Guide de démarrage (GD) pour Cisco Firepower Management Center 1600, 2600 et 4600

Dernière modification : 2026-05-14

Guide de démarrage pour Cisco Firepower Management Center 1600, 2600 et 4600

Le *Guide de démarrage du Firepower Management Center 1600, 2600 et 4600* explique l'installation, la connexion, la configuration, les paramètres administratifs initiaux et la configuration de votre réseau sécurisé. Ce document décrit également les activités de maintenance telles que la mise en place de moyens d'accès alternatifs au Firewall Management Center, l'ajout d'appareils gérés au Firewall Management Center, la réinitialisation aux paramètres d'usine, l'enregistrement et le chargement des configurations, l'effacement du disque dur et l'exécution d'un arrêt ou d'un redémarrage.

Dans un déploiement type sur un grand réseau, vous installez plusieurs dispositifs gérés sur des segments de réseau. Chaque appareil contrôle, inspecte, supervise et analyse le trafic, puis envoie un rapport à un Firewall Management Center. Firewall Management Center fournit une console de gestion centralisée avec une interface Web que vous pouvez utiliser pour effectuer des tâches d'administration, de gestion, d'analyse et de création de rapports en cours de services pour sécuriser votre réseau local.

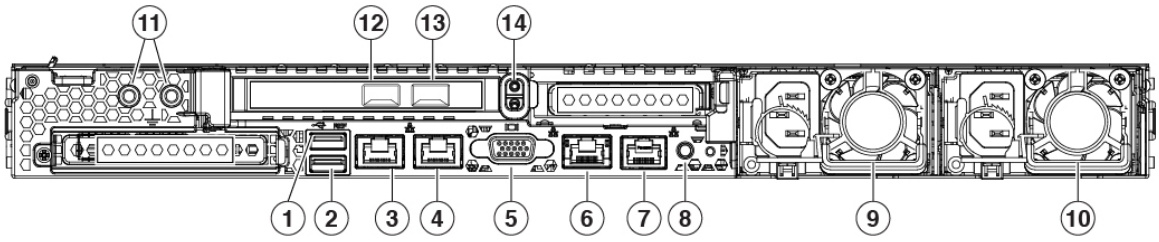
À propos des modèles Cisco Firepower Management Center 1600, 2600 et 4600

Les rubriques suivantes fournissent des renseignements sur les fonctionnalités des panneaux avant et arrière dont vous devez suivre les instructions dans ce document.

Fonctionnalités du panneau arrière

L'illustration suivante présente le panneau arrière des Firepower Management Center 1600, 2600 et 4600. Pour en savoir plus sur les fonctionnalités du panneau arrière, consultez Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Illustration 1 : Panneau arrière

