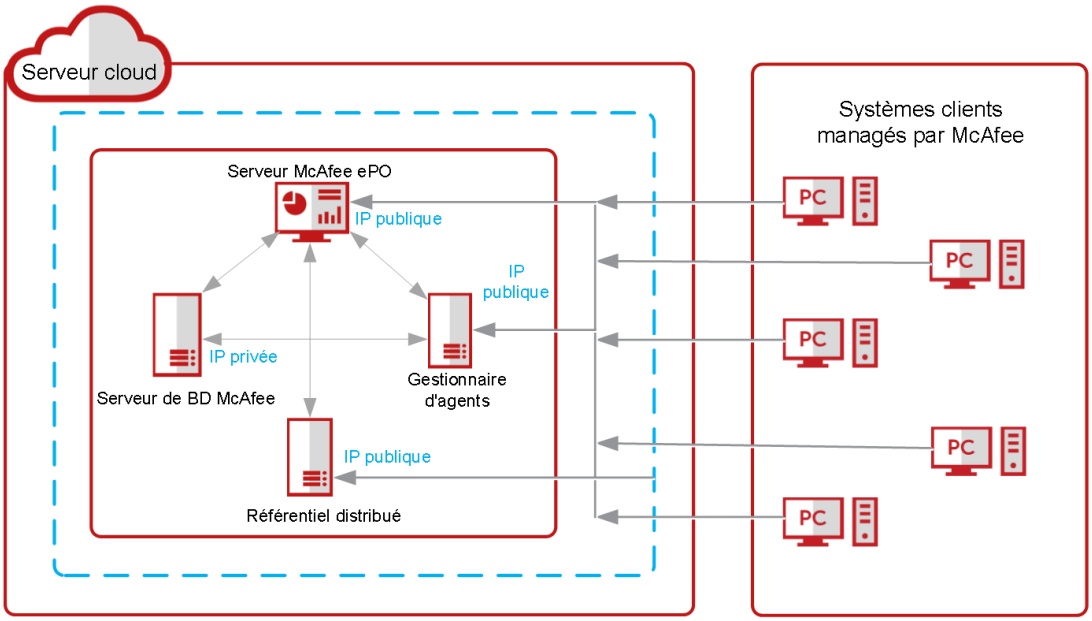
Pour plus d'informations, consultez https://aws.amazon.com/quickstart/.

Utilisation d'un serveur Microsoft Azure pour McAfee ePO

L'installation de McAfee ePO sur un serveur virtuel Microsoft Azure vous permet de redimensionner votre serveur au fur et à mesure que votre réseau augmente et de supprimer le risque de panne matérielle.

Un serveur virtuel Azure fournit les mêmes fonctionnalités et performances que le matériel configuré en local. Le schéma suivant illustre la configuration de base de McAfee ePO installé sur un serveur Azure.

Figure 5-1 Serveur cloud avec configuration de McAfee ePO



Limites

Il existe des limitations dont vous devez tenir compte lorsqu'une communication initiée par le serveur est nécessaire.

- Si le serveur McAfee ePO ou le Gestionnaire d'agents ne peut pas communiquer avec les Agents dans un réseau privé, les fonctionnalités suivantes ne fonctionneront pas.
  - L'agent de diffusion ne fonctionne pas : un réseau privé virtuel permet de résoudre ce problème.
  - La réactivation d'agent à l'aide du Gestionnaire d'agents ne fonctionne pas : utilisez un VPN ou configurez DXL pour contourner ce problème.
  - L'exécution d'une tâche client à l'aide du Gestionnaire d'agents ne fonctionne pas : utilisez un VPN ou configurez DXL pour contourner ce problème.
- Si le serveur McAfee ePO ou le Gestionnaire d'agents ne peut pas communiquer avec les serveurs distants dans un réseau privé, les fonctionnalités suivantes ne fonctionneront pas.
  - Les référentiels distribués comme SuperAgent, FTP, HTTP et UNC ne fonctionnent pas.
  - Un serveur enregistré qui ne peut pas communiquer avec le serveur McAfee ePO ne fonctionne pas.
  - Si McAfee ePO ne peut pas joindre le serveur SMTP, le service de messagerie ne fonctionne pas.

Si McAfee ePO peut communiquer avec les agents et serveurs à distance, ces fonctionnalités fonctionnent comme prévu, à condition que les ports requis soient configurés dans les règles de sécurité Azure.

Configuration requise pour les ports

Configurez ces ports afin d'établir une communication permanente entre le serveur McAfee ePO, les référentiels et les agents.

Les ports TCP 80 et 443 sont les ports par défaut utilisés pour la communication entre McAfee ePO et McAfee Agent. Vous pouvez modifier les ports lors de l'installation de McAfee ePO.

Les règles de sécurité de trafic entrant Azure doivent permettre cette communication. Pour plus d'informations sur la configuration requise des ports, consultez l'article KB66797.

Outre les ports mentionnés dans l'article, le tableau suivant répertorie les ports à configurer pour ces différents serveurs :

Type de serveur	Détails du port
Serveur distribué	• Configurez le port 2049 dans le groupe de sécurité du trafic sortant du serveur McAfee ePO. • Configurez le port 2049 dans le groupe de sécurité du trafic entrant du serveur de référentiel distribué.
Serveur de génération de rapports CSR	• Configurez le port 9112 dans le groupe de sécurité du trafic sortant du serveur McAfee ePO. • Configurez les ports 9111, 9112, 9121 et 9129 dans le groupe de sécurité du trafic entrant du serveur de génération de rapports CSR.
Serveur syslog	• Configurez le port 6514 dans le groupe de sécurité du trafic sortant du serveur McAfee ePO. • Configurez le port 6514 dans le groupe de sécurité du trafic entrant du serveur syslog.

McAfee Agent 5.x et les versions ultérieures ne prennent pas en charge le port 80.

Configuration du serveur Microsoft Azure pour McAfee ePO

Sur le serveur Azure, vous devez créer un serveur virtuel et lancer une instance de machine virtuelle (VM) pour installer McAfee ePO.

Avant de commencer

Vous devez disposer d'un compte Microsoft Azure pour effectuer cette tâche.

Procédez comme suit pour installer et configurer McAfee ePO sur un serveur Azure pour gérer vos clients.

Procédure

1 Obtenez un compte Azure à partir de https://azure.microsoft.com/.

2 Connectez-vous à la console Azure et configurez votre serveur virtuel.

a Lancez une instance de machine virtuelle.

Sélectionnez l'emplacement de votre serveur virtuel, le plus proche de la plupart de vos systèmes McAfee ePO managés.

b Configurez les règles de sécurité du trafic entrant sur Azure.

Dans Azure, un pare-feu est appelé *Règles de sécurité de trafic entrant* et doit être créé pour permettre à un McAfee Agent de se connecter au serveur McAfee ePO.

Assurez-vous de configurer vos *Règles de sécurité de trafic entrant* conformément aux exigences de port de serveur McAfee ePO.

c Capturez le nom de DNS public, ou l'adresse IP de l'instance Azure, créés par Azure.

Affectez une adresse IP élastique au nom de DNS public ou à l'adresse IP.

3 Utilisez la Connexion Bureau à distance et le nom de DNS, ou l'adresse IP publique, pour vous connecter au serveur Azure.

4 Installez McAfee ePO à l'aide du logiciel fourni par McAfee et des informations du serveur de base de données SQL Azure.

5 Créez une URL McAfee Agent ou un package d'installation McAfee Agent.

Le serveur McAfee ePO commence à gérer vos systèmes.

Installation de McAfee ePO sur un serveur Azure

La procédure d'installation de McAfee ePO sur un serveur Azure est similaire à celle des logiciels sur un serveur physique.

Avant de commencer

- Le serveur Azure doit être créé.
- Vous devez connaître le nom du serveur SQL Server.

Procédure

1 Connectez-vous au serveur Azure à l'aide du logiciel Connexion Bureau à distance de Microsoft et de l'adresse IP statique ou du nom DNS configurés.

2 Lancez le processus d'installation de McAfee ePO.

3 Sous **Informations de base de données**, entrez le nom du serveur Microsoft SQL Server configuré.

Par défaut, le nom du serveur SQL Server McAfee ePO est <nom_serveur_AWS>\EPOSERVER.

4 Procédez à l'installation du serveur McAfee ePO.

5 (Facultatif) Créez une image de sauvegarde de votre serveur Azure. Consultez la documentation d'Azure pour obtenir des instructions.

Vous venez d'installer et de configurer un serveur McAfee ePO auquel vous pouvez vous connecter à partir d'un navigateur distant à l'aide de la commande suivante :

```
https://<Nom DNS public du serveur EPO>:<port>
```

Mise à jour du nom de DNS public de McAfee ePO

Vous devez mettre à jour le nom de DNS public de McAfee ePO dans la console.

Avant de commencer

McAfee ePO doit être installé sur votre serveur Azure.

Procédure

1 Sélectionnez **Menu** | **Configuration** | **Paramètres serveur**.

2 Sélectionnez **DNS public du serveur McAfee ePO** dans le volet **Catégories de paramètres** et cliquez sur **Modifier**.

3 Entrez le nom de DNS public et cliquez sur **Enregistrer**.

Gestion des Gestionnaires d'agents

Vous pouvez installer un Gestionnaire d'agents sur votre serveur Azure comme sur un serveur physique.

> **Avant de commencer**
> McAfee ePO doit être installé sur votre serveur Azure.

Pour installer et configurer un Gestionnaire d'agents, consultez le Guide produit de McAfee ePO.

Procédure

- Utilisez un équilibreur de charge élastique (ELB) avec le Gestionnaire d'agents afin de distribuer le trafic.
  - Si un Gestionnaire d'agents est utilisé sans équilibreur de charge :
    1 Accédez à **Menu** | **Configuration** | **Gestionnaires d'agents**.
    2 Cliquez sur **Gestionnaires d'agents** sous **Etat des gestionnaires**.
    3 Cliquez sur le **Nom DNS du gestionnaire** dans la **Liste des gestionnaires**.
    4 Entrez le **Nom DNS publié** et l'**Adresse IP publiée.**
    5 Cliquez sur **Enregistrer**.
  - Si un Gestionnaire d'agents est utilisé avec un équilibreur de charge :
    1 Configurez l'ELB sur la console de gestion Microsoft Azure.
      a Ajoutez les machines virtuelles des Gestionnaires d'agents.
      b Configurez les règles de sécurité Azure pour l'ELB selon les exigences relatives aux ports du Gestionnaire d'agents.
    2 Pour plus d'informations sur la configuration de l'équilibreur de charge, consultez le Guide produit de McAfee ePO.

Connexion aux référentiels distribués

McAfee Agent récupère le contenu de sécurité à partir de plusieurs types de référentiels afin de maintenir l'environnement à jour.

Les packages inclus dans le référentiel maître sont répliqués vers un référentiel distribué dans le réseau.

Vous pouvez créer différents utilisateurs pour les divers types de référentiels et les associer lors du partage du dossier.

Pour le référentiel UNC (Universal Naming Convention), installez le système NFS dans le serveur de référentiel et partagez le dossier UNC à l'aide d'un partage NFS. Ouvrez le port NFS 2049 sur le serveur McAfee ePO et sur le serveur de référentiel.

6 Installation de McAfee ePO dans un environnement de cluster

McAfee ePO permet d'assurer la haute disponibilité nécessaire aux clusters de serveurs mis en place avec le logiciel Microsoft Cluster Server (MSCS).

L'installation du logiciel dans un environnement Microsoft Cluster Server requiert la réalisation d'opérations supplémentaires. L'installation en cluster est prise en charge sur les systèmes Windows Server 2008 R2, Windows Server 2012 et Windows Server 2016.

L'installation est possible si la configuration de Microsoft Cluster Server est correcte. Pour plus d'informations sur la configuration de MSCS, consultez la documentation Microsoft.

Terminologie utilisée dans le cadre de l'installation en cluster

La terminologie suivante est employée dans les instructions de l'installation en cluster.

Durée	Définition
Lecteur de données	L'un des deux lecteurs requis par Microsoft Cluster Server et McAfee ePO. Le lecteur de données est un lecteur distant accessible par tous les nœuds du cluster. Il constitue l'emplacement où vous installez les fichiers de McAfee ePO.
Ressource Adresse IP virtuelle d'ePO	Ressource Adresse IP que vous créez lors de l'installation en cluster de McAfee ePO. Cette adresse IP virtuelle représente l'installation en cluster de McAfee ePO dans son ensemble. Les références à cette adresse IP pointent vers le nœud actuellement actif dans le cluster.
Ressource Nom réseau virtuel d'ePO	Ressource Nom du réseau que vous créez lors de l'installation en cluster de McAfee ePO. Ce nom de réseau virtuel représente l'installation en cluster de McAfee ePO dans son ensemble. Les références à ce nom de réseau pointent vers le nœud actuellement actif dans le cluster.
Lecteur quorum	L'un des deux lecteurs requis par le logiciel Microsoft Cluster Server. N'installez aucun fichier McAfee ePO sur ce lecteur.

Conditions préalables à l'installation en cluster

Avant de débuter l'installation en cluster, consultez la liste ci-dessous et vérifiez que toutes les conditions requises sont remplies. Ces exigences s'appliquent aux installations sur des systèmes Windows Server 2008 R2, Windows Server 2012 et Windows Server 2016.

- McAfee ePO prend en charge uniquement les environnements de cluster à deux nœuds. En d'autres termes, les environnements comportant plus de deux nœuds ne sont pas pris en charge.
- Microsoft Cluster Server est installé et en cours d'exécution sur un cluster composé de deux serveurs.
- Un lecteur quorum est présent et configuré selon les instructions de Microsoft.
- Un lecteur de données est présent et accessible pour tous les nœuds du cluster.
- Un serveur SQL Server distant pris en charge est configuré.

Pour vérifier la communication entre McAfee ePO et ce serveur pendant l'installation :

- Vérifiez que le service Explorateur SQL Server est en cours d'exécution.
- Vérifiez que le protocole TCP/IP est activé dans le Gestionnaire de configuration SQL Server.

- Vous devrez peut-être fournir les informations suivantes pendant l'installation (selon votre configuration) sur la page Informations de base de données :
  - Nom de votre serveur SQL Server. Selon la configuration, utilisez le nom du serveur SQL ou bien le nom du serveur SQL *incluant* le nom de l'instance.
  - Numéro de port dynamique utilisé, le cas échéant, par le serveur SQL. Indiquez ce numéro de port dynamique pendant l'installation, sur la page Informations de base de données.

Sommaire

Création du rôle d'application McAfee ePO

Le rôle d'application McAfee ePO est nécessaire pour autoriser Microsoft Cluster Services à contrôler McAfee ePO.

Procédure

1. Ouvrez le gestionnaire du cluster de basculement : cliquez sur **Gestionnaire de serveur** | **Outils** | **Gestionnaire du cluster de basculement**.
2. Double-cliquez sur **Rôles** dans l'Arborescence des systèmes, puis sélectionnez **Créer un rôle vide**.
3. Cliquez sur **OK**.
4. Cliquez avec le bouton droit sur le rôle vide, puis sélectionnez **Propriétés**.
5. Dans la boîte de dialogue **Nouveau rôle**, attribuez un nom au rôle, par exemple `ePO`.
6. Cliquez sur **OK**.

Création du point d'accès client

Le point d'accès client définit l'adresse IP virtuelle et les noms de réseau virtuel McAfee ePO pour que les nœuds de votre cluster puissent communiquer avec le serveur McAfee ePO.

Procédure

1. Cliquez avec le bouton droit sur le rôle d'application **ePO**, puis sélectionnez **Ajouter une ressource** | **Point d'accès client**.

   L'Assistant **Point d'accès client** s'affiche.

2 Entrez le **Nom virtuel d'ePolicy Orchestrator** dans le champ **Nom** et indiquez l'**Adresse IP virtuelle d'ePolicy Orchestrator** dans le champ **Adresse**, puis cliquez sur **Suivant**.

La page **Confirmation** s'affiche.

3 Cliquez sur **Suivant** pour appliquer les modifications du Point d'accès client, puis cliquez sur **Terminer** à la fin de l'exécution de l'Assistant.

4 Si le **point d'accès client** est hors ligne, cliquez avec le bouton droit sur son nom et sélectionnez **Mettre en ligne**.

Ajout du lecteur de données

Le lecteur de données est l'emplacement dans lequel vous installez le logiciel McAfee ePO. Utilisez un lecteur distant auquel peuvent accéder tous les nœuds de votre cluster.

Procédure

1 Cliquez avec le bouton droit sur le rôle d'application **ePO** et sélectionnez **Ajouter un stockage**.

2 Dans la boîte de dialogue **Ajouter un stockage**, sélectionnez le lecteur de données à utiliser pour l'installation de McAfee ePO, puis cliquez sur **OK**.

Installation du logiciel McAfee ePO sur chaque nœud de cluster

Exécutez l'installation de type cluster sur chaque nœud.

Procédure

1 Connectez-vous au système Windows Server à utiliser comme premier nœud du cluster de serveurs McAfee ePO.

Utilisez un compte disposant d'autorisations d'administrateur local.

2 Localisez le logiciel que vous avez téléchargé depuis le site web de McAfee et extrayez les fichiers dans un emplacement temporaire. Cliquez avec le bouton droit de la souris sur le fichier **Setup.exe** et sélectionnez **Exécuter en tant qu'administrateur**.

L'exécutable se trouve dans le fichier d'installation de McAfee ePO téléchargé.

L'installation échoue si vous lancez `Setup.exe` sans avoir préalablement extrait le contenu du fichier .zip.

Le programme **McAfee ePolicy Orchestrator - Assistant InstallShield** démarre. Cliquez sur **Suivant**.

3 Sur la page **Type d'installation**, sélectionnez l'option **Cluster**, puis cliquez sur **Suivant**.

4 Sur la page **Choisir l'emplacement de destination**, indiquez le chemin d'accès du lecteur de données partagé, puis cliquez sur **Suivant**.

Utilisez le même chemin d'accès pour chaque nœud.

5 Sur la page Définir les paramètres du serveur virtuel du premier nœud, indiquez les informations d'identification suivantes pour le cluster McAfee ePO :

- Adresse IP du serveur virtuel McAfee ePO
- Nom du cluster virtuel McAfee ePO
- Nom de domaine complet du cluster virtuel McAfee ePO

Sur les nœuds suivants, les champs Adresse IP du serveur virtuel, Nom du cluster virtuel et Nom de domaine complet du cluster virtuel sont automatiquement renseignés. Vous devez ajouter la phrase secrète de configuration du cluster à chacun des nœuds suivants.

6 Le programme d'installation recherche les serveurs SQL Server. S'il trouve un serveur SQL Server, il passe automatiquement à l'étape suivante et les serveurs qu'il trouve peuvent être sélectionnés dans une liste déroulante.

S'il ne trouve aucun serveur SQL Server, une boîte de dialogue s'affiche vous demandant si vous souhaitez ou non lancer une nouvelle recherche. Cliquez sur **Non** pour passer à l'étape suivante dans laquelle les informations sur SQL Server peuvent être saisies manuellement.

