

Firewall Management Center Virtual Administration et configuration initiale

Après avoir terminé le processus de configuration initiale de Firewall Management Center Virtual et vérifié sa réussite, nous vous recommandons d'effectuer diverses tâches administratives qui faciliteront la gestion de votre déploiement. Vous devez également effectuer toutes les tâches que vous avez ignorées lors de la configuration initiale, par exemple l'octroi de licences. Pour des informations détaillées sur l'une des tâches décrites dans les sections suivantes, ainsi que des renseignements sur la façon dont vous pouvez commencer à configurer votre déploiement, consultez les guides complets : Guide de configuration de Secure Firewall Management Center et pour votre version.

- Comptes d'utilisateurs individuels, à la page 1
- Enregistrement de l'appareil, à la page 2
- Politiques d'intégrité et politiques système, à la page 2
- Mises à jour logicielles et de base de données, à la page 3
- Dépannage, à la page 3

Comptes d'utilisateurs individuels

Après avoir terminé la configuration initiale, le seul utilisateur d'interface Web sur le système est l'utilisateur **admin**, qui a le rôle et l'accès administrateur. Les utilisateurs ayant ce rôle ont un accès complet au menu et à la configuration du système. Nous vous recommandons de limiter l'utilisation du compte **admin** (et du rôle d'administrateur) pour des raisons de sécurité et d'audit. Dans l'interface graphique Firewall Management Center Virtual, gérez les comptes utilisateur sur la page **System 'Système)** > **Users (Utilisateurs)** > **User (Utilisateur)**.

Remarque Les comptes **admin** permettant d'accéder à Firewall Management Center Virtual à l'aide de l'interface Shell et d'accéder à Firewall Management Center Virtual à l'aide de l'interface Web ne sont pas identiques et peuvent utiliser des mots de passe différents.

La création d'un compte distinct pour chaque personne qui utilise le système permet à votre organisation non seulement de vérifier les actions et les modifications effectuées par chaque utilisateur, mais aussi de limiter le rôle ou les rôles d'accès d'utilisateur associés à chaque personne. Cela est particulièrement important sur le Firewall Management Center Virtual, où vous effectuez la plupart de vos tâches de configuration et d'analyse.

Par exemple, un analyste a besoin d'accéder aux données d'événements pour analyser la sécurité de votre réseau, mais n'a peut-être pas besoin d'accéder aux fonctions d'administration du déploiement.

Le système inclut dix rôles utilisateur prédéfinis conçus pour divers administrateurs et analystes de l'interface Web. Vous pouvez également créer des rôles utilisateur personnalisés avec des privilèges d'accès spécialisés.

Enregistrement de l'appareil

Le On-Prem Firewall Management Center peut gérer n'importe quel périphérique, physique ou virtuel, actuellement pris en charge par le système :

- Firewall Threat Defense : fournit un pare-feu unifié de prochaine génération et un périphérique IPS de prochaine génération.
- Firewall Threat Defense Virtual : un périphérique virtuel de 64 bits conçu pour fonctionner dans plusieurs environnements hyperviseur, réduire les frais administratifs et accroître l'efficacité opérationnelle.
- Cisco Pare-feu ASA avec services FirePOWER (ou un module ASA FirePOWER) : fournit la politique système de première ligne et transmet le trafic au système pour la découverte et le contrôle d'accès. Cependant, vous ne pouvez pas utiliser l'interface Web On-Prem Firewall Management Center pour configurer les interfaces ASA FirePOWER. Cisco Pare-feu ASA avec services FirePOWER dispose d'un logiciel et d'une interface de ligne de commande uniques à la plateforme ASA que vous pouvez utiliser pour installer le système et effectuer d'autres tâches administratives spécifiques à la plateforme.
- Périphériques séries 7000 et 8000 : périphériques physiques conçus pour le système. Les périphériques séries 7000 et 8000 offrent une gamme de débits, tout en partageant la plupart des mêmes capacités. En général, les périphériques Série 8000 sont plus puissants que les périphériques Série 7000 ; ils prennent également en charge des fonctionnalités supplémentaires telles que les règles fastpath Série 8000, l'agrégation de liens et le stacking. Vous devez configurer la gestion à distance sur le périphérique avant de pouvoir l'enregistrer sur le On-Prem Firewall Management Center.
- NGIPSv : un périphérique virtuel de 64 bits déployé dans l'environnement VMware VSphere. Les périphériques NGIPSv ne prennent en charge aucune des fonctionnalités matérielles du système, comme la redondance et le partage des ressources, la commutation et le routage.

Pour enregistrer des périphériques gérés sur le On-Prem Firewall Management Center, utilisez la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** sur l'interface graphique utilisateur du On-Prem Firewall Management Center ; consultez les informations de gestion des périphériques dans le guide de configuration de Secure Firewall Management Center pour votre version.

Politiques d'intégrité et politiques système

Par défaut, tous les appareils ont une politique système initiale appliquée. La politique de système régit les paramètres susceptibles d'être similaires pour plusieurs périphériques d'un déploiement, tels que les préférences d'hôte de relais de messagerie et les paramètres de synchronisation de l'heure. Nous vous recommandons d'utiliser le On-Prem Firewall Management Center pour appliquer la même stratégie système à lui-même et à tous les périphériques qu'il gère.

