Guide de démarrage pour Cisco Firepower Management Center 750, 1500, 2000, 3500 et 4000

Dernière mise à jour : 6 avril 2020

Ce guide est organisé comme suit :

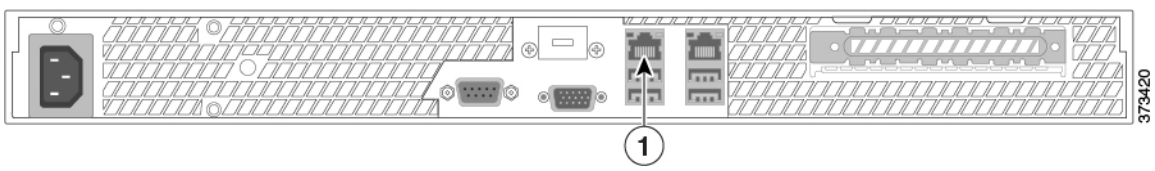
Contenu de l'emballage

Cette section dresse la liste des éléments inclus avec chaque modèle. Prenez note que le contenu pourrait changer et que votre emballage pourrait contenir plus ou moins d'éléments.

Modèles de châssis

- Firepower Centre de gestion 750 (modèle 1U). L'illustration suivante de l'arrière du châssis indique l'emplacement de l'interface de gestion sur un MC750.

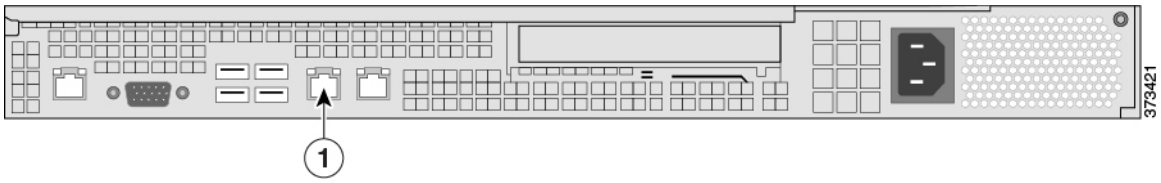
Figure 1 MC750 Châssis et interface de gestion



1	Interface de gestion		

- Firepower Centre de gestion 1500 (modèle 1U). L'illustration suivante de l'arrière du châssis indique l'emplacement de l'interface de gestion sur un MC1500.

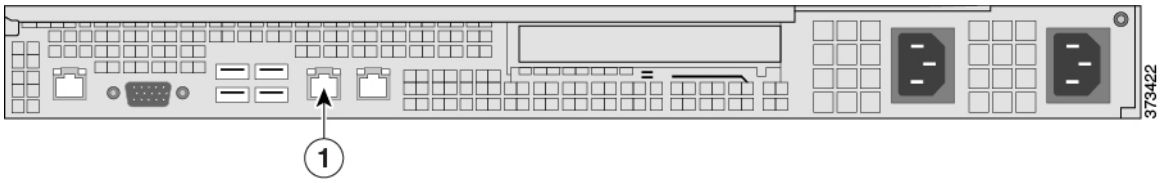
Figure 2 MCChâssis 1500 et interface de gestion



1	Interface de gestion		

- Firepower Centre de gestion 3500 (modèle 1U). L'illustration suivante de l'arrière du châssis indique l'emplacement de l'interface de gestion sur un MC3500.

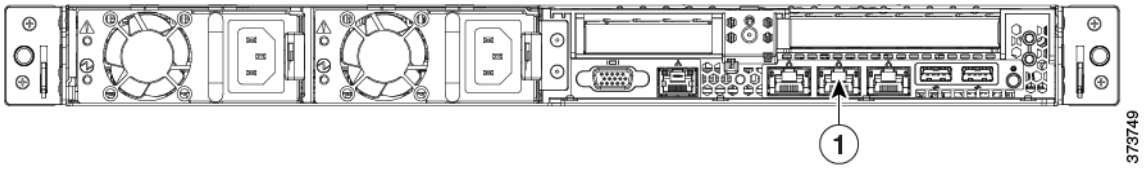
Figure 3 MCChâssis 3500 et interface de gestion



1	Interface de gestion		

- Firepower Centre de gestion 2000/4000 (modèle 1U). L'illustration suivante de l'arrière du châssis indique l'emplacement de l'interface de gestion.

Figure 4 MC 2000 et MC 4000



1	Interface de gestion		

Éléments inclus

- Un cordon d'alimentation par bloc d'alimentation.
- Un câble Ethernet Cat 5e droit par châssis.
- Un kit de montage en rack par châssis.

Exigences de licence

Vous pouvez obtenir des licences pour diverses fonctionnalités afin de créer un déploiement de système Firepower optimal pour votre organisation. Vous utilisez le Firepower Management Center pour gérer les licences pour lui-même et les périphériques qu'il gère. Les types de licences proposés par le système Firepower dépendent du type de périphérique que vous souhaitez gérer :

Licences traditionnelles

Pour les séries 7000 et 8000, ASA FirePOWER et NGIPSv, vous devez utiliser des licences classiques. Les périphériques qui utilisent des licences Classic sont parfois appelés périphériques Classic.

Si votre FMC utilise une version de Firepower antérieure à 6.5 : Cisco , il est recommandé d'utiliser la page de configuration initiale pour ajouter les licences classiques achetées par votre organisation; voir Paramètres des licences, page 17. Si vous n'ajoutez pas les licences classiques lors de la configuration initiale, tous les appareils que vous enregistrez pendant cette configuration seront ajoutés à Centre de gestion comme non licenciés; vous devrez les attribuer une licence individuellement une fois le processus de configuration initiale terminé. Notez que si vous configurez un appareil recréé et que vous avez conservé vos paramètres de licence dans le cadre du processus de restauration, cette section de la page de configuration initiale peut être préremplie.

Si votre FMC utilise la version Firepower 6.5 ou ultérieure : Vous devez ajouter des licences classiques pour les appareils gérés après avoir terminé l'assistant de configuration initiale. Vous pouvez attribuer des licences aux appareils gérés lorsque vous les enregistrez dans le Firepower Management Center, ou après les avoir enregistrés dans le Firepower Management Center.

Licences Smart

Pour les périphériques Firepower Threat Defense physiques et virtuels, vous devez utiliser des licences Smart.

Cisco Smart Software Licensing vous permet d'acheter et de gérer un ensemble de licences de manière centralisée. Contrairement aux licences de clé d'autorisation de produit (PAK), les licences Smart ne sont pas liées à un numéro de série ou à une clé de licence spécifique. Les licences Smart vous permettent d'évaluer votre utilisation et vos besoins en licences en un clin d'œil.

Le *Guide de configuration de Firepower Management Center* fournit de plus amples renseignements sur les licences Classic et les licences Smart, les types de licences pour chaque classe et la façon de gérer les licences dans votre déploiement.

Accédez à la CLI ou au Shell Linux sur le FMC

L'accès à l'interface CLI du FMC ou à l'environnement Linux nécessite une séquence d'étapes différente selon la version de Firepower exécutée par le FMC. Consultez cette rubrique lorsque ce document vous demande d'ouvrir une session dans l'interface CLI du FMC ou dans l'environnement Linux.

Mise en garde : Nous recommandons fortement de ne pas utiliser l'environnement Linux, sauf si le TAC vous le demande ou si des instructions explicites dans la documentation utilisateur vous y invitent.

Avant de commencer

Établissez une connexion physique directe avec le FMC à l'aide d'un clavier et d'un moniteur, ou établissez une session SSH avec l'interface de gestion du FMC.

Procédure

.1 Ouvrez une session sur le FMC à l'aide des identifiants de l'utilisateur **administrateur** CLI.

Déterminez votre prochaine action en fonction de la version Firepower utilisée :

– Si votre FMC exécute Firepower version 5.4 à 6.2.x, vous accédez directement à l'environnement Linux.

- Si votre FMC exécute Firepower version 6.3.x ou 6.4.x et que l'interface CLI du FMC n'est pas activée, vous accédez directement à l'environnement Linux.
- Si votre FMC exécute Firepower version 6.3.x ou 6.4.x et que l'interface CLI du FMC est activée, vous accédez à l'interface CLI du FMC. Pour accéder à l'interface Shell Linux , passez à l'étape 2.
- Si votre FMC exécute la version Firepower 6.5 ou une version ultérieure, cela vous donne accès à l'interface de ligne de commande du FMC. Pour accéder à l'interface Shell Linux , passez à l'étape 2.

.2 Pour accéder à l'interface à partir de l'interface CLI du FMC, saisissez la commande **expert**.

Installation et configuration initiale pour les versions 6.5 et ultérieures

Remarque : Les versions Firepower 6.5 et ultérieures ne sont pas prises en charge sur les modèles FMC 750, 1500 et 3500.

La première fois que vous vous connectez au FMC avec la version 6.5 ou ultérieure, un assistant de configuration initiale s'affiche. Il vous guide dans la configuration du nouvel appareil afin qu'il puisse communiquer sur votre réseau de gestion de confiance. L'assistant présente un processus de configuration initiale simplifié et établit automatiquement des activités de maintenance hebdomadaires pour maintenir votre système à jour et vos données sauvegardées.

L'interface de gestion FMC est préconfigurée pour accepter une adresse IPv4 attribuée par le protocole DHCP (Dynamic Host Configuration Protocol). Si le FMC ne parvient pas à obtenir de bail DHCP, l'interface de gestion utilise une adresse IPv4 de repli de 192.168.45.45.

Remarque : Si vous vousconnectez à un FMC pour la première fois après une restauration du système et que vous avez choisi de conserver les licences et les paramètres réseau, l'adresse IP de l'interface de gestion demeure inchangée. Elle est identique à celle utilisée avant la restauration du système. Passez directement à Assistant de configuration initiale du centre du Firepower Management Center, page 7.

Pour installer et configurer un FMC utilisant la version 6.5 ou une version ultérieure :

.1 Installez le périphérique comme décrit dans Installation de l'appliance, page 4.

.2 Pour effectuer la configuration initiale, vous avez l'une des deux possibilités suivantes :

- Si votre réseau n'utilise pas DHCP et que votre PC ne peut pas joindre l'adresse de repli, la connexion initiale peut échouer. Il en va de même si l'adresse conservée après une restauration du système est inaccessible. Dans ce cas, nous recommandons d'effectuer la configuration initiale en connectant un ordinateur directement à l'interface de gestion physique du FMC. Suivez la procédure décrite dans la section correspondante de la documentationAccéder au Firepower Management Center à l'aide de l'interface de gestion, page 5.
- Si votre protocole DHCP local attribue une adresse au FMC, utilisez un clavier et un moniteur pour configurer le périphérique ; voir Accéder au Firepower Management Center à l'aide d'un clavier et d'un moniteur, page 6.

Installation de l'appliance

Ces instructions sont une version abrégée des étapes d'installation physique du périphérique. Pour plus de renseignements sur les instructions, consultez le *Guide d'installation du matériel pour Cisco Firepower Management Center 750, 1500, 2000, 3500 et 4000*.

Procédure

1. Montez l'appareil dans votre rack à l'aide de la trousse de montage et des instructions fournies.
2. Fixez les cordons d'alimentation aux deux blocs d'alimentation et branchez-les dans des sources d'alimentation distinctes.

   Si vous ne connectez pas les deux blocs d'alimentation, un indicateur d'avertissement ambre s'allume sur le panneau avant du châssis et l'interface Web du FMC affiche une alerte d'intégrité.
3. Mettez l'appareil sous tension en appuyant sur le commutateur d'alimentation situé sur le panneau avant.

   Après avoir enfoncé le commutateur d'alimentation, le périphérique peut s'allumer brièvement, puis sembler s'éteindre, à l'exception du voyant d'alimentation ambre sur le panneau avant du châssis. Cette situation est normale ; appuyez à nouveau sur le bouton d'alimentation pour mettre l'appareil sous tension avec le voyant d'alimentation vert.

Étape suivante

- L'interface de gestion FMC est préconfigurée pour accepter une adresse IPv4 attribuée par DHCP, mais ne parvient pas à obtenir de bail DHCP, l'interface de gestion utilise une adresse IPv4 de repli de192.168.45.45. Si vous vous connectez à un FMC pour la première fois après une restauration du système et que vous avez choisi de conserver les paramètres de licence et réseau, l'adresse IP demeure inchangée. Elle est la même que celle utilisée avant la restauration du système. Assurez-vous d'avoir établi l'une des méthodes suivantes pour accéder au périphérique avant de continuer :
  - Si votre réseau n'utilise pas DHCP et que votre PC ne peut pas joindre l'adresse de repli, la connexion initiale peut échouer. Il en va de même si l'adresse conservée après une restauration du système est inaccessible. Dans ce cas, nous recommandons d'effectuer la configuration initiale en connectant un ordinateur directement à l'interface de gestion physique du FMC. Suivez la procédure décrite dans la section correspondante de la documentation Accéder au Firepower Management Center à l'aide de l'interface de gestion, page 5.
  - Si votre protocole DHCP local attribue une adresse au FMC, utilisez un clavier et un moniteur pour configurer le périphérique ; voir Accéder au Firepower Management Center à l'aide d'un clavier et d'un moniteur, page 6.
- Effectuer le processus de configuration initiale ; voir Assistant de configuration initiale du centre du Firepower Management Center, page 7.
- Vous pouvez également utiliser la boîte de dialogue contextuelle Smart License pour configurer les licences Smart. Consultez Boîte de dialogue Licences Smart, page 9.
- Une fois que vous avez terminé le processus de configuration initiale, vous pouvez éventuellement configurer le FMC pour l'accès en série ou en série sur LAN (SOL); voir Rediriger la sortie de la console, page 21 et Configurer Lights-Out Management, page 22.

Après avoir terminé la configuration, vous utiliserez l'interface Web de Firepower Centre de gestion pour effectuer la plupart des tâches de gestion et d'analyse pour votre déploiement. Pour en savoir plus, consultez Recommandations d'administration, page 19.

Accéder au Firepower Management Center à l'aide de l'interface de gestion

L'interface de gestion du FMC est préconfigurée pour accepter une adresse IPv4 attribuée par DHCP, mais dans les scénarios où DHCP n'est pas impliqué, l'interface de gestion utilise l'adresse IPv4 192.168.45.45. Si vous vous connectez à un FMC pour la première fois après une restauration du système et que vous avez choisi de conserver les paramètres de licence et réseau, l'adresse IP demeure inchangée. Elle est la même que celle utilisée avant la restauration du système.

Avant de commencer

- Configurez un ordinateur local, qui ne doit pas être connecté à Internet, avec les paramètres réseau suivants :
  - Adresse IP : 192.168.45.2
  - Masque réseau : 255.255.255.0
  - Passerelle par défaut : 192.168.45.1
- Déterminez l'adresse IP attribuée à l'interface de gestion du FMC :
  - Si vous vous connectez à un FMC pour la première fois après avoir effectué une restauration du système (voir Restauration d'un Cisco Firepower Management Center aux valeurs d'usine par défaut, page 24), et que vous avez choisi de conserver les licences ainsi que les paramètres réseau, l'adresse IP ne change pas. Elle demeure identique à celle qui était configurée avant la restauration du système.
  - Sinon, l'adresse IP de l'interface de gestion FMC est 192.168.45.45.

Procédure

1. À l'aide du câble Ethernet fourni, connectez l'interface réseau de l'ordinateur préconfiguré directement à l'interface de gestion du périphérique.

   Vérifiez que le voyant DEL de liaison est activé pour l'interface réseau sur l'ordinateur local et pour l'interface de gestion du périphérique.

2. Utilisez un navigateur Web pour accéder à l'adresse IP de l'appareil :

   ```
   https://<Management IP Address>
   ```

   La page d'ouverture de session s'affiche.

3. Connectez-vous à l'interface Web en utilisant `admin` comme nom d'utilisateur et `Admin123` comme mot de passe. (Remarque : les mots de passe sont sensibles à la casse.)

Étape suivante

- Terminez le processus d'installation en utilisant les procédures dans Assistant de configuration initiale du centre du Firepower Management Center, page 7.