7 A l'étape Informations de base de données, indiquez les informations sur votre base de données et cliquez sur **Suivant**.

a Spécifiez le **Serveur de base de données serveur** ainsi que le **Nom de la base de données**.

Serveur de base de données	Si le programme d'installation trouve le serveur SQL Server à l'étape précédente, sélectionnez votre serveur dans la liste déroulante. Si le serveur n'est pas répertorié dans la liste, entrez manuellement le nom du serveur SQL Server. Si vous utilisez des ports SQL dynamiques, entrez le nom du serveur SQL Server et le nom de l'instance SQL en les séparant au moyen d'une barre oblique inverse. Par exemple, si votre serveur SQL Server s'appelle SQL Server et que vous utilisez le nom d'instance par défaut MSSQLSERVER, entrez `SQLServer\MSSQLSERVER`.
Nom de la base de données	Ce champ est automatiquement renseigné avec le nom de la base de données. Entrez un nouveau nom de base de données pour le modifier.

b Indiquez le type d'**Informations d'identification pour le serveur de base de données** à utiliser.

Authentification Windows	Dans le menu **Domaine**, dans la liste déroulante, sélectionnez le domaine du compte utilisateur à utiliser pour accéder au serveur SQL Server. Si le domaine requis n'est pas répertorié dans la liste, saisissez le nom de domaine, le nom utilisateur et le mot de passe.
Authentification SQL	Saisissez le nom utilisateur et le mot de passe de votre serveur SQL Server. Les informations d'identification que vous fournissez doivent correspondre à un utilisateur existant sur le serveur SQL Server muni de droits d'accès appropriés.

Le menu **Domaine** est grisé si vous utilisez l'authentification SQL.

c Cliquez sur **Suivant**.

Le programme d'installation tente de se connecter au serveur SQL Server avec les informations d'identification spécifiées. Si le programme d'installation ne peut pas déterminer automatiquement le port, le message suivant s'affiche : **Le programme d'installation ne peut pas accéder au port UDP SQL 1434**. Cliquez sur **OK** pour revenir à la page **Informations sur la base de données**. Toutefois, le champ Port TCP du serveur SQL est désormais disponible. Entrez le port, puis cliquez sur **Suivant**.

8 Pre-Installation Auditor démarre automatiquement. Examinez les résultats et corrigez les éventuelles erreurs, puis cliquez sur **Réexécuter**. Une fois que tous les contrôles ont été passés, cliquez sur **Terminer**.

9 A l'étape Informations de port HTTP, examinez les ports par défaut affectés, puis cliquez sur **Suivant** pour vérifier qu'ils ne sont pas déjà utilisés sur ce système.

Vous pouvez modifier certains de ces ports maintenant. Une fois l'installation terminée, vous pouvez uniquement modifier le **Port de communication de réactivation de l'agent** et le **Port de communication de diffusion de l'agent**.

10 A l'étape Informations sur l'administrateur, entrez ces informations, puis cliquez sur **Suivant**.

a Entrez le nom utilisateur et le mot de passe que vous souhaitez utiliser pour le compte de l'administrateur principal.

b Saisissez la phrase secrète de récupération du serveur.

La phrase secrète comprend entre 14 et 200 caractères, ne doit pas contenir de barres obliques inverses (\) de début ou de fin, d'espaces, de guillemets doubles droits (") ni aucun des caractères en dessous d'ASCII 32 ou au-dessus d'ASCII 65535.

Notez cette phrase secrète ; elle est requise pour restaurer McAfee ePO à l'aide des enregistrements de capture instantanée pour reprise sur sinistre, or McAfee ne peut pas la récupérer.

11 A l'étape Entrer la clé de licence, indiquez votre clé de licence, puis cliquez sur **Suivant**.

Si vous ne possédez aucune clé de licence, sélectionnez **Evaluation** pour poursuivre l'installation du logiciel en mode d'évaluation. La période d'évaluation est limitée à 90 jours. Vous pouvez entrer une clé de licence après l'installation, à partir des paramètres de McAfee ePO ou du Catalogue de logiciels. Par ailleurs, pour que McAfee ePO télécharge automatiquement les produits pour lesquels vous détenez une licence à l'issue de l'installation, sélectionnez **Activer l'installation automatique du produit**. Pour plus d'informations, consultez la section *Installation automatique des produits*.

L'option **Activer l'installation automatique des produits** est activée par défaut et est disponible uniquement si vous disposez d'une clé de licence.

12 Acceptez l'Accord de licence utilisateur final McAfee et cliquez sur **OK**.

13 Dans la boîte de dialogue Prêt pour l'installation du programme, indiquez si vous souhaitez ou non autoriser McAfee à collecter les données télémétriques sur les systèmes et les logiciels, puis cliquez sur **Installer** pour lancer l'installation du logiciel.

14 Une fois l'installation terminée, ne sélectionnez pas **Oui, je souhaite lancer McAfee ePolicy Orchestrator maintenant.** Cliquez sur **Terminer** pour quitter le programme d'installation sur le premier nœud du cluster.

15 Dans le gestionnaire du cluster de basculement, déplacez le **rôle d'application ePO** vers le deuxième nœud du cluster en cliquant avec le bouton droit sur le rôle, puis en sélectionnant **Déplacer** | **Sélectionner le nœud**. Sélectionnez le deuxième nœud du cluster, puis cliquez sur **OK**.

Le rôle est déplacé vers le deuxième nœud du cluster.

Vous pouvez également arrêter le premier serveur de nœud de cluster : cette opération déplace automatiquement le rôle vers le deuxième nœud.

16 Connectez-vous à l'ordinateur Windows Server à utiliser comme deuxième nœud du cluster de serveurs McAfee ePO.

Utilisez un compte disposant d'autorisations d'administrateur local.

17 Localisez le logiciel que vous avez téléchargé depuis le site web de McAfee et extrayez les fichiers dans un emplacement temporaire. Cliquez avec le bouton droit de la souris sur le fichier **Setup.exe** et sélectionnez **Exécuter en tant qu'administrateur**.

L'exécutable se trouve dans le fichier d'installation de McAfee ePO téléchargé.

L'installation échoue si vous lancez `Setup.exe` sans avoir préalablement extrait le contenu du fichier .zip.

Le programme **McAfee ePolicy Orchestrator - Assistant InstallShield** démarre. Cliquez sur **Suivant**.

18 Sur la page **Type d'installation**, sélectionnez l'option **Cluster**, puis cliquez sur **Suivant**.

19 Sur la page **Choisir l'emplacement de destination**, cliquez sur **Modifier**, et accédez à l'emplacement sur le lecteur partagé où McAfee ePO a été installé à l'étape 4, puis cliquez sur **OK** | **Suivant**.

20 A l'étape **Définir les paramètres du serveur virtuel**, les détails de l'adresse IP du serveur virtuel McAfee ePO, le nom du cluster virtuel McAfee ePO et le nom de domaine complet du cluster virtuel McAfee ePO sont déjà renseignés. Entrez la phrase secrète de configuration du cluster que vous avez choisie à l'étape 5 et cliquez sur **Suivant**.

21 Dans la boîte de dialogue **Prêt pour l'installation du programme**, indiquez si vous souhaitez ou non autoriser McAfee à collecter les données télémétriques sur les systèmes et les logiciels, puis cliquez sur **Installer** pour lancer l'installation du logiciel.

Le processus d'installation sur le deuxième nœud s'exécute beaucoup plus rapidement que sur le premier nœud.

22 Une fois l'installation terminée, ne sélectionnez pas **Oui, je souhaite lancer McAfee ePolicy Orchestrator maintenant**. Cliquez sur **Terminer** pour quitter le programme d'installation sur le premier nœud du cluster.

Création des ressources Service générique

Les ressources Service générique permettent au serveur de cluster de contrôler le serveur McAfee ePO, en démarrant, puis en arrêtant les services McAfee ePO sur le cluster approprié.

Créez trois ressources Service générique.

Procédure

1 Dans le gestionnaire du cluster de basculement, cliquez avec le bouton droit sur le rôle d'application **ePO**, puis sélectionnez **Ajouter une ressource** | **Service générique**.

2 Dans l'Assistant Nouvelle ressource, sélectionnez le service Serveur d'applications ePolicy Orchestrator, puis cliquez sur **Suivant**.

3 Sur la page Confirmation, cliquez sur **Suivant** pour créer le service, puis cliquez sur **Terminer** pour créer le service générique.

4 Répétez les étapes 1 à 3 pour le service Serveur ePolicy Orchestrator et pour le service Analyseur d'événements ePolicy Orchestrator.

Les ressources Service générique nouvellement créées s'affichent dans l'onglet **Ressources** du gestionnaire du cluster de basculement, sous la section **Rôles**. Procédez comme suit pour configurer ces ressources.

5 Cliquez avec le bouton droit sur la ressource Serveur d'applications ePolicy Orchestrator, puis sélectionnez **Propriétés**. Dans la boîte de dialogue **Propriétés**, sélectionnez l'onglet **Dépendances**, ajoutez les dépendances suivantes, puis cliquez sur **Appliquer** | **OK**.

a Ressource Nom de serveur

b Ressource Stockage partagé

6 Cliquez avec le bouton droit sur la ressource Serveur ePolicy Orchestrator, puis sélectionnez **Propriétés**. Dans la boîte de dialogue boîte **Propriétés**, effacez le contenu du champ Paramètres de démarrage et entrez un espace unique. Le service ne démarre pas si des paramètres sont spécifiés.

7 Sélectionnez l'onglet **Dépendances**, ajoutez la **ressource Serveur d'applications ePolicy Orchestrator** comme dépendance, puis cliquez sur **Appliquer** | **OK**.

8 Cliquez avec le bouton droit sur la ressource Analyseur d'événements ePolicy Orchestrator, puis sélectionnez **Propriétés**. Dans la boîte de dialogue **Propriétés**, sélectionnez l'onglet **Dépendances**, ajoutez les dépendances suivantes, puis cliquez sur **Appliquer** | **OK**.

   a Ressource Nom de serveur

   b Ressource Stockage partagé

9 Dans le gestionnaire du cluster de basculement, cliquez avec le bouton droit sur le **rôle d'application ePO** et sélectionnez **Démarrer le rôle** pour que le **rôle d'application ePO** passe en mode en ligne.

Test de l'installation en cluster de McAfee ePO

Une fois le rôle McAfee ePO en ligne et exécuté en mode Gestionnaire du cluster de basculement, cette tâche vous permet de vérifier que le logiciel fonctionne dans les situations de basculement.

Procédure

1 Sur un système séparé, ouvrez un navigateur web et connectez-vous à la console McAfee ePO. L'URL de la console est https://<Nom de la ressource de serveur>:<port de la console>, où <Nom de la ressource de serveur> est le nom du serveur utilisé lorsque le point d'accès client a été créé, et <port de la console> est le port choisi pour la console lors de l'installation (8443 par défaut).

2 Dans le Gestionnaire du cluster de basculement, déplacez le rôle d'application McAfee ePO vers le deuxième nœud du cluster en cliquant avec le bouton droit sur le rôle, puis en sélectionnant **Déplacer** | **Sélectionner le nœud**. Sélectionnez l'autre nœud du cluster, puis cliquez sur **OK**.

   Le rôle est déplacé vers l'autre nœud du cluster.

   Le nœud passif devient automatiquement le nœud actif. Le délai nécessaire à l'activation du nœud passif dépend de votre environnement particulier.

3 Actualisez manuellement la session du navigateur. Si le basculement est correctement effectué, vous êtes redirigé vers la page de connexion de McAfee ePO.

7 Configuration de l'environnement McAfee ePO

Configurer les fonctionnalités essentielles de votre serveur McAfee ePO pour être opérationnel rapidement.

Vous pouvez configurer votre environnement *automatiquement* ou *manuellement*. Ces deux méthodes incluent les tâches principales ci-dessous :

1. Installer les packages logiciels de produit sous licence sur le serveur McAfee ePO.
2. Ajouter les systèmes à l'Arborescence des systèmes.
3. Déployer McAfee Agent sur vos systèmes pour qu'ils soient gérés par McAfee ePO.
4. Déployer les logiciels sur vos systèmes managés.
5. Configurer les mises à jour de produit pour vos systèmes managés.
6. Définir les paramètres de proxy, si cette opération est requise par McAfee ePO.
7. Activer la licence de logiciel.
8. Confirmer que vos systèmes sont gérés par McAfee ePO.
9. Exécuter un test de virus pour confirmer que le logiciel fonctionne sur vos systèmes, et que vos systèmes sont protégés contre les menaces.

   Pour plus d'informations sur l'utilisation du test antimalware EICAR avec des produits McAfee, consultez l'article KB59742.

Sommaire

Configuration automatique de votre environnement

Installation automatique des produits sur votre serveur McAfee ePO

Vos produits logiciels sous licence doivent tout d'abord être archivés sur le serveur McAfee ePO pour pouvoir être installés sur les systèmes managés.

Si vous avez sélectionné l'option **Activer l'installation automatique des produits** au cours de l'installation de McAfee ePO, la page Etat de l'installation du produit s'affiche automatiquement lorsque vous vous connectez à McAfee ePO pour la première fois. Le logiciel archive automatiquement les produits sous licence sur le serveur McAfee ePO.

La page Etat de l'installation du produit s'ouvre uniquement si vous avez sélectionné l'option **Autoriser l'installation automatique du produit** lors de l'installation de McAfee ePO. Elle n'est disponible que durant 24 heures après votre première connexion à McAfee ePO.

Procédure

1. Sur le bureau de votre serveur McAfee ePO, cliquez sur l'icône **Lancer ePolicy Orchestrator**.
2. Lorsque l'écran de connexion s'ouvre, saisissez vos informations d'identification et sélectionnez la langue par défaut de la console.

   Le logiciel Etat de l'installation du produit effectue automatiquement le téléchargement et l'installation du logiciel sous licence disponible pour votre organisation. La page affiche les informations suivantes :

   - **Produits** : tous les logiciels sous licence et leur dernière version disponible.
   - **Etat** : progression de l'installation du produit.
3. Attendez que l'état de chaque produit soit défini sur **Complète**.

   En cas d'échec de l'installation d'un produit, cochez la case en regard du nom du produit pour relancer l'installation. Si l'installation échoue à nouveau, utilisez le catalogue de logiciels pour effectuer l'installation.

Configuration manuelle de votre environnement

Sommaire

Éléments à prendre en compte avant la configuration manuelle

La configuration manuelle de votre environnement se compose des tâches suivantes :

- Installation des produits logiciels sous licence sur le serveur McAfee ePO
- Ajout de systèmes à l'arborescence des systèmes
- Préparation de la gestion des systèmes en déployant McAfee Agent sur ces derniers
- Déploiement des logiciels de sécurité sur vos systèmes managés

Vous pouvez effectuer la plupart de ces tâches selon plusieurs méthodes. La méthode choisie pour chaque tâche dépend de la taille et de la composition de votre environnement.

Méthodes manuelles d'ajout de systèmes à manager

Vous pouvez ajouter manuellement des systèmes à McAfee ePO selon plusieurs méthodes. Le choix de la méthode dépend de la taille et de la complexité de votre réseau. Vous pouvez choisir une méthode ou une combinaison de méthodes.

Méthode	Description
URL du programme d'installation SmartInstall	• Créé par défaut. • Les utilisateurs système doivent disposer de droits d'administrateur pour pouvoir installer le logiciel. • Le système n'est managé et protégé qu'une fois que les utilisateurs ont exécuté le programme d'installation SmartInstall.
Scripts de connexion	• Déployez FramePkg.exe (package d'installation de McAfee Agent) sur des systèmes individuels. • Il peut être intégré à l'aide de scripts de connexion existants. • Vous devez savoir comment créer le script et l'exécuter lorsque l'utilisateur se connecte. • Le système n'est managé et protégé qu'une fois que l'utilisateur est connecté.
Ajout manuel des systèmes à partir du domaine	• Nécessite des réseaux et des domaines organisés.
Ajout de systèmes à l'aide d'Active Directory	• Nécessite une configuration d'Active Directory rigoureuse.
Utilisation d'outils de déploiement tiers	• Méthode la plus courante pour les entreprises. • Permet de déployer McAfee Agent sur Windows, Linux et macOS, en fonction de la solution de déploiement utilisée. • Le système n'est managé et protégé qu'une fois que McAfee Agent est déployé. • Tous les packages McAfee peuvent être déployés à l'aide des outils de déploiement tiers. Il n'est pas nécessaire de déployer le logiciel à partir de McAfee ePO.
Ajout à un poste de travail ou à une image serveur	McAfee Agent appartient à l'image lorsqu'un nouveau poste ou un nouveau serveur est créé.

Installation de McAfee Agent et des logiciels sous licence

Vous devez installer McAfee Agent sur un système avant de déployer d'autres logiciels.

McAfee Agent est un composant côté client qui est installé sur les systèmes de votre environnement. Il fournit une communication sécurisée entre McAfee ePO et vos systèmes managés et entre McAfee ePO et les produits managés.

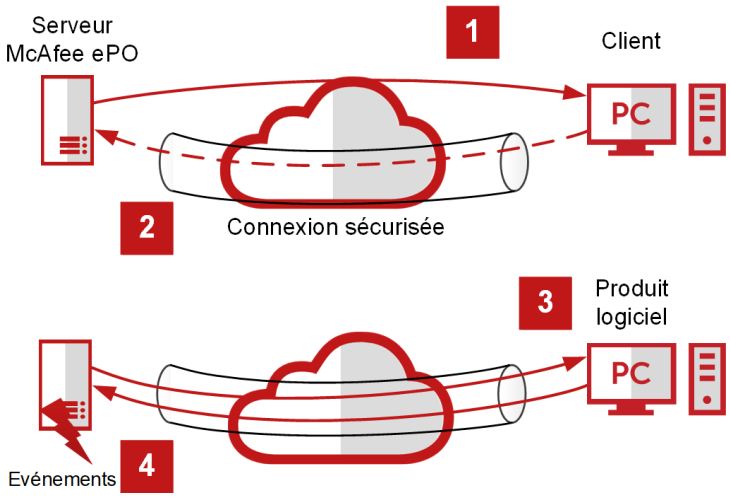
Il constitue également une interface de mise à jour pour les produits McAfee managés et non managés.

Que se passe-t-il lorsque vous installez l'agent ?

1. McAfee Agent est installé sur un client. L'agent établit automatiquement une communication avec McAfee ePO dans les dix minutes suivant l'installation du logiciel.
2. McAfee Agent établit une connexion sécurisée entre le client et McAfee ePO.

3 McAfee Agent télécharge le logiciel sur le client via la connexion sécurisée, selon les tâches de déploiement définies à l'aide de McAfee ePO.

4 McAfee Agent renvoie les propriétés, les événements et les autres informations sur le client à McAfee ePO.



Que fait l'agent dans votre environnement ?