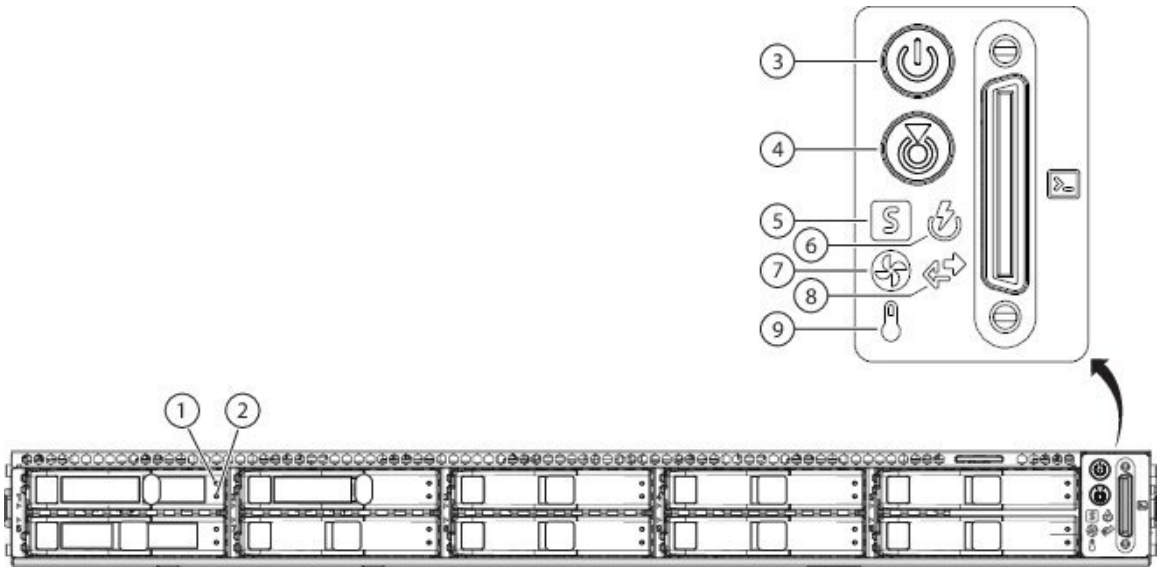


1	USB 3.0 de type A (USB 1) Vous pouvez connecter un clavier et un moniteur sur le port VGA, vous pouvez accéder à la console.	**2**	USB 3.0 de type A (USB 2) Vous pouvez connecter un clavier et un moniteur sur le port VGA, vous pouvez accéder à la console.
3	Interface de gestion eth0 (étiquetée « 1 ») Prend en charge 100/1000/10000 Mbit/s, selon les capacités du partenaire de liaison.	**4**	interface de gestion eth1 (étiquetée « 2 ») Interface Gigabit Ethernet 100/1000/10000 Mbit/s, RJ-45, LAN2
5	Port VGA vidéo (connecteur DE-15)	**6**	Interface CIMC (étiquetée M) Prise en charge pour la gestion Lights-Out *uniquement*.
7	Port série de console (connecteur RJ-45) L'option est désactivée par défaut.	**8**	Bouton d'identification des unités
9	Bloc d'alimentation CA de 770 W (PSU 1)	**10**	Bloc d'alimentation CA de 770 W (PSU 2)
11	Trous filetés pour cosse de mise à la terre à deux trous.	**12**	Interface de gestion eth2 Prise en charge SFP+ 4x10-Gigabit Ethernet SFP-10G- SR et SFP-10G-LR sont qualifiés pour une utilisation sur le Firewall Management Center.
13	Interface de gestion eth3 Prise en charge SFP+ 4x10-Gigabit Ethernet SFP-10G- SR et SFP-10G-LR sont qualifiés pour une utilisation sur le Firewall Management Center.	**14**	Poignée d'extension Non pris en charge

Voyants DEL du panneau avant et leurs états

La figure suivante illustre le panneau avant du Cisco Firepower Management Center 1600, 2600 et 4600, identifie les voyants DEL et fournit les renseignements dont vous avez besoin pour déterminer l'état de l'appareil en fonction des voyants DEL. Le Cisco Firepower Management Center 2600 est doté de quatre disques SAS et le Cisco Firepower Management Center 4600 de six disques SAS, chacun avec les mêmes voyants DEL de défaillance de lecteur et d'activité de lecteur, comme indiqué dans le schéma. Pour en savoir plus sur toutes les fonctionnalités du panneau avant, consultez Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Illustration 2 : Voyants DEL du panneau avant et leurs états



1	Voyants DEL de panne du lecteur : • Éteint : le disque fonctionne correctement. • Orange : défaillance de lecteur détectée. • Orange, clignotant : le lecteur est en cours de reconstruction. • Orange, clignotant avec un intervalle d'une seconde : fonction de localisation de lecteur activée dans le logiciel.	**2**	Voyants DEL d'activité du lecteur : • Éteint : il n'y a pas de lecteur dans le tiroir (aucun accès, pas d'erreur). • Vert : le lecteur est prêt. • Vert, clignotant : le lecteur lit ou écrit des données.
3	Voyant DEL d'alimentation : • Éteint : aucune alimentation CA au châssis. • Orange : le châssis est en mode veille. • Vert : le châssis est en mode d'alimentation principal. L'alimentation est fournie à tous les composants.	**4**	Voyants DEL d'identification des unités : • Éteint : la fonction d'identification de l'unité n'est pas utilisée. • Bleu, clignotant : la fonction d'identification de l'unité est activée.