Accéder au Firepower Management Center à l'aide d'un clavier et d'un moniteur

Vous pouvez connecter un clavier USB et un moniteur VGA au périphérique, ce qui est utile pour les périphériques montés en rack connectés à un commutateur KVM (clavier, vidéo et souris). L'interface de gestion FMC est préconfigurée pour accepter une adresse IPv4 attribuée par DHCP, mais ne parvient pas à obtenir de bail DHCP, l'interface de gestion utilise une adresse IPv4 de repli de192.168.45.45. Si votre réseau n'utilise pas DHCP et que votre PC ne peut pas atteindre cette adresse, nous vous recommandons d'effectuer la configuration initiale en vous connectant directement au FMC, comme décrit dans Accéder au Firepower Management Center à l'aide de l'interface de gestion, page 5.

Avant de commencer

Déterminez l'adresse IP attribuée à l'interface de gestion du FMC :

- Si vous configurez un nouveau FMC pour la première fois, vérifiez auprès de votre administrateur réseau pour déterminer l'adresse IP que le DHCP attribuera à l'adresse MAC du FMC lorsque vous le connectez au réseau local. (Vous pouvez trouver l'adresse MAC sur une étiquette ou une carte amovible sur le périphérique.)

- S'il n'y a pas de DHCP ou si le DHCP n'a pas d'adresses libres dans son ensemble, l'interface de gestion FMC utilise l'adresse IP 192.168.45.45. Dans ce cas, si votre PC ne peut pas atteindre cette adresse nous vous recommandons d'effectuer la configuration initiale en vous connectant directement au FMC, comme décrit dans Accéder au Firepower Management Center à l'aide de l'interface de gestion, page 5.
- Si vous vous connectez à un FMC pour la première fois après avoir effectué une restauration du système (voir Restauration d'un Cisco Firepower Management Center aux valeurs d'usine par défaut, page 24) et que vous avez choisi de conserver les licences et les paramètres réseau, l'adresse IP est la même que celle qu'elle était avant d'effectuer la restauration du système.

Procédure

1. À l'aide du câble Ethernet fourni, connectez l'interface de gestion à l'arrière du FMC à un réseau de gestion protégé.
2. Utilisez un navigateur Web pour accéder à la page de connexion à l'interface Web du FMC :

   ```
   https://<Management IP Address>
   ```

   La page d'ouverture de session s'affiche.
3. Utilisez le nom d'utilisateur `admin` et le mot de passe `Admin123` pour vous connecter. Remarque : les mots de passe sont sensibles à la casse.

Étape suivante

- Terminez le processus d'installation en utilisant les procédures dans Assistant de configuration initiale du centre du Firepower Management Center, page 7.

Assistant de configuration initiale du centre du Firepower Management Center

Lorsque vous vous connectez à l'interface Web du FMC pour la première fois sur un nouvel appareil, ou un appareil sur lequel vous venez d'effectuer une restauration du système, le FMC 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 :

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

Lorsque vous avez terminé l'assistant de configuration initiale et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans « Device Management Basics » dans le *Guide de configuration de Firepower Management Center* pour votre version.

Pour assurer la sécurité et la confidentialité du système, la première fois que vous vous connectez à l'FMC, vous devez changer le mot de passe `admin`. Lorsque l'écran de l'assistant de modification du mot de passe s'affiche, vous avez deux options :

- 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.

- 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.)

Cochez la case **Show password** (afficher le mot de passe) pour voir le mot de passe lorsque vous utilisez cet écran. L'assistant affiche une liste de critères que le nouveau mot de passe doit satisfaire; une coche verte s'affiche à côté de chaque critère rempli. Si le nouveau mot de passe ne répond pas à tous les critères répertoriés, l'assistant rejette le mot de passe et vous empêche de passer à la page suivante.

Le FMC compare votre mot de passe à un dictionnaire utilisé pour casser les mots de passe. Ce dictionnaire vérifie non seulement un grand nombre de mots du dictionnaire anglais, mais aussi d'autres chaînes de caractères qui pourraient être facilement compromises à l'aide de techniques courantes de piratage de mots de passe. Par exemple, le script de configuration initiale peut rejeter des mots de passe tels que « abcdefg » ou « passw0rd ».

Remarque : Une fois le processus de configuration initiale terminé, le système attribue la même valeur aux mots de passe des deux comptes **administrateurs** (l'un pour l'accès Web et l'autre pour l'accès CLI), conformément aux exigences relatives aux mots de passe robustes décrites dans le *Guide de configuration du Firepower 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.

Remarque : 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.

Contrat de licence de l'utilisateur final (End User License Agreement ou EULA)

Avant d'utiliser le centre de gestion Firepower Management Center, vous devez accepter l'EULA affiché sur le deuxième écran de l'assistant de configuration initiale. Lisez L'EULA et cliquez sur (**Accept**)(accepter) pour continuer. Si vous cliquez sur **Decline** (Refuser), l'assistant vous déconnecte de l'FMC

Modifier les paramètres réseau

Le dernier écran de l'assistant de configuration initiale vous permet de modifier les paramètres réseau utilisés par le FMC pour les communications réseau par le biais de son interface de gestion (eth0) Si vous vous connectez pour la première fois après avoir effectué une restauration du système dans laquelle vous avez choisi de conserver les paramètres de réseau et de licence, l'assistant est prérempli avec les mêmes valeurs que le FMC a utilisées avant la restauration du système.

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 FMC 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 **Finish**(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 du FMC 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 FMC et le navigateur. Dans ce cas, l' assistant n'affiche aucune information sur l'état de connectivité pour le DNS ou le NTP.

Vous pouvez renseigner les champs suivants :

Nom complet du domaine

Vous devez fournir un FQDN. Vous pouvez effectuer l'une des opérations suivantes :

- Accepter la valeur affichée, si elle s'affiche
- Sinon, saisissez un nom de domaine complet (syntaxe `<hostname>.<domain>`) ou le nom d'hôte.

Protocole de démarrage pour la configuration IPv4

Choisissez l'une des méthodes suivantes d'affectation d'adresses IP dans la liste déroulante **Configurer IPv4** :

- **Utilisation du protocole DHCP**
- **Utilisation statique/manuelle**

Adresse IPv4

Ce champ est obligatoire. Vous pouvez accepter la valeur affichée, le cas échéant, ou saisir une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 192.168.45.45).

Network Mask (Masque réseau)

Ce champ est obligatoire. Vous pouvez accepter la valeur affichée, le cas échéant, ou saisir une nouvelle valeur. Utilisez la forme décimale à points (par exemple, 255.255.0.0).

Passerelle

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

Groupe DNS

Choisissez un groupe de serveurs de nom de domaine facultatif pour le FMC. Vous pouvez réaliser les actions suivantes :

- Accepter la valeur par défaut, **Cisco Umbrella DNS**.
- Sélectionnez **Serveurs DNS personnalisés** dans la liste déroulante, puis saisissez des adresses IPv4 pour le **DNS principal** et le **DNS secondaire**.
- Configurez l'absence de serveur **DNS en sélectionnant** Serveurs DNS personnalisés dans la liste déroulante et en laissant les champs **DNS principal** et **DNS secondaire** vides.

Groupe de serveurs NTP

Vous devez utiliser un serveur NTP pour assurer une bonne synchronisation entre le FMC et ses périphériques gérés. Choisissez l'une des options suivantes dans la liste déroulante :

- **Default NTP Servers** Par défaut, le système utilise `0.sourcefire.pool.ntp.org` comme serveur NTP principal, et `1.sourcefire.pool.ntp.org` comme serveur NTP secondaire.
- **Serveurs NTP personnalisés** Saisissez le FQDN ou les adresses IP d'un ou de deux serveurs NTP accessibles depuis votre réseau.

Boîte de dialogue Licences Smart

Après avoir cliqué sur **Finish** sur l'écran Change Network Settings de l'assistant de configuration initiale, 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 FMC gère des périphériques Firepower 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 « Licensing the Firepower System » dans le *Guide de configuration de Firepower Management Center* pour votre version.

Configuration initiale automatique

Une fois que vous avez terminé l'assistant de configuration initiale, le FMC configure automatiquement les activités de maintenance hebdomadaires pour maintenir votre système à jour et vos données sauvegardées :

Les 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 affecté, les tâches planifiées ont lieu une heure « ultérieurement » en été qu'en été, en fonction de l'heure locale.

Remarque : Nous vous recommandons de passer en revue les configurations planifiées automatiquement et de les régler au besoin.

- Mises à jour hebdomadaires de GeoDB

  Le FMC planifie automatiquement les mises à jour de la GeoDB chaque semaine, à une heure aléatoire déterminée. Vous pouvez observer l'état de cette tâche à l'aide de l'interface Web du centre de messages. Si le système ne parvient pas à configurer la mise à jour et que votre FMC a accès à Internet, nous vous recommandons de configurer des mises à jour régulières de GeoDB comme décrit dans le *Guide de configuration de Firepower Management Center* pour votre version.

- Mises à jour logicielles hebdomadaires du FMC

  Le FMC planifie automatiquement une tâche hebdomadaire pour télécharger la version logicielle la plus récente pour le FMC 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. Si la planification des tâches échoue et que votre FMC 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 de configuration de Firepower Management Center* pour 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 Firepower Management Center* pour obtenir plus d'information.

- Sauvegarde hebdomadaire de la configuration du FMC

  Le FMC 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. Si la planification des tâches échoue, nous vous recommandons de planifier une tâche récurrente pour effectuer une sauvegarde, comme décrit dans le *Guide de configuration de Firepower Management Center* pour votre version.

- Mise à jour de la base de données de vulnérabilités

  Dans les versions 6.6 et ultérieures, le FMC 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 FMC 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 de configuration de Firepower Management Center* pour votre version.

- Mise à jour quotidienne des règles d'intrusion

  Dans les versions 6.6 et ultérieures, le FMC configure une mise à jour quotidienne automatique des règles de prévention des intrusions à partir du site d'assistance de Cisco. Le FMC 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 mise à jour 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 FMC 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 de configuration de Firepower Management Center* pour votre version.

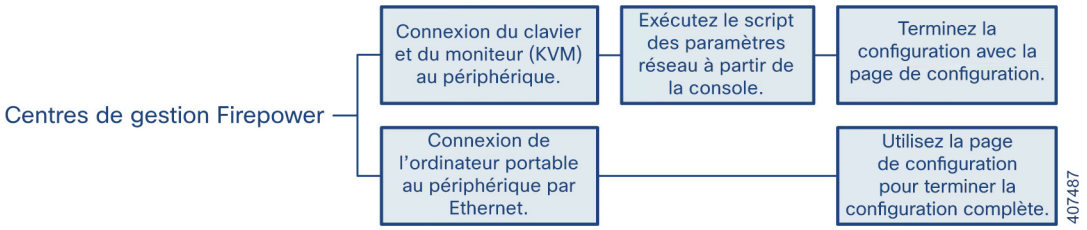
Installation et configuration initiale pour les versions 5.4 à 6.4.x

Les versions de Firepower 5.4 à 6.4.x sont prises en charge sur tous les modèles de FMC présentés dans ce document : 750, 1500, 2000, 3500 et 4000.

Lorsque vous installez un appareil, assurez-vous de pouvoir accéder à la console du périphérique pour la configuration initiale. Vous pouvez accéder à la console pour la configuration initiale à l'aide d'un clavier et d'un moniteur avec KVM, ou en utilisant une connexion Ethernet avec l'interface de gestion.

La première fois que vous vous connectez à l'interface Web de FMC, la page d'administration initiale vous permet de configurer le nouvel appareil pour qu'il communique sur votre réseau de gestion de confiance. Vous devez également effectuer des tâches initiales de niveau administratif telles que la modification du mot de passe administrateur , l'acceptation du contrat de licence d'utilisateur final (CLUF), la définition de l'heure et la planification des mises à jour. Les options que vous choisissez lors de la configuration et de l'enregistrement déterminent les interfaces par défaut, les ensembles en ligne, les zones et les politiques que le système crée et applique aux périphériques gérés.

Vous pouvez effectuer ce processus de configuration initiale en accédant au FMC en utilisant un ordinateur portable directement connecté au périphérique ou en utilisant une connexion Ethernet par l'intermédiaire de votre réseau de gestion local de confiance. Le diagramme suivant illustre les choix que vous pouvez faire lors de la configuration des FMC exécutant les versions Firepower 5.4 à 6.4.x :



Remarque : Si vous déployez plusieurs périphériques, configurez d'abord vos périphériques, puis leur gestion Firepower Centre de gestion. Le processus de configuration initiale d'un périphérique vous permet de le préenregistrer auprès d'un Centre de gestion; le processus de configuration d'un Centre de gestion vous permet d'ajouter des périphériques gérés préenregistrés et d'obtenir une licence.

Remarque : Si vous configurez un équipement après l'avoir restauré aux paramètres d'usine (voir Restauration d'un Cisco Firepower Management Center aux valeurs d'usine par défaut, page 24) et que vous n'avez pas supprimé la licence de l'équipement ni ses paramètres réseau, vous pouvez utiliser un ordinateur sur votre réseau de gestion pour accéder directement à l'interface web de l'équipement afin d'effectuer la configuration. Passez à Configuration initialeCentre de gestion, page 14.

Pour installer et configurer un FMC utilisant les versions 5.4 à 6.4.x :

1. Installez le périphérique comme décrit dans Installation de l'appliance, page 4.

2. Avant de connecter le FMC à votre réseau, vous devez modifier l'adresse IP eth0 du FMC pour qu'elle corresponde à votre réseau et effectuer la configuration initiale; vous avez l'un des deux choix suivants :
   - Accédez au FMC à l'aide de la connexion VGA/clé pour définir l'adresse IP eth0 avant d'effectuer la configuration initiale; voir Accéder au Firepower Management Center à l'aide d'un clavier et d'un moniteur, page 6.

     Accédez ensuite au FMC avec un navigateur Web pour effectuer le processus de configuration initiale; voir Configuration initialeCentre de gestion, page 14.
   - Accédez au FMC à l'aide d'une connexion Ethernet directement à partir de l'interface eth0 vers un ordinateur local; voir Accéder au Firepower Management Center à l'aide de l'interface de gestion, page 5.

     Accédez ensuite au FMC avec un navigateur Web pour effectuer la configuration initiale et définir l'adresse IP eth0 dans le cadre de ce processus; voir Configuration initialeCentre de gestion, page 14.

Installation de l'appliance

Ces instructions sont une version abrégée des étapes d'installation physique du périphérique. Pour des instructions détaillées, consultez le *Guide d'installation du matériel pour Cisco Firepower Management Center 1000, 2500 et 4500*.

Procédure

1. Montez l'appareil dans votre rack à l'aide de la trousse de montage et des instructions fournies.
2. Branchez le cordon d'alimentation à l'appareil et branchez-le dans une source d'alimentation.

   Si votre appareil dispose de blocs d'alimentation redondants, fixez les cordons d'alimentation aux deux blocs d'alimentation et branchez-les dans des sources d'alimentation distinctes.
3. Allumez l'appareil.

Étape suivante

- Si vous connectez un ordinateur directement à l'interface de gestion physique du périphérique pour configurer ce dernier, passez à Configuration du centre de gestion à l'aide de l'interface de gestion, page 12.
- Si vous utilisez un clavier et un moniteur pour configurer le périphérique, passez à Configuration du centre de gestion à l'aide d'un clavier et d'un moniteur (KVM), page 13.

Configuration du centre de gestion à l'aide de l'interface de gestion

Procédure

1. Configurez un ordinateur local, qui ne doit pas être connecté à Internet, avec les paramètres réseau suivants :
   - Adresse IP : 192.168.45.2
   - Masque réseau : 255.255.255.0
   - Passerelle par défaut : 192.168.45.1

   (L'interface de gestion FMC est préconfigurée avec une adresse IPv4 par défaut. Cependant, vous pouvez reconfigurer l'interface de gestion avec une adresse IPv6 dans le cadre du processus de configuration.)
2. À l'aide du câble Ethernet fourni, connectez l'interface réseau de l'ordinateur préconfiguré directement à l'interface de gestion du périphérique.