McAfee Agent n'est pas un produit de sécurité en soi ; il communique plutôt avec tous les produits de sécurité McAfee et tiers et transmet les informations depuis et vers le serveur McAfee ePO. McAfee Agent prend en charge Windows, macOS et Linux.

Voici les principales fonctionnalités de McAfee Agent :

- Gestion de toutes les communications depuis et vers le serveur McAfee ePO et transmission de ces données aux produits client
  - Collecte de toutes les stratégies de produit depuis le serveur McAfee ePO et affectation de ces stratégies aux produits appropriés installés sur le client
  - Collecte de toutes les tâches du client depuis le serveur McAfee ePO et transmission de ces tâches aux produits concernés
- Déploiement de contenu comme les signatures, les vérifications d'audits et les moteurs
- Déploiement des mises à niveau de produit, des nouveaux produits, application de patchs et HotFix
- Mise à niveau autonome silencieuse dès qu'une nouvelle version est disponible

Modularité de McAfee Agent

La conception modulaire de McAfee Agent vous permet d'ajouter de nouvelles offres de sécurité à votre environnement selon vos besoins, en utilisant la même structure. McAfee a normalisé la façon dont les stratégies, les événements et les tâches sont communiqués aux produits client. A aucun moment vous n'avez à vous soucier de la communication ni des ports à ouvrir lorsque vous ajoutez un produit à votre client. McAfee Agent contrôle tous ces éléments. Cette architecture modulaire possède de nombreux avantages :

- Un composant permet de communiquer avec le serveur.
- Vous pouvez choisir les produits qui conviennent à votre organisation.
- Le processus d'application d'un patch est le même pour tous les produits.

- Vous pouvez ajouter de nouveaux produits dès leur sortie.
- Vous pouvez utiliser la même instance de McAfee Agent pour les produits partenaires, ce qui réduit la surcharge de gestion.

Dans le répertoire McAfee Agent

Si vous consultez le répertoire d'installation McAfee Agent, vous comprenez pourquoi il est unique.

Par défaut, le fichier d'installation de McAfee Agent se trouve à l'emplacement suivant sur votre serveur McAfee ePO :

```
C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Software\Current
\EPOAGENT3000\Install\0409\
```

Chaque McAfee Agent est automatiquement personnalisé selon votre serveur McAfee ePO et inclut les clés de communication pour votre serveur McAfee ePO spécifique et un fichier Sitelist.xml spécifique au serveur McAfee ePO. Sans ces clés, les agents ne peuvent pas communiquer avec votre serveur McAfee ePO. Le fichier Sitelist.xml file configure vos agents afin de détecter le serveur McAfee ePO et les Gestionnaires d'agents à partir de leur adresse et de leur nom DNS. Ce fichier doit être mis à jour si vous renommez votre serveur McAfee ePO, lui attribuez une nouvelle adresse IP ou ajoutez d'autres Gestionnaires d'agents. Ce processus se fait automatiquement.

Chaque serveur McAfee ePO a son propre fichier d'installation de McAfee Agent unique. Si vous possédez plusieurs serveurs, chaque agent communique exclusivement avec le serveur sur lequel il a été créé.

Meilleure pratique : maintenir le fichier McAfee Agent à jour

Il est important de télécharger la dernière version du fichier McAfee Agent afin que chaque équipe dispose de la dernière version du fichier McAfee Agent pour les nouveaux déploiements. Assurez-vous de connaître l'emplacement du fichier exécutable McAfee Agent dans votre environnement et de le contrôler à tout moment en mettant à jour un partage central chaque fois que vous mettez à jour votre instance de McAfee Agent.

Cette instance personnalisée de McAfee Agent est très certainement obsolète si vous l'avez fournie à vos utilisateurs il y a un an. Elle devient obsolète si vous avez modifié votre serveur McAfee ePO, ajouté ou modifié des Gestionnaires d'agents, ou archivé une version plus récente de McAfee Agent sur votre serveur.

Si vous avez archivé une version plus récente de McAfee Agent, vous devez également mettre à jour l'extension de McAfee Agent dans McAfee ePO. La dernière extension de McAfee Agent est rétrocompatible, et peut donc gérer toutes les versions précédentes de McAfee Agent. La mise à jour de l'extension de McAfee Agent est l'étape suivante avant de commencer à utiliser une nouvelle version de McAfee Agent.

Installation manuelle de packages de produit sur votre serveur McAfee ePO

Vos produits logiciels sous licence doivent tout d'abord être archivés dans le serveur McAfee ePO avant de pouvoir les installer sur les systèmes managés.

Si vous n'avez pas sélectionné l'option **Autoriser l'installation automatique du produit** pendant l'installation de McAfee ePO, vous pouvez archiver manuellement les produits dans le serveur McAfee ePO.

Procédure

1. Sur le bureau de votre serveur McAfee ePO, cliquez sur l'icône **Lancer ePolicy Orchestrator**.
2. Lorsque l'écran de connexion s'ouvre, entrez vos informations d'identification et sélectionnez une langue par défaut pour la console.

   Le tableau de bord par défaut s'affiche lors de votre première connexion.

3 Sélectionnez **Menu** | **Logiciels** | **Catalogue de logiciels**.

4 Dans la liste **Catégorie** de la page **Catalogue de logiciels**, filtrez les produits par catégorie ou utilisez la zone de recherche pour trouver votre logiciel.

5 Lorsque vous avez repéré le logiciel souhaité, cliquez sur **Tout archiver**.

6 Sous **Archiver**, vérifiez et acceptez les détails du produit et l'Accord de licence utilisateur final, sélectionnez la **Branche du package client**, puis cliquez sur **Archiver** pour terminer l'opération.

Déploiement des agents sur les systèmes à gérer

McAfee Agent est un fichier exécutable que vous pouvez exécuter manuellement sur chaque client ou déployer à grande échelle sur plusieurs centaines ou milliers de nœuds.

McAfee Agent peut être déployé vers vos systèmes client à l'aide de l'une des méthodes suivantes :

- URL de déploiement d'agent ou programme d'installation de McAfee SmartInstall
- Script de connexion
- Image qui inclut McAfee Agent
- Exécution manuelle
- Serveur McAfee ePO
- Outils tiers

Pour plus d'informations sur ces méthodes de déploiement, consultez le Guide Produit de McAfee Agent.

Procédure

1 Créez le programme d'installation de McAfee Agent à l'aide de l'une des opérations suivantes :
   - Création d'un programme d'installation à l'aide d'une URL McAfee Agent
   - Création d'un fichier de package ou .zip McAfee Agent

2 Installez le fichier de package ou de programme d'installation à l'aide d'une URL.
   - **Programme d'installation à l'aide d'une URL McAfee Agent** : envoyer l'URL par e-mail à vos utilisateurs système. Lorsque les utilisateurs ouvrent l'URL, ils sont invités à télécharger ou à exécuter le programme d'installation de McAfee Agent.
   - **Fichier de package McAfee Agent** : utilisez l'une des méthodes suivantes pour installer le fichier de package :
     - Installation manuelle sous Windows
     - Scripts de connexion sous Windows
     - Options de ligne de commande

   Une fois les agents installés, un intervalle de communication agent-serveur doit s'écouler avant que les systèmes managés apparaissent comme **managés** dans l'Arborescence des systèmes.

3 Sélectionnez **Menu** | **Système** | **Arborescence des systèmes** pour vérifier que les systèmes managés ont installé McAfee Agent et qu'ils communiquent avec le serveur McAfee ePO.

Déploiement d'McAfee Agent à l'aide d'une URL

Vous pouvez créer une URL de téléchargement de McAfee Agent côté client sur laquelle les utilisateurs n'ont qu'à cliquer pour télécharger et installer McAfee Agent sur le client managé.

Procédure

1. Sélectionnez **Menu** | **Section systèmes** | **Arborescence des systèmes**, puis cliquez sur l'onglet **Déploiement d'agent**.
2. Dans le menu **Actions**, cliquez sur **Créer l'URL de déploiement d'agent**.
3. Entrez le nom de l'URL, la version de l'agent et indiquez si l'URL s'applique à tous les Gestionnaires d'agents, ou à des Gestionnaires d'agents spécifiques.

Après avoir ouvert l'URL, les utilisateurs sont invités à télécharger ou à exécuter le programme d'installation de McAfee Agent. L'exécutable d'installation peut également être enregistré, puis inclus dans un script de connexion.

Déploiement de McAfee Agent à l'aide d'outils tiers

Vous pouvez déployer McAfee Agent à l'aide d'un outil tiers que vous utilisez déjà pour les déploiements de patchs et de nouveaux produits.

L'utilisation d'outils tiers n'est pas obligatoire, mais il se peut que votre organisation ait mis en œuvre des stratégies stipulant le mode de déploiement des produits. Parmi les outils de déploiement les plus utilisés figurent ceux-ci-dessous :

- Microsoft SCCM (anciennement connu sous le nom de SMS)
- IBM Tivoli
- Novell Zenworks
- BMC Client Automation (anciennement connu sous le nom de Marimba)
- Scripts de connexion simples

Le processus utilisé pour déployer McAfee Agent pour la première fois à l'aide de ces outils tiers est simple. Pour plus d'informations, consultez le *Guide Produit de McAfee Agent*.

Le fichier McAfee Agent (nommé FramePkg.exe) inclut plusieurs commutateurs d'installation. Configurez McAfee Agent pour qu'il s'installe, au minimum. (Facultatif) Vous pouvez utiliser le commutateur `/s` pour masquer l'interface utilisateur graphique d'installation côté utilisateur. Voici un exemple de commande :

```
FramePkg.exe /install=agent /s
```

Meilleure pratique : synchronisation du déploiement de McAfee Agent à l'aide d'Active Directory

Vous pouvez utiliser le déploiement du serveur McAfee ePO seul ou avec la synchronisation avec Active Directory (AD).

McAfee ePO peut importer vos systèmes à partir d'AD, puis déployer le logiciel de l'agent à partir du serveur McAfee ePO à l'aide de la fonctionnalité de déploiement distant. Les tâches serveur vous permettent d'exécuter le déploiement distant à un intervalle spécifique, par exemple une fois par jour. Ce processus est soumis aux conditions suivantes :

- Les systèmes de votre arborescence AD doivent être gérés. Placez les systèmes dans les conteneurs appropriés d'AD pour que McAfee ePO crée une copie miroir correcte de votre structure AD.
- Vous devez disposer des informations d'identification appropriés, le partage admin$ doit être activé et aucun pare-feu local ne doit bloquer les ports NetBIOS sur le client de destination.
- Le système cible doit être sous tension. L'existence du système dans AD ne signifie pas qu'il est sous tension et actif dans votre réseau.

Le déploiement d'agent à partir du serveur McAfee ePO fonctionne, tant que votre structure AD est correctement gérée. Si ce n'est pas le cas, vous obtenez un trop grand nombre de systèmes shell (des systèmes qui n'existent pas, et ne peuvent donc pas disposer d'un agent installé), ou espaces réservés, dans votre Arborescence des systèmes. Il s'agit de systèmes importés à partir de votre serveur AD, mais qui n'ont jamais reçu de McAfee Agent. Les systèmes shell s'affichent dans la colonne Etat managé en tant que Non managé.

Vérifiez que votre environnement Active Directory est doté de suffisamment d'agents pour éviter ces systèmes shell. Ces systèmes peuvent causer les problèmes suivants :

- Votre Arborescence des systèmes désorganisée.
- Les systèmes shell faussent vos rapports et vos requêtes en n'étant jamais conformes, car il ne s'agit que de systèmes substituables, et non de systèmes qui communiquent effectivement avec le serveur McAfee ePO.

Vous pouvez filtrer ces systèmes shell dans vos rapports, mais il est préférable de vous assurer que votre environnement McAfee ePO n'inclut que des systèmes réels.

Supprimez régulièrement les systèmes shell à l'aide d'une tâche serveur McAfee ePO.

Meilleure pratique : ajout de McAfee Agent à votre image

L'ajout de McAfee Agent pendant le processus de création d'une image est une stratégie de conformité McAfee ePO satisfaisante. Elle garantit l'installation de McAfee Agent sur l'ensemble de vos systèmes.

Cette stratégie requiert des opérations de planification ainsi que la participation de votre équipe de développement pour assurer la conformité McAfee ePO, en vue de vous assurer que les conditions suivantes sont remplies :

- L'agent McAfee Agent actuel fait partie intégrante de chaque système créé.
- Les produits McAfee requis et stratégies associées sont extraits à partir du serveur McAfee ePO par l'agent McAfee Agent sur vos systèmes.
- Vous disposez d'une couverture de sécurité maximum pour tous les systèmes dans votre environnement.

Deux options sont mises à votre disposition pour intégrer McAfee Agent à votre processus de développement et l'installer sur vos systèmes managés :

- **Option 1** : inclure McAfee Agent dans votre image Windows avant de figer ou de finaliser l'image. Assurez-vous de supprimer le GUID McAfee Agent avant de figer l'image.
- **Option 2** : lancer l'exécutable McAfee Agent avant de créer l'image à l'aide d'un script reproductible.

Reportez-vous au Guide Produit correspondant à la version de McAfee Agent à installer sur une image virtuelle non persistante, ou en mode VDI (infrastructure de postes de travail virtuels).

Vous pouvez installer tous les produits client sur vos systèmes managés en procédant comme suit :

- Laisser McAfee Agent appeler automatiquement le serveur McAfee ePO au bout de 10 minutes et recevoir les stratégies et produits indiqués par McAfee ePO.
- (Recommandé) Intégrer les produits de terminal à votre processus de développement et les inclure dans l'image d'origine.

Consultez les quelques indications ci-dessous pour identifier l'option à choisir :

Avantage	Inconvénient
Si les produits de terminal sont inclus dans votre processus de création d'une image, votre processus de développement peut avoir lieu sur un réseau sur lequel les systèmes pour lesquels vous avez créé une image ne disposent pas d'une connectivité au serveur McAfee ePO.	McAfee Agent peut finir par utiliser une quantité excessive de bande passante lorsque vous le laissez extraire plusieurs produits de terminal. Si vous êtes soumis à des limitations au niveau de la bande passante, intégrez les produits à votre image d'origine.
Si vous disposez d'un délai réduit, intégrez les produits McAfee à votre image. Cela vous évitera d'avoir à patienter 15 à 20 minutes pour que les produits soient installés, délai pendant lequel vos systèmes risquent d'être vulnérables aux menaces.	Une fois que vous avez installé McAfee Agent sur un client, le téléchargement, l'installation et la mise à jour des produits à l'aide d'une tâche client prennent plusieurs minutes. Ce décalage se produit y compris lorsque la première communication agent-serveur a lieu de façon immédiate.

Vérification de la suppression du GUID McAfee Agent avant de figer l'image

Assurez-vous d'avoir supprimé le GUID McAfee Agent avant de figer l'image lorsque vous intégrez McAfee Agent à votre image.

Si le GUID n'est pas supprimé, tous les systèmes créés à partir de l'image utilisent le même GUID. Or, ces GUID en double peuvent provoquer des conflits dans votre environnement. Reportez-vous au Guide Produit correspondant à votre version de l'agent et à la section consacrée à la suppression du GUID.

L'impossibilité de supprimer le GUID McAfee Agent avant de finaliser votre image peut compliquer la gestion des images dans les environnements plus vastes.

Pour obtenir des instructions sur la procédure de réinitialisation du GUID de l'agent lorsqu'aucun ordinateur n'apparaît dans le répertoire McAfee ePO, consultez l'article KB56086.

Ajout manuel de systèmes à l'Arborescence des systèmes

L'ajout manuel de systèmes à l'**Arborescence des systèmes** et le déploiement de McAfee Agent offre des résultats satisfaisants dans les réseaux de petite taille.

Avant de commencer

- Le serveur McAfee ePO doit être en mesure de communiquer avec les systèmes cibles.
- Assurez-vous que les systèmes clients sont accessibles à partir du serveur McAfee ePO.
- Le serveur McAfee ePO doit disposer de droits d'administrateur local sur tous les systèmes cibles.

Procédure

1. Utilisez les commandes `ping` pour tester la capacité de résolution et de connexion aux systèmes managés à partir du serveur McAfee ePO.
2. Pour confirmer que le dossier de partage `Admin$` sur les systèmes cibles Windows est accessible à partir du serveur McAfee ePO, cliquez sur **Démarrer** | **Exécuter**, puis entrez le chemin d'accès au partage `Admin$` sur le système cible, en spécifiant le nom ou l'adresse IP du système. Par exemple, entrez `\\<Nom du système>\Admin$`.

   Une boîte de dialogue Windows Explorer s'affiche si les systèmes sont connectés au réseau, si vos informations d'identification disposent des droits suffisants, et si le dossier de partage Admin$ est présent.
3. Sélectionnez **Menu** | **Systèmes** | **Arborescence des systèmes**, puis cliquez sur **Nouveaux systèmes** sur la page Arborescence des systèmes.
4. Dans la page Nouveaux systèmes, cliquez sur **Envoyer les agents en mode Push et ajouter les systèmes au groupe actif** et sur **Parcourir**.
5. Dans la boîte de dialogue Informations d'identification du domaine NT, entrez les informations suivantes et cliquez sur **OK**.
   - **Domaine** : entrez le nom de domaine en incluant vos systèmes cibles. Utilisez un point (« . ») pour représenter un compte (non domaine) local.
   - **Nom utilisateur** : entrez votre nom utilisateur.
   - **Mot de passe** : entrez votre mot de passe.
6. Sur la page Rechercher des systèmes, sélectionnez le serveur de domaine dans la liste **Domaine**.
7. Sélectionnez les systèmes ou les groupes de systèmes à ajouter à l'**Arborescence des systèmes**, puis cliquez sur **OK**.

   Les systèmes sélectionnés (séparés par une virgule) s'affichent dans le champ Systèmes cibles.
8. Dans **Version de l'agent**, sélectionnez **Windows** ou **Autre que Windows** ainsi que la version dans la liste.
9. Dans la section **Informations d'identification pour l'installation de l'agent** :
   - Entrez le nom du domaine.
   - Entrez votre nom d'utilisateur du domaine.
   - Entrez et confirmez le mot de passe du domaine.
   - Cliquez sur **Mémoriser mes informations d'identification pour les déploiements ultérieurs.**
10. Utilisez les valeurs par défaut des paramètres finaux et cliquez sur **OK**.

Les systèmes sélectionnés sont ajoutés à l'Arborescence des systèmes et apparaissent avec l'état **Non managé** dans la colonne **Etat managé**. Après communications avec les serveurs McAfee ePO dans le cadre de l'installation du logiciel produit et de la mise à jour des tâches et des stratégies, la valeur **Etat managé** est remplacée par **Managé**. Ce processus peut prendre plusieurs heures.

Finalisation de la configuration de votre serveur

Sommaire

Définition des paramètres de proxy

Si vous utilisez un serveur proxy dans votre environnement réseau, vous devez définir les paramètres de proxy sur la page Paramètres serveur.

