

Configuration initiale Firewall Management Center Virtual

Ce chapitre décrit le processus de configuration initiale que vous devez effectuer après avoir déployé l'appareil Firewall Management Center Virtual.

- On-Prem Firewall Management Center Configuration initiale à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 1
- Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures, à la page 4
- Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 8

On-Prem Firewall Management Center Configuration initiale à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures

Après avoir déployé un Firewall Management Center Virtual, vous pouvez accéder à la console de l'appareil pour la configuration initiale.Vous pouvez effectuer la configuration initiale à l'aide de l'interface de ligne de commande au lieu d'utiliser l'interface Web. Vous devez effectuer un assistant de configuration initiale qui configure le nouveau périphérique pour qu'il communique sur votre réseau de gestion de confiance. L' assistant vous demande d'accepter le contrat de licence d'utilisateur final (CLUF) et de changer le mot de passe administrateur.

Avant de commencer

- Assurez-vous que les informations suivantes sont nécessaires pour que le Firewall Management Center Virtual communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4 :

    L'interface On-Prem Firewall Management Center est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour connaître l'adresse IP que le DHCP attribue à l'adresse MAC On-Prem Firewall Management Center. Dans les scénarios où aucun DHCP n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.

  - Un masque réseau et une passerelle par défaut (si vous n'utilisez pas DHCP).

Procédure

Étape 1 Connectez-vous au Firewall Management Center Virtual sur la console en utilisant **admin** comme nom d'utilisateur et **Admin123** comme mot de passe pour le compte **admin**. Remarque : les mots de passe sont sensibles à la casse.

Étape 2 Lorsque vous y êtes invité, appuyez sur **Entrée** pour afficher le contrat de licence de l'utilisateur final (CLUF).

Étape 3 Passez en revue le CLUF. Lorsque vous y êtes invité, saisissez **`Yes (oui)`**, **`Yes (oui`**) ou appuyez sur **Enter** (Entrée) pour accepter le CLUF.

Important
Vous ne pouvez pas continuer sans accepter le CLUF. Si vous répondez par autre chose que **`Yes (oui)`**, **`Yes (oui`**) ou **Enter** (Entrée), le système vous déconnecte.

Étape 4 Pour assurer la sécurité et la confidentialité du système, la première fois que vous vous connectez à On-Prem Firewall Management Center, vous devez changer le mot de passe **admin**. Lorsque le système demande un nouveau mot de passe, saisissez un nouveau mot de passe conforme aux restrictions affichées, puis saisissez à nouveau le même mot de passe lorsque le système demande une confirmation.

Remarque
Le On-Prem Firewall Management Center compare votre mot de passe à un dictionnaire de craquage qui vérifie non seulement de nombreux mots du dictionnaire, mais aussi d'autres chaînes de caractères qui pourraient être facilement déchiffrées à l'aide de techniques courantes d'intrusion de mots de passe. Par exemple, le script de configuration initiale peut rejeter des mots de passe tels que « abcdefg » ou « passw0rd ».

Remarque
À l'achèvement du processus de configuration initiale, le système définit les mots de passe des deux comptes **d'administrateur** (un pour l'accès Web et l'autre pour l'accès à l'interface de ligne de commande) à la même valeur, conformément aux exigences relatives aux mot de passe sécurisés décrites dans le *Guide d'administration de Cisco Secure Firewall Management Center* pour votre version. Si vous modifiez les mots de passe de l'un ou l'autre des comptes **administrateurs** par la suite, ils ne seront plus identiques et l'exigence relative au mot de passe fort peut être supprimée du compte **administrateur** de l'interface Web.

Étape 5 Répondez aux invites pour configurer les paramètres réseau.

Lorsque vous suivez les invites, pour les questions à choix multiples, vos options sont répertoriées entre parenthèses, par exemple (**`o/n`**) pour oui ou non. Les valeurs par défaut sont indiquées entre crochets, par exemple [**`o`**]. Notez les éléments suivants lorsque vous répondez aux invites :

- Appuyez sur **Enter** (Entrée) à une invite pour accepter la valeur par défaut.
- Pour le nom d'hôte, indiquez un nom de domaine complet (`<hostname>.<domain>`) ou le nom d'hôte. Ce champ est obligatoire.
- Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)**pour réinitialiser le réseau.
- Si vous choisissez de configurer IPv4 manuellement, le système vous demandera l'adresse IPv4, le masque réseau et la passerelle par défaut.