   Vérifiez que le voyant DEL de liaison est activé pour l'interface réseau sur l'ordinateur local et pour l'interface de gestion du périphérique.

3. Utilisez un navigateur Web pour accéder à l'adresse IP par défaut du périphérique :

   ```
   https:// 192.168.45.45
   ```

   La page d'ouverture de session s'affiche.

4. Utilisez le nom d'utilisateur `admin` et le mot de passe `Admin123` pour vous connecter.

Étape suivante

- Terminez le processus d'installation en utilisant les procédures dans Configuration initialeCentre de gestion, page 14.

Configuration du centre de gestion à l'aide d'un clavier et d'un moniteur (KVM)

Vous pouvez connecter un clavier USB et un moniteur VGA au périphérique, ce qui est utile pour les périphériques montés en rack connectés à un commutateur KVM (clavier, vidéo et souris).

Avant de commencer

Assurez-vous d'avoir, au minimum, les informations nécessaires pour que le périphérique communique sur votre réseau de gestion :

- Une adresse IP de gestion IPv4 ou IPv6
- Un masque de réseau ou une longueur de préfixe
- Une passerelle par défaut

Procédure

1. À l'aide du câble Ethernet fourni, connectez l'interface de gestion à l'arrière du périphérique à un réseau de gestion protégé.
2. Connectez le moniteur au port VGA et le clavier à l'un des ports USB.
3. Accédez à l'interface Shell Linux sur le FMC en utilisant `admin` comme nom d'utilisateur et `Admin123` comme mot de passe. (Remarque : le mot de passe est sensible à la casse.) Suivez les étapes adaptées à votre version; consultez Accédez à la CLI ou au Shell Linux sur le FMC, page 3.
4. Exécutez le script suivant :

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

   Le message suivant (ajouté à la valeur actuelle) s'affiche :

   ```
   Adresse IP de gestion?
   ```

5. Saisissez l'adresse IP que vous souhaitez attribuer à l'interface de gestion ou appuyez sur Entrée pour accepter la valeur actuelle. Par exemple :

   ```
   10.2.2.20
   ```

   Le message suivant (ajouté à la valeur actuelle) s'affiche :

   ```
   Masque réseau de gestion?
   ```

6. Saisissez le masque réseau pour l'adresse IP de l'interface ou appuyez sur Entrée pour accepter la valeur actuelle. Par exemple :

   ```
   255.255.255.0
   ```

   Le message suivant (ajouté à la valeur actuelle) s'affiche :

   ```
   Passerelle de gestion ?
   ```

7. Saisissez la passerelle pour l'adresse IP de l'interface ou appuyez sur Enter (Entrée) pour accepter la valeur actuelle. Par exemple :

   ```
   10.2.1.1
   ```

   Le message suivant s'affiche :

   ```
   Ces paramètres sont-ils corrects (o o n) ?
   ```

8. 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 vous redemande alors les informations.

9. Après avoir accepté les paramètres, déconnectez-vous de l'interface Shell.

Étape suivante

- Terminez le processus d'installation en utilisant les procédures dans Configuration initialeCentre de gestion, page 14.

Configuration initialeCentre de gestion

Pour tous les Centre de gestion, vous devez terminer le processus de configuration en vous connectant à l'interface Web Centre de gestion et en sélectionnant les options de configuration initiale sur une page de configuration. Vous devez changer le mot de passe administrateur, définir les paramètres réseau (au besoin) et accepter le CLUF.

Dans les versions 5.4.x, le processus de configuration vous permet également d'enregistrer des périphériques et de les obtenir sous licence. Avant de pouvoir enregistrer un périphérique, vous devez terminer le processus de configuration sur le périphérique lui-même, ainsi qu'ajouter le Centre de gestion en tant que gestionnaire à distance, sinon l'enregistrement échouera.

Procédure

1. Dirigez votre navigateur vers `https://mgmt_ip/`, où *`mgmt_ip`* est l'adresse IP de l'interface Centre de gestion :
   - Pour le Centre de gestion connecté à un ordinateur avec un câble Ethernet, dirigez le navigateur sur cet ordinateur vers l'adresse IPv4 de l'interface de gestion par défaut : `https://192.168.45.45/`.
   - Pour un Centre de gestion où les paramètres réseau sont déjà configurés, utilisez un ordinateur de votre réseau de gestion pour accéder à l'adresse IP de l'interface de gestion du Centre de gestion.
2. Utilisez le nom d'utilisateur `admin` et le mot de passe `Admin123` pour vous connecter.

   Consultez les sections suivantes pour obtenir des renseignements sur la configuration :
   - Modifier le mot de passe, page 15
   - Paramètres de réseau, page 15
   - Paramètres de l'heure, page 16
   - Recurring Rule Update Imports, page 16
   - Mises à jour récurrentes de la géolocalisation, page 16
   - Sauvegardes automatiques, page 16
   - Paramètres des licences, page 17
   - Enregistrement de l'appareil, page 17
   - Contrat de licence de l'utilisateur final, page 19

3. Lorsque vous avez terminé, cliquez sur **Apply**.

   Le Centre de gestion est configuré en fonction de vos sélections. Vous êtes connecté à l'interface Web en tant qu'utilisateur `admin`, qui a le rôle d'administrateur.

   Remarque : Si vous vous êtes connecté directement au périphérique à l'aide d'un câble Ethernet, déconnectez l'ordinateur et connectez l'interface de gestion de Centre de gestion au réseau de gestion. Utilisez un navigateur sur un ordinateur du réseau de gestion pour accéder à Centre de gestion à l'adresse IP ou au nom d'hôte que vous venez de configurer, et complétez le reste des procédures de ce guide.

4. Confirmez que la configuration initiale a réussi :

   - Pour les versions antérieures à 6.0, utilisez la page État de la tâche (**Système > Surveillance > État de la tâche**) pour vérifier que la configuration initiale a réussi.

     La page est actualisée automatiquement toutes les dix secondes. Surveillez la page jusqu'à ce que l'état **Completed** s'affiche pour les tâches d'enregistrement initial de l'équipement et d'application de la politique. Si, dans le cadre de la configuration, vous avez configuré une mise à jour des règles d'intrusion ou de géolocalisation, vous pouvez également surveiller ces tâches.

   - Pour les versions 6.0 et ultérieures, cliquez sur l'icône État du système et affichez l'onglet Tâches dans le centre de messages.

   Le Centre de gestion est prêt à l'emploi. Consultez la section *Guide de configuration de Firepower Management Center* pour obtenir plus d'informations sur la configuration de votre déploiement.

Étape suivante

- Continuez avec Recommandations d'administration, page 19.

Options de configuration

Modifier le mot de passe

Vous devez changer le mot de passe du compte `admin`. Ce compte a des privilèges d'administrateur et ne peut pas être supprimé.

Cisco recommande d'utiliser un mot de passe robuste d'au moins huit caractères alphanumériques, avec mélange de casse, et comprenant au moins un chiffre. Évitez d'utiliser des mots qui apparaissent dans un dictionnaire.

Remarque : Les comptes admin pour accéder à un Firepower Management Center via l'interface Shell et via l'interface Web ne sont pas identiques et peuvent utiliser des mots de passe différents.

Paramètres de réseau

Les paramètres réseau du Centre de gestion lui permettent de communiquer sur votre réseau de gestion. Si vous avez déjà configuré les paramètres réseau, cette section de la page peut être préremplie.

Le Système Firepower offre une implémentation à double pile pour les environnements de gestion IPv4 et IPv6. Vous devez préciser le protocole de réseau de gestion (**IPv4**, **IPv6**, ou **les deux**). Selon votre choix, la page de configuration affiche divers champs où vous devez saisir l'adresse IP de gestion IPv4 ou IPv6, la longueur du masque réseau ou du préfixe, et la passerelle par défaut

- Pour IPv4, vous devez saisir l'adresse et le masque réseau sous forme décimale à points (par exemple : un masque réseau de 255.255.0.0).
- Pour les réseaux IPv6, vous pouvez cocher la case **Assign the IPv6 address using router autoconfiguration** pour attribuer automatiquement les paramètres réseau IPv6. Sinon, vous devez définir l'adresse en hexadécimal séparé par des deux-points et le nombre de bits du préfixe (par exemple : une longueur de préfixe de 112).

Vous pouvez également spécifier jusqu'à trois serveurs DNS, ainsi que le nom d'hôte et le domaine du périphérique.

Paramètres de l'heure

Vous pouvez définir l'heure d'un Centre de gestion soit manuellement, soit via le protocole de temps réseau (NTP) d'un serveur NTP.

Vous pouvez également préciser le fuseau horaire utilisé sur l'interface Web locale pour le compte `admin`. Cliquez sur le fuseau horaire actuel pour le modifier à l'aide d'une fenêtre contextuelle.

Recurring Rule Update Imports

À mesure que de nouvelles vulnérabilités sont connues, le Cisco Talos Intelligence Group publie des mises à jour des règles de prévention des intrusions. Les mises à jour de règles peuvent également supprimer des règles et fournir de nouvelles catégories de règles et des variables système. Les mises à jour de règles peuvent également supprimer des règles et fournir de nouvelles catégories de règles et des variables système.

Si vous prévoyez d'effectuer la détection et la prévention des intrusions dans votre déploiement, Cisco recommande d'**activer les importations de mises à jour de règles récurrentes à partir du site de soutien**.

Vous pouvez spécifier la **fréquence d'importation**, ainsi que configurer le système pour effectuer un **déploiement de stratégie** après chaque mise à jour de règle. Pour effectuer une mise à jour des règles dans le cadre du processus de configuration initiale, sélectionnez **Installer maintenant**.

Les mises à jour de règles peuvent contenir de nouveaux binaires. Assurez-vous que votre processus de téléchargement et d'installation des mises à jour de règles est conforme à vos politiques de sécurité. De plus, les mises à jour de règles peuvent être volumineuses, alors assurez-vous d'importer des règles pendant les périodes de faible utilisation du réseau.

Mises à jour récurrentes de la géolocalisation

Firepower Centre de gestion peuvent afficher des informations géographiques sur les adresses IP routées associées aux événements générés par le système, ainsi que surveiller des statistiques de géolocalisation dans le tableau de bord et Context Explorer.

La base de données de géolocalisation (GeoDB) des Centre de gestion contient des informations telles que le fournisseur d'accès à Internet associé à une adresse IP, le type de connexion, les informations sur le proxy et l'emplacement exact. L'activation de mises à jour régulières de GeoDB garantit que le système utilise des informations de géolocalisation à jour. Si vous prévoyez d'effectuer une analyse basée sur la géolocalisation dans votre déploiement, Cisco vous recommande d'**activer les mises à jour hebdomadaires récurrentes à partir du site d'assistance**.

Vous pouvez préciser la fréquence de mise à jour hebdomadaire de la base de données GeoDB. Cliquez sur le fuseau horaire pour le modifier à l'aide d'une fenêtre contextuelle. Pour télécharger la base de données dans le cadre du processus de configuration initiale, sélectionnez **Installer maintenant**.

Les mises à jour de GeoDB peuvent être importantes et prendre jusqu'à 45 minutes après le téléchargement. Vous devez mettre à jour la GeoDB pendant les périodes de faible utilisation du réseau.

Sauvegardes automatiques

Le Firepower Centre de gestion fournit un mécanisme d'archivage des données afin que les configurations puissent être restaurées en cas de défaillance. Dans le cadre de la configuration initiale, vous pouvez **activer les sauvegardes automatiques**.

L'activation de ce paramètre crée une tâche planifiée qui crée une sauvegarde hebdomadaire des configurations sur le Centre de gestion.

Paramètres des licences

Vous utilisez le Firepower Management Center pour gérer les licences pour lui-même et les périphériques qu'il gère. Les types de licences proposés par le système Firepower dépendent du type de périphérique que vous souhaitez gérer :

- Pour les séries 7000 et 8000, ASA FirePOWER et NGIPSv, vous devez utiliser des licences classiques. Les périphériques qui utilisent des licences Classic sont parfois appelés périphériques Classic.
- Pour les périphériques Firepower Threat Defense physiques et virtuels, vous devez utiliser des licences Smart.

Avant d'ajouter une licence classique au Firepower Management Center, assurez-vous d'avoir la clé d'autorisation de produit (PAK) fournie par Cisco lorsque vous avez acheté la licence. Si vous avez une licence antérieure à Cisco, communiquez avec le service d'assistance.

Remarque : Vous devez attribuer des licences Classicà vos périphériques gérés avant de pouvoir utiliser les fonctionnalités sous licence sur ces derniers. Vous pouvez activer une licence lors de la configuration initiale du Firepower Centre de gestion, lorsque vous ajoutez un périphérique au Firepower Management Center, ou en modifiant les propriétés générales du périphérique après l'ajout.

Procédure

1. Obtenez la clé de licence pour votre châssis dans la section des paramètres de licence de la page de configuration initiale.

   La clé de licence est clairement étiquetée : par exemple, 66:18:E7:6E:D9:93:35.

   Remarque : Vous pouvez trouver la clé de licence sur un Firepower Centre de gestion à tout moment lorsque vous cliquez sur le bouton **Ajouter une nouvelle licence** à partir de la page **System>Licences>Classic Licenses**.

2. Pour obtenir votre licence, accédez à https://www.cisco.com/go/license/ où vous êtes invité à entrer la clé de licence (par exemple, 66:18:E7:6E:D9:93:35) et la clé PAK.

   Remarque : Si vous avez commandé des licences supplémentaires, vous pouvez saisir les clés PAK pour ces licences en même temps, en les séparant par des virgules.

3. Suivez les instructions à l'écran pour générer une ou plusieurs licence qui vous seront envoyées par courriel.
4. Collez la ou les licences dans la zone de validation et cliquez sur **Add/Verify** (Ajouter/vérifier).

Étape suivante

- Poursuivre la configuration initiale.

Remarque : Si vous avez des périphériques qui utilisent les licences intelligentes Cisco, vous utilisez la page **System>Licenses>Smart Licenses** pour ajouter et vérifier les licences. Consultez la documentation produit de ces périphériques pour savoir comment ajouter des licences Smart à Firepower Centre de gestion. Le *Guide de configuration de Firepower Management Center* fournit de plus amples renseignements sur les licences Classic et les licences Smart, les types de licences pour chaque classe et la façon de gérer les licences dans votre déploiement.

Enregistrement de l'appareil

Un Firepower Centre de gestion peut gérer n'importe quel périphérique, physique ou virtuel, actuellement pris en charge par le Système Firepower. Vous **devez** configurer la gestion à distance sur le périphérique avant de pouvoir l'enregistrer sur un Centre de gestion.

Si vous utilisez Système Firepower version 6.0 ou ultérieure, consultez les informations de gestion des périphériques dans le *Guide de configuration de Firepower Management Center* pour obtenir des instructions sur l'enregistrement de vos périphériques.

Si vous utilisez une version Système Firepower antérieure à la version 6.0, vous pouvez ajouter des périphériques de série 7000 et 8000 à Centre de gestion au cours du processus de configuration initiale. Toutefois, si un périphérique et le Centre de gestion sont séparés par un périphérique NAT, vous devez l'ajouter une fois le processus de configuration terminé; consultez le *Guide d'installation des séries Firepower 7000 et 8000*.

Vous devez configurer les deux canaux de trafic pour utiliser la même interface de gestion lorsque vous utilisez une interface de gestion autre que celle par défaut pour connecter votre Centre de gestion et le périphérique géré et que ces périphériques sont séparés par un périphérique NAT. Consultez la section « Déploiement sur un réseau de gestion » dans *Guide d'installation des séries Firepower 7000 et 8000* pour en savoir plus.

Lorsque vous enregistrez un périphérique géré sur un système Centre de gestion, laissez la case **« Appliquer les politiques de contrôle d'accès par défaut »** cochée si vous souhaitez que des politiques de contrôle d'accès soient automatiquement appliquées aux périphériques lors de leur enregistrement. Notez que vous ne pouvez pas choisir quelle politique le Centre de gestion applique à chaque périphérique, mais seulement décider si elles doivent être appliquées ou non. La politique appliquée à chaque périphérique dépend du mode de détection (voir Configuration des périphériques gérés Firepower dans le *Guide d'installation des séries Firepower 7000 et 8000*) que vous avez choisi lors de la configuration du périphérique, comme indiqué dans le tableau suivant.