Procédure

1 Sélectionnez **Menu** | **Configuration** | **Paramètres serveur**, et **Paramètres de proxy** dans la liste **Catégories de paramètres**, puis cliquez sur **Modifier**.

2 Sélectionnez **Configurer manuellement les paramètres de proxy**, indiquez les informations de configuration spécifiques que votre serveur proxy utilise pour chaque ensemble d'options, puis cliquez sur **Enregistrer**.

Activation de la licence de logiciel

Votre clé de licence vous donne droit à une installation complète du logiciel et elle indique au catalogue de logiciels les logiciels McAfee sous licence détenus par votre entreprise.

Sans clé de licence, votre logiciel est exécuté en mode d'évaluation. Il cesse de fonctionner une fois la période d'évaluation expirée. Vous pouvez ajouter une clé de licence à tout moment pendant ou après la période d'évaluation.

Procédure

1 Sélectionnez **Menu** | **Configuration** | **Paramètres serveur**, puis **Clé de licence** dans la liste **Catégories de paramètres**, et cliquez sur **Modifier**.

2 Entrez la **Clé de licence** et cliquez sur **Enregistrer**.

Confirmation de la gestion de vos systèmes

Après avoir déployé McAfee Agent et les produits logiciels, assurez-vous que les systèmes sont inclus dans l'Arborescence des systèmes et qu'ils apparaissent comme managés.

Avant de commencer

Vous devez avoir déployé McAfee Agent et avoir téléchargé le logiciel produit sur vos systèmes.

Procédure

1 Sélectionnez **Menu** | **Systèmes** | **Arborescence des systèmes**, puis cliquez sur l'onglet **Systèmes** pour afficher la liste des systèmes managés.

Si aucun système ne s'affiche, cliquez sur **Ce groupe et tous les sous-groupes** dans la liste **Prédéfini**.

2 Dans la colonne Etat managé, confirmez que la valeur **Managé** apparaît pour chaque ligne de systèmes.

La présence de l'état **Non managé** dans la colonne Etat managé indique que le système a été ajouté dans l'Arborescence des systèmes, mais que McAfee Agent et le logiciel produit ne sont pas installés sur le système.

3 Pour afficher les informations concernant un système, sélectionnez le nom du système pour ouvrir la page Informations système.

Vérification de l'arrêt d'un échantillon de menace par votre logiciel de protection

Exécuter un échantillon de menace sur un système managé afin de vérifier que votre logiciel de protection le détecte et l'arrête.

> **Avant de commencer**
>
> Pour exécuter le fichier de test antimalware, Endpoint Security doit être installé sur le système managé.

Lorsque votre protection antimalware fonctionne correctement, le fichier de test est supprimé ou son exécution est bloquée.

Pour exécuter un fichier de test antimalware, vous pouvez vous connecter au système de test en local ou à distance.

Procédure

1. Connectez-vous au système de test avec des droits d'administrateur.
2. Dans un navigateur web, connectez-vous au site EICAR :

   http://www.eicar.org/86-0-Intended-use.html
3. Suivez les instructions pour télécharger et exécuter le fichier de test antimalware eicar.com de 68 octets.
4. Sous Windows, cliquez sur **Démarrer** | **Tous les programmes** | **McAfee** | **McAfee Endpoint Security**, puis cliquez sur **Etat**.

   Une synthèse sur les menaces répertorie le nombre de menaces reçues et le type de chacune d'elles.
5. Cliquez sur **Journal des événements** pour afficher les événements de menace dans le tableau Evénement et supprimez l'échantillon de menace.

   Les détails des événements de menace s'affichent dans le volet du bas du tableau.

Confirmation de la réponse aux menaces dans McAfee ePO

Il est primordial de savoir où rechercher les événements de menace dans McAfee ePO pour pouvoir garantir la protection des systèmes managés.

> **Avant de commencer**
>
> Vous devez exécuter le fichier de test antimalware EICAR pour vérifier si un événement de menace a été déclenché.

Procédure

1. Connectez-vous àMcAfee ePO et cliquez sur **Menu** | **Génération de rapports** | **Tableaux de bord**.
2. Dans la barre de titre de la liste Tableaux de bord, sélectionnez un tableau de bord.
   - **Synthèse ePO** : affiche les menaces récentes dans le graphique linéaire Historique des détections de programmes malveillants.
   - **Tableau de bord de gestion** : affiche un graphique linéaire Historique des détections de programmes malveillants.

- **Evénements de menace** : affiche les menaces récentes dans les tableaux de bord suivants :
  - Tableau Descriptions des événements de menace les plus nombreux
  - Tableau et graphique à secteurs Evénements de menace par groupe de l'Arborescence des systèmes
  - Tableau et graphique à secteurs Descriptions des événements de menace au cours des dernières 24 heures
  - Graphique linéaire Evénements de menace au cours des 2 dernières semaines

3 Sélectionnez **Menu** | **Génération de rapports** | **Journal des événements de menace** pour afficher une description de la menace récente.

Exemples d'informations incluses dans le tableau :

- Date de génération de l'événement
- ID d'événement
- Description de l'événement
- Catégorie d'événements
- Adresse IPv4 cible de la menace
- Action entreprise
- Type de menace

4 Cliquez sur l'événement dans le tableau pour afficher toutes les informations sur la menace.

5 Pour afficher les informations détaillées sur le système concerné, cliquez sur **Accéder au système associé**.

Et après...

Une fois que vous avez terminé la configuration initiale et vérifié que tous vos systèmes managés sont protégés, vous pouvez étudier d'autres étapes de configuration, selon les besoins de votre réseau en matière de sécurité.

Quelques étapes supplémentaires simples vous aident à manager McAfee ePO

Assurez-vous d'avoir au moins un compte administrateur global McAfee ePO supplémentaire dont le mot de passe est stocké en toute sécurité, afin d'empêcher le verrouillage de McAfee ePO en cas de perte du mot de passe d'administrateur.

- Ajoutez des utilisateurs et des autorisations McAfee ePO supplémentaires.
- Organisez votre Arborescence des systèmes de façon logique afin de refléter des frontières géographiques, politiques ou fonctionnelles.
- Ajoutez des marqueurs pour identifier et trier les systèmes ou trier les requêtes et les rapports.
- Configurez une réponse automatique lorsque certaines règles sont respectées.

Pour les réseaux managés plus vastes ou plus complexes

- Création de tâches serveur ou client personnalisées.
- Création de configurations manuelles de gestion des stratégies, de logiciels produit et de mise à jour.
- Ajout de Gestionnaires d'agents et de référentiels distants.
- Création de certificats SSL personnalisés.
- Contrôle de l'utilisation de la bande passante et de son impact sur les performances de McAfee ePO.

- Exécution de tâches de maintenance en vue de l'optimisation et de la protection des données du serveur McAfee ePO.
- Exécution de requêtes et de rapports automatiques.

8 Mise à niveau de McAfee ePO vers une nouvelle version

La mise à niveau de votre environnement McAfee ePO existant nécessite une planification et une préparation soigneuses pour garantir la réussite et la fluidité du processus.

Collecte des informations requises

Avant de commencer le processus de mise à niveau, assurez-vous que vous disposez de ces informations.

- Grant Number
- Nom du serveur de base de données et de la base de données
- Informations d'identification du serveur de base de données (Windows ou SQL Server)
  - Domaine (Windows uniquement)
  - Nom utilisateur
  - Mot de passe
- Informations d'identification de compte administrateur principal
  - Nom utilisateur
  - Mot de passe
- Phrase secrète de la capture instantanée pour la reprise sur sinistre

Assurez-vous de disposer d'une capture instantanée du serveur McAfee ePO et d'une sauvegarde de la base de données McAfee ePO.

Planification de votre mise à niveau

Le temps nécessaire pour la mise à niveau dépend de votre environnement et de la taille de votre base de données.

Au cours de la mise à niveau, vos systèmes managés sont toujours protégés, mais les mises à jour des logiciels de sécurité ne sont pas effectuées.

Veillez à notifier vos administrateurs McAfee ePO du temps d'indisponibilité à venir.

Sommaire

Préparation de votre environnement

Avant d'installer ou de mettre à niveau McAfee ePO, exécutez Pre-Installation Auditor afin de réduire les problèmes liés à la mise à niveau ou de les empêcher. L'exécution de Pre-Installation Auditor automatise de nombreuses tâches de vérification incluses dans le processus de mise à niveau.

Sauvegarde des bases de données et répertoires McAfee ePO

Avant de sauvegarder des bases de données et des répertoires McAfee ePO, exécutez une tâche serveur de capture instantanée pour reprise sur sinistre.

Avant de mettre à niveau votre logiciel, sauvegardez l'ensemble des bases de données et des répertoires McAfee ePO afin de pouvoir récupérer sans heurt les données si un problème avait lieu pendant la mise à niveau.

Pour plus d'informations sur les sauvegardes, consultez l'article KB66616.

Vérification de la présence d'espace disque suffisant sur le serveur Windows Server

Vérifiez que le lecteur temporaire de votre système et que le lecteur d'installation de McAfee ePO disposent de suffisamment d'espace disque pour la mise à niveau.

- **Disque temporaire du système** : nécessite au moins 2 Go d'espace disque disponible.
- **Lecteur d'installation** : requiert trois fois la taille du dossier McAfee\ePolicy Orchestrator ou 20 Go, la valeur la plus élevée étant celle qui prévaut.

Par exemple, si le serveur McAfee ePO est installé sur le même disque que le dossier temporaire du système et que la taille du répertoire d'installation de McAfee ePO est de 15 Go, l'espace requis sur le disque dur est de 47 Go (15 Go X 3 + 2 Go). Si la taille du répertoire d'installation de McAfee ePO est de 5 Go, 22 Go (20 Go + 2 Go) d'espace libre minimum sont requis sur le lecteur.

Si vous ne disposez pas de l'espace suffisant, purgez les fichiers journaux et les fichiers temporaires du répertoire d'installation de McAfee ePO avant de lancer la mise à niveau :

Procédure

1. Arrêtez les services McAfee ePO.
   a. Appuyez sur les touches **Windows+R**, entrez `services.msc`, puis cliquez sur **OK**.
   b. Cliquez avec le bouton droit sur les services suivants, puis sélectionnez **Arrêter** :
      - Serveur d'applications McAfee ePolicy Orchestrator
      - Serveur McAfee ePolicy Orchestrator
      - Analyseur d'événements McAfee ePolicy Orchestrator
2. Supprimez les fichiers présents dans les dossiers suivants :
   - <répertoire d'installation de McAfee ePO>\Server\Logs
   - <répertoire d'installation de McAfee ePO>\DB\Logs
   - <répertoire d'installation de McAfee ePO>\Apache2\Logs
   - <répertoire d'installation de McAfee ePO>\Server\Temp

3 Démarrez les services McAfee ePO.

   a Appuyez sur les touches **Windows+R**, entrez `services.msc`, puis cliquez sur **OK**.

   b Cliquez avec le bouton droit sur les services suivants, puis sélectionnez **Démarrer** :

   - **Serveur d'applications McAfee ePolicy Orchestrator**
   - **Serveur McAfee ePolicy Orchestrator**
   - **Analyseur d'événements McAfee ePolicy Orchestrator**

Vérification de l'activation de la convention d'affectation de noms Windows 8.3

Activez la convention d'affectation de noms 8.3 sur le lecteur sur lequel McAfee ePO est installé.

Pour obtenir des instructions sur l'activation de la convention d'affectation de noms 8.3, reportez-vous à la Solution 1 dans l'article KB51431.

Fonction de vérification de la compatibilité des produits

La fonction de vérification de la compatibilité des produits confirme si vos produits managés sont compatibles ou non avec la dernière version de McAfee ePO. Elle s'exécute automatiquement lors de la mise à niveau.

Lorsqu'elle détecte des incohérences, cette fonction crée une liste des extensions bloquées ou désactivées.

Les extensions bloquées empêchent la mise à niveau du logiciel McAfee ePO. Les extensions désactivées ne bloquent pas la mise à niveau, mais l'extension n'est initialisée qu'après installation d'une extension de remplacement connue.

Une liste de compatibilité des produits initiale est incluse dans le package logiciel McAfee ePO téléchargé depuis le site web McAfee.

Liste de contrôle pour la mise à niveau

Cette liste de contrôle indique toutes les étapes nécessaires pour mettre à niveau un serveur McAfee ePO autonome.

D'autres étapes de mise à niveau sont requises si vous avez installé McAfee ePO dans un environnement de cluster.

Liste de contrôle pour la mise à niveau
1. Planification en vue d'une mise à niveau réussie
☐ Lecture des notes de publication.
☐ Examen des problèmes connus, séquences de mise à niveau et produits pris en charge.
☐ Collecte des informations requises.
☐ Exécution de Pre-Installation Auditor.  Les étapes de vérification signalées au moyen d'un astérisque (*) sont réalisées par le Pre-Installation Auditor.
☐ Planification de la mise à niveau et envoi d'une notification aux utilisateurs.
2. Préparation de l'environnement
☐ Sauvegarde des bases de données et répertoires McAfee ePO.

Liste de contrôle pour la mise à niveau
☐ Mise à jour des certificats des serveurs enregistrés.
☐ Vérification de la présence de l'espace disque suffisant sur le serveur Windows.*
☐ Vérification de l'activation de la convention d'affectation de noms Windows 8.3.*
☐ Désactivation des tâches d'installation de McAfee Agent définies comme devant être exécutées immédiatement.
☐ Désactivation des tâches serveur et Windows planifiées.
☐ Désactivation des logiciels tiers.
3. Préparation de la base de données SQL
☐ Mise à jour du serveur Windows Server.
☐ Vérification de l'utilisation des autorisations appropriées.*
☐ Vérification de l'instance SQL utilisée par McAfee ePO.*
☐ Vérification de la définition du paramètre Fermeture automatique sur False.*
☐ Vérification de la définition du paramètre Annulation arithmétique activée sur True.*
☐ Vérification de la définition du niveau de compatibilité sur 100 ou plus.*
☐ Vérification de la définition du classement de base de données approprié.*
☐ Vérification de l'exécution du service SQL Browser.*
☐ Vérification de l'activation de l'option IPv6.
4. Exécution de la mise à niveau
☐ Téléchargement et extraction du logiciel.
☐ Arrêt des mises à jour automatiques.
☐ Arrêt des gestionnaires d'agents distants.
☐ Arrêt des services McAfee ePO.
☐ Démarrage de l'Assistant InstallShield et exécution de ses opérations.
☐ Mise à niveau des gestionnaires d'agents distants.
5. Redémarrage des processus et vérification de la mise à niveau
☐ Redémarrage des mises à jour automatiques.
☐ Migrez les certificats SHA-1 vers l'algorithme SHA-2 ou version supérieure.
☐ Vérification de la mise à niveau.

Pre-Installation Auditor

Exécutez McAfee ePO Pre-Installation Auditor pour limiter ou éviter les problèmes liés à la mise à niveau de McAfee ePO.

Effectuez un audit avant l'installation et la mise à niveau, afin de vous assurer que votre environnement respecte la configuration requise pour l'installation. Pour plus d'informations sur le téléchargement et l'utilisation de Pre-Installation Auditor, consultez les notes de publication de l'outil.

McAfee ePO Pre-Installation Auditor effectue les vérifications suivantes :

- Confirme que votre serveur présente la configuration matérielle requise pour McAfee ePO et SQL Server.
- Confirme que vous disposez des droits d'accès et des autorisations SQL Server nécessaires.
- Vérifie que les services devant être arrêtés peuvent l'être, et qu'aucun logiciel tiers ne risque d'entraîner le démarrage inattendu des services.
- Identifie l'état de SQL Server Browser.
- Détermine si le chiffrement de la base de données est activé.
- Détermine si la fonctionnalité de fermeture automatique de SQL Server est activée.
- Identifie le modèle de récupération de la base de données.
- Vérifie si des tâches planifiées et des mises à jour automatiques Microsoft Windows sont disponibles.
- Détermine si la fonctionnalité d'affectation de noms Microsoft Windows 8.3 est activée.
- Vérifie si le registre suivant contient des opérations de renommage de fichier en attente :
  HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\PendingFileRenameOperations
- Vérifie les autorisations d'accès au système d'exploitation.
- Identifie les versions de McAfee ePO prises en charge par le système d'exploitation et la version du serveur.
- Vérifie si l'option de base de données pour une annulation arithmétique est activée.
- Vérifie le niveau de compatibilité de la base de données SQL.
- Vérifie que la fragmentation des index de base de données est inférieure à la limite suggérée.
- Vérifie que la version de McAfee ePO à mettre à niveau prend en charge la migration vers les certificats SHA-2.
- Vérifie l'état de la réplication de la base de données.
- Vérifie la valeur seuil du curseur de la requête de base de données.
- Vérifie qu'aucun descripteur de fichier n'est ouvert dans le répertoire McAfee ePO.
- Fournit une liste des tâches serveur McAfee ePO en cours d'exécution et vous demande de les désactiver.
- Détermine le temps nécessaire à la mise à niveau.
- Valide que la clé de certificat de la banque de clés est supérieure ou égale à 2 048 bits.
- Vérifie si la communication entre McAfee ePO et la base de données n'a pas été configurée pour valider le certificat SSL.
- Confirme que la haute disponibilité/reprise sur sinistre SQL Server est désactivée.
- Confirme que la mise en miroir de la base de données SQL Server est désactivée.

- Indique si les indicateurs TRACE SQL Server sont définis pour les paramètres recommandés nécessaires pour la mise à niveau.
- Indique si le serveur McAfee ePO utilise les protocoles TLS 1.1 ou TLS 1.2 pour la communication avec le serveur SQL Server.

Préparez votre base de données SQL

Sommaire

Vérification de votre environnement SQL Server

Effectuez les tâches suivantes sur votre serveur SQL Server pour éviter tout problème de mise à niveau et réduire le temps de mise à niveau.

Avant d'installer ou de mettre à niveau McAfee ePO, exécutez Pre-Installation Auditor afin de réduire les problèmes liés à l'installation ou à la mise à niveau ou de les empêcher. L'exécution de McAfee ePO Pre-Installation Auditor automatise de nombreuses tâches de vérification incluses dans le processus de mise à niveau.

Procédure

1. Vérifiez l'instance SQL que McAfee ePO utilise selon l'une des méthodes suivantes :
   - Vérifiez le nom du service SQL Server : (SQL Server (SQLEXPRESS)) ou (SQL Server (EPOSERVER)).
   - Dans SQL Server Management Studio, exécutez cette requête :

     ```
     Sélectionnez @@servername
     go
     ```
2. Vérifiez vos autorisations SQL Server (voir KB75766).
   - Démarrez le serveur SQL Server Management Studio à partir du menu **Démarrer** et vérifiez que la base de données par défaut est maître.
   - Assurez-vous que votre compte est db_owner dans les propriétés de sécurité de base de données.
   - Si vous utilisez un compte Windows pour l'authentification à la base de données McAfee ePO, assurez-vous que le compte dispose de droits d'administrateur local sur le serveur McAfee ePO.
3. Vérifiez les paramètres SQL Server suivants pour éviter d'éventuels problèmes de mise à niveau.
   - **automatique fermer** = False
   - **abandonner arithmétique** = True
   - **Compatibility Level** = 110 ou supérieur
   - Database collation = SQL_Latin1_General_CP1_CI_AS (voir KB73717)
4. Vérifiez que le service Explorateur SQL Server est en cours d'exécution.
5. Dans un environnement IPv6, assurez-vous que seul IPv6 est activé sur le serveur SQL Server qui héberge la base de données McAfee ePO.
6. Mettez à jour le serveur Windows sur lequel votre serveur SQL Server est installé avec les derniers Service Packs et correctifs Microsoft.