Par défaut, le On-Prem Firewall Management Center dispose également d'une politique d'intégrité. Une politique d'intégrité, dans le cadre de la fonctionnalité de surveillance de l'intégrité, fournit les critères permettant au système de surveiller en permanence les performances des périphériques de votre déploiement.

Nous vous recommandons d'utiliser le On-Prem Firewall Management Center pour appliquer une stratégie d'intégrité à tous les périphériques qu'il gère.

Mises à jour logicielles et de base de données

Vous devez mettre à jour le logiciel système sur vos périphériques avant de commencer tout déploiement. Nous recommandons que tous les périphériques de votre déploiement exécutent la version la plus récente du système. Si vous les utilisez dans votre déploiement, vous devez également installer les dernières mises à jour des règles de prévention des intrusions, VDB et GeoDB.

Mise en garde Avant de mettre à jour une partie du système, vous devez lire les notes de version ou le texte d'avis qui accompagne la mise à jour. Les notes de version fournissent des informations importantes, notamment sur les plateformes prises en charge, la compatibilité, les conditions préalables, les avertissements, et les instructions d'installation et de désinstallation spécifiques.

Si votre On-Prem Firewall Management Center exécute les versions 6.5 et ultérieures :

Dans le cadre de la configuration , le On-Prem Firewall Management Center établit les activités suivantes pour maintenir votre système à jour et vos données sauvegardées :

- Mises à jour automatiques hebdomadaires de GeoDB
- Tâche hebdomadaire visant à télécharger les mises à jour logicielles pour le On-Prem Firewall Management Center et ses périphériques gérés.

Important Cette tâche ne télécharge que les mises à jour logicielles sur le On-Prem Firewall Management Center. Il est de votre responsabilité d'installer les mises à jour téléchargées par cette tâche. Voir le *Guide de mise à niveau de Cisco Secure Firewall Management Center* pour obtenir plus d'information.

- Une tâche hebdomadaire planifiée pour effectuer une sauvegarde de la configuration stockée uniquement localement de On-Prem Firewall Management Center.

Si votreOn-Prem Firewall Management Center exécute les versions 6.6 et ultérieures, dans le cadre de la configuration initiale, le On-Prem Firewall Management Center télécharge et installe la dernière mise à jour de la base de données des vulnérabilités (VDB) à partir du site d'assistance de Cisco. Il s'agit d'une opération unique.

Vous pouvez suivre l'état de ces activités à l'aide de l'interface Web du centre de messages. Si le système ne parvient pas à configurer l'une de ces activités et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de configurer ces activités vous-même, comme décrit dans le *guide de configuration de Cisco Secure Firewall Management Center* pour votre version.

Dépannage

Cette section décrit des étapes de dépannage de base liées à votre déploiement du Firewall Management Center Virtual sur votre machine virtuelle.

Échec de connexion SSH

Le Firewall Management Center Virtual est entièrement opérationnel, l'interface utilisateur et la connexion à la console fonctionnent correctement, à l'exception de la connexion SSH . Dans certains cas, les fichiers clés d'hôte SSH peuvent être corrompus lors du démarrage initial de Firewall Management Center Virtual, ce qui entraîne des échecs de connexion SSH .

Vous pouvez vérifier les indicateurs suivants qui suggérent un échec de la connexion SSH :

1. Une erreur d'E/S de disque peut se produire lors du démarrage initial de Firewall Management Center Virtual, en particulier au démarrage du daemon SSH (sshd). Il en résulte que les fichiers clés SSH (fichiers ssh_host* générés par sshd) sont vides.

   ls -lrt /etc/ssh total 16

   ```
   -rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
   -rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
   -rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
   -rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
   ```

2. Pour le problème d'E/S de disque, vous pouvez vérifier le fichier `/var/log/messages`, qui peut contenir des données erronées (indiquant une erreur d'E/S) près de l'horodatage de génération des clés.

Pour résoudre la défaillance SSH qui pourrait se produire lors du démarrage initial de Firewall Management Center Virtual, comme décrit ci-dessus, vous devez effectuer les étapes suivantes :

1. Connectez-vous à Firewall Management Center Virtual.
2. Exécutez la commande **sudo reboot** en mode **expert** sur l'interface de ligne de commande Firewall Management Center Virtual pour lancer un redémarrage progressif.
3. Exécutez la commande suivante pour supprimer les fichiers de clé SSH vides :

   ```
   cd /etc/ssh/
   rm ssh_host*
   ```

4. Exécutez la commande suivante pour redémarrer le service `sshd` afin de régénérer les fichiers de clé SSH correctement.

   ```
   /etc/rc.d/init.d/sshd stop
   /etc/rc.d/init.d/sshd start
   ```



Remarque Suivez les étapes de cette solution de contournement uniquement si vous êtes sûr que les fichiers de clé SSH sont vides. Si vous avez des doutes, il est conseillé de soumettre un dossier au TAC pour une enquête plus approfondie.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.