Table 1 Politique de contrôle d'accès par défaut appliquée par mode de détection

Mode de détection	Politique de contrôle d'accès par défaut
En ligne	Prévention contre les intrusions par défaut
Passif	Prévention contre les intrusions par défaut
Contrôle d'accès	Contrôle d'accès par défaut
Détection du réseau	Détection du réseau par défaut

Une exception se produit si vous avez précédemment géré un périphérique avec un Centre de gestion et que vous avez modifié la configuration initiale de l'interface du périphérique. Dans ce cas, la politique appliquée par cette nouvelle page Centre de gestion dépend de la configuration modifiée (actuelle) du périphérique. Si des interfaces sont configurées, le Centre de gestion applique la politique de prévention des intrusions par défaut. Sinon, le Centre de gestion applique la politique de contrôle d'accès par défaut.

Si un périphérique est incompatible avec une stratégie de contrôle d'accès, l'application de la politique échoue. Cette incompatibilité peut se produire pour plusieurs raisons, notamment les incompatibilités de licences, les restrictions de modèle, les problèmes de périphériques passifs par rapport à en ligne et d'autres erreurs de configuration. Si l'application initiale de la stratégie de contrôle d'accès échoue, l'application initiale de la politique de découverte du réseau échoue également. Après avoir résolu le problème à l'origine de l'échec, vous devez appliquer manuellement les politiques de contrôle d'accès et de découverte de réseau au périphérique. Pour en savoir plus sur les problèmes pouvant entraîner l'échec de l'application de la stratégie de contrôle d'accès, consultez le *Guide de configuration de Firepower Management Center*.

Pour ajouter un périphérique, saisissez son **nom d'hôte** ou **son adresse IP**, ainsi que la **clé d'enregistrement** que vous avez spécifiée lors de l'enregistrement du périphérique. N'oubliez pas qu'il s'agit d'une clé simple que vous avez spécifiée, pouvant comporter jusqu'à 37 caractères, et qui n'est pas la même chose qu'une clé de licence.

Ensuite, utilisez les cases à cocher pour ajouter des fonctionnalités sous licence au périphérique. Vous ne pouvez sélectionner que les licences que vous avez déjà ajoutées au Centre de gestion; voir Paramètres des licences, page 17.

Toutes les licences ne sont pas prises en charge sur tous les périphériques gérés. Cependant, la page de configuration ne vous empêche **pas** d'activer des licences non prises en charge sur les périphériques gérés ou d'activer une capacité pour laquelle vous n'avez pas de licence spécifique au modèle. En effet, l'identification du modèle du périphérique par Centre de gestionn'intervient que plus tard. Le système ne peut pas activer une licence non valide, et toute tentative d'activation d'une licence non valide ne diminue pas le nombre de licences disponibles.

Après avoir activé les licences, cliquez sur **Ajouter** pour enregistrer les paramètres d'enregistrement du périphérique et, éventuellement, ajouter d'autres périphériques. Si vous avez sélectionné les mauvaises options ou mal saisi le nom de périphérique, cliquez sur **Supprimer** pour le supprimer. Vous pouvez ensuite rajouter l'appareil.

Contrat de licence de l'utilisateur final

Lisez attentivement l'EULA et, si vous acceptez de vous conformer à ses dispositions, cochez la case. Assurez-vous que toutes les informations que vous avez fournies sont correctes, puis cliquez sur **Apply** (Appliquer).

Le Centre de gestion est configuré en fonction de vos sélections. Vous êtes connecté à l'interface Web en tant qu'utilisateur `admin`, qui a le rôle d'administrateur. Poursuivez avec l'étape 3 dans Configuration initialeCentre de gestion, page 14 pour terminer la configuration initiale de Centre de gestion.

Recommandations d'administration

Une fois le processus de configuration initiale d'un appareil terminé et son succès vérifié, Ciscorecommande d'effectuer plusieurs tâches administratives afin de faciliter la gestion de votre déploiement. Vous devez également effectuer toutes les tâches que vous avez ignorées lors de la configuration initiale, telles que l'enregistrement du périphérique et l'octroi de licences. Pour des informations détaillées sur les tâches décrites dans les sections suivantes, ainsi que des renseignements sur la façon dont vous pouvez commencer à configurer votre déploiement, consultez le *Guide de configuration de Firepower Management Center* de votre version de logiciel.

Comptes d'utilisateurs individuels

Après avoir terminé la configuration initiale, le seul utilisateur présent sur le système est l'utilisateur `admin`, qui dispose du rôle et des droits d'administrateur. Les utilisateurs disposant de ce rôle ont un accès complet aux menus et à la configuration du système, y compris via l'interfacce shell ou de ligne de commande (CLI). Ciscorecommande de limiter l'utilisation du compte `admin` (et du rôle Administrateur) pour des raisons de sécurité et d'audit.

Remarque : Les comptes `admin` pour accéder à un Cisco Firepower Management Center via l'interface Shell ou pour accéder à un Cisco Firepower Management Center via l'interface Web ne sont pas les mêmes 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 Centre de gestion, 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 comprend dix rôles d'utilisateur prédéfinis conçus pour divers administrateurs et analystes. Vous pouvez également créer des rôles utilisateur personnalisés avec des privilèges d'accès spécialisés.

Enregistrement de l'appareil

Pour toutes les versions de Firepower, vous pouvez enregistrer des périphériques dans le FMC après avoir terminé la configuration initiale du FMC.

Remarque : Si vous utilisez une version Système Firepower antérieure à la version 6.0, vous pouvez ajouter des périphériques de série 7000 et 8000 à Centre de gestion au cours du processus de configuration initiale; consultez Enregistrement de l'appareil, page 17 pour obtenir des renseignements.

Un Firepower Centre de gestion peut gérer n'importe quel périphérique, physique ou virtuel, actuellement pris en charge par votre version du système Firepower. Selon votre version de Firepower, cela peut inclure :

- Firepower séries 7000 et 8000 appareils—périphériques physiques conçus pour le système Firepower. Les appareils Firepower séries 7000 et 8000 ont une gamme de débits, mais partagent la plupart des mêmes capacités. En général, les périphériques Séries 8000 sont plus puissants que les périphériques Séries 7000 ; ils prennent également en charge des fonctionnalités supplémentaires telles que les règles fastpath Séries 8000, l'agrégation de liens et le stacking. Vous devez configurer la gestion à distance sur le périphérique avant de pouvoir l'enregistrer sur un Firepower Centre de gestion.
- NGIPSv—un périphérique virtuel de 64 bits déployé dans l'environnement VMware VSphere. Les appareils NGIPSv ne prennent en charge aucune des fonctionnalités matérielles du système, comme la redondance et le partage des ressources, la commutation et le routage.
- Solution Cisco ASA avec les services FirePOWER : (ou un *Module ASA FirePOWER*)—fournit la politique système de première ligne et transmet le trafic au système Firepower pour la découverte et le contrôle d'accès. Cependant, vous ne pouvez pas utiliser l'interface Web Firepower Centre de gestion pour configurer les interfaces ASA FirePOWER. Solution Cisco ASA avec les services FirePOWER : dispose d'un logiciel et d'une interface de ligne de commande uniques à la plateforme ASA pour installer le système et effectuer d'autres tâches administratives spécifiques à la plateforme.
- Firepower Threat Defense—fournit un pare-feu unifié de prochaine génération et un périphérique IPS de prochaine génération.
- Firepower 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.

Pour enregistrer des périphériques gérés dans un Firepower Centre de gestion, consultez les renseignements de gestion des périphériques dans le *Guide de configuration de Firepower Management Center* pour la version de votre logiciel. Pour en savoir plus sur la compatibilité entre les périphériques Firepower et les versions logicielles, consultez le *Guide de compatibilité de Cisco Firepower*.

Politiques d'intégrité et politiques système

Par défaut, tous les appareils ont une politique système initiale appliquée. La politique système régit les paramètres susceptibles d'être similaires pour plusieurs appareils au sein d'un déploiement, tels que les préférences du relais de messagerie et les paramètres de synchronisation de l'heure. Cisco recommande d'utiliser le Centre de gestion pour appliquer la même politique système à lui-même ainsi qu'à tous les périphériques qu'il gère.

Par défaut, le Centre de gestion 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. Cisco recommande d'utiliser le Centre de gestion pour appliquer une politique d'intégrité à tous les appareils 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. Cisco recommande que tous les périphériques de votre déploiement exécutent la version la plus récente de Système Firepower. 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. Pour les versions 6.5 et ultérieures, l'assistant de configuration initiale configure automatiquement certaines de ces activités de mise à jour pour vous; consultez Configuration initiale automatique, page 10 pour obtenir de plus amples renseignements.

Mise en garde : Avant de mettre à jour une partie du Système Firepower, 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.

Rediriger la sortie de la console

Par défaut, les Centre de gestion envoient des messages sur l'état d'initialisation ou *init*, au port VGA. Si vous souhaitez utiliser le port série physique ou SOL pour accéder à la console, Cisco recommande de rediriger la sortie de la console vers le port série après avoir terminé la configuration initiale.

Pour rediriger la sortie de la console à l'aide de l'interface shell, vous exécutez un script depuis l'interface shell de l'appareil.

Utilisation de l'interface Shell pour rediriger la sortie de la console

Procédure

1. À l'aide de votre clavier/moniteur ou d'une connexion série, connectez-vous à l'interface Shell du périphérique en utilisant un compte disposant de privilèges d'administrateur. Suivez les étapes adaptées à votre version de Firepower; consultez Accédez à la CLI ou au Shell Linux sur le FMC, page 3.

   L'invite du périphérique s'affiche.
2. À l'invite, définissez la sortie de la console en saisissant l'une des commandes suivantes :
   - Pour accéder au périphérique à l'aide du port VGA :

     ```
     sudo /usr/local/sf/bin/configure_console.sh vga
     ```
   - Pour accéder au périphérique à l'aide du port série physique :

     ```
     sudo /usr/local/sf/bin/configure_console.sh serial
     ```
   - Pour accéder au périphérique à l'aide de LOM via SOL :

     ```
     sudo /usr/local/sf/bin/configure_console.sh sol
     ```
3. Pour mettre en œuvre vos modifications, redémarrez l'appliance en tapant `sudo reboot`.

   L'appliance redémarre.

Utilisation de l'interface Web pour rediriger la sortie de la console

Procédure

1. Sélectionnez **Système > Configuration**.
2. Sélectionnez **Console Configuration**.
3. Choisissez une option d'accès par console à distance :
   - Choisissez **VGA** pour utiliser le port VGA de l'appliance. Il s'agit de l'option par défaut.
   - Sélectionnez **Port série physique** pour utiliser le port série de l'appliance, ou pour utiliser le LOM/SOL sur unCentre de gestion.

   Si vous avez sélectionné **Physical Serial Port**, les paramètres LOM s'affichent.
4. Pour configurer LOM via SOL, saisissez les paramètres appropriés :
   - **Configuration DHCP** pour l'appliance (**DHCP** ou **Static**).
   - **Adresse IP** à utiliser pour LOM. L'adresse IP LOM doit être différente de l'adresse IP de l'interface de gestion de l'appareil.
   - **Masque réseau** pour l'appareil.
   - **Passerelle par défaut** pour l'appareil.

.5 Cliquez sur **Save** (enregistrer).

La configuration de la console à distance pour l'appareil est enregistrée. Si vous avez configuré Lights-Out Management, vous devez l'activer pour au moins un utilisateur ; voir Activation de LOM et des utilisateurs LOM, page 41.

Configurer Lights-Out Management

Si vous devez restaurer unFirepower appareil aux paramètres d'usine et que vous n'avez pas d'accès physique à l'équipement, vous pouvez utiliser la gestion hors bande (LOM) pour effectuer le processus de restauration. Notez que vous pouvez utiliser Lights-Out Management sur l'interface de gestion par défaut (`eth0`) uniquement.

La fonction Lights-Out Management (LOM) vous permet d'effectuer un ensemble limité d'actions sur un appareil Firepower à l'aide d'une connexion Serial over LAN (SOL). Avec LOM, vous utilisez une interface de ligne de commande sur une connexion de gestion hors bande pour effectuer des tâches telles que l'affichage du numéro de série du châssis ou la surveillance de conditions telles que la vitesse et la température du ventilateur.

Mise en garde : Les centres de gestion Firepower Management Center 2000 et 4000 ont introduit la plateforme Cisco Unified Computing System (UCS) dans le système Firepower. Ces modèles ne prennent pas en charge les fonctionnalités Cisco qui utilisent des outils sur le contrôleur de gestion de la carte mère (BMC), comme UCS Manager ou Cisco Integrated Management Controller (CIMC), pour apporter des modifications de configuration ou des mises à jour de micrologiciel.

La syntaxe des commandes LOM dépend de l'utilitaire que vous utilisez, mais les commandes LOM contiennent généralement les éléments répertoriés dans le tableau suivant.

Table 2 Syntaxe de la commande LOM :

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
IPMItool	IPMIutil	appelle l'utilitaire IPMI.
S.O.	-V4	Pour ipmiutil uniquement, active les privilèges d'administrateur pour la session LOM.
-I lanplus	-J3	Active le chiffrement pour la session LOM.
-H *adresse IP*	-N *adresse IP*	Précise l'adresse IP de l'interface de gestion sur le périphérique.
-U *username*	-U *username*	Indique le nom d'utilisateur d'un compte LOM autorisé.
s.o. (invite lors de la connexion)	-P *password*	Pour ipmiutil uniquement, spécifie le mot de passe d'un compte LOM autorisé.
commande	commande	La commande que vous souhaitez émettre au périphérique . Notez que l'endroit où vous exécutez la commande dépend de l'utilitaire : ■ Pour IPMItool, saisissez la commande en dernier. ■ Pour ipmiutil, saisissez la commande en premier.

Par conséquent, pour IPMItool :

```
ipmitool -I lanplus -H IP_address -U username command
```

Ou, pour ipmiutil :

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

Notez que les commandes `mise hors tension du châssis` et `cycle d'alimentation du châssis` ne sont pas valides sur les appareils Gamme 70xx. Pour obtenir la liste complète des commandes LOM prises en charge par le Système Firepower, consultez le chapitre de configuration des paramètres de l'appareil dans le *Guide de configuration de Firepower Management Center*.

Remarque : Dans certains scénarios de cycle d'alimentation, le contrôleur de gestion de la carte mère (BMC) d'un Firepower 7050 connecté au réseau par l'intermédiaire de l'interface de gestion peut perdre l'adresse IP qui lui est attribuée par le serveur DHCP. Pour cette raison, Cisco vous recommande de configurer le Firepower 7050 BMC avec une adresse IP statique. Sinon, vous pouvez déconnecter le câble réseau et le reconnecter, ou couper et rétablir l'alimentation du périphérique pour forcer la renégociation du lien.

Avant de pouvoir restaurer un appareil à l'aide de LOM, vous devez activer LOM pour le périphérique et l'utilisateur qui effectuera la restauration. Ensuite, utilisez un utilitaire tiers d'interface de gestion de plateforme intelligente (IPMI) pour accéder au périphérique. Vous devez également vous assurer de rediriger la sortie de la console du périphérique vers le port série.

Pour en savoir plus, consultez les sections suivantes :

- Activation de LOM et des utilisateurs LOM, page 41
- Installation d'un utilitaire IPMI, page 42

Activation de LOM et des utilisateurs LOM

Avant de pouvoir utiliser LOM pour restaurer un appareil, vous devez activer et configurer la fonctionnalité. Vous devez également explicitement accorder des autorisations LOM aux utilisateurs qui utiliseront la fonctionnalité.