Mise à jour de vos certificats de serveur de base de données

Assurez-vous que les certificats des serveurs enregistrés avec lesquels McAfee ePO communique sont pris en charge par McAfee ePO.

TLS 1.0 est désactivé par défaut pour la communication avec les serveurs externes, tels que SQL Server. Pour plus d'informations sur la prise en charge de TLS, reportez-vous à l'article KB90222.

- Utilisez des certificats avec une clé publique RSA de 2 048 bits ou plus pour les serveurs enregistrés auxquels McAfee ePO se connecte.

  McAfee ePO n'est peut-être pas en mesure de se connecter aux serveurs enregistrés qui utilisent des certificats moins sécurisés, telles que les certificats de longueur de clé publique RSA de 1024 bits seulement.

  Pour plus d'informations, notamment sur les algorithmes de clé publique et les longueurs de clé pris en charge, consultez l'article KB87731.

Mettez à niveau votre logiciel McAfee ePO

Sommaire

Téléchargement et installation du logiciel

Téléchargez le logiciel McAfee ePO sur votre serveur Windows.

Procédure

1. Connectez-vous à la page Mes produits au moyen de votre Grant Number.
2. Cliquez sur le lien correspondant à votre suite de produits. Dans l'onglet Versions actuelles, cliquez sur **McAfee ePolicy Orchestrator**.
3. Dans l'onglet Téléchargements de logiciels, cliquez sur le lien de téléchargement.
4. Extrayez le fichier .zip téléchargé vers un emplacement temporaire.

   L'installation échoue si vous essayez de lancer l'exécutable Setup.exe avant d'extraire le contenu du fichier .zip.

Arrêt des services McAfee ePO

Procédez comme suit pour arrêter le service McAfee ePO Application Server.

Si vous ne suivez pas ces étapes, le service Apache Tomcat peut continuer à s'exécuter dans certains environnements, ce qui peut causer des problèmes lors de la mise à niveau.

Procédure

1. Appuyez sur **Windows+R**, entrez `services.msc`, puis cliquez sur **OK**.
2. Arrêtez les services :
   - **Service Serveur ePolicy Orchestrator**
   - **Analyseur d'événements ePolicy Orchestrator**
3. Redémarrez le service Serveur d'applications McAfee ePO.

Arrêt des services des Gestionnaires d'agents avant la mise à niveau

Si vous utilisez des Gestionnaires d'agents dans votre environnement, vous devrez interrompre deux services McAfee sur chaque serveur de Gestionnaire d'agents pour mener à bien cette mise à niveau.

Après avoir interrompu les services serveur et analyseur d'événements des gestionnaires d'agents distants, vous pouvez mettre votre serveur McAfee ePO à niveau. Une fois la mise à niveau terminée, mettez à niveau le logiciel des Gestionnaires d'agents.

Démarrage et exécution de l'Assistant InstallShield

Utilisez `Setup.exe` pour mettre à niveau votre serveur McAfee ePO.

L'emplacement par défaut du logiciel McAfee ePO est : `C:\Program Files (x86) \McAfee\ePolicy Orchestrator`

Surveillez le processus de mise à niveau. Vous devrez peut-être redémarrer le système.

Procédure

1. Connectez-vous au système à l'aide d'un compte bénéficiant d'autorisations d'administrateur local, et recherchez le fichier `Setup.exe`.

   Le fichier exécutable se trouve dans le dossier dans lequel il a été extrait.

   Si vous lancez `Setup.exe` avant d'extraire le contenu du fichier .zip, l'installation échoue.

2. Pour démarrer l'Assistant InstallShield de McAfee ePO, cliquez avec le bouton droit sur le fichier **Setup.exe**, et cliquez avec le bouton droit sur **Exécuter en tant qu'administrateur**.
3. Dans la boîte de dialogue de Bienvenue de l'Assistant d'installation, cliquez sur **Suivant**.

   Un message d'avertissement peut s'afficher pour indiquer les produits de l'ancienne version de McAfee ePO qui ne sont plus pris en charge par cette version du logiciel. Ces produits ne sont pas migrés vers le nouveau référentiel McAfee ePO.
4. L'étape Installer des logiciels supplémentaires affiche la liste des autres composants requis. Cliquez sur **Suivant** pour les installer.
5. A l'étape Informations de base de données, vérifiez que le **Serveur de base de données** et le **Nom de la base de données** automatiquement sélectionnés sont corrects. Si ce n'est pas le cas, sélectionnez les informations correctes dans les listes.

6 Indiquez le type d'**Informations d'identification pour le serveur de base de données** à utiliser, puis cliquez sur **Suivant**.

- **Windows authentication** — From the **Domain** menu, select the domain of the user account you're going to use to access the SQL Server. Entrez le **Nom d'utilisateur** et le **Mot de passe**. Si vous utilisez un serveur SQL Server déjà installé, vérifiez que le compte utilisateur dispose de droits d'accès.
- **Authentification SQL** : entrez le **Nom d'utilisateur** et le **Mot de passe** associés à votre serveur SQL Server. Les informations d'identification que vous fournissez doivent correspondre à un utilisateur existant sur le serveur SQL Server muni de droits d'accès appropriés.

  Le menu **Domaine** est grisé si vous utilisez l'authentification SQL.

McAfee ePO Pre-Installation Auditor s'exécute et analyse votre environnement McAfee ePO pour vérifier qu'il respecte toutes les conditions requises.

7 A l'étape Informations sur l'administrateur :

a Dans le champ **Nom d'utilisateur**, remplacez la valeur admin par défaut et entrez le nom utilisateur de votre compte administrateur principal.

b Dans le champ **Mot de passe**, entrez le mot de passe de votre compte administrateur principal.

c Dans le champ **Mot de passe de récupération du serveur**, entrez un mot de passe pour chiffrer les enregistrements de capture instantanée pour la reprise sur sinistre.

La phrase secrète comprend 14 à 200 caractères, ne doit pas contenir de barres obliques inverses au début ou à la fin (\), d'espaces, de guillemets doubles (") ou de caractères non compris entre ASCII 32 et ASCII 65535.

Notez ce mot de passe. Si un jour vous souhaitez restaurer votre base de données McAfee ePO à partir d'une capture instantanée, vous devrez indiquer ce mot de passe pour déchiffrer les enregistrements de capture instantanée pour la reprise sur sinistre.

8 A l'étape **Entrer la clé de licence**, cliquez sur **Suivant**.

Votre clé de licence existante est automatiquement entrée dans le champ et l'utilitaire de compatibilité pour la mise à niveau s'exécute.

9 Acceptez l'**Accord de licence utilisateur final McAfee** et cliquez sur **OK**.

10 Dans la boîte de dialogue Prêt pour l'installation du programme, indiquez si vous souhaitez Envoyer des informations anonymes sur l'utilisation à McAfee, puis cliquez sur **Installer**.

Désactivez la case à cocher **Envoyer des informations anonymes sur l'utilisation à McAfee** si vous ne souhaitez pas que McAfee collecte des données anonymes sur les diagnostics et l'utilisation.

11 Dans la boîte de dialogue Installation de McAfee ePolicy Orchestrator, la zone **Etat** affiche la progression de la mise à niveau. Une fois la mise à niveau effectuée, cliquez sur **Suivant**.

Si votre base de données McAfee ePO est volumineuse, le processus de mise à niveau peut prendre du temps et le message suivant peut s'afficher : Votre base de données McAfee ePO inclut un nombre excessif d'événements. La mise à niveau risque de prendre beaucoup de temps.

Pour plus d'informations sur la suppression d'anciens événements, voir KB68961 .

12 Dans la boîte de dialogue Assistant InstallShield terminé, cliquez sur **Terminer** pour achever l'installation.

Si vous le souhaitez, cliquez sur **Oui, je souhaiter lancer McAfee ePolicy Orchestrator maintenant.**.

Le logiciel McAfee ePO est à présent mis à jour. Double-cliquez sur l'icône McAfee de votre bureau pour commencer à utiliser votre serveur McAfee ePO, ou accédez au serveur à partir d'une console web à distance (`https://<nomduserveur>:<port>`).

Mise à niveau des Gestionnaires d'agents

Lors d'une mise à niveau du logiciel serveur McAfee ePO, mettez à niveau les Gestionnaires d'agents installés dans votre environnement. Ces gestionnaires doivent être mis à niveau séparément.

Les Gestionnaires d'agents installés avec les versions antérieures du logiciel ne sont pas compatibles avec cette nouvelle version et ne sont pas automatiquement mis à niveau.

La procédure de mise à niveau est une version simplifiée de la procédure utilisée pour la première installation d'un Gestionnaire d'agents.

Procédure

1. Copiez le dossier Agent Handler, inclus au package d'installation du logiciel McAfee ePO, sur le système cible.
2. Cliquez avec le bouton droit sur **Setup.exe** et sélectionnez **Exécuter en tant qu'administrateur** pour lancer l'assistant InstallShield du Gestionnaire d'agents de McAfee ePO.
3. Cliquez sur **Suivant** pour débuter la mise à niveau.
4. Acceptez les conditions de l'accord de licence, puis cliquez sur **OK**.

   L'étape Dossier de destination s'ouvre.
5. Acceptez la destination par défaut ou cliquez sur **Modifier** pour en sélectionner une autre, puis cliquez sur **Suivant**.
6. Configurez les informations du serveur.
   a. Entrez le nom du système du serveur McAfee ePO avec lequel le gestionnaire d'agents doit communiquer.
   b. Indiquez le port à utiliser pour la communication entre le gestionnaire d'agents et le serveur. Le port par défaut est 8444, qui est également le port de communication authentifiée client-serveur.
   c. Entrez le nom utilisateur et le mot de passe d'un utilisateur disposant des droits d'administrateur global McAfee ePO, puis cliquez sur **Suivant**.
   d. Entrez le mot de passe permettant d'accéder à la base de données SQL de McAfee ePO, puis cliquez sur **Suivant**. La page **Informations de base de données** est remplie avec ces paramètres serveur McAfee ePO.
      - **Serveur de base de données** avec le nom de l'instance Par exemple, SERVEUR-BD\NOMSERVEUR.
      - Type d'authentification
      - Nom du **Domaine** qui héberge le serveur de base de données
      - **Nom d'utilisateur** et **Mot de passe**
      - **Nom de la base de données** s'il n'est pas automatiquement renseigné
7. Cliquez sur **Installer** pour démarrer l'installation.
8. L'Assistant InstallShield effectue alors l'installation sans requérir votre intervention. Au terme de l'exécution de l'assistant, cliquez sur **Terminer**.
9. Lorsque la mise à niveau est terminée, vous devez activer votre Gestionnaire d'agents distant à partir de l'interface McAfee ePO.

Redémarrage des mises à jour et vérification de la mise à niveau

Redémarrez les mises à jour automatiques de Windows. Assurez-vous que vos stratégies, tâches, déploiements de produit et référentiels sont correctement mis à jour et qu'ils reflètent vos sélections et personnalisations.

Procédure

1. Activez les mises à jour Windows afin de garantir la réception des mises à jour et correctifs les plus récents par vos serveurs.
2. Assurez-vous que vos stratégies, tâches, déploiements de produit et référentiels sont exacts et qu'ils reflètent vos sélections et personnalisations.
3. Pour vérifier que McAfee ePO fonctionne correctement, exécutez une tâche serveur ou une requête.
4. Pour vérifier la connectivité, effectuez un appel de réactivation de McAfee Agent sur un ou plusieurs systèmes managés.
5. Assurez-vous que les serveurs enregistrés communiquent avec McAfee ePO.

Migrer les certificats SHA-1 vers l'algorithme SHA-2 ou version supérieure

Pour corriger les vulnérabilités de votre environnement McAfee ePO, migrez vos certificats existants vers des algorithmes plus sécurisés ou régénérez-les.

L'algorithme SHA-1 a atteint sa fin de vie. Beaucoup d'organisations ont cessé d'utiliser les certificats TLS/SSL signés par l'algorithme SHA-1. Si vous continuez à utiliser les certificats SHA-1, les navigateurs tels que Google Chrome ou Microsoft Internet Explorer signaleront la console McAfee ePO comme étant un site HTTPS non sécurisé.

Toutefois, si vous avez mis à niveau McAfee ePO à partir d'une version antérieure, vous pouvez migrer les certificats McAfee ePO vers la dernière version de l'algorithme de hachage. Lors d'une nouvelle installation de McAfee ePO, les nouveaux certificats avec algorithme de hachage sont installés.

La page **Gestionnaire de certificats** permet d'effectuer les opérations suivantes :

- migration des certificats signés par un algorithme plus ancien vers le nouvel algorithme, par exemple de l'algorithme SHA-1 vers l'algorithme SHA-256 ;
- régénération des certificats lorsque les certificats existants sont compromis en raison de vulnérabilités au niveau de l'environnement ;
- migration ou régénération des certificats pour les produits managés dérivés de l'autorité de certification racine McAfee ePO.

Cette tâche remplace les certificats utilisés pour toutes les opérations McAfee ePO suivantes :

- Communication agent-serveur
- Authentification auprès des navigateurs
- Authentification utilisateur par certificat

Lisez attentivement ces instructions avant de commencer. Si vous activez les nouveaux certificats avant qu'ils ne soient remplis sur les systèmes de votre réseau, ces systèmes ne pourront pas se connecter à votre serveur McAfee ePO tant que vous n'aurez pas réinstallé les agents.

Procédure

1 Connectez-vous en tant qu'administrateur, puis cliquez sur **Menu** | **Configuration** | **Gestionnaire de certificats**.

Le Gestionnaire de certificats fournit des informations sur le certificat racine installé, les certificats des Gestionnaires d'agents, les certificats serveur et les autres certificats dérivés de l'autorité de certification racine de McAfee ePO.

2 Cliquez sur **Régénérer le certificat**, puis cliquez sur **OK** pour confirmer la génération du certificat.

L'autorité de certification racine de McAfee ePO et les autres certificats dérivés de cette dernière sont régénérés et stockés dans un emplacement temporaire sur le serveur. La durée du processus de régénération dépend du nombre de Gestionnaires d'agents et du nombre d'extensions dérivées de l'autorité de certification racine McAfee ePO.

3 Une fois la régénération effectuée, attendez que les nouveaux certificats de votre environnement atteignent un niveau de saturation suffisant.

Les agents reçoivent le nouveau certificat quand ils communiquent avec le serveur McAfee ePO. Le pourcentage d'agents ayant reçu les certificats récemment générés est fourni dans le **Gestionnaire de certificats**, sous **Produit : Gestionnaire d'agents** | **Etat**.

Ce pourcentage de distribution est basé sur le nombre de communications agent-serveur qui ont été établies depuis la régénération des certificats. Les systèmes inactifs non managés auront un impact sur ce pourcentage.

Avant de continuer, veillez à ce que le pourcentage de distribution soit aussi proche de 100 % que possible. Dans le cas contraire, les systèmes en attente ne recevront pas les certificats qui viennent d'être générés et seront incapables de communiquer avec le serveur McAfee ePO après l'activation des certificats. Vous pouvez maintenir cet état aussi longtemps que nécessaire pour atteindre un niveau de saturation suffisant.

4 Une fois que vous avez atteint un pourcentage de distribution proche de 100 %, cliquez sur **Activer les certificats** pour que toutes les opérations à venir utilisent les nouveaux certificats.

Une sauvegarde des certificats d'origine est créée et un message est affiché.

5 Cliquez sur **OK**. Vous devez réinstaller les agents qui utilisent d'anciens certificats afin de restaurer la communication agent-serveur.

6 Une fois l'activation des certificats terminée, procédez comme suit.

a Arrêtez les services de Gestionnaire d'agents (y compris les Gestionnaires d'agents distincts).

b Redémarrez les services McAfee ePO.

c Démarrez les services du Gestionnaire d'agents.

7 Surveillez votre environnement et vérifiez que les agents communiquent correctement.

A ce stade, vous pouvez annuler la migration pour restaurer le certificat et rétablir la communication agent-serveur. Toutefois, cette annulation n'est pas possible une fois que vous avez effectué l'étape suivante.

8 Cliquez sur **Finaliser la migration** pour terminer la migration des certificats.

La sauvegarde des certificats créée pendant l'activation est supprimée.

En cas de problème pendant la migration, cliquez sur **Annuler la migration** pour rétablir les précédents certificats. Si vous annulez la migration, arrêtez les services du Gestionnaire d'agents, redémarrez le service McAfee ePO, puis redémarrez le Gestionnaire d'agents.

Une fois les problèmes résolus, vous pouvez relancer la migration.

Mise à niveau du serveur de cluster McAfee ePO

La mise à niveau du logiciel McAfee ePO dans un environnement de cluster exige certaines précautions.

Avant de commencer

Pour effectuer la mise à niveau vers votre serveur McAfee ePO, votre environnement actuel doit être pris en charge.

Procédure

1. A partir du nœud actif, ouvrez le **Groupe ePO** dans le Gestionnaire du cluster de basculement.
2. Assurez-vous que le nœud principal est le serveur actif.
3. Déconnectez cette ressource de service générique, puis supprimez-la :
   - Serveur d'applications ePolicy Orchestrator

   Ne modifiez pas ces ressources, dans la mesure où elles sont nécessaires au bon déroulement de la mise à niveau :
   - Lecteur de données
   - Adresse IP virtuelle de McAfee ePO
   - Nom réseau virtuel de McAfee ePO
4. Ouvrez le Gestionnaire de contrôle des services et démarrez chacun des services suivants sur le nœud principal :
   - Serveur ePolicy Orchestrator
   - Serveur d'applications ePolicy Orchestrator
   - Analyseur d'événements ePolicy Orchestrator
5. Installez le nouveau logiciel McAfee ePO sur le nœud principal.
6. Dans le Gestionnaire du cluster de basculement, déplacez le **rôle d'application ePO** vers le deuxième nœud du cluster en cliquant avec le bouton droit sur le rôle, puis en sélectionnant **Déplacer** | **Sélectionner le nœud**. Sélectionnez le deuxième nœud du cluster, puis cliquez sur **OK**.

   Le rôle est déplacé vers le deuxième nœud du cluster.