- La configuration d'un serveur DNS est facultative ; pour spécifier aucun serveur DNS, saisissez **None** (aucun). Sinon, spécifiez les adresses IPv4 pour un ou deux serveurs DNS. Si vous spécifiez deux adresses, séparez-les par une virgule. (Si vous spécifiez plus de deux serveurs DNS, le système ignore les entrées supplémentaires.) Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser de DNS en dehors de votre réseau local.

  Remarque
  Si vous utilisez une licence d'évaluation, le fait de préciser que DNS est facultatif pour le moment, mais requis pour des licences permanentes.

- Vous devez saisir le nom de domaine complet ou l'adresse IP pour au moins un serveur NTP accessible à partir de votre réseau. (Vous ne pouvez pas préciser de noms de domaine complets pour les serveurs NTP si vous n'utilisez pas DHCP.) Vous pouvez définir deux serveurs (un principal et un secondaire) ; séparez les informations par une virgule. (Si vous spécifiez plus de deux serveurs DNS, le système ignore les entrées supplémentaires.) Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser un serveur NTP en dehors de votre réseau local.

Exemple :

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

Étape 6 Le système affiche un résumé de vos sélections de configuration . Passez en revue les paramètres que vous avez saisis.

Exemple :

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

Étape 7 La dernière invite vous donne la possibilité de confirmer les paramètres.

- Si les paramètres sont corrects, saisissez **o** et appuyez sur **Enter** (Entrée) pour accepter les paramètres et continuer.
- Si les paramètres sont incorrects, saisissez **n** et appuyez sur **Enter** (Entrée). Le système demande de nouveau les informations, en commençant par le nom d'hôte.

Exemple :

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

Étape 8 Après avoir accepté les paramètres, vous pouvez saisir **exit** (sortie) pour quitter l'interface de ligne de commande On-Prem Firewall Management Center.

Prochaine étape

- Vous pouvez vous connecter à l'interface Web Firewall Management Center Virtual en utilisant les informations sur le réseau que vous venez de configurer.
- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 8 .

Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures

Après avoir déployé Firewall Management Center Virtual, vous pouvez effectuer la configuration initiale en utilisant HTTPS sur l'interface Web de l'appareil.

Lorsque vous vous connectez à l'interface Web On-Prem Firewall Management Center pour la première fois, le On-Prem Firewall Management Center présente un assistant de configuration initiale pour vous permettre de configurer rapidement et facilement les paramètres de base du périphérique. Cet assistant se compose de trois écrans et d'une boîte de dialogue contextuelle :

- Le premier écran vous force à modifier le mot de passe de l'utilisateur **admin** à partir de la valeur par défaut de **Admin123**.
- Le deuxième écran présente le contrat de licence d'utilisateur final (CLUF) que vous devez accepter avant d'utiliser l'appareil.
- Le troisième écran vous permet de modifier les paramètres réseau de l'interface de gestion des appareils. Cette page est préremplie avec les paramètres actuels, que vous pouvez modifier.
- L' assistant effectue la validation des valeurs que vous saisissez dans cet écran pour confirmer les éléments suivants :
  - Correction syntaxique
  - Compatibilité des valeurs saisies (par exemple, adresse IP et passerelle compatibles, ou DNS fourni lorsque les serveurs NTP sont précisés à l'aide de FQDN)
  - Connectivité réseau entre le Firewall Management Center Virtual et les serveurs DNS et NTP

  L' assistant affiche les résultats de ces tests en temps réel à l'écran, ce qui vous permet d'apporter des corrections et de tester la fiabilité de votre configuration avant de cliquer sur **Finish** (Terminer) au bas de l'écran. Les tests de connectivité NTP et DNS ne sont pas bloquants ; vous pouvez cliquer sur **Terminer** avant que l' assistant ne termine les tests de connectivité . Si le système signale un problème de connectivité après que vous ayez cliqué sur **Finish** (Terminer), vous ne pouvez pas modifier les paramètres dans l' assistant, mais vous pouvez configurer ces connexions à l'aide de l'interface Web après avoir terminé la configuration initiale.