Vous configurez LOM et les utilisateurs LOM pour chaque appareil à l'aide de l'interface Web locale de chaque appareil. C'est-à-dire que vous ne pouvez pas utiliser le Centre de gestion pour configurer LOM sur un Firepower périphérique. De même, comme les utilisateurs sont gérés indépendamment pour chaque périphérique, l'activation ou la création d'un utilisateur prenant en charge LOM sur le Centre de gestion ne transfère pas cette capacité aux utilisateurs sur les périphériques Firepower.

Les utilisateurs de LOM sont également soumis aux restrictions suivantes :

- Vous devez attribuer le rôle d'administrateur à l'utilisateur.
- Le nom d'utilisateur peut comporter jusqu'à 16 caractères alphanumériques. Les tirets et les noms d'utilisateur plus longs ne sont pas pris en charge pour les utilisateurs LOM.
- Le mot de passe peut comporter jusqu'à 20 caractères alphanumériques. Les mots de passe plus longs ne sont pas pris en charge pour les utilisateurs LOM. Le mot de passe LOM d'un utilisateur est identique au mot de passe système de cet utilisateur.
- Les Centre de gestion peuvent avoir jusqu'à treize utilisateurs LOM.

  Remarque : Pour des instructions détaillées sur les tâches suivantes, consultez le chapitre Configuration des paramètres de l'appareil dans *Guide de configuration de Firepower Management Center*.

Pour activer LOM :

1. Sélectionnez **System > Configuration**, puis cliquez sur **Console Configuration**.
2. Pour **Console**, choisissez **Port série physique**..
3. Précisez l'adresse IP LOM, le masque réseau et la passerelle par défaut (ou utilisez DHCP pour que ces valeurs soient automatiquement affectées).

Remarque : L'adresse IP LOM doit être différente de l'adresse IP de l'interface de gestion du périphérique.

Pour activer les fonctionnalités LOM pour un utilisateur Système Firepower :

1. Sélectionnez **Système > Gestion des utilisateurs**, puis modifiez un utilisateur existant pour ajouter des autorisations LOM ou créez un nouvel utilisateur que vous utiliserez pour l'accès LOM au périphérique.
2. Sur la page de configuration des utilisateurs, activez le rôle **d'administrateur** s'il n'est pas déjà activé.
3. Cochez la case **Autoriser l'accès Lights-Out Management** et enregistrez vos modifications.

Installation d'un utilitaire IPMI

Vous utilisez un utilitaire IPMI tiers sur votre ordinateur pour créer une connexion SOL avec l'appareil.

Si votre ordinateur exécute Linux ou Mac OS, utilisez IPMItool. Bien qu'IPMItool soit standard avec de nombreuses distributions Linux, vous devez installer IPMItool sur un Mac. Tout d'abord, vérifiez que les outils XCode pour développeur d'Apple sont installés sur votre Mac. Assurez-vous que les composants facultatifs pour le développement de ligne de commande sont installés (outils système et de développement UNIX dans les versions plus récentes ou assistance de ligne de commande dans les versions antérieures). Enfin, installez MacPorts et IPMItool. Utilisez votre moteur de recherche préféré pour obtenir de plus amples renseignements ou consultez les sites suivants :

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Pour les environnements Windows , utilisez ipmiutil, que vous devez compiler vous-même. Si vous n'avez pas accès à un compilateur, vous pouvez utiliser ipmiutil pour compiler. Utilisez votre moteur de recherche préféré pour obtenir de plus amples renseignements ou essayez ce site :

```
http://ipmiutil.sourceforge.net/
```

Restauration d'un Cisco Firepower Management Center aux valeurs d'usine par défaut

Cisco fournit des images ISO sur son site d'assistance pour restaurer ou recréer l'image des centres de gestion Firepower aux paramètres d'usine d'origine.

Pour en savoir plus, consultez les sections suivantes :

Avant de commencer

Avant de commencer à restaurer vos périphériques aux valeurs par défaut, vous devriez vous familiariser avec le comportement attendu du système pendant le processus de restauration.

Recréation d'image du matériel de la version 5.x vers la version 6.3 ou ultérieures

En raison d'une modification des noms d'image ISO, vous ne pouvez pas installer la version 6.3 ou ultérieure sur un appareil Firepower physique qui exécute actuellement la version 5.x. Cela inclut les modèles de centres de gestion Cisco Firepower Management Center suivants, couverts par ce guide :

- 750, 1500, 1500
- 2000, 4000

Le chemin le plus rapide vers la version 6.3 est le suivant :

1. Installez la version 6.2.3, puis
2. Nouvellement installé (ou mise à niveau vers) la version 6.3 ou ultérieure.

Remarque : Après avoir recréé l'image d'un centre de défense/centre de gestion en version 5.x vers un Cisco Firepower Management Center en version 6.2.3, il ne peut pas gérer ses anciens périphériques. Vous devez également recréer l'image de ces périphériques, puis les rajouter au centre de gestion.

Consultez les notes de mise à jour de Firepower pour en savoir plus sur le changement du nom d'image ISO.

Directives de configuration et de sauvegarde d'événements

Avant de commencer le processus de restauration, Cisco recommande de supprimer ou de déplacer tous les fichiers de sauvegarde qui résident sur votre appareil, puis de sauvegarder les données des événements et de la configuration actuels vers un emplacement externe.

La restauration de votre périphérique aux valeurs par défaut entraîne la perte de presque **toutes** les données de configuration et d'événements sur le périphérique. Bien que l'utilitaire de restauration puisse conserver les paramètres de licence, de réseau et (dans certains cas) de gestion Lights-Out (LOM) du périphérique, vous devez effectuer toutes les autres tâches de configuration une fois le processus de restauration terminé.

La conservation des paramètres LOM après le processus de restauration varie selon le modèle et la version de Firepower :

- Si vous restaurez un modèle FMC 750, 1500 ou 3500 aux paramètres d'usine par défaut, la suppression de la licence et des paramètres réseau réinitialise également les paramètres LOM.

Mise en garde : Lors de la restauration des modèles FMC 750, 1500 ou 3500 aux paramètres d'usine à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

- Si vous restaurez un modèle FMC 2000 ou 4000 aux paramètres d'usine par défaut :
  - Si vous restaurez le FMC à la version 6.2.3 ou antérieure, le système *ne* réinitialise pas les paramètres LOM, que vous choisissiez ou non de supprimer la licence et les paramètres réseau.
  - Si vous restaurez le FMC à la version 6.3 ou ultérieure, le système réinitialise les paramètres LOM, que vous choisissiez ou non de supprimer la licence et les paramètres réseau.

Mise en garde : Lors de la restauration des modèles FMC 2000 ou 4000 à la version 6.3+ à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

Flux du trafic pendant le processus de restauration

Pour éviter de perturber le flux de trafic sur votre réseau, Cisco recommande de restaurer vos périphériques pendant une fenêtre de maintenance ou à un moment où l'interruption aura le moins d'impact sur votre déploiement.

La restauration d'un périphérique Firepower qui est déployé en ligne réinitialise le périphérique à une configuration non de contournement (échec de la fermeture), perturbant le trafic sur votre réseau. Le trafic est bloqué jusqu'à ce que vous configuriez les ensembles en ligne compatibles avec le contournement sur le périphérique. Pour plus d'informations sur la modification de la configuration de votre appareil pour configurer le contournement, consultez le chapitre Gestion des appareils*Guide de configuration de Firepower Management Center*.

Comprendre le processus de restauration

Pour restaurer un appareil Firepower, démarrez à partir du lecteur flash interne du périphérique et utilisez un menu interactif pour télécharger et installer l'image ISO sur le périphérique. Pour plus de commodité, vous pouvez installer le logiciel système et les mises à jour des règles de prévention des intrusions dans le cadre du processus de restauration.

Ne recréez l'image de vos périphériques que pendant une fenêtre de maintenance. La recréation d'image réinitialise les périphériques en mode de contournement à une configuration sans contournement et interrompt le trafic sur votre réseau jusqu'à ce que vous reconfiguriez le mode de contournement. Pour en savoir plus, consultez Flux du trafic pendant le processus de restauration, page 25.

Notez que vous **ne pouvez pas** restaurer un périphérique à l'aide de son interface Web. Pour restaurer un périphérique, vous devez vous y connecter de l'une des manières suivantes :

Clavier et moniteur/KVM

Vous pouvez connecter un clavier USB et un moniteur VGA au périphérique, ce qui est utile pour les périphériques montés en rack connectés à un commutateur KVM (clavier, vidéo et souris). Si vous avez un KVM accessible à distance, vous pouvez restaurer des périphériques sans accès physique.

Connexion série/Ordinateur portable.

Vous pouvez utiliser un câble série inversé (également appelé câble de modem NULL ou câble de console Cisco) pour connecter un ordinateur au périphérique. Consultez la fiche technique du matériel de votre appareil pour localiser le port série. Pour interagir avec le périphérique, utilisez un logiciel d'émulation de terminal comme HyperTerminal ou XModem.

Lights-Out Management à l'aide de Serial over LAN :

Vous pouvez effectuer un ensemble limité d'actions sur les Centre de gestion et les Firepower appareils en utilisant Lights-Out Management (LOM) avec une connexion Serial over LAN (SOL). Si vous n'avez pas d'accès physique à un périphérique, vous pouvez utiliser LOM pour effectuer le processus de restauration. Après vous être connecté à un périphérique via LOM, vous exécutez les commandes de l'utilitaire de restauration comme avec une connexion série physique. Notez que vous pouvez utiliser Lights-Out Management sur l'interface de gestion par défaut (`eth0`) uniquement. Pour en savoir plus, consultez Configurer Lights-Out Management, page 40.

Avant de commencer

- Obtenez l'image ISO de restauration pour le périphérique auprès du site d'assistance. Consultez Obtention de l'image ISO de restauration et des fichiers de mise à jour, page 27.
- La recréation d'image d'un centre de gestion Cisco Firepower Management Center peut entraîner un état de non-conformité (OOC) avec l'autorité de licence de Cisco. En tant que bonne pratique, lors de la recréation d'image d'un centre de gestion Cisco Firepower Management Center, annulez d'abord l'enregistrement du centre de gestion Cisco Firepower Management Center du Cisco Smart Software Manager. Sélectionnez **Système > Licences > Licences Smart** et cliquez sur l'icône d'annulation d'enregistrement.

Pour restaurer un périphérique Firepower

1. Copiez l'image sur un support de stockage approprié.
2. Connectez l'appliance.
3. Redémarrez l'appliance et invoquez l'utilitaire de restauration.

Étape suivante

- Installez l'image ISO en suivant la procédure décrite dans Démarrage du processus de restauration, page 28.

Obtention de l'image ISO de restauration et des fichiers de mise à jour

Cisco fournit des images ISO pour la restauration des paramètres d'usine d'origine. Avant de restaurer un appareil, procurez-vous l'image ISO correcte auprès du site d'assistance.

L'image ISO que vous utilisez pour restaurer un appareil dépend du moment où Cisco a introduit la prise en charge de ce modèle d'appareil. À moins que l'image ISO ne soit publiée avec une version mineure pour s'adapter à un nouveau modèle de périphérique, les images ISO sont généralement associées à des versions majeures du logiciel système (par exemple, 5.2 ou 5.3). Pour éviter d'installer une version incompatible du système, Cisco recommande de toujours utiliser la dernière image ISO disponible pour votre appareil.

Les appareils Firepower utilisent un lecteur flash interne pour démarrer le périphérique afin de pouvoir exécuter l'utilitaire de restauration.

Cisco recommande également de toujours exécuter la dernière version du logiciel système prise en charge par votre périphérique. Après avoir restauré un périphérique à la dernière version majeure prise en charge, vous devez mettre à jour son logiciel système, ses règles de prévention des intrusions et sa base de données de vulnérabilités (VDB). Pour en savoir plus, consultez les notes de version de la mise à jour que vous souhaitez appliquer, ainsi que le *Guide de configuration de Firepower Management Center*.

Pour plus de commodité, vous pouvez installer le logiciel système et les mises à jour des règles de prévention des intrusions dans le cadre du processus de restauration. Par exemple, vous pouvez restaurer un périphérique à la version 6.0 et mettre à jour le périphérique à la version 6.0.0.1 dans le cadre de ce processus. Gardez à l'esprit que seuls les Centre de gestionnécessitent des mises à jour de règles.

Pour obtenir l'image ISO de restauration et d'autres fichiers de mise à jour :

1. En utilisant le nom d'utilisateur et le mot de passe de votre compte d'assistance, connectez-vous au site d'assistance (https://sso.cisco.com/autho/forms/CDClogin.html).
2. Accédez à la section de téléchargement de logiciels (https://software.cisco.com/download/navigator.html).
3. Saisissez une chaîne de recherche dans la zone **Rechercher**de la page qui s'affiche pour le logiciel système que vous souhaitez télécharger et installer.

   Par exemple, pour trouver des téléchargements de logiciels pour Firepower, vous devez saisir **Firepower**.
4. Recherchez l'image (image ISO) que vous souhaitez télécharger.

   Vous pouvez cliquer sur l'un des liens situés sur le côté gauche de la page pour afficher la section correspondante de la page. Par exemple, vous cliquerez sur **6.0 Images** pour afficher les images et les notes de mise à jour pour la version 6.0 de Système Firepower.
5. Cliquez sur l'image ISO que vous souhaitez télécharger.

   Le téléchargement du fichier commence.
6. Copiez les fichiers sur un serveur HTTP (Web), un serveur FTP ou un hôte SCP auquel le périphérique peut accéder sur son réseau de gestion.

Mise en garde : Ne transférez pasles fichiers ISO ou de mise à jour par e-mail ; ils peuvent être corrompus. De plus, ne modifiez pas le nom des fichiers; l'utilitaire de restauration exige qu'ils soient nommés comme ils le sont sur le site d'assistance.

Démarrage du processus de restauration

Commencez le processus de restauration en démarrant le périphérique à partir d'un lecteur flash interne.

Après vous être assuré que vous disposez du niveau d'accès et de connexion appropriés à un appareil, ainsi que de l'image ISO correcte, utilisez l'une des procédures suivantes pour restaurer votre appareil :

- Démarrage de l'utilitaire de restauration à l'aide d'un protocole KVM ou d'un port série physique, page 28 explique comment démarrer le processus de restauration d'un périphérique auquel vous n'avez pas accès à LOM.
- Démarrage de l'utilitaire de restauration à l'aide de Lights-Out Management, page 30 explique comment utiliser LOM pour démarrer le processus de restauration par l'intermédiaire d'une connexion SOL.

Mise en garde : Les procédures de ce chapitre expliquent comment restaurer un périphérique sans l'éteindre. Cependant, si vous devez éteindre l'appareil pour quelque raison que ce soit, utilisez l'interface web de l'équipement, la commande `d'arrêt du système` depuis la CLI, ou la commande `shutdown -h now` depuis l'interface shell de l'appareil (parfois appelé mode expert).

Démarrage de l'utilitaire de restauration à l'aide d'un protocole KVM ou d'un port série physique

Pour les Firepower périphériques, Ciscofournit un utilitaire de restauration sur un disque flash interne.

Remarque : N'utilisez **pas** une console KVM avec stockage de masse USB pour accéder au périphérique pour la configuration initiale, car le périphérique peut tenter d'utiliser le périphérique de stockage de masse comme périphérique de démarrage.

Si vous devez restaurer un appareil aux paramètres d'usine et que vous n'y avez pas d'accès physique, vous pouvez utiliser LOM pour effectuer le processus de restauration ; consultez Démarrage de l'utilitaire de restauration à l'aide de Lights-Out Management, page 30.

Pour démarrer l'utilitaire de restauration :

1. À l'aide de votre clavier/moniteur ou d'une connexion série, connectez-vous au périphérique à l'aide du compte `admin`. Suivez les étapes adaptées à votre version de Firepower ; consultez Accédez à la CLI ou au Shell Linux sur le FMC, page 3.
2. Redémarrez le périphérique; saisissez `sudo reboot`. Indiquez le mot de passe `admin` lorsque vous y êtes invité(e).
3. Surveillez l'état du redémarrage :
   - Si le système effectue une vérification de la base de données, le message suivant peut s'afficher :

     ```
     Le système n'est pas encore opérationnel. La vérification et la réparation de la base de données sont en cours. Cela peut prendre du temps.
     ```

   - Pour une connexion du clavier et du moniteur, appuyez rapidement sur l'une des touches fléchées à plusieurs reprises pour empêcher le périphérique de démarrer la version actuellement installée du système.
   - Pour une connexion série, lorsque les options de démarrage du BIOS apparaissent, appuyez lentement et à plusieurs reprises sur la touche Tab afin d'empêcher l'appareil de démarrer la version actuellement installée du système.