   (Facultatif) Arrêtez le premier serveur de nœud du cluster : il déplace automatiquement le rôle vers le deuxième nœud.
7. Installez le nouveau logiciel McAfee ePO sur le nœud secondaire.
8. Une fois l'installation terminée sur chaque nœud, créez les nouvelles ressources Service générique.

   Pour plus d'informations, consultez la section *Création des ressources de service générique* du chapitre *Installation de McAfee ePO dans un environnement de cluster*.

9 Résolution des problèmes d'installation

Sommaire

Résolution des problèmes et références des fichiers journaux

Cette section répertorie les messages d'erreur les plus courants qui peuvent s'afficher lors de l'installation de McAfee ePO, ainsi que les solutions correspondantes. Les informations suivantes permettent de résoudre divers problèmes d'installation.

Si les informations de cette section ne vous permettent pas de résoudre un problème précis, effectuez les procédures ci-dessous avant de contacter l'équipe de support technique :

1. Vérifiez que l'ordinateur présente la configuration minimale requise pour l'installation.
2. Consultez les notes de version de et cliquez sur le lien d'accès à l'article de la base de connaissances McAfee pour consulter les problèmes d'installation connus.
3. Vérifiez que le compte que vous utilisez pour vous connecter à l'ordinateur sur lequel vous installez le logiciel dispose de droits d'administrateur complets sur cet ordinateur.
4. Prenez note du texte exact de tous les messages et notez les codes de message éventuels.
5. Collectez les journaux d'installation dans C:\Program Data\McAfee\ePO.

Messages d'installation courants avec détail des causes et des solutions

Lors de l'installation, le logiciel McAfee ePO fournit des informations qui peuvent nécessiter des actions supplémentaires. Le tableau ci-dessous répertorie les messages qui peuvent s'afficher et indique les actions correspondantes à effectuer.

Message	Cause	Solution
Vous essayez d'effectuer une mise à niveau depuis une version de produit non prise en charge.	Aucune version du logiciel McAfee ePO n'est installée sur cet ordinateur. Vous pouvez effectuer une mise à niveau uniquement depuis une version prise en charge du serveur McAfee ePO.	Sélectionnez l'option d'installation appropriée.
Vous devez installer Internet Explorer 8.0 ou version ultérieure, ou Firefox 10 avant de poursuivre l'installation.	L'ordinateur sur lequel vous essayez d'installer le logiciel utilise une version non prise en charge du navigateur.	Avant de poursuivre, installez un navigateur Internet pris en charge.
Une autre instance du programme d'installation de McAfee ePO est déjà en cours d'exécution.	Le programme d'installation de McAfee ePO est déjà en cours d'exécution. Vous ne pouvez pas exécuter plusieurs instances de ce programme en même temps.	Attendez que la première instance du programme d'installation soit finie, ou arrêtez-la et relancez l'installation.
McAfee n'autorise pas les mots de passe vides pour des raisons de sécurité. Entrez un mot de passe valide pour continuer.	Le champ **Mot de passe** est vide.	Indiquez le mot de passe associé au compte utilisateur que vous souhaitez utiliser.
Il est conseillé de définir la résolution d'écran sur 1366 x 768 ou plus.	L'ordinateur sur lequel vous essayez d'installer le logiciel ne présente pas la configuration minimale requise en termes de résolution d'écran.	Modifiez la résolution d'écran à au moins 1024 x 768, puis continuez l'installation. Sinon, vous risquez de ne pas voir l'écran dans son intégralité lorsque vous lancerez le logiciel. Pour des instructions détaillées sur le paramétrage de la résolution d'écran, voir le fichier d'aide de Windows (cliquez sur **Démarrer**, puis sélectionnez **Aide**).
Il est conseillé d'installer le logiciel sur un ordinateur muni d'au moins 8 Go de RAM.	L'ordinateur sur lequel vous essayez d'installer le logiciel ne présente pas la configuration minimale requise en termes de mémoire.	Ajoutez de la mémoire à votre système ou sélectionnez un autre système disposant d'au moins 8 Go de RAM pour l'installation.
Pour installer McAfee ePO, votre ordinateur doit exécuter Windows Server 2008, Windows Server 2012, ou Windows Server 2016.	L'ordinateur sur lequel vous essayez d'installer le logiciel utilise une version non prise en charge du système d'exploitation.	Utilisez un système d'exploitation serveur pris en charge.
Entrez une valeur dans le champ Port de communication de diffusion de l'agent.	Le champ **Port de communication de diffusion de l'agent** est vide.	Indiquez le numéro de port (par défaut, 8082) que le serveur McAfee ePO doit utiliser pour envoyer aux SuperAgents des appels de réactivation de l'agent.
Entrez une valeur dans le champ Port de communication agent-serveur.	Le champ **Port de communication agent-serveur** est vide.	Indiquez le numéro de port que l'agent doit utiliser pour communiquer avec le serveur.
Entrez une valeur dans le champ Port de communication de réactivation de l'agent.	Le champ **Port de communication de réactivation de l'agent** est vide.	Indiquez le numéro de port (par défaut, 8081) que le serveur McAfee ePO doit utiliser pour envoyer des appels de réactivation de McAfee Agent.

Message	Cause	Solution
McAfee ePO doit être installé dans un dossier. Entrez un dossier de destination pour continuer.	Le **Dossier de destination** est vide ou affiche la racine d'un lecteur.	Cliquez sur **Parcourir** pour sélectionner un emplacement. Emplacement par défaut : `C \Program Files\McAfee \ePolicy Orchestrator`.
Entrez une valeur dans le champ Nom utilisateur.	Le champ **Nom utilisateur** est vide.	Indiquez le nom utilisateur associé au compte que vous souhaitez utiliser.
Le fichier de licence est manquant ou endommagé. Contactez le support technique pour obtenir de l'aide.	Le programme d'installation ne peut pas lire les informations de licence requises pour installer le logiciel.	Contactez le support technique.
Le système d'exploitation ou le Service Pack utilisé n'est pas pris en charge actuellement.	L'ordinateur sur lequel vous essayez d'installer le logiciel utilise une version non prise en charge du système d'exploitation.	Utilisez un système d'exploitation serveur pris en charge.
Les mots de passe ne correspondent pas. Entrez un mot de passe valide pour continuer.	Les valeurs que vous avez saisies dans les champs **Mot de passe** et **Confirmer le mot de passe** ne correspondent pas.	Indiquez le mot de passe associé au compte que vous souhaitez utiliser.
La licence McAfee ePO a expiré.	Votre licence d'utilisation du logiciel a expiré.	Contactez votre administrateur ou le représentant McAfee désigné.
Ce système n'est pas configuré avec une adresse IP statique, laquelle est recommandée pour le serveur McAfee ePO.	L'ordinateur sur lequel vous essayez d'installer le logiciel n'utilise pas une adresse IP statique. Or il est conseillé d'utiliser des adresses IP statiques pour les serveurs McAfee ePO afin d'améliorer les performances et de réduire la consommation de bande passante.	Indiquez une adresse IP statique à utiliser avec votre serveur McAfee ePO.
Impossible d'établir une connexion avec le serveur de base de données. Vérifiez que vous avez entré correctement les informations d'identification du compte et le nom du serveur de base de données, puis réessayez.	Impossible d'établir la connexion au serveur de base de données McAfee ePO correspondant.	**1** Vérifiez que vous avez correctement saisi le **Domaine**, le **Nom utilisateur** et le **Mot de passe**. **2** Vérifiez que le serveur de base de données est en cours d'exécution. **3** Vérifiez que le compte utilisateur indiqué est valable pour le serveur de base de données.
Connexion impossible avec les informations fournies. Vérifiez que les informations indiquées sont correctes, puis réessayez.	Il est impossible d'accéder au compte utilisateur que vous avez indiqué.	**1** Vérifiez que vous avez correctement saisi le **Domaine**, le **Nom utilisateur** et le **Mot de passe**. **2** Vérifiez que le compte que vous avez utilisé pour vous connecter à cet ordinateur a accès à ce domaine.

Fichiers journaux destinés à la résolution de problèmes

McAfee ePO fournit des fichiers journaux contenant des informations importantes pour la résolution des problèmes.

Ces fichiers journaux sont répartis en trois catégories :

- **Journaux du programme d'installation** : informations relatives au chemin d'installation, aux informations d'identification de l'utilisateur, à la base de données utilisée et aux ports de communication configurés.
- **Journaux de serveur** : informations relatives aux fonctionnalités serveur, à l'historique des événements de client et aux services d'administrateur.
- **Journaux d'agent** : informations relatives à l'installation de l'agent, aux appels de réactivation, aux mises à jour et à la mise en œuvre de stratégie.

Journaux du programme d'installation

Les fichiers journaux du programme d'installation contiennent les informations relatives à la procédure d'installation de McAfee ePO.

Ces journaux fournissent les informations suivantes :

- Actions entreprises par des composants spécifiques
- Services d'administrateur utilisés par le serveur
- Réussite et échec de processus essentiels

Nom du fichier	Type de journal	Emplacement	Description
`AH5100-Install-MSI.log,`	Installation de gestionnaires d'agents	`C:\ProgramData\McAfee\ePO`	Ce fichier contient toutes les informations relatives à l'installation de gestionnaires d'agents, notamment : • Actions du programme d'installation • Echecs d'installation
`AH5100-ahetupdll.log`	Temporaire	`%temp%` (sur le serveur de gestionnaire d'agents)	Consigne les événements du système principal gestionnaire d'agents.
`core-install.log`	Temporaire	`%temp%\McAfeeLogs\ePO5100-Troubleshoot\MFS`	Généré lorsque le programme d'installation appelle le programme d'installation MFS ANT. Il fournit des informations sur les opérations suivantes : • Création des tables de la base de données de serveur • Installation des composants serveur Ce fichier est supprimé si l'installation réussit.
`epo-Install.log`	Installation	`C:\ProgramData\McAfee\ePO`	Généré lorsque le programme d'installation appelle le programme d'installation ANT.

Nom du fichier	Type de journal	Emplacement	Description
`EPO5100-Checkin-Failure.log situé`	Installation	`C:\ProgramData\McAfee\ePO`	Généré lorsque le programme d'installation ne peut pas archiver un package de l'un des types suivants : • Extensions • Plugins • Packages de déploiement • Packages de l'agent
`EPO5100-CommonSetup.log`	Installation	`C:\ProgramData\McAfee\ePO`	Contient les informations relatives au programme d'installation, notamment : • Journalisation des actions personnalisées • Appels SQL, appels DTS (Microsoft Data Transformation Services) et appels liés aux services • Enregistrement et annulation de l'enregistrement des fichiers DLL • Fichiers et dossiers sélectionnés pour suppression au redémarrage
`EPO5100-Install-MSI.log,`	Installation	`C:\ProgramData\McAfee\ePO`	Journal d'installation principal. Contient des informations relatives à l'installation, telles que les actions du programme d'installation et les échecs d'installation.
`<NomFichierExtension>.cmd`	Temporaire	`%temp%\McAfeeLogs\ePO5100-troubleshoot\OutputFiles`	Généré par le programme d'installation. Contient la commande (envoyé au client distant) pour archiver les extensions. Ces fichiers sont supprimés si l'installation réussit.
`MFS5100-CommonSetup.log`	Installation	`C:\ProgramData\McAfee\ePO`	Contient les informations sur le programme d'installation des fonctionnalités principales.

Journaux de serveur

Les fichiers journaux de serveur contiennent les informations relatives aux fonctionnalités serveur et aux différents services d'administrateur utilisés par McAfee ePO.

Nom du fichier	Type de journal	Emplacement	Description
`EpoApSvr_<nom_serveur>.log`	Principal	`[Répertoire d'installation]\DB\Logs`	Fichier journal du serveur d'applications contenant des informations sur les actions s'appliquant aux référentiels, telles que : • Tâches d'extraction • Archivage des packages de déploiement dans le référentiel • Suppression des packages de déploiement du référentiel Ce fichier n'est généré qu'après le démarrage initial du service.
`Errorlog.<DATE ET HEURE ACTUELLES>`	Apache	`[RÉPERTOIRE D'INSTALLATION]\Apache2\logs`	Contient les informations relatives au service Apache. Ce fichier n'est généré qu'après le démarrage initial du service Apache.
`Eventparser_<nom_serveur>.log`	Principal	`[Répertoire d'installation]\DB\Logs`	Contient les informations relatives au service Analyseur d'événements McAfee ePO, telles que la réussite ou l'échec de l'analyse d'événements de produit.
`Jakarta_service_<DATE>_<nom_serveur>.log`	Tomcat	`[Répertoire d'installation]\Server\logs` *	Contient les informations relatives au service Serveur d'applications McAfee ePO. Ce fichier n'est généré qu'après le démarrage initial du service Tomcat.
`Localhost_access_log.<DATE>.txt`	Tomcat	`[Répertoire d'installation]\Server\logs` *	Enregistre toutes les requêtes du serveur McAfee ePO envoyées par les systèmes clients. Ce fichier n'est généré qu'après le démarrage initial du service Tomcat.
`Orion_<nom_serveur>.log`	Principal	`[Répertoire d'installation]\Server\logs` *	Contient les informations relatives à la plate-forme et à toutes les extensions chargées par défaut. Ce fichier n'est généré qu'après le démarrage initial du service Serveur d'applications McAfee ePO.
`Replication_<nom_serveur>.log`	Serveur	`[Répertoire d'installation]\DB\Logs`	Fichier journal de réplication du serveur McAfee ePO. Ce fichier n'est généré que lorsque tous les critères suivants sont remplis : • Présence de référentiels distribués. • Une tâche de réplication a été configurée. • Une tâche de réplication a été exécutée.

Nom du fichier	Type de journal	Emplacement	Description
`Server_<nom _serveur>.log`	Principal	`[Répertoire d'installation]\DB \Logs`	Contient les informations relatives aux services suivants du serveur McAfee ePO : • Communications agent-serveur • Gestionnaire d'agents du serveur McAfee ePO Ce fichier n'est généré qu'après le démarrage initial du service.
`Stderr_<nom _serveur>.log`	Tomcat	`[Répertoire d'installation] \Server\logs` *	Contient toutes les sorties d'erreur standard capturées par le service Tomcat. Ce fichier n'est généré qu'après le démarrage initial du service Tomcat.
`<GUID de l'agent> _<Horodatage> _Server_manifest .xml`	Stratégie	`[Répertoire d'installation]\DB \DEBUG`	Contient les informations relatives aux problèmes de mise à jour des stratégies. Pour activer ce fichier : **1** Accédez à la clé de Registre suivante : `HKEY _LOCAL_MACHINE\Software\Network Associates\ePolicy Orchestrator\` **2** Attribuez la valeur 1 à la clé DWORD suivante : `SaveAgentPolicy` **3** Redémarrez le service McAfee ePolicy Orchestrator Server (Apache). Activez le fichier uniquement le temps de recueillir les informations nécessaires, car la taille des fichiers générés augmente rapidement.

* Dans un environnement en cluster, le fichier journal se trouve dans `[RÉPERTOIRE D'INSTALLATION]\Bin\Server\logs`.

Journaux de McAfee Agent

Les fichiers journaux de McAfee Agent répertorient les actions déclenchées ou entreprises par McAfee Agent.

Les noms de fichier dans cette liste correspondent à McAfee Agent version 5.5.0 pour Windows.

Nom de fichier McAfee Agent 5.5.0	Type de journal	Emplacement	Description
masvc_<nom_hôte>.log	Serveur	[Chemin d'accès aux données de l'agent]\logs	Généré lorsque le programme masvc.exe est utilisé. Le fichier contient les informations relatives aux éléments suivants : • Collecte des propriétés • Communication agent-serveur • Mise en œuvre de stratégie • Sessions de mise à jour • Planification des tâches
macmnsvc_<nom_hôte>.log	McAfee Agent	[Chemin d'accès aux données de l'agent]\logs	Généré lors de l'utilisation du programme macmnsvc.exe. Le fichier contient les informations relatives aux éléments suivants : • Serveur homologue à homologue • SuperAgent • Réactivation • RelayServer
macompatsvc_<nom_hôte>.log	McAfee Agent	[Chemin d'accès aux données de l'agent]\logs	Généré lorsque le programme macompatsvc.exe est utilisé. Le fichier contient les informations relatives à la compatibilité des produits managés avec les services McAfee Agent.
masvc_<nom_hôte>_sauvegarde_<nombre_de_sauvegardes>.log	McAfee Agent	[Chemin d'accès aux données de l'agent]\logs	Généré lors de la sauvegarde de fichiers pour les services McAfee Agent.
marepomirror.log	Serveur		Généré lors de l'utilisation du programme marepomirror.exe. Le fichier contient les informations relatives à la mise en miroir du référentiel.
FrmInst_<nom_hôte>.log	McAfee Agent	%temp%\McAfeeLogs	Généré lorsque le programme FrmInst.exe est utilisé pour installer McAfee Agent. Ce fichier contient les informations suivantes : • Messages d'information • Messages indicateurs de progression • Messages d'échec lorsque l'installation échoue
mcScript.log	Débogage de McAfee Agent	[Chemin d'accès aux données de l'agent]\logs	Contient les résultats des commandes de script utilisées lors du déploiement ou de la mise à jour d'un agent. Pour activer le mode de débogage (DEBUG) pour ce journal, définissez la valeur DWORD suivante dans la clé de Registre du client : HKEY_LOCAL_MACHINE\SOFTWARE\NETWORK ASSOCIATES\TVD\SHARED COMPONENTS\FRAMEWORK\DWDEBUGSCRIPT=2 Supprimez cette clé une fois le problème résolu.

Nom de fichier McAfee Agent 5.5.0	Type de journal	Emplacement	Description
`MFEAgent.msi .<horodatage du système>.log`	McAfee Agent	`%temp% \McAfeeLogs`	Contient les informations relatives à l'installation MSI de l'agent.
`UpdaterUI _<système>.log`	McAfee Agent	`%temp% \McAfeeLogs`	Contient les informations sur les mises à jour des produits managés sur le système client.

Journaux d'erreurs de McAfee Agent

Les erreurs identifiées par McAfee Agent sont consignées dans les journaux d'erreurs de McAfee Agent. Ces journaux sont générés sous `%temp%\McAfeeLogs` pendant l'installation. Les journaux d'erreurs McAfee Agent sont nommés en fonction du journal principal correspondant. Ainsi, lorsque des erreurs surviennent lors de l'exécution de tâches client, le fichier journal `MCScript_Error.log` est créé. Les journaux d'erreurs contiennent uniquement les informations relatives aux erreurs.

Après l'installation, les journaux McAfee Agent sont enregistrés sous `%ProgramData%`.

A

Ajout d'un certificat SSL à une collection approuvée

Les navigateurs pris en charge affichent un avertissement lorsqu'ils ne peuvent pas vérifier le certificat SSL d'un serveur.

Par défaut, le serveur McAfee ePO utilise un certificat autosigné pour la communication SSL avec le navigateur web, qui n'approuve pas le certificat. Un message d'avertissement s'affiche chaque fois que vous accédez à la console McAfee ePO.