  Le système n'effectue pas de tests de connectivité si vous saisissez des valeurs de configuration qui conduiraient à couper la connexion existante entre le Firewall Management Center Virtual et le navigateur. Dans ce cas, l' assistant n'affiche aucune information sur l'état de connectivité pour le DNS ou le NTP.

- Après avoir terminé les trois écrans, une boîte de dialogue contextuelle s'affiche et vous permet de configurer rapidement et facilement les licences Smart.

Lorsque vous avez terminé l'assistant de configuration initial et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans « Device Management » (gestion des périphériques) dans le Guide de configuration Cisco Secure Firewall Management Center Device pour votre version.

Avant de commencer

- Assurez-vous que les informations suivantes sont nécessaires pour que le On-Prem Firewall Management Center communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4.

    L'interface On-Prem Firewall Management Center est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour déterminer l'IP attribuée par DHCP à l'adresse MAC On-Prem Firewall Management Center. Dans les scénarios où aucun DHCP n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.

  - Un masque réseau et une passerelle par défaut (si vous n'utilisez pas DHCP).
- Si vous n'utilisez pas DHCP, configurez un ordinateur local avec les paramètres réseau suivants :
  - Adresse IP : 192.168.45.2
  - Masque réseau : 255.255.255.0
  - La passerelle par défaut est 192.168.45.1.

  Désactivez toutes les autres connexions réseau sur cet ordinateur.

Procédure

Étape 1 À l'aide d'un navigateur, accédez à l'adresse IP du Firewall Management Center Virtual :*https://<Management Center-IP>*.

La page d'ouverture de session s'affiche.

Étape 2 Connectez-vous au Firewall Management Center Virtual en utilisant **admin** comme nom d'utilisateur et **Admin123** comme mot de passe pour le compte admin. (Les mots de passe sont sensibles à la casse.)

Étape 3 À l'écran **de modification du mot de passe** :

a) (Facultatif), cochez la case **Show password** (afficher le mot de passe) pour voir le mot de passe lorsque vous utilisez cette boîte de dialogue.

b) Cliquez sur **Generate Password** (générer un mot de passe) pour que le système crée un mot de passe conforme aux critères de la liste. (Les mots de passe générés ne sont pas mnémoniques ; prenez soin de noter le mot de passe si vous choisissez cette option.)

c) Pour définir le mot de passe de votre choix, saisissez un nouveau mot de passe dans les zones de texte **New Password** (Nouveau mot de passe) et **Confirm Password** (Confirmer le mot de passe).

Le mot de passe doit être conforme aux critères énumérés dans la boîte de dialogue.

Remarque
Le On-Prem Firewall Management Center vérifie les mots de passe à l'aide d'un dictionnaire spécial contenant non seulement de nombreux mots du dictionnaire, mais aussi d'autres chaînes de caractères qui pourraient être facilement déchiffrées à l'aide de techniques courantes d'intrusion de mots de passe. Par exemple, le script de configuration initiale peut rejeter des mots de passe tels que « abcdefg » ou « passw0rd ».

Remarque
À l'achèvement du processus de configuration initiale, le système définit les mots de passe des deux comptes d' **administrateur** (un pour l'accès Web et l'autre pour l'accès à l'interface de ligne de commande) à la même valeur. Le mot de passe doit être conforme aux exigences décrites dans le Guide d'administration Cisco Secure Firewall Management Center de votre version. Si vous modifiez les mots de passe de l'un ou l'autre des comptes **administrateurs** par la suite, ils ne seront plus identiques et l'exigence relative au mot de passe fort peut être supprimée du compte **administrateur** de l'interface Web.

d) Cliquez sur **Next** (suivant).

Une fois que vous avez cliqué sur **Next** (Suivant) sur l'écran **Change Password** (modifier le mot de passe) et que l'assistant a accepté le nouveau mot de passe **admin**, ce mot de passe est en vigueur pour l'interface Web et les comptes **admin** de l'interface de ligne de commande, même si vous ne terminez pas les activités restantes de l'assistant.

Étape 4 À l'écran du **contrat d'utilisateur**, lisez le CLUF et cliquez sur **Accept** (accepter) pour continuer.

Si vous cliquez sur **Decline** (Refuser), l'assistant vous déconnecte de Firewall Management Center Virtual.

Étape 5 Cliquez sur **Next** (suivant).