4. Le système répond différemment selon le modèle de matériel et le type de connexion :

   Pour les modèles 750, 1500 et 3500 :

   - **Pour une connexion de clavier et de moniteur :**

     Le menu rouge LILO apparaît et offre trois options : pour démarrer la version actuelle du système, effectuer une restauration du système à l'aide de la console standard (**System_Restore**) ou effectuer une restauration du système à l'aide d'une connexion série (**Restore_Serial**). Utilisez les touches fléchées pour sélectionner **System_Restore** et appuyez sur Enter (Entrée).

   - **Pour une connexion série :**

     L'invite de démarrage LILO s'affiche. Par exemple :

     ```
     LILO 24.2 démarrage :
     6.4.0         System_Restore      Restore_Serial
     démarrage :
     ```

     Tapez `Restore_Serial` et appuyez sur Entrée.

   Pour les modèles 2000 et 4000 :

   - **Pour une connexion de clavier et de moniteur :**

     Le menu rouge LILO apparaît, offrant deux options : pour restaurer la version actuelle du système ou pour effectuer une restauration du système (**System_Restore**). Utilisez les touches fléchées pour sélectionner **System_Restore** et appuyez sur Enter (Entrée).

     Le message `boot` : s'affiche après les choix suivants :

     ```
     10. Charger avec une console standard
     1. Charger avec une console série
     ```

     Tapez `0` et appuyez sur Entrée.

   - **Pour une connexion série :**

     L'invite de démarrage LILO s'affiche. Par exemple :

     ```
     LILO 24.2 démarrage :
     6.4.0         System_Restore
     démarrage :
     ```

     Tapez `System_Restore` et appuyez sur Entrée.

     Le message `boot` : s'affiche après les choix suivants :

     ```
     10. Charger avec une console standard
     1. Charger avec une console série
     ```

     Tapez `1` et appuyez sur Enter.

5. Appuyez sur Entrée pour confirmer l'avis de droit d'auteur.

6. À moins que ce ne soit la première fois que vous restaurez l'appareil vers cette version majeure, l'utilitaire charge automatiquement la dernière configuration de restauration que vous avez utilisée. Pour continuer, confirmez les paramètres dans une série de pages jusqu'à ce que « Cisco Firepower Appliance <Version> Configuration Menu » s'affiche.

Étape suivante

- Continuez avec Utilisation du menu interactif pour restaurer un appareil, page 31.

Démarrage de l'utilitaire de restauration à l'aide de Lights-Out Management

Si vous devez restaurer un appareil aux paramètres d'usine et que vous ne disposez pas d'un accès physique à celui-ci, vous pouvez utiliser LOM pour effectuer le processus de restauration. Notez que vous pouvez utiliser Lights-Out Management sur l'interface de gestion par défaut (`eth0`) uniquement.

Mise en garde : Lors de la restauration des modèles FMC 750, 1500 ou 3500 aux paramètres d'usine à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

Mise en garde : Lors de la restauration des modèles FMC 2000 ou 4000 à la version 6.3+ à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

Remarque : Avant de pouvoir restaurer un appareil à l'aide de LOM, vous devez activer cette fonctionnalité; consultez Configurer Lights-Out Management, page 40.

Pour démarrer l'utilitaire de restauration à l'aide de Lights-Out Management :

1. Accédez à l'interpréteur de commandes de Linux en utilisant le compte `admin`. Suivez les étapes adaptées à votre version de Firepower; consultez Accédez à la CLI ou au Shell Linux sur le FMC, page 3.
2. À l'invite de commande de votre ordinateur, saisissez la commande IPMI pour démarrer la session SOL :

   Pour IPMItool, saisissez :

   ```
   sudo ipmitool -I lanplus -H IP_address -U nom d'utilisateur sol activate
   ```

   Pour ipmiutil, saisissez :

   ```
   sudo ipmiutil sol -a -V4 -J3 -N IP_address -U nom d'utilisateur -P mot de passe
   ```

   Où *IP_address* est l'adresse IP de l'interface de gestion sur le périphérique, *nom d'utilisateur* est le nom d'utilisateur d'un compte LOM autorisé et *mot de passe* est le mot de passe de ce compte. Notez qu'IPMItool vous invite à saisir le mot de passe après avoir exécuté la commande **sol activate**.
3. Redémarrez le périphérique; saisissez `sudo reboot`. Indiquez le mot de passe `admin` lorsque vous y êtes invité(e).
4. Supervisez le processus de redémarrage.

   Si le système effectue une vérification de la base de données, le message suivant peut s'afficher :

   ```
   Le système n'est pas encore opérationnel. La vérification et la réparation de la base
   de données sont en cours. Cela peut prendre du temps.
   ```

   Lorsque vous voyez les options de démarrage BIOS, appuyez sur Onglet lentement et de manière répétée (pour empêcher le périphérique de démarrer la version actuellement installée du système) jusqu'à ce que l'invite de démarrage LILO s'affiche. Par exemple :

   ```
   GNU/Linux - LILO 24 - Menu de démarrage
   6.1.0
   System_Restore
   Restore_Serial
   ```
5. À l'invite de démarrage, démarrez l'utilitaire de restauration en saisissant **Restore_Serial**.

   L'invite de démarrage s'affiche après les choix suivants :

   ```
   10. Charger avec une console standard
   1. Charger avec une console série
   ```

6. Saisissez `1` et appuyez sur Enter (Entrée) pour téléverser le menu de restauration interactif par l'intermédiaire de la connexion série du périphérique.

Remarque : Si vous ne sélectionnez pas de mode d'affichage, l'utilitaire de restauration revient par défaut à la console standard après 30 secondes.

7. Appuyez sur Entrée pour confirmer l'avis de droit d'auteur.
8. À moins que ce ne soit la première fois que vous restaurez l'appareil vers cette version majeure, l'utilitaire charge automatiquement la dernière configuration de restauration que vous avez utilisée. Pour continuer, confirmez les paramètres dans une série de pages jusqu'à ce que « Cisco Firepower Appliance <Version> Configuration Menu » s'affiche.

Étape suivante

- Continuez avec Utilisation du menu interactif pour restaurer un appareil, page 31.

Utilisation du menu interactif pour restaurer un appareil

L'utilitaire de restauration pour les périphériques Firepower utilise un menu interactif pour vous guider dans la restauration.

Remarque : Ne recréez l'image de vos périphériques que pendant une fenêtre de maintenance. La recréation d'image réinitialise les périphériques en mode de contournement à une configuration sans contournement et interrompt le trafic sur votre réseau jusqu'à ce que vous reconfiguriez le mode de contournement. Pour en savoir plus, consultez Flux du trafic pendant le processus de restauration, page 25.

Le menu affiche les options répertoriées dans le tableau suivant.

Table 3 Options de menu de restauration

Option	Description	Pour plus de renseignements, consultez...
1 Configuration IP	Précisez les informations réseau de l'interface de gestion de l'appareil que vous souhaitez restaurer. L'appareil pourra ainsi communiquer avec le serveur sur lequel vous avez placé l'image ISO et les fichiers de mise à jour.	Identification de l'interface de gestion du périphérique, page 33
2 Choisir le protocole de transport	Précisez l'emplacement de l'image ISO que vous utiliserez pour restaurer le périphérique, ainsi que les informations d'authentification dont le périphérique a besoin pour télécharger le fichier.	Spécification de l'emplacement de l'image ISO et de la méthode de transport, page 33
3 Sélectionner des correctifs/mises à jour de règles	Précisez une mise à jour du logiciel système et des règles de prévention des intrusions à appliquer après la restauration du périphérique à la version de base dans l'image ISO.	Mise à jour du logiciel système et des règles d'intrusion pendant la restauration, page 34
4 Télécharger et monter l'image ISO	Téléchargez l'image ISO appropriée et les mises à jour de logiciel système ou de règles de prévention des intrusions. Montez l'image ISO.	Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35

Table 3 Options de menu de restauration (suite)

Option	Description	Pour plus de renseignements, consultez...
5 Exécuter l'installation	Appelez le processus de restauration.	Appel du processus de restauration, page 36
6 Enregistrer la configuration 7 Charger la configuration	Enregistrez tout ensemble de configurations de restauration pour une utilisation ultérieure ou chargez un ensemble sauvegardé.	Enregistrement et chargement des configurations de restauration, page 38
8 Effacer le contenu du disque	Nettoyez le disque dur en toute sécurité pour vous assurer que son contenu n'est plus accessible.	Nettoyage du disque dur, page 45

Naviguez dans le menu à l'aide de vos touches fléchées. Pour sélectionner une option de menu, utilisez les flèches vers le haut et vers le bas. Utilisez les touches fléchées de droite et de gauche pour basculer entre les boutons **OK** et **Annuler** en bas de la page.

Le menu présente deux types d'options différents :

- Pour sélectionner une option numérotée, mettez d'abord en surbrillance l'option correcte à l'aide des flèches vers le haut et le bas, puis appuyez sur Enter (Entrée) pendant que le bouton **OK** au bas de la page est en surbrillance.
- Pour sélectionner une option à choix multiple (bouton radio), mettez d'abord en surbrillance l'option correcte à l'aide des touches haut et bas, puis appuyez sur la barre d'espace pour marquer cette option d'un x. Pour accepter votre sélection, appuyez sur Enter (Entrée) lorsque le bouton **OK** est mis en surbrillance.

Dans la plupart des cas, complétez les options de menu **1**, **2**, **4** et **5**, dans l'ordre. Vous pouvez également ajouter l'option de menu **3** pour installer les mises à jour du logiciel système et des règles de prévention des intrusions pendant le processus de restauration.

Si vous restaurez un appareil vers une version majeure différente de celle actuellement installée sur l'appareil, un processus de restauration en deux étapes est nécessaire. La première passe met à jour le système d'exploitation et la deuxième installe la nouvelle version du logiciel système.

S'il s'agit de votre deuxième passe ou si l'utilitaire de restauration a automatiquement chargé la configuration de restauration que vous souhaitez utiliser, vous pouvez commencer par l'option de menu **4** : Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35. Cependant, Cisco vous recommande de vérifier deux fois les paramètres dans la configuration de restauration avant de continuer.

Remarque : Pour utiliser une configuration précédemment enregistrée, commencez par l'option de menu **6** : Enregistrement et chargement des configurations de restauration, page 38. Après avoir chargé la configuration, passez à l'option de menu **4** : Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35.

Pour restaurer un appareil à l'aide du menu interactif, procédez comme suit :

.1 **1 Configuration IP** : consultez Identification de l'interface de gestion du périphérique, page 33.

.2 **2 Choisissez le protocole de transport** — consultez Spécification de l'emplacement de l'image ISO et de la méthode de transport, page 33.

.3 **3 Sélectionnez Correctifs/Mises à jour de règles** (facultatif) — Mise à jour du logiciel système et des règles d'intrusion pendant la restauration, page 34.

.4 **4 Téléchargez et montez l'ISO** — consultez Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35.

.5 **5 Exécutez l'installation** — consultez Appel du processus de restauration, page 36.

Identification de l'interface de gestion du périphérique

La première étape pour exécuter l'utilitaire de restauration consiste à identifier l'interface de gestion de l'appareil que vous souhaitez restaurer, afin que celui-ci puisse communiquer avec le serveur sur lequel vous avez copié l'ISO et les éventuels fichiers de mise à jour. Si vous utilisez LOM, n'oubliez pas que l'adresse IP de gestion du périphérique n'est **pas** l'adresse IP LOM.

Pour identifier l'interface de gestion du périphérique :

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **1 IP Configuration**.
2. Sélectionnez l'interface de gestion du périphérique (généralement **eth0**).
3. Sélectionnez le protocole que vous utilisez pour votre réseau de gestion : **IPv4** ou **IPv6**.

   Les options pour attribuer une adresse IP à l'interface de gestion s'affichent.
4. Sélectionnez une méthode pour attribuer une adresse IP à l'interface de gestion : **Statique** ou **DHCP** :
   - Si vous sélectionnez **Statique**, une série de pages vous invite à saisir manuellement l'adresse IP, le masque réseau ou la longueur du préfixe, ainsi que la passerelle par défaut pour l'interface de gestion.
   - Si vous sélectionnez **DHCP**, le périphérique détecte automatiquement l'adresse IP, le masque réseau ou la longueur du préfixe et la passerelle par défaut de l'interface de gestion, puis affiche l'adresse IP.
5. Lorsque vous y êtes invité, confirmez vos paramètres.

   Si vous y êtes invité, confirmez l'adresse IP attribuée à l'interface de gestion du périphérique.

Étape suivante

- Passez à la section suivante, Spécification de l'emplacement de l'image ISO et de la méthode de transport

Spécification de l'emplacement de l'image ISO et de la méthode de transport

Après avoir configuré l'adresse IP de gestion que le processus de restauration utilisera pour télécharger les fichiers dont il a besoin, vous devez identifier l'image ISO que vous utiliserez pour restaurer le périphérique. Il s'agit de l'image ISO que vous avez téléchargée à partir du site de soutien (voir Obtention de l'image ISO de restauration et des fichiers de mise à jour, page 27) et stockée sur un serveur Web, un serveur FTP ou un hôte compatible avec le protocole SCP.

Le menu interactif vous invite à saisir les informations nécessaires pour terminer le téléchargement, comme indiqué dans le tableau suivant.

Table 4 Informations nécessaires pour télécharger les fichiers de restauration

Pour utiliser...	Vous devez fournir...
HTTP	■ Adresse IP du serveur Web ■ chemin complet vers le répertoire de l'image ISO (par exemple, `/téléchargements/ISOs/`)
FTP	■ Adresse IP du serveur FTP ■ chemin d'accès au répertoire de l'image ISO, par rapport au répertoire d'accueil de l'utilisateur dont vous souhaitez utiliser les informations d'authentification (par exemple, `mestéléchargements/ISOs/`) ■ nom d'utilisateur et mot de passe autorisés pour le serveur FTP
SCP	■ Adresse IP du serveur SCP ■ nom d'utilisateur autorisé pour le serveur SCP ■ chemin d'accès complet au répertoire de l'image ISO ■ mot de passe pour le nom d'utilisateur que vous avez saisi plus tôt Notez qu'avant de saisir votre mot de passe, le périphérique peut vous demander d'ajouter le serveur SCP à sa liste d'hôtes de confiance. Vous devez accepter pour continuer.

Notez que l'utilitaire de restauration recherchera également les fichiers de mise à jour dans le répertoire de l'image ISO.

Pour préciser l'emplacement et la méthode de transport des fichiers de restauration :

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **2 Choisissez le protocole de transport**.
2. Dans la page qui s'affiche, sélectionnez soit **HTTP**, **FTP**, ou **SCP**.
3. Utilisez la série de pages présentées par l'utilitaire de restauration pour fournir les informations nécessaires pour le protocole que vous avez choisi, comme décrit dans Table 4 à la page -34.

   Si vos informations sont correctes, le périphérique se connecte au serveur et affiche une liste des images ISO Cisco à l'emplacement que vous avez spécifié.
4. Sélectionnez l'image ISO que vous souhaitez utiliser.
5. Lorsque vous y êtes invité, confirmez vos paramètres.
6. Voulez-vous installer une mise à jour de logiciel système ou de règle de prévention des intrusions dans le cadre du processus de restauration?
   - Si oui, continuez avec la section suivante, Mise à jour du logiciel système et des règles d'intrusion pendant la restauration.
   - Si non, continuez avec Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35. Notez que vous pouvez utiliser l'interface web du système pour installer manuellement les mises à jour une fois le processus de restauration terminé.