Pour que ce message n'apparaisse plus, effectuez l'une des opérations suivantes :

- Ajoutez le certificat serveur McAfee ePO à la collection de certificats approuvés du navigateur.
- Ajoutez le certificat pour tous les navigateurs interagissant avec McAfee ePO. En cas de changement du certificat du navigateur, ajoutez à nouveau le certificat serveur.
- (Recommandé) Remplacez le certificat serveur McAfee ePO par défaut par un certificat valide signé par une autorité de certification approuvée par le navigateur. Vous devez ajouter le certificat une seule fois pour les navigateurs web dans votre environnement.
- Si le nom d'hôte du serveur change, remplacez le certificat serveur par un nouveau certificat d'autorité de certification approuvé.

Pour plus d'informations, reportez-vous à l'article KB72511.

Pour remplacer le certificat serveur McAfee ePO, vous devez préalablement obtenir un certificat signé par une autorité de certification fiable. Vous devez également obtenir la clé privée du certificat ainsi que son mot de passe, le cas échéant. Vous pouvez ensuite utiliser tous ces fichiers pour remplacer le certificat du serveur.

Le serveur McAfee ePO s'attend à ce que le certificat serveur respecte les formats suivants : fichier PKCS7, fichier PEM codé, fichier DER codé ou fichier PKCS12 avec extension .cer, .crt, .p12, .p7b, etc.

Le navigateur McAfee ePO s'attend à ce que les fichiers utilisent le format PEM pour les clés privées.

Si le certificat serveur ou la clé privée utilisent un autre format, convertissez-les dans l'un des formats pris en charge avant de remplacer le certificat par défaut.

Si votre organisation requiert un niveau plus élevé de chiffrement, remplacez le certificat SHA-256 par défaut par un certificat utilisant un hachage SHA-384 ou supérieur.

Sommaire

Remplacement du certificat serveur

Mettez à jour le certificat serveur par défaut utilisé pour la communication HTTPS avec les navigateurs.

Avant de commencer

Vous devez avoir accès au nouveau certificat et aux fichiers de clé privée.

Procédure

1. Ouvrez la page **Modifier le certificat serveur**.
   a. Sélectionnez **Menu** | **Configuration** | **Paramètres serveur**.
   b. Dans la liste **Catégories de paramètres**, sélectionnez **Certificat serveur**, puis cliquez sur **Modifier**.
2. Accédez au fichier de certificat serveur, puis cliquez sur **Ouvrir**.

   Vous pouvez créer votre propre certificat autosigné avec Open SSL.
3. Si nécessaire, entrez le mot de passe et le nom d'alias du certificat PKCS12.
4. Accédez au fichier de clé privée, puis cliquez sur **Ouvrir**.
5. Si nécessaire, entrez le mot de passe de la clé privée, puis cliquez sur **Enregistrer**.
6. Redémarrez McAfee ePO pour que la modification prenne effet.

Installation du certificat de sécurité pour Internet Explorer

Empêche l'invite de certificat d'apparaître à chaque fois que vous vous connectez en installant le certificat de sécurité.

Procédure

1. A partir de votre navigateur, ouvrez McAfee ePO. La page Erreur de certificat : Navigation bloquée s'affiche.
2. Cliquez sur **Poursuivre avec ce site Web (non recommandé)** pour ouvrir la page de connexion. La barre d'adresse est rouge, indiquant que le navigateur ne peut pas vérifier le certificat de sécurité.
3. A droite de la barre d'adresse, cliquez sur **Erreur de certificat** pour afficher le message d'avertissement concernant le certificat non valide.
4. Au bas du message d'avertissement, cliquez sur **Afficher les certificats** pour ouvrir la boîte de dialogue Certificat.

   Ne cliquez pas sur **Installer le certificat** dans l'onglet **Général**. Cela provoquerait l'échec de la procédure.
5. Sélectionnez l'onglet **Chemin d'accès de certification**, puis **Orion_CA_<nom_serveur>** et cliquez sur **Afficher le certificat**. Une nouvelle boîte de dialogue s'ouvre dans l'onglet **Général** et affiche les informations sur le certificat.
6. Cliquez sur **Installer le certificat** pour ouvrir l'Assistant Importation de certificat.
   a. Cliquez sur **Suivant** pour spécifier l'emplacement du certificat.
   b. Sélectionnez **Placer tous les certificats dans le magasin suivant**, puis cliquez sur **Parcourir** pour sélectionner un emplacement.

c Dans la liste, sélectionnez le dossier **Autorités de certification racines de confiance**, cliquez sur **OK**, puis sur **Suivant**.

d Cliquez sur **Terminer**. Dans l'avertissement de sécurité qui s'affiche, cliquez sur **Oui**.

7 Fermez le navigateur.

8 Modifiez la cible du raccourci du bureau McAfee ePO afin d'utiliser le nom NetBIOS du serveur McAfee ePO au lieu de « localhost ».

9 Redémarrez McAfee ePO.

Désormais, vous n'êtes plus invité à accepter le certificat lorsque vous vous connectez à McAfee ePO.

Installation du certificat de sécurité pour Firefox

Vous pouvez installer le certificat de sécurité lorsque vous utilisez Firefox 3.5 ou version ultérieure pour que la boîte de dialogue d'avertissement ne s'affiche pas à chaque connexion.

Procédure

1 A partir de votre navigateur, ouvrez McAfee ePO. La page Cette connexion n'est pas approuvée s'affiche.

2 Cliquez sur **Je comprends les risques** au bas de la page.

3 Cliquez sur **Ajouter une exception**.

4 Cliquez sur **Obtenir le certificat**. Le champ Etat du certificat est renseigné, et le bouton Confirmer l'exception de sécurité est activé.

5 Assurez-vous que **Conserver cette exception de façon permanente** est activé, puis cliquez sur **Confirmer l'exception de sécurité**.

Désormais, vous n'êtes plus invité à accepter le certificat lorsque vous vous connectez à McAfee ePO.

B

Installation de gestionnaires d'agents

Installez des gestionnaires d'agents dans votre environnement pour faciliter la gestion des communications agent-serveur et équilibrer la charge. Vous pouvez installer des gestionnaires d'agents à tout moment.

Avant de commencer

Mettez à jour le système avec les dernières mises à jour de sécurité Microsoft, puis désactivez les mises à jour Windows pour la durée de l'installation.

Chaque serveur McAfee ePO contient un gestionnaire d'agents maître. L'installation de gestionnaires d'agents supplémentaires permet de gérer davantage de produits et de systèmes managés avec un seul serveur McAfee ePO lorsque le processeur et l'E/S du serveur de base de données ne sont pas surchargés.

Les gestionnaires d'agents requièrent le même accès réseau haut débit à votre base de données que le serveur McAfee ePO principal.

Installez les gestionnaires d'agents supplémentaires dans le même centre de données que le système SQL Server. N'installez pas de gestionnaires d'agents à des emplacements distants, car cela risque de réduire les performances de l'ensemble de l'environnement McAfee ePO.

Pour utiliser des adresses IP supplémentaires pour les communications agent-serveur, créez un groupe de gestionnaires d'agents et ajoutez l'adresse IP supplémentaire dans le champ de saisie des adresses IP virtuelles.

Procédure

1. Ouvrez le dossier dans lequel vous avez extrait le contenu du package d'installation du logiciel McAfee ePO.
2. Copiez le dossier `Agent Handler` sur le système serveur à convertir en gestionnaire d'agents.
3. Cliquez avec le bouton droit sur **Setup.exe** et sélectionnez **Exécuter en tant qu'administrateur** pour lancer l'assistant InstallShield du gestionnaire d'agents McAfee.

   Après l'exécution d'opérations d'installation en arrière-plan, l'Assistant InstallShield s'affiche. Cliquez sur **Suivant** pour commencer l'installation.
4. Acceptez les termes de l'accord de licence

   L'étape Dossier de destination s'ouvre.
5. Acceptez la destination par défaut ou cliquez sur **Modifier** pour en sélectionner une autre, puis cliquez sur **Suivant**.

   Le chemin de destination ne doit pas contenir de caractères codés sur deux octets. Les caractères du chemin d'accès sont limités par le serveur web Apache. L'utilisation de caractères codés sur deux octets entraîne l'échec de l'installation du gestionnaire d'agents et du démarrage du service du serveur web Apache.

6 Configurez les informations du serveur.

   a Entrez le nom de système du serveur McAfee ePO avec lequel le gestionnaire d'agents doit communiquer.

   b Indiquez le port à utiliser pour la communication entre le gestionnaire d'agents et le serveur. Le port par défaut est 8443 ; ce port est également utilisé pour la communication authentifiée client-serveur.

   c Entrez le nom utilisateur et le mot de passe d'un utilisateur détenant des droits d'administrateur global de McAfee ePO, puis cliquez sur **Suivant**.

   d Saisissez le mot de passe d'accès à la base de données SQL de McAfee ePO, puis cliquez sur **Suivant**.

   La page Informations de base de données est remplie avec ces paramètres de serveur McAfee ePO.

   - **Serveur de base de données** avec le nom de l'instance (par exemple `SERVEUR-BD\NOMSERVEUR`)
   - Type d'authentification
   - Nom du **Domaine** qui héberge le serveur de base de données
   - **Nom utilisateur** et **Mot de passe**
   - **Nom de la base de données** s'il n'est pas automatiquement renseigné

7 Cliquez sur **Installer** pour démarrer l'installation.

8 Au terme de l'installation, activez votre gestionnaire d'agents dans l'interface McAfee ePO.

C

Restauration de McAfee à partir d'un instantané de reprise sur sinistre

Sommaire

Configuration requise pour l'utilisation d'une capture instantanée pour la reprise sur sinistre

Assurez-vous que les conditions suivantes sont remplies avant de commencer à restaurer McAfee ePO à partir d'une capture instantanée pour la reprise sur sinistre.

- Base de données SQL McAfee ePO contenant une capture instantanée pour la reprise sur sinistre valide
- Nom utilisateur et mot de passe d'un compte administrateur global qui utilise l'authentification McAfee ePO
- Phrase secrète de reprise sur sinistre pour la capture instantanée dans la base de données

Pour plus d'informations sur le processus de reprise sur sinistre, consultez le Guide Produit de McAfee ePO.

Restauration du logiciel McAfee ePO dans un environnement de serveur unique

Restaurez McAfee ePO à partir de l'instantané stocké dans une base de données McAfee ePO. Pour cela, vous pouvez réinstaller le logiciel McAfee ePO sur un serveur en activant l'option **Restaurer ePO à partir d'une capture instantanée de base de données** et configurer l'installation pour utiliser une base de données McAfee ePO existante.

Avant de commencer

Collectez les informations suivantes et procédez comme suit avant de commencer l'installation. Ces étapes permettent de vérifier que le logiciel McAfee ePO peut communiquer avec le serveur SQL Server qui héberge la base de données McAfee ePO.

- Si vous utilisez des ports dynamiques pour le serveur SQL Server, vérifiez que le service Explorateur SQL Server est en cours d'exécution.
- Si vous n'utilisez pas de ports dynamiques pour le serveur SQL Server, vérifiez que vous connaissez les ports utilisés par l'instance SQL.
- Vérifiez que le protocole TCP/IP est activé dans le Gestionnaire de configuration SQL Server.

Surveillez le processus, car vous pourrez avoir besoin de redémarrer votre système.

Procédure

1. Si des gestionnaires d'agents distants sont configurés, connectez-vous aux systèmes sur lesquels ils sont installés, puis ouvrez le volet **Services** Windows et arrêtez les services **Analyseur d'événements McAfee** et **McAfee Apache**.

   Pour plus d'informations sur l'utilisation du volet Services Windows, consultez la documentation produit de Microsoft.

2. En utilisant un compte ayant des autorisations d'administrateur local, connectez-vous au serveur Windows Server sur lequel vous souhaitez restaurer McAfee ePO.

3. Extrayez les fichiers vers un emplacement temporaire et double-cliquez sur **Setup.exe**.

   La version de McAfee ePO restaurée doit être identique à celle utilisée pour créer la capture instantanée dans la base de données. Vous pouvez télécharger la version correcte à partir du site web de McAfee.

   Si vous lancez **Setup.exe** sans extraire au préalable le contenu du fichier .zip, l'installation échoue.

   Le programme **McAfee ePolicy Orchestrator - Assistant InstallShield** démarre.

4. Sélectionnez **Restaurer ePO à partir d'une capture instantanée de base de données existante**, puis sur **Suivant** pour lancer l'installation.

5. A l'étape Installer des logiciels supplémentaires, tous les autres composants requis sont affichés. Cliquez sur **Suivant** pour les installer.

6. A l'étape Dossier de destination, cliquez sur :
   - **Suivant** pour installer le logiciel McAfee ePO à l'emplacement par défaut (C:\Program Files (x86)\McAfee \ePolicy Orchestrator).
   - **Modifier** pour indiquer un emplacement de destination personnalisé pour le logiciel McAfee ePO. Lorsque la fenêtre **Modifier le dossier de destination actuel** s'ouvre, accédez au dossier de destination et si nécessaire, créez des dossiers. Lorsque vous avez terminé, cliquez sur **OK** | **Suivant**.

7. À l'étape Informations de base de données, sélectionnez le nom du serveur SQL Server dans la liste déroulante Serveur de base de données ou entrez manuellement le nom du serveur SQL Server.

8 Dans le champ Nom de base de données, entrez le nom de la base de données McAfee ePO existante contenant l'instantané, spécifiez le type d'informations d'identification pour le serveur de base de données à utiliser, puis cliquez sur **Suivant**.

- **Authentification Windows** : dans le menu Domaine, sélectionnez le domaine du compte utilisateur que vous souhaitez utiliser pour accéder au serveur SQL Server. Entrez le nom utilisateur et le mot de passe d'un compte disposant des autorisations suffisantes pour accéder au serveur SQL Server hébergeant la base de données McAfee ePO.
- **Authentification SQL** : entrez le nom utilisateur et le mot de passe d'un compte disposant des autorisations suffisantes pour accéder au serveur SQL Server hébergeant la base de données McAfee ePO.

  Le menu Domaine est grisé si vous utilisez l'authentification SQL.

Vous devrez peut-être entrer le Port TCP SQL Server à utiliser pour les communications entre le serveur McAfee ePO et le serveur de base de données. L'installation McAfee ePO tente de se connecter à l'aide du port TCP par défaut 1433, et de déterminer si un port dynamique est utilisé en interrogeant le service Explorateur SQL Server sur le port UDP 1434. En cas d'échec, vous êtes invité à indiquer un port TCP SQL Server.

9 À l'étape Informations de port HTTP, examinez les affectations de port par défaut, puis cliquez sur **Suivant** pour vérifier que les ports ne sont pas déjà utilisés sur ce système.

10 A l'étape Informations sur l'administrateur, entrez le nom utilisateur et le mot de passe que vous utilisiez pour le compte administrateur global de l'ancien serveur McAfee ePO.

11 Entrez la phrase secrète de chiffrement de la banque de clés (ou phrase secrète de la capture instantanée) pour la capture instantanée de la base de données McAfee ePO.

12 Cliquez sur **Installer** pour commencer l'installation.

13 Lorsque l'installation est terminée, cliquez sur **Terminer** pour quitter l'Assistant InstallShield.

14 Si vous avez restauré McAfee ePO sur un serveur ayant une adresse IP ou un nom DNS différents de ceux de l'ancien serveur, configurez les paramètres nécessaires pour permettre à vos systèmes managés de se connecter à votre nouveau serveur McAfee ePO.

- Créez un enregistrement CNAME dans DNS qui redirige les requêtes à l'ancien nom DNS à l'adresse IP du nouveau serveur McAfee ePO.

15 Si vous avez arrêté les gestionnaires d'agents distants à l'étape 1 et restauré McAfee ePO sur un système ayant les mêmes nom de serveur et adresse IP que précédemment, connectez-vous aux systèmes sur lesquels les gestionnaires sont installés, puis ouvrez le volet **Services** Windows et démarrez les services **Analyseur d'événements McAfee** et **McAfee Apache**.

Si vous avez restauré McAfee ePO sur un système avec un nom ou une adresse IP différente, consultez la section *Restauration des connexions de Gestionnaire d'agents*.

Le logiciel McAfee ePO est à présent restauré. Si nécessaire, double-cliquez sur l'icône **Lancer ePolicy Orchestrator** de votre bureau pour commencer à utiliser votre serveur McAfee ePO, ou accédez au serveur à partir d'une console web à distance (https:// <nom_serveur>:<port>).

Restauration du logiciel McAfee ePO dans un environnement de cluster

Pour restaurer les serveurs McAfee ePO installés sur les clusters de serveurs munis du logiciel MSCS (Microsoft Cluster Server), réinstallez le logiciel McAfee ePO sur tous les serveurs dans le cluster de serveurs.

Avant de commencer

Collectez les informations ci-dessous et suivez les étapes ci-après avant de lancer l'installation. Ces étapes permettent de vérifier que le logiciel McAfee ePO peut communiquer avec le serveur SQL hébergeant la base de données McAfee ePO :

- Si vous utilisez des ports dynamiques pour le serveur SQL Server, vérifiez que le service SQL Browser est en cours d'exécution.
- Si vous n'utilisez aucun port dynamique pour le serveur SQL Server, vérifiez que vous connaissez les ports que votre instance SQL utilise.
- Vérifiez que le protocole TCP/IP est activé dans le Gestionnaire de configuration SQL Server.

La restauration du logiciel McAfee ePO dans un environnement Microsoft Cluster Server est similaire à l'installation initiale.

Surveillez l'installation de type **restauration**. Vous devrez peut-être redémarrer le système.

Procédure

1. Si des gestionnaires d'agents sont configurés, connectez-vous aux systèmes sur lesquels ils sont installés, puis ouvrez le volet **Services** Windows et arrêtez les services **Analyseur d'événements McAfee** et **McAfee Apache**.

   Pour plus d'informations sur l'utilisation du volet Services Windows, consultez la documentation produit de Microsoft.

2. A l'aide d'un compte disposant d'autorisations d'administrateur local, connectez-vous à l'ordinateur Windows Server (premier nœud du cluster) utilisé comme serveur McAfee ePO de restauration.

3. Le cas échéant, dans le gestionnaire du cluster de basculement, créez les ressources rôle d'application McAfee ePO, point d'accès client et lecteur de données partagé.

   Pour plus d'informations, consultez la section *Installation du logiciel dans un environnement en cluster*.

4. Extrayez les fichiers vers un emplacement temporaire et double-cliquez sur **Setup.exe**.

   La version de McAfee ePO en cours de restauration doit être identique à celle utilisée pour créer la capture instantanée dans la base de données. Vous pouvez télécharger la version appropriée à partir du site web McAfee.

   L'installation échoue si vous lancez **Setup.exe** sans avoir préalablement extrait le contenu du fichier .zip.

   Le programme **McAfee ePolicy Orchestrator - Assistant InstallShield** démarre.