Étape 6 À l'écran **de modification des paramètres réseau** :

a) Saisissez un **nom de domaine complet (FQDN)**. Si la valeur par défaut s'affiche, vous pouvez l'utiliser si elle est compatible avec la configuration de votre réseau. Sinon, saisissez un nom de domaine complet (syntaxe `<hostname>.<domain>`) ou le nom d'hôte.

b) Choisissez le protocole de démarrage pour l'option **Configure IPv4** (Configuration IPv4), soit **à l'aide de DHCP**, soit **à l'aide de Static/Manual**.

Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)**pour réinitialiser le réseau.

c) Acceptez la valeur affichée, si une est affichée, pour **l'adresse IPv4** ou saisissez une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 192.168.45.45).

Remarque
Si vous modifiez l'adresse IP pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

d) Acceptez la valeur affichée, le cas échéant, pour **le masque réseau** ou saisissez une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 255.255.0.0).

Remarque
Si vous modifiez le masque réseau pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

e) Vous pouvez accepter la valeur affichée, le cas échéant, pour **la passerelle** ou saisir une nouvelle passerelle par défaut. Utilisez la forme décimale à points (par exemple, 192.168.0.1).

Remarque
Si vous modifiez l'adresse de la passerelle pendant la configuration initiale, vous devrez peut-être vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

f) (Facultatif) Pour le **groupe DNS,** vous pouvez accepter la valeur par défaut, **Cisco Umbrella DNS**.

Pour modifier les paramètres DNS, choisissez **Custom DNS Servers** (serveurs DNS personnalisés) dans la liste déroulante et saisissez les adresses IPv4 pour le **DNS principal** et le **DNS secondaire**. Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser de DNS en dehors de votre réseau local. Configurez le serveur DNS en sélectionnant **Custom DNS Servers** (serveurs DNS personnalisés) dans la liste déroulante et en supprimant les champs **Primary DNS** (DNS principal) et **Secondary DNS** (DNS secondaire).

Remarque
Si vous utilisez des noms de domaine complets plutôt que des adresses IP pour spécifier des serveurs NTP, vous devez préciser le DNS à ce moment. Si vous utilisez une licence d'évaluation, le DNS est facultatif, mais le DNS est requis pour utiliser des licences permanentes pour votre déploiement.

g) Pour les **serveurs de groupe NTP** vous pouvez accepter la valeur par défaut, **Default NTP Servers** (Serveurs NTP par défaut). Dans ce cas, le système utilise **0.sourcefire.pool.ntp.org** comme serveur NTP principal et **1.sourcefire.pool.ntp.org** comme serveur NTP secondaire.

Pour configurer d'autres serveurs NTP, choisissez **Custom NTP Group Servers** (serveurs de groupe NTP personnalisés) dans la liste déroulante et saisissez les noms de domaine complets ou les adresses IP d'un ou deux serveurs NTP accessibles à partir de votre réseau. Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser un serveur NTP en dehors de votre réseau local.

Remarque
Si vous modifiez les paramètres réseau pendant la configuration initiale, vous devez vous reconnecter au On-Prem Firewall Management Center en utilisant les nouvelles informations réseau.

Étape 7 Cliquez sur **Finish** (terminer).

L' assistant effectue la validation des valeurs que vous saisissez sur cet écran pour confirmer l'exactitude syntaxique, la compatibilité des valeurs saisies et la connectivité réseau entre le On-Prem Firewall Management Center et les serveurs DNS et NTP. Si le système signale un problème de connectivité après que vous ayez cliqué sur **Finish** (Terminer), vous ne pouvez pas modifier les paramètres dans l' assistant, mais vous pouvez configurer ces connexions à l'aide de l'interface Web On-Prem Firewall Management Center après avoir terminé la configuration initiale.

Prochaine étape

- Le système affiche une fenêtre contextuelle qui vous permet de configurer rapidement et facilement les licences Smart. L'utilisation de cette boîte de dialogue est facultative; si votre Firewall Management Center Virtual gère des périphériques Cisco Firewall Threat Defense et que vous connaissez bien les licences Smart, utilisez cette boîte de dialogue. Sinon, ignorez cette boîte de dialogue et consultez la section « Licences » dans le Guide d'administration Cisco Secure Firewall Management Center de votre version.
- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 8 .

- Une fois que vous avez terminé l'assistant de configuration initial et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans le *Guide de configuration des périphériques de Cisco Secure Firewall Management Center*.

Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures

Dans le cadre de la configuration initiale (qu'elle soit effectuée par l'intermédiaire de l'assistant de configuration initial ou de l'interface de ligne de commande), le On-Prem Firewall Management Center configure automatiquement les tâches de maintenance pour maintenir votre système à jour et vos données sauvegardées.

Ces tâches sont planifiées en UTC, ce qui signifie que le moment où elles se produisent *localement* dépend de la date et de votre emplacement spécifique. En outre, étant donné que les tâches sont planifiées en heure UTC, elles ne s'ajustent pas à l'heure avancée, à l'heure d'été, ni à tout autre ajustement saisonnier propre à votre emplacement. Si vous êtes concerné, les tâches planifiées se produisent une heure « ultérieurement » en été qu'en hiver, en fonction de l'heure locale.

Remarque Nous vous recommandons *fortement* de passer en revue les configurations de la planification automatique, de confirmer que On-Prem Firewall Management Center les a établies avec succès et de les ajuster si nécessaire.

- Mises à jour hebdomadaires de GeoDB

  Le On-Prem Firewall Management Center planifie automatiquement les mises à jour de la GeoDB chaque semaine, à une heure aléatoire déterminée. Vous pouvez observer l'état de cette mise à jour à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette mise à jour automatique dans l'interface Web sous **Système** > **Mises à jour** > **Mises à jour de géolocalisation**>**RecurRING Geolocation Updates** (Mises à jour de géolocalisation récurrentes). Si le système ne parvient pas à configurer la mise à jour et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de configurer des mises à jour régulières de GeoDB comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version.

- Mises à jour logicielles On-Prem Firewall Management Center hebdomadaires

  Le On-Prem Firewall Management Centerplanifie automatiquement une tâche hebdomadaire pour télécharger la version logicielle la plus récente pour le On-Prem Firewall Management Center et ses périphériques gérés. Cette tâche est planifiée pour se produire entre 2 et 3 h, heure UTC, le dimanche matin. Selon la date et votre emplacement, cela peut correspondre du samedi après-midi au dimanche après-midi en heure locale. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Outils** > **Planification**. Si la planification des tâches échoue et que votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de planifier une tâche récurrente pour le téléchargement des mises à jour logicielles, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version.

  Cette tâche télécharge uniquement les correctifs et mises à jour urgentes (hotfix) pour la version actuellement exécutée par vos appliances ; il vous revient d'installer les mises à jour téléchargées par cette tâche. Voir le *Guide de mise à niveau de Cisco On-Prem Firewall Management Center* pour obtenir plus d'information.

- Sauvegarde hebdomadaire de la configuration On-Prem Firewall Management Center

  Le On-Prem Firewall Management Center planifie automatiquement une tâche hebdomadaire pour effectuer une sauvegarde de la configuration uniquement stockée localement à 2 h UTC le lundi matin ; Selon la date et votre emplacement, cela peut se produire à tout moment, du samedi après-midi au dimanche après-midi à l'heure locale. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Outils** > **Planification**. Si la planification des tâches échoue, nous vous recommandons de planifier une tâche récurrente pour effectuer une sauvegarde, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

- Mise à jour de la base de données de vulnérabilités

  Dans les versions 6.6 et ultérieures, 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 observer l'état de cette mise à jour à l'aide de l'interface Web du centre de messages. Pour maintenir votre système à jour, si votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de planifier des tâches pour effectuer des téléchargements et des installations de mises à jour automatiques récurrentes de la VDB, comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

- Mise à jour quotidienne des règles d'intrusion

  Dans les versions 6.6 et ultérieures, le On-Prem Firewall Management Center configure une mise à jour quotidienne automatique des règles de prévention des intrusions à partir du site d'assistance de Cisco. La solution On-Prem Firewall Management Center déploie les mises à jour automatiques des règles d'intrusion sur les appareils gérés ciblés lors du prochain déploiement des politiques concernées. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Vous pouvez voir la configuration pour cette tâche dans l'interface Web sous **Système** > **Mises à jour** > **Mises à jour des règles**. Si la configuration de la mise à jour échoue et que votre On-Prem Firewall Management Center dispose d'un accès Internet, nous vous recommandons de configurer les mises à jour régulières des règles de prévention des intrusions comme décrit dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

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.