Mise à jour du logiciel système et des règles d'intrusion pendant la restauration

Vous pouvez également utiliser l'utilitaire de restauration pour mettre à jour le logiciel système et les règles d'intrusion une fois que l'appareil a été restauré vers la version de base contenue dans l'image ISO. Gardez à l'esprit que seuls les Centre de gestion nécessitent des mises à jour de règles.

L'utilitaire de restauration ne peut utiliser qu'une seule mise à jour de logiciel système et une seule mise à jour de règle. Cependant, les mises à jour du système sont cumulatives depuis la dernière version majeure ; les mises à jour des règles sont également cumulatives. Cisco recommande d'obtenir les dernières mises à jour disponibles pour votre appareil ; voir Obtention de l'image ISO de restauration et des fichiers de mise à jour, page 27.

Si vous choisissez de ne pas mettre à jour le périphérique pendant le processus de restauration, vous pouvez le mettre à jour ultérieurement en utilisant l'interface Web du système. Pour en savoir plus, consultez les notes de version pour la mise à jour que vous souhaitez installer, ainsi que le chapitre Mise à jour du logiciel système dans *Guide de configuration de Firepower Management Center*.

Pour installer les mises à jour dans le cadre du processus de restauration :

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **3 Sélectionner des correctifs/Mises à jour de règles**.

   L'utilitaire de restauration utilise le protocole et l'emplacement que vous avez spécifiés dans la procédure précédente (voir Spécification de l'emplacement de l'image ISO et de la méthode de transport, page 33) pour récupérer et afficher la liste des éventuels fichiers de mise à jour du logiciel système présents à cet emplacement. Si vous utilisez SCP, saisissez votre mot de passe lorsque vous y êtes invité pour afficher la liste des fichiers de mise à jour.

2. Sélectionnez la mise à jour du logiciel système, le cas échéant, que vous souhaitez utiliser.

   Vous n'avez pas à sélectionner une mise à jour; appuyez sur Enter (entrée) sans sélectionner de mise à jour pour continuer. S'il n'y a aucune mise à jour de logiciel système à l'emplacement approprié, le système vous invite à appuyer sur Enter (Entrée) pour continuer.

   L'utilitaire de restauration récupère et affiche une liste des fichiers de mise à jour de règles. Si vous utilisez SCP, saisissez votre mot de passe lorsque vous y êtes invité pour afficher la liste.

3. Sélectionnez la mise à jour de règle, le cas échéant, que vous souhaitez utiliser.

   Vous n'avez pas à sélectionner une mise à jour; appuyez sur Enter (entrée) sans sélectionner de mise à jour pour continuer. S'il n'y a aucune mise à jour de règles à l'emplacement approprié, le système vous invite à appuyer sur Enter (Entrée) pour continuer.

Étape suivante

- Passez à la section suivante, Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image

Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image

La dernière étape avant de lancer le processus de restauration consiste à télécharger les fichiers nécessaires et à monter l'image ISO.

Avant de commencer

- Avant de commencer cette étape, vous pouvez enregistrer votre configuration de restauration pour une utilisation ultérieure. Pour en savoir plus, consultez Enregistrement et chargement des configurations de restauration, page 38.

Pour télécharger et monter l'image ISO :

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **4 Télécharger et monter l'ISO**.
2. Lorsque vous y êtes invité, confirmez votre choix. Si vous téléchargez à partir d'un serveur SCP, saisissez votre mot de passe lorsque vous y êtes invité.

   Les fichiers appropriés sont téléchargés et montés.

Étape suivante

- Passez à la section suivante, Appel du processus de restauration

Appel du processus de restauration

Après avoir téléchargé et monté l'image ISO, vous pouvez appeler le processus de restauration. Si vous restaurez un appareil vers une version majeure différente de celle actuellement installée sur l'appareil, un processus de restauration en deux étapes est nécessaire. La première passe met à jour le système d'exploitation et la deuxième installe la nouvelle version du logiciel système.

Première passe de deux (modification des versions majeures uniquement)

Lors de la restauration d'un appareil vers une version majeure différente, un premier passage de l'utilitaire de restauration met à jour le système d'exploitation de l'appareil et, si nécessaire, l'utilitaire de restauration lui-même.

Remarque : Si vous restaurez un appareil à la même version principale ou s'il s'agit de votre deuxième transmission directe du processus, passez à la procédure suivante : Deuxième ou seul passage, page 37.

Pour effectuer la première passe d'un processus de restauration en deux temps :

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **5 Exécuter l'installation**.
2. Lorsque vous y êtes invité (deux fois), confirmez que vous souhaitez redémarrer le périphérique.
3. Surveillez le redémarrage et invoquez à nouveau le processus de restauration :

   Si le système effectue une vérification de la base de données, le message suivant peut s'afficher :

   ```
   Le système n'est pas encore opérationnel. La vérification et la réparation de la base
   de données sont en cours. Cela peut prendre du temps.
   ```

   Pour une connexion avec clavier et moniteur, appuyez rapidement sur l'une des touches fléchées afin d'empêcher l'appareil de démarrer la version actuellement installée du système.

   Pour une connexion de série ou SOL/LOM, lorsque vous voyez les options de démarrage BIOS, appuyez sur Tab lentement et de manière répétée jusqu'à ce que l'invite de démarrage LILO s'affiche. Par exemple :

   ```
   GNU/Linux - LILO 24 - Menu de démarrage
   6.1.0
   System_Restore
   Restore_Serial
   ```

4. Indiquez que vous souhaitez restaurer le système :
   - Pour une connexion de clavier et de moniteur, utilisez les touches fléchées pour sélectionner **System_Restore** et appuyez sur Enter (Entrée).
   - Pour une connexion série ou SOL/LOM, saisissez **Restore_Serial** à l'invite et appuyez sur Enter (Entrée).

   Dans les deux cas, l'invite de démarrage s'affiche après les choix suivants :

   ```
   10. Charger avec une console standard
   1. Charger avec une console série
   ```

5. Sélectionnez un mode d'affichage pour le menu interactif de l'utilitaire de restauration :
   - Pour une connexion de clavier et de moniteur, saisissez `0` et appuyez sur Enter (Entrée).
   - Pour une connexion de série ou SOL/LOM, saisissez `1` et appuyez sur Entrée.

   Si vous ne sélectionnez pas de mode d'affichage, l'utilitaire de restauration revient par défaut à la console standard après 30 secondes.

À moins que ce ne soit la première fois que vous restaurez l'appareil vers cette version majeure, l'utilitaire charge automatiquement la dernière configuration de restauration que vous avez utilisée. Pour continuer, confirmez les paramètres dans une série de pages.

6. Appuyez sur Entrée pour confirmer l'avis de droit d'auteur.

Que faire ensuite?

- Commencez la deuxième passe du processus, en commençant par Utilisation du menu interactif pour restaurer un appareil, page 31.

Deuxième ou seul passage

Utilisez la procédure suivante pour effectuer le deuxième ou seul passage du processus de restauration.

Pour effectuer le deuxième ou seul passage du processus de restauration :

1. Si vous effectuez la deuxième passe d'un processus de restauration en deux temps, téléchargez et montez à nouveau l'image ISO, comme décrit dans Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35.
2. Dans le menu principal de l'utilitaire de restauration, sélectionnez **5 Exécuter l'installation**.
3. Confirmez que vous souhaitez restaurer le périphérique et passez à l'étape suivante.
4. Choisissez si vous souhaitez supprimer la licence du périphérique et les paramètres réseau.

   Dans la plupart des cas, vous ne souhaitez pas supprimer ces paramètres, car cela peut raccourcir le processus de configuration initiale. La modification des paramètres après la restauration et la configuration initiale ultérieure prend souvent moins de temps que d'essayer de les réinitialiser maintenant. Pour en savoir plus, consultez Prochaines étapes, page 39.

Mise en garde : Lors de la restauration des modèles FMC 750, 1500 ou 3500 aux paramètres d'usine à l'aide de LOM, si vous ne disposez pas d'un accès physique à l'appareil et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

Mise en garde : Lors de la restauration des modèles FMC 2000 ou 4000 à la version 6.3+ à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

5. Saisissez votre confirmation finale que vous souhaitez restaurer le périphérique.

   L'étape finale du processus de restauration commence. Lorsqu'il a terminé, si vous y êtes invité, confirmez que vous souhaitez redémarrer le périphérique.

Mise en garde : Assurez-vous de prévoir suffisamment de temps pour que le processus de restauration se termine. Sur les périphériques avec disques flash internes, l'utilitaire met d'abord à jour le disque flash, qui est ensuite utilisé pour effectuer d'autres tâches de restauration. Si vous quittez (en appuyant sur Ctrl + C, par exemple) pendant la mise à jour de la mémoire non volatile, vous risquez de provoquer une erreur irrécupérable. Si vous pensez que la restauration prend trop de temps ou si vous rencontrez d'autres problèmes avec le processus, ne quittez pas. Communiquez avec l'équipe de soutien.

Remarque : La recréation d'image réinitialise les périphériques en mode de contournement à une configuration sans contournement et interrompt le trafic sur votre réseau jusqu'à ce que vous reconfiguriez le mode de contournement. Pour en savoir plus, consultez Flux du trafic pendant le processus de restauration, page 25.

Étape suivante

- Continuez avec Prochaines étapes, page 39.

Enregistrement et chargement des configurations de restauration

Vous pouvez utiliser l'utilitaire de restauration pour enregistrer une configuration de restauration à utiliser si vous devez restaurer à nouveau un périphérique Firepower. Bien que l'utilitaire de restauration enregistre automatiquement la dernière configuration utilisée, vous pouvez enregistrer plusieurs configurations, notamment :

- les informations réseau concernant l'interface de gestion de l'appareil; consultez.Identification de l'interface de gestion du périphérique, page 33.
- l'emplacement de l'image ISO de restauration, ainsi que le protocole de transport et les informations d'authentification dont le périphérique a besoin pour télécharger le fichier; voir Spécification de l'emplacement de l'image ISO et de la méthode de transport, page 33
- les mises à jour du logiciel système et des règles de prévention des intrusions, le cas échéant, que vous souhaitez appliquer après la restauration du périphérique à la version de base dans l'image ISO; voir Mise à jour du logiciel système et des règles d'intrusion pendant la restauration, page 34

Les mots de passe SCP ne sont pas enregistrés. Si la configuration spécifie que l'utilitaire doit utiliser SCP pour transférer les fichiers ISO et d'autres fichiers vers le périphérique, vous devrez vous authentifier de nouveau auprès du serveur pour terminer le processus de restauration.

Le meilleur moment pour enregistrer une configuration de restauration est après avoir fourni les informations répertoriées ci-dessus, mais avant de télécharger et de monter l'image ISO.

Pour enregistrer une configuration de restauration

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **6 : Enregistrer la configuration**.

   L'utilitaire affiche les paramètres de la configuration que vous enregistrez.
2. Lorsque vous y êtes invité, confirmez que vous souhaitez enregistrer la configuration.
3. Lorsque vous y êtes invité, saisissez un nom pour la configuration.

Étape suivante

- Pour utiliser la configuration que vous venez d'enregistrer pour restaurer le périphérique, passez à Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35.

Pour charger une configuration de restauration enregistrée

1. Dans le menu principal de l'utilitaire de restauration, sélectionnez **7 : Charger la configuration**.

   L'utilitaire présente une liste des configurations de restauration enregistrées. La première option, **default_config**, est la configuration que vous avez utilisée en dernier pour restaurer le périphérique. Les autres options sont des configurations de restauration que vous avez enregistrées.
2. Sélectionnez la configuration que vous souhaitez utiliser.

   L'utilitaire affiche les paramètres de la configuration que vous chargez.
3. Lorsque vous y êtes invité, confirmez que vous souhaitez charger la configuration.

   La configuration est chargée. Si vous y êtes invité, confirmez l'adresse IP attribuée à l'interface de gestion du périphérique.

Étape suivante

- Pour utiliser la configuration que vous venez de charger pour restaurer le périphérique, continuez avec Téléchargement de l'image ISO et mise à jour des fichiers, et montage de l'image, page 35.

Prochaines étapes

La restauration de votre périphérique aux paramètres d'usine par défaut entraîne la perte de presque **toutes** les données de configuration et d'événements sur le périphérique. Notez que la suppression des paramètres de licence et de réseau réinitialise également les paramètres LOM dans certains cas.

La conservation des paramètres LOM après le processus de restauration varie selon le modèle et la version de Firepower :

- Si vous restaurez un modèle FMC 750, 1500 ou 3500 aux paramètres d'usine par défaut, la suppression de la licence et des paramètres réseau réinitialise également les paramètres LOM.

Mise en garde : Lors de la restauration des modèles FMC 750, 1500 ou 3500 aux paramètres d'usine à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

- Si vous restaurez un modèle FMC 2000 ou 4000 aux paramètres d'usine par défaut :
  - Si vous restaurez le périphérique à la version 6.2.3 ou antérieure, le système *ne* réinitialise pas les paramètres LOM, que vous choisissiez ou non de supprimer la licence et les paramètres réseau.
  - Si vous restaurez le périphérique à la version 6.3+, le système réinitialise les paramètres LOM, que vous choisissiez ou non de supprimer la licence et les paramètres réseau.

Mise en garde : Lors de la restauration des modèles FMC 2000 ou 4000 à la version 6.3+ à l'aide de LOM, si vous n'avez pas d'accès physique au périphérique et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder au FMC après la restauration.

Après avoir restauré un périphérique, vous devez effectuer un processus de configuration initiale :

- Si vous n'avez pas supprimé la licence et les paramètres réseau du périphérique, vous pouvez utiliser un ordinateur de votre réseau de gestion pour accéder directement à l'interface Web du périphérique afin d'effectuer la configuration. Pour en savoir plus :
  - Pour les versions 5.4.x – 6.4.x, consultez Configuration initialeCentre de gestion, page 14.
  - Pour les versions 6.5 et ultérieures, consultez Assistant de configuration initiale du centre du Firepower Management Center, page 7.
- Si vous avez supprimé les paramètres de licence et le réseau, vous devez configurer l'appareil comme s'il était nouveau, en commençant par le configurer pour qu'il communique sur votre réseau de gestion. Pour en savoir plus :
  - Pour les versions 5.4.x – 6.4.x, consultez Installation et configuration initiale pour les versions 5.4 à 6.4.x, page 11.
  - Pour les versions 6.5 et ultérieures, consultez Installation et configuration initiale pour les versions 6.5 et ultérieures, page 4.
- Si vous avez désinscrit le Firepower Management Center de Cisco Smart Software Manager, enregistrez le périphérique dans Cisco Smart Software Manager. Sélectionnez **Système > Licences > Licences Smart** et cliquez sur l'icône d'enregistrement.

Une fois le processus de configuration initiale terminé :

- Si vous souhaitez utiliser une connexion série ou SOL/LOM pour accéder à la console de votre appareil, vous devez rediriger la sortie de la console; consultez Rediriger la sortie de la console, page 21.
- Si LOM a été réinitialisé pendant la restauration et que vous souhaitez utiliser LOM, vous devez réactiver la fonctionnalité et activer au moins un utilisateur LOM; consultez Activation de LOM et des utilisateurs LOM, page 41.

Configurer Lights-Out Management

Si vous devez restaurer unFirepower appareil aux paramètres d'usine et que vous n'avez pas d'accès physique à l'équipement, vous pouvez utiliser la gestion hors bande (LOM) pour effectuer le processus de restauration. Notez que vous pouvez utiliser Lights-Out Management sur l'interface de gestion par défaut (`eth0`) uniquement.

La fonction Lights-Out Management (LOM) vous permet d'effectuer un ensemble limité d'actions sur un appareil Firepower à l'aide d'une connexion Serial over LAN (SOL). Avec LOM, vous utilisez une interface de ligne de commande sur une connexion de gestion hors bande pour effectuer des tâches telles que l'affichage du numéro de série du châssis ou la surveillance de conditions telles que la vitesse et la température du ventilateur.