5. Cliquez sur **Restaurer ePO à partir d'une capture instantanée de base de données existante**, puis sur **Suivant** pour lancer le processus d'installation.

6. A l'étape Installer des logiciels supplémentaires, tous les autres composants requis sont affichés. Cliquez sur **Suivant** pour les installer.

7. A l'étape Dossier de destination, cliquez sur **Modifier** pour spécifier un emplacement de destination personnalisé pour le logiciel McAfee ePO. Lorsque la fenêtre **Modifier le dossier de destination actuel** s'ouvre, accédez au dossier de destination et si nécessaire créez des dossiers. Lorsque vous avez terminé, cliquez sur **OK**.

   Veillez à spécifier un dossier de destination accessible à partir de tous les nœuds du cluster.

8 A l'étape Définir les paramètres du serveur virtuel, indiquez l'adresse IP du serveur virtuel, le nom du cluster virtuel McAfee ePO, le nom de domaine complet du cluster virtuel McAfee ePO ainsi que la phrase secrète de configuration du cluster, puis cliquez sur **Suivant**.

9 À l'étape Informations de base de données, sélectionnez le nom du serveur SQL Server dans la liste déroulante Serveur de base de données ou entrez manuellement le nom du serveur SQL Server.

10 Dans le champ Nom de la base de données, saisissez le nom de la base de données McAfee ePO existante contenant la capture instantanée, spécifiez le type d'informations d'identification pour le serveur de base de données à utiliser, puis cliquez sur **Suivant**.

- **Authentification Windows** : dans le menu Domaine, entrez le domaine du compte utilisateur que vous souhaitez utiliser pour accéder au serveur SQL Server. Entrez le nom utilisateur et le mot de passe d'un compte disposant des autorisations suffisantes pour accéder au serveur SQL Server hébergeant la base de données McAfee ePO.
- **Authentification SQL** : entrez le nom utilisateur et le mot de passe d'un compte disposant des autorisations suffisantes pour accéder au serveur SQL Server hébergeant la base de données McAfee ePO.

  Le menu Domaine est grisé si vous utilisez l'authentification SQL.

Vous devrez peut-être entrer le port TCP SQL Server à utiliser pour les communications entre le serveur McAfee ePO et le serveur de base de données. L'installation McAfee ePO tente de se connecter à l'aide du port TCP 1433 par défaut et de déterminer si un port dynamique est utilisé en interrogeant le service SQL Browser sur le port UDP 1434. En cas d'échec de ces ports, vous êtes invité à indiquer un port TCP SQL Server.

11 A l'étape Informations de port HTTP, examinez les ports par défaut affectés, puis cliquez sur **Suivant** pour vérifier qu'ils ne sont pas déjà utilisés sur ce système.

12 A l'étape Informations sur l'administrateur, entrez le nom utilisateur et le mot de passe que vous utilisiez pour le compte administrateur global de l'ancien serveur McAfee ePO.

13 Saisissez la phrase secrète de chiffrement de la banque de clés (également appelée phrase secrète de capture instantanée) correspondant à la capture instantanée dans la base de données McAfee ePO.

14 Cliquez sur **Installer** pour commencer l'installation.

15 A l'issue de l'installation sur le premier nœud, cliquez sur **Terminer**, et déplacez le **rôle d'application ePO** vers le deuxième nœud.

Vous pouvez également arrêter le premier nœud afin de forcer le rôle à se déplacer vers le deuxième nœud.

16 Sur le deuxième nœud, exécutez le programme d'installation de McAfee ePO.

Ne sélectionnez pas l'option **Restaurer ePO à partir d'une capture instantanée de la base de données existante**.

17 A l'étape Dossier de destination, cliquez sur **Modifier**, accédez à la destination sur le lecteur de données partagé où McAfee ePO est installé, puis cliquez sur **OK** | **Suivant**.

18 A l'étape Définir les paramètres du serveur virtuel, l'adresse IP du serveur virtuel, le nom du cluster virtuel McAfee ePO et le nom de domaine complet du cluster virtuel McAfee ePO sont automatiquement renseignés. Entrez la phrase secrète de configuration du cluster, puis cliquez sur **Suivant**.

19 Cliquez sur **Installer** pour démarrer l'installation sur le deuxième nœud, puis sur **Terminer**.

Ce processus prend beaucoup moins de temps que l'installation sur le premier nœud.

20 Créez les trois ressources Service générique. Lorsque vous avez terminé, mettez le **rôle d'application ePO** en ligne.

Pour plus d'informations, consultez la section *Installation du logiciel dans un environnement en cluster*.

21 Si vous avez arrêté les gestionnaires d'agents à l'étape 1, connectez-vous aux systèmes sur lesquels ils sont installés, puis ouvrez le volet **Services** Windows et démarrez les services **Analyseur d'événements McAfee** et **McAfee Apache**.

22 Vérifiez que McAfee ePO fonctionne correctement et testez la fonction de cluster en déplaçant le **rôle d'application ePO** vers l'autre nœud.

Une fois ces étapes terminées, votre logiciel McAfee ePO est restauré.

Restauration des connexions des gestionnaires d'agents

Si vous avez restauré McAfee ePO sur un système avec un nouveau nom ou une nouvelle adresse IP, vous devez modifier les paramètres des gestionnaires d'agents pour que ceux-ci se connectent au serveur restauré.

Procédure

1 Sur le serveur de gestionnaire d'agents, extrayez le package d'installation du logiciel McAfee ePO dans un emplacement temporaire.

2 Dans le dossier extrait, ouvrez le dossier Agent Handler, et double-cliquez sur **Setup.exe** pour lancer l'assistant InstallShield du gestionnaire d'agents McAfee.

3 Cliquez sur **Suivant** pour commencer la procédure de modification.

4 Dans la boîte de dialogue **Maintenance du programme**, cliquez sur **Modifier** pour modifier les fonctionnalités de programme installées, puis sur **Suivant**.

5 Configurez les paramètres suivants :

   a Entrez le nom du système restauré du serveur McAfee ePO avec lequel le gestionnaire d'agents doit communiquer.

   b Indiquez le port à utiliser pour la communication entre le gestionnaire d'agents et le serveur. Le port par défaut est le port 8443.

   c Entrez le **Nom de l'administrateur ePO** et le **Mot de passe de l'administrateur ePO** d'un utilisateur muni de droits d'administrateur global.

   d Cliquez sur **Suivant**.

   Le programme d'installation contacte le serveur McAfee ePO et obtient les détails du serveur SQL Server hébergeant la base de données McAfee ePO. Les détails de la base de données et du serveur SQL Server, à l'exception du mot de passe, sont saisis automatiquement.

6 Entrez le mot de passe du compte que vous avez spécifié, puis cliquez sur **Suivant**.

7 Cliquez sur **Installer** pour exécuter les modifications de l'installation.

8 Une fois l'installation terminée, cliquez sur **Terminer**.

Les gestionnaires d'agents sont désormais en mesure de communiquer avec le serveur McAfee ePO et la base de données SQL restaurés.

D Utilisation de McAfee ePO en mode FIPS

Sommaire

Notions de base concernant la norme FIPS

McAfee ePO fournit un mode de fonctionnement offrant une sécurité renforcée pour les environnements le nécessitant. Le mode FIPS respecte les directives en matière de sécurité détaillées à l'Article 140 de la norme Federal Information Processing Standard (FIPS).

La norme FIPS (Federal Information Processing Standards) a été mise en place par le gouvernement des Etats-Unis afin de définir les procédures, l'architecture, les algorithmes, et autres techniques utilisées dans les systèmes informatiques. La norme du gouvernement américain FIPS 140-2 s'applique aux modules de chiffrement et cryptographiques et répond aux situations dans lesquelles chaque composant de chiffrement individuel inclus dans une solution globale requiert une certification indépendante.

Elle spécifie les configurations requises par les produits matériels et logiciels qui implémentent la fonctionnalité de cryptographie. Conformément à l'Article 5131 de la loi de droit public 104–106 ITMRA (Information Technology Management Reform Act) de1996, la norme FIPS 140-2 s'applique à tous les organismes fédéraux qui utilisent des systèmes de sécurité basés sur la cryptographie pour protéger les informations confidentielles (mais non classifiées) stockées sur les systèmes informatiques et de télécommunications (y compris vocaux). Le suffixe « -2 » dans « FIPS 140-2 » indique que la norme a été révisée.

L'intégralité du contenu de la norme FIPS est disponible en ligne sur le site web du National Institute of Standards and Technology (NIST).

Modules cryptographiques et certification FIPS 140-2

McAfee tire parti des modules cryptographiques ci-dessous pour assurer le respect des exigences en matière de conformité à la norme FIPS.

Tableau D-1 Modules cryptographiques FIPS 140-2 validés utilisés par McAfee ePO

Module cryptographique	Numéro de certificat	Lier
RSA BSAFE Crypto-C Micro Edition (Crypto-C ME) 4.1.2	2294	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2294
Bouncy Castle FIPS (BC-FJA) 1.0.1 de l'API Java	3152	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3152
OpenSSL FIPS Object Module 2.0.16 Ce module est réservé aux communications TLS entre McAfee ePO et McAfee Agent.	2398	https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/2398

Modes de fonctionnement de McAfee ePO

Selon votre environnement et vos choix d'installation, McAfee ePO fonctionne en mode FIPS ou en mode Mixte.

Le mode d'exécution de McAfee ePO est déterminé pendant l'installation ou la mise à niveau, et n'est pas modifiable.

Mode FIPS

Un serveur McAfee ePO s'exécute en mode FIPS à l'issue d'une nouvelle installation avec activation du mode FIPS.

En mode FIPS, McAfee ePO :

- Place des contraintes supplémentaires au niveau des types de méthodes de sécurité autorisées
- Réalise des tests supplémentaires au démarrage
- Autorise les connexions uniquement à partir d'une version de McAfee Agent conforme à la norme FIPS

Pourquoi utiliser McAfee ePO en mode FIPS ?

Votre organisation peut avoir besoin d'activer le mode FIPS au niveau de McAfee ePO dans les circonstances suivantes :

- Votre organisation est une entité gouvernementale américaine tenue d'utiliser des modèles cryptographiques conformes à la norme FIPS 140-2, en vertu de la loi FISMA ou d'autres lois fédérales, d'Etat, ou locales.
- Votre organisation est tenue, conformément à la politique de l'entreprise, d'utiliser des modules cryptographiques standardisés et évalués de manière indépendante.

Raisons de ne pas installer McAfee ePO en mode FIPS

N'utilisez pas McAfee ePO en mode FIPS dans les circonstances suivantes :

- Vous utilisez des systèmes ou des produits hérités qui ne prennent pas en charge McAfee ePO en mode FIPS.
- La stratégie de votre organisation vous offre la possibilité de choisir les produits ou les modules cryptographiques à utiliser en mode FIPS. Par exemple, une organisation peut opter pour ne pas utiliser McAfee ePO en mode FIPS, et pour activer le mode FIPS uniquement au niveau de McAfee® Drive Encryption sur les ordinateurs portables.

Mode Mixte

Ce mode correspond à l'exécution standard et non-FIPS de McAfee ePO.

En mode Mixte, McAfee ePO ne respecte pas les contraintes et les tests applicables au mode FIPS, et n'est pas conforme aux niveaux FIPS de sécurité.

La sécurité de vos systèmes managés reste garantie, mais les certificats et les protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) sont différents.

Périmètre cryptographique

La conformité à la norme FIPS requiert une séparation physique ou logique entre les interfaces utilisées pour l'entrée et la sortie des paramètres de sécurité critiques au niveau du module cryptographique et toutes les autres interfaces.

Pour garantir cette séparation, McAfee ePO trace un *périmètre* autour du module cryptographique. Un ensemble approuvé d'interfaces est utilisé pour accéder au module dans les limites du périmètre. Aucun autre mécanisme d'accès à ces modules n'est autorisé ni fourni en mode FIPS.

Les modules inclus dans le périmètre réalisent les opérations suivantes :

- Application des méthodes de sécurité homologuées FIPS via l'exécution de services de cryptographie, de hachage, et associés dans McAfee ePO
- Opérations de démarrage et tests de vérification requis par la norme FIPS
- Vérification de signatures des extensions et des exécutables
- Gestion des connexions TLS
- Encapsulation des API cryptographiques

Certaines versions antérieures des produits McAfee utilisent des méthodes non conformes à la norme FIPS pour accéder aux services de cryptographie et de hachage McAfee ePO. Ces produits ne respectent pas le périmètre cryptographique, et ne peuvent donc pas être utilisés en mode FIPS. Reportez-vous aux nouvelles versions des produits McAfee dès leur publication afin d'en savoir plus sur leur conformité FIPS.

Installation de McAfee ePO en mode FIPS

L'installation en mode FIPS requiert l'exécution du programme d'installation `Setup.exe` à partir de la ligne de commande et ajoute pour cela une option de ligne de commande.

Procédure

1. Dans une fenêtre d'invite de commande, remplacez les répertoires par le dossier qui inclut le programme d'installation de McAfee ePO.
2. Invoquez le programme d'installation à l'aide de la commande `setup.exe ENABLEFIPSMODE=1`.
3. Poursuivez l'installation.

Ne modifiez pas le paramètre par défaut du port sécurisé de communication agent-serveur (ASSC). Laissez sa valeur sur 443. En mode FIPS, les agents utilisent le port sécurisé ASSC pour communiquer avec le serveur McAfee ePO.

Mise à niveau d'un serveur McAfee ePO conforme avec la norme FIPS

La mise à niveau en mode FIPS requiert l'exécution du programme d'installation `Setup.exe` à partir de la ligne de commande et ajoute pour cela une option de ligne de commande.

Avant de commencer

Si votre serveur McAfee ePO existant ne s'exécute pas en mode FIPS, procédez à sa réinstallation complète afin de le faire basculer vers le mode FIPS.

L'installation de McAfee ePO en mode FIPS ne prend pas en charge la restauration d'une base de données McAfee ePO à partir d'un serveur McAfee ePO non-FIPS antérieur.

Procédure

1. Dans une fenêtre d'invite de commande, remplacez les répertoires par le dossier contenant le nouveau programme d'installation de McAfee ePO.
2. Invoquez le programme d'installation à l'aide de la commande `setup.exe ENABLEFIPSMODE=1`.
3. Poursuivez la mise à niveau.

Restauration du serveur McAfee ePO en mode FIPS

Vous devez avoir préalablement exécuté le serveur McAfee ePO en mode FIPS pour pouvoir le restaurer en mode FIPS.

Vous ne pouvez pas restaurer un serveur McAfee ePO en tant que serveur McAfee ePO en mode FIPS s'il ne fonctionnait pas en mode FIPS. Le logiciel et la base de données McAfee ePO doivent être réinstallés sous forme de nouvelle instance de McAfee ePO.

La réinstallation complète de McAfee ePO est requise dans la mesure où l'ensemble du contenu signé et chiffré existant a été signé à l'aide de clés en mode non-FIPS. En outre, la base de données inclut du contenu chiffré au moyen de clés en mode non-FIPS et ne peut pas être déchiffrée à l'aide de clés en mode FIPS.

Vérifier que le gestionnaire d'agents est en mode FIPS 140-2

Affichez le fichier server.ini pour vous assurer que le gestionnaire d'agents fonctionne en mode FIPS.

Procédure

1. Ouvrez le fichier server.ini dans un éditeur de texte.

   Le fichier server.ini se trouve dans le répertoire d'installation de McAfee ePO : <répertoire d'installation d'ePO>\DB\server.ini
2. Consultez la valeur FipsMode.

   Cette valeur indique le mode de fonctionnement du serveur :

   - FipsMode=0 : le serveur fonctionne en mode Mixte (normal). Pour mettre votre serveur en mode FIPS, répétez la procédure de d'installation ou de mise à niveau.
   - FipsMode=1 : le serveur fonctionne en mode FIPS.

Vérifier que le serveur Apache est en mode FIPS 140-2

Le serveur Apache contient un paramètre de configuration d'activation FIPS.

Procédure

1. Accédez au dossier d'installation du Gestionnaire d'agents. Dossier par défaut : C:\Program Files (x86)\McAfee\ ePolicy Orchestrator.
2. Accédez au dossier de configuration d'Apache : apache2\conf
3. A l'aide d'un éditeur de texte, ouvrez le fichier httpd.conf et recherchez **SSLFIPS**.
   - Désactivé : Apache mod_ssl n'est pas configuré pour l'activation FIPS.
   - Activé : Apache mod_ssl est configuré pour l'activation FIPS.

Vérification du serveur d'application en mode FIPS 140-2

Accédez au mode de sécurité afin de vérifier que le serveur d'application McAfee ePO s'exécute en mode FIPS.

- Sélectionnez **Menu** | **Configuration** | **Paramètres serveur** | **Clés de sécurité**, puis confirmez que le **Mode de sécurité** est **FIPS 140-2**.

E Suppression du logiciel

Sommaire

Désinstallation de McAfee ePO

La désinstallation du logiciel McAfee ePO implique des considérations spécifiques concernant la base de données.

Avant de commencer

Si vous allez réinstaller le logiciel McAfee ePO par la suite et souhaitez gérer les agents qui ont été déployés avec l'installation actuelle, sauvegardez les clés de communication agent-serveur. Vous ne pouvez pas régénérer ces clés ultérieurement.

Procédure

1. Fermez tous les logiciels de gestion de base de données.
2. Sur le système hébergeant le serveur McAfee ePO, ouvrez le **Panneau de configuration** de Windows, puis cliquez sur **Programmes et fonctionnalités** | **McAfee ePolicy Orchestrator** | **Désinstaller/Modifier**.

   La boîte de dialogue **Supprimer McAfee ePolicy Orchestrator** s'affiche.
3. Si vous le souhaitez, sélectionnez **Supprimer également la base de données ePolicy Orchestrator**, puis cliquez sur **Supprimer**.

   Fournissez des informations d'identification octroyant des autorisations suffisantes pour supprimer la base de données. Si ces informations d'identification ne confèrent pas les autorisations nécessaires, vous pouvez effectuer la désinstallation sans supprimer la base de données.

Désinstallation de McAfee ePO à partir d'un cluster

Lorsque vous désinstallez McAfee ePO dans un environnement de cluster, vous devez suivre une procédure spécifique en fonction du système d'exploitation serveur utilisé.

Procédure

1. Pour déconnecter tous les services McAfee ePO, ouvrez l'outil Administrateur de cluster ou Gestion du cluster de Windows et cliquez sur **Démarrer** | **Programmes** | **Outils d'administration** | **Gestionnaire du cluster de basculement**.
2. Dans le groupe d'applications McAfee ePO, cliquez avec le bouton droit sur chaque ressource McAfee ePO et sélectionnez **Supprimer**.
3. Pour désinstaller le logiciel, cliquez sur **Programmes et fonctionnalités** | **McAfee ePolicy Orchestrator** | **Désinstaller/Modifier**.
4. Répétez cette procédure sur chaque nœud du cluster.

Index

H

I

J

L

M

N

O

P

R

S

V

W