Mise en garde : Les centres de gestion Firepower Management Center 2000 et 4000 ont introduit la plateforme Cisco Unified Computing System (UCS) dans le système Firepower. Ces modèles ne prennent pas en charge les fonctionnalités Cisco qui utilisent des outils sur le contrôleur de gestion de la carte mère (BMC), comme UCS Manager ou Cisco Integrated Management Controller (CIMC), pour apporter des modifications de configuration ou des mises à jour de micrologiciel.

La syntaxe des commandes LOM dépend de l'utilitaire que vous utilisez, mais les commandes LOM contiennent généralement les éléments répertoriés dans le tableau suivant.

Table 5 Syntaxe de la commande LOM :

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
IPMItool	IPMIutil	appelle l'utilitaire IPMI.
S.O.	-V4	Pour ipmiutil uniquement, active les privilèges d'administrateur pour la session LOM.
-I lanplus	-J3	Active le chiffrement pour la session LOM.
-H *adresse IP*	-N *adresse IP*	Précise l'adresse IP de l'interface de gestion sur le périphérique.
-U *username*	-U *username*	Indique le nom d'utilisateur d'un compte LOM autorisé.
s.o. (invite lors de la connexion)	-P *password*	Pour ipmiutil uniquement, spécifie le mot de passe d'un compte LOM autorisé.
commande	commande	La commande que vous souhaitez émettre au périphérique . Notez que l'endroit où vous exécutez la commande dépend de l'utilitaire : ■ Pour IPMItool, saisissez la commande en dernier. ■ Pour ipmiutil, saisissez la commande en premier.

Par conséquent, pour IPMItool :

```
ipmitool -I lanplus -H IP_address -U username command
```

Ou, pour ipmiutil :

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

Notez que les commandes `mise hors tension du châssis` et `cycle d'alimentation du châssis` ne sont pas valides sur les appareils Gamme 70xx. Pour obtenir la liste complète des commandes LOM prises en charge par le Système Firepower, consultez le chapitre de configuration des paramètres de l'appareil dans le *Guide de configuration de Firepower Management Center*.

Remarque : Dans certains scénarios de cycle d'alimentation, le contrôleur de gestion de la carte mère (BMC) d'un Firepower 7050 connecté au réseau par l'intermédiaire de l'interface de gestion peut perdre l'adresse IP qui lui est attribuée par le serveur DHCP. Pour cette raison, Cisco vous recommande de configurer le Firepower 7050 BMC avec une adresse IP statique. Sinon, vous pouvez déconnecter le câble réseau et le reconnecter, ou couper et rétablir l'alimentation du périphérique pour forcer la renégociation du lien.

Avant de pouvoir restaurer un appareil à l'aide de LOM, vous devez activer LOM pour le périphérique et l'utilisateur qui effectuera la restauration. Ensuite, utilisez un utilitaire tiers d'interface de gestion de plateforme intelligente (IPMI) pour accéder au périphérique. Vous devez également vous assurer de rediriger la sortie de la console du périphérique vers le port série.

Pour en savoir plus, consultez les sections suivantes :

- Activation de LOM et des utilisateurs LOM, page 41
- Installation d'un utilitaire IPMI, page 42

Activation de LOM et des utilisateurs LOM

Avant de pouvoir utiliser LOM pour restaurer un appareil, vous devez activer et configurer la fonctionnalité. Vous devez également explicitement accorder des autorisations LOM aux utilisateurs qui utiliseront la fonctionnalité.

Vous configurez LOM et les utilisateurs LOM pour chaque appareil à l'aide de l'interface Web locale de chaque appareil. C'est-à-dire que vous ne pouvez pas utiliser le Centre de gestion pour configurer LOM sur un Firepower périphérique. De même, comme les utilisateurs sont gérés indépendamment pour chaque périphérique, l'activation ou la création d'un utilisateur prenant en charge LOM sur le Centre de gestion ne transfère pas cette capacité aux utilisateurs sur les périphériques Firepower.

Les utilisateurs de LOM sont également soumis aux restrictions suivantes :

- Vous devez attribuer le rôle d'administrateur à l'utilisateur.
- Le nom d'utilisateur peut comporter jusqu'à 16 caractères alphanumériques. Les tirets et les noms d'utilisateur plus longs ne sont pas pris en charge pour les utilisateurs LOM.
- Le mot de passe peut comporter jusqu'à 20 caractères alphanumériques. Les mots de passe plus longs ne sont pas pris en charge pour les utilisateurs LOM. Le mot de passe LOM d'un utilisateur est identique au mot de passe système de cet utilisateur.
- Les Centre de gestion peuvent avoir jusqu'à treize utilisateurs LOM.

  Remarque : Pour des instructions détaillées sur les tâches suivantes, consultez le chapitre Configuration des paramètres de l'appareil dans *Guide de configuration de Firepower Management Center*.

Pour activer LOM :

1. Sélectionnez **System > Configuration**, puis cliquez sur **Console Configuration**.
2. Activez l'accès à distance à l'aide du **port de série physique** avant de préciser l'adresse IP LOM, le masque réseau et la passerelle par défaut (ou utilisez DHCP pour que ces valeurs soient automatiquement affectées).

Remarque : L'adresse IP LOM doit être différente de l'adresse IP de l'interface de gestion du périphérique.

Pour activer les fonctionnalités LOM pour un utilisateur Système Firepower :

1. Sélectionnez **Système > Gestion des utilisateurs**, puis modifiez un utilisateur existant pour ajouter des autorisations LOM ou créez un nouvel utilisateur que vous utiliserez pour l'accès LOM au périphérique.
2. Sur la page de configuration des utilisateurs, activez le rôle **d'administrateur** s'il n'est pas déjà activé.
3. Cochez la case **Autoriser l'accès Lights-Out Management** et enregistrez vos modifications.

Installation d'un utilitaire IPMI

Vous utilisez un utilitaire IPMI tiers sur votre ordinateur pour créer une connexion SOL avec l'appareil.

Si votre ordinateur exécute Linux ou Mac OS, utilisez IPMItool. Bien qu'IPMItool soit standard avec de nombreuses distributions Linux, vous devez installer IPMItool sur un Mac. Tout d'abord, vérifiez que les outils XCode pour développeur d'Apple sont installés sur votre Mac. Assurez-vous que les composants facultatifs pour le développement de ligne de commande sont installés (outils système et de développement UNIX dans les versions plus récentes ou assistance de ligne de commande dans les versions antérieures). Enfin, installez MacPorts et IPMItool. Utilisez votre moteur de recherche préféré pour obtenir de plus amples renseignements ou consultez les sites suivants :

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Pour les environnements Windows , utilisez ipmiutil, que vous devez compiler vous-même. Si vous n'avez pas accès à un compilateur, vous pouvez utiliser ipmiutil pour compiler. Utilisez votre moteur de recherche préféré pour obtenir de plus amples renseignements ou essayez ce site :

```
http://ipmiutil.sourceforge.net/
```

Préconfiguration du Firepower Centre de gestions

Vous pouvez préconfigurer votre Centre de gestion à un emplacement *de mise en place* (un emplacement central pour préconfigurer ou mettre en place plusieurs périphériques) en vue d'un déploiement à un emplacement *cible* (tout emplacement autre que l'emplacement de mise en place).

Pour préconfigurer et déployer un appareil à un emplacement cible, procédez comme suit :

- Installez le système sur l'appareil à l'emplacement de préconfiguration.
- Arrêtez et expédiez le périphérique vers l'emplacement cible.
- Déployez les périphériques dans les emplacements cibles.

Remarque : Conservez tous les matériels d'emballage et incluez tout le matériel de référence et les cordons d'alimentation lors du remballage de l'appareil.

Avant de commencer

Avant de préconfigurer l'appareil, collectez les paramètres réseau, les licences et les autres informations pertinentes pour l'emplacement de mise en place et l'emplacement cible.

Remarque : Il peut être utile de créer une feuille de calcul pour gérer ces informations à l'emplacement de mise en place et à l'emplacement cible.

Lors de la configuration initiale, vous configurez votre appareil avec suffisamment de renseignements pour le connecter au réseau et installer le système.

Informations de préconfiguration requises

Vous avez besoin des renseignements suivants au minimum pour préconfigurer votre appareil :

- Le nouveau mot de passe (la configuration initiale nécessite la modification du mot de passe)
- Le nom d'hôte de l'appliance
- Le nom de domaine de l'appareil
- L'adresse IP de l'appareil
- Le masque réseau de l'appareil à l'emplacement cible

- La passerelle par défaut de l'appareil à l'emplacement cible
- L'adresse IP du serveur DNS à l'emplacement de mise en place ou, si accessible, à l'emplacement cible
- L'adresse IP du serveur NTP à l'emplacement de mise en place ou, si accessible, à l'emplacement cible

Renseignements facultatifs sur la préconfiguration

Vous pouvez modifier certaines configurations par défaut, telles que :

- Définissez le fuseau horaire si vous choisissez de régler manuellement l'heure pour vos appareils
- Définissez l'emplacement de stockage distant pour les sauvegardes automatiques.
- Définir l'adresse IP de Lights-Out Management (LOM) pour activer LOM

Remarque : Dans certains scénarios de cycle d'alimentation, le contrôleur de gestion de la carte mère (BMC) d'un appareil 3D7050 connecté au réseau par l'intermédiaire de l'interface de gestion peut perdre l'adresse IP qui lui est attribuée par le serveur DHCP. Pour cette raison, Cisco vous recommande de configurer le BMC 3D7050 avec une adresse IP statique. Sinon, vous pouvez déconnecter le câble réseau et le reconnecter, ou couper et rétablir l'alimentation du périphérique pour forcer la renégociation du lien.

Préconfiguration de la gestion du temps

Gardez à l'esprit les considérations suivantes :

- Cisco vous recommande de synchroniser l'heure avec un serveur NTP physique.
- Si le réseau de votre emplacement de mise en place peut accéder aux serveurs DNS et NTP de l'emplacement cible, utilisez les adresses IP pour les serveurs DNS et NTP de l'emplacement cible. Sinon, utilisez les informations d'emplacement de stockage et réinitialisez-le à l'emplacement cible.
- Utilisez le fuseau horaire pour le déploiement cible si vous réglez l'heure sur le périphérique manuellement au lieu d'utiliser le protocole NTP; consultez le *Guide de configuration de Firepower Management Center* pour obtenir plus d'informations.

Installation du système

Utilisez les procédures d'installation décrites dans Installation et configuration initiale pour les versions 5.4 à 6.4.x, page 11 et Installation de l'appliance, page 12. Pour de l'information supplémentaire, reportez-vous au *Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 750, 1500, 2000, 3500 et 4000*.

Lors de la préconfiguration du système, gardez les éléments suivants à l'esprit :

- Ajoutez des licences pour les périphériques gérés lors de la configuration initiale. Si vous n'ajoutez pas de licences à ce moment-là, tous les périphériques que vous enregistrez lors de la configuration initiale sont ajoutés à Centre de gestion comme sans licence; vous devez obtenir une licence pour chacun d'entre eux individuellement une fois le processus de configuration initiale terminé. Consultez Paramètres des licences, page 17.

Préparation de l'appareil pour l'expédition

Pour préparer l'appareil avant l'expédition, vous devez le mettre hors tension et le remballer en toute sécurité :

- Pour mettre l'appareil hors tension en toute sécurité, consultez le *Guide d'installation du matériel pour Cisco Firepower Management Center 1000, 2500 et 4500*.
- Pour vous assurer que votre appareil est préparé en toute sécurité pour l'expédition, consultez Facteurs à prendre en considération pour l'expédition, page 44.

Suppression d'une licence à partir d'un Centre de gestion

Utilisez la procédure suivante si vous devez supprimer une licence pour quelque raison que ce soit. Gardez à l'esprit que, comme Cisco génère des licences en fonction de la clé de licence unique de chaque Centre de gestion, vous ne pouvez pas supprimer une licence d'un Centre de gestion et la réutiliser sur un autre Centre de gestion. Pour en savoir plus, consultez le Système Firepower dans le *Guide de configuration de Firepower Management Center*.

Pour supprimer une licence :

1. Sélectionnez **Systèmes > Licences**.
2. À côté de la licence que vous souhaitez supprimer, cliquez sur l'icône de suppression ( ).

   La suppression d'une licence supprime la capacité sous licence de tous les périphériques utilisant cette licence. Par exemple, si votre licence Protection est valide et activée pour 100 appareils gérés, la suppression de la licence supprime les capacités de protection pour l'ensemble de ces 100 appareils.
3. Confirmez que vous souhaitez supprimer la licence.

   La licence est supprimée

Facteurs à prendre en considération pour l'expédition

Pour préparer l'appareil en vue de son envoi vers l'emplacement cible, vous devez le mettre hors tension et le remballer en toute sécurité. Gardez à l'esprit les considérations suivantes :

- Utilisez l'emballage d'origine pour remballer l'appareil.
- Incluez toute la documentation de référence ainsi que les cordons d'alimentation avec l'appareil.
- Fournissez toutes les informations de paramètre et de configuration à l'emplacement cible, y compris le nouveau mot de passe et le mode de détection.

Dépannage de la préconfiguration du périphérique

Si votre appareil est correctement préconfiguré pour le déploiement cible, vous pouvez l'installer et le déployer sans autre configuration.

Si vous avez des difficultés à vous connecter au périphérique, la préconfiguration peut avoir une erreur. Essayez les procédures de dépannage suivantes :

- Confirmez que tous les câbles d'alimentation et les câbles de communication sont connectés correctement au périphérique.
- Confirmez que vous avez le mot de passe actuel pour votre appareil. La configuration initiale à l'emplacement de mise en place vous invite à modifier votre mot de passe. Consultez les renseignements de configuration fournis par l'emplacement de mise en place pour le nouveau mot de passe.
- Confirmez que les paramètres réseau sont corrects. Consultez Configuration initialeCentre de gestion, page 14.
- Confirmez que les ports de communication appropriés fonctionnent correctement. Consultez la documentation de votre pare-feu pour en savoir plus sur la gestion des ports de pare-feu. Consultez *Guide de configuration de Firepower Management Center* pour connaître les ports requis.

Si vous continuez à rencontrer des difficultés, communiquez avec votre service des technologies de l'information.

Nettoyage du disque dur

Vous pouvez effacer en toute sécurité le disque dur sur les centres de gestion et les périphériques Firepower pour vous assurer que son contenu ne peut plus être accessible. Par exemple, si vous devez retourner un appareil défectueux contenant des données sensibles, vous pouvez utiliser cette fonctionnalité pour écraser ces données.

Ce mode de nettoyage du disque est conforme à la norme Militaire suivante :

NORMES

La séquence d'effacement DoD est conforme à la procédure DoD 5220.22-M pour l'assainissement des disques rigides, amovibles ou non, qui exige l'écrasement de toutes les zones adressables avec un caractère, son complément, puis un caractère aléatoire, suivi d'une vérification. Veuillez consulter le document DoD pour connaître les contraintes supplémentaires.

Mise en garde : L'effacement de votre disque dur entraîne la perte de toutes les données sur le périphérique, ce qui le rend inutilisable.

Vous effacez le disque dur à l'aide d'une option dans le menu interactif décrit dans Utilisation du menu interactif pour restaurer un appareil, page 31.

Pour effacer le disque dur :

1. Suivez les instructions dans l'une des sections suivantes pour afficher le menu interactif de l'utilitaire de restauration, en fonction de la façon dont vous accédez au périphérique :
   - Démarrage de l'utilitaire de restauration à l'aide d'un protocole KVM ou d'un port série physique, page 28
   - Démarrage de l'utilitaire de restauration à l'aide de Lights-Out Management, page 30
2. Dans le menu principal de l'utilitaire de restauration, sélectionnez **8 Effacer le contenu du disque**.
3. Lorsque vous y êtes invité, confirmez que vous souhaitez effacer le disque dur.

Le disque dur est effacé. Le processus d'effacement peut prendre quelques heures; les disques plus volumineux prennent plus de temps.

Documentation associée

Pour obtenir une liste complète de la documentation sur la gamme Cisco Firepower Management Center et savoir où la trouver, consultez la feuille de route de la documentation à l'URL suivante :

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html