5	Voyants DEL d'état du système :
	• Vert : le châssis fonctionne dans des conditions normales.
	• Vert, clignotant : le châssis exécute l'initialisation du système et la vérification de la mémoire.
	• Orange : le châssis est dans un état opérationnel dégradé (défaillance mineure).
	  • La redondance de l'alimentation électrique est perdue.
	  • Les processeurs ne correspondent pas.
	  • Au moins un processeur est défaillant.
	  • Au moins un module DIMM est défaillant.
	  • Au moins un lecteur dans la configuration RAID a échoué.
	• Orange, deux clignotements : il y a une défaillance majeure de la carte système.
	• Orange, trois clignotements : il y a une défaillance majeure des modules DIMM.
	• Orange, quatre clignotements : il y a une défaillance majeure des CPU.
		6	Voyant DEL de l'état de l'alimentation :
			• Vert : tous les modules d'alimentation fonctionnent normalement.
			• Orange : un ou plusieurs modules d'alimentation sont en état de fonctionnement dégradé.
			• Orange, clignotant : un ou plusieurs modules d'alimentation sont en état de défaillance critique.

7	DEL d'état du ventilateur : • Vert : tous les ventilateurs fonctionnent correctement. • Orange, clignotant : un ou plusieurs ventilateurs ont dépassé le seuil irrécupérable.	**8**	Voyant DEL de l'activité des liaisons du réseau : • Éteint : la liaison Ethernet est inactive. • Vert : un ou plusieurs ports Ethernet sont à liaison active, mais il n'y a aucune activité. • Vert, clignotant : un ou plusieurs ports Ethernet sont à liaison active avec l'activité.
9	Voyant DEL de température : • Vert : le châssis fonctionne à une température normale. • Orange : un ou plusieurs capteurs de température ont atteint le seuil critique. • Orange, clignotant : un ou plusieurs capteurs de température ont atteint le seuil irrécupérable.		

Documentation associée

Pour plus de renseignements sur l'installation du matériel, consultez le Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Pour obtenir une liste complète de la documentation sur la gamme Cisco Secure Firewall et savoir où la trouver, consultez la feuille de route de la documentation.

Accéder à la CLI ou au Shell Linux sur le On-Prem Firewall Management Center

L'accès à l'interface de ligne de commande Firewall Management Center ou à l'interface Shell Linux nécessite une séquence d'étapes différente selon la version de Firewall Management Center.

⚠

Mise en garde Nous vous recommandons fortement de ne pas utiliser l'interface Shell Linux, sauf sur instruction contraire du TAC de Cisco ou selon des instructions explicites dans la documentation .

Avant de commencer

Établissez une connexion physique directe avec le Firewall Management Center à l'aide du port série, d'un clavier et d'un moniteur, ou établissez une session SSH avec l'interface Firewall Management Center.

Procédure

Étape 1 Connectez-vous au Firewall Management Center en utilisant les informations d'authentification de l'utilisateur **admin** de l'interface de ligne de commande.

Étape 2 Déterminez votre prochaine action en fonction de la version utilisée :

- Si votre Firewall Management Center exécute la version 6.3 ou 6.4 et que l'interface de ligne de commande Firewall Management Center n'est pas activée, cela vous donne un accès direct à l'interface Shell Linux .
- Si votre Firewall Management Center exécute la version 6.3 ou 6.4 et que l'interface de commande en ligne Firewall Management Center est activée, cela vous donne accès à l'interface de commande en ligne Firewall Management Center. Pour accéder à l'interface Shell Linux , passez à l'étape 3.
- Si votre Firewall Management Center exécute la version 6.5 ou une version ultérieure, cela vous donne accès à l'interface de ligne de commande Firewall Management Center. Pour accéder à l'interface Shell Linux , passez à l'étape 3.

Étape 3 Pour accéder à l'interface Shell Linux à partir de l'interface de ligne de commande Firewall Management Center, saisissez la commande **expert**.

Arrêter ou redémarrer le Centre de gestion

Utilisez l'interface Web pour lancer un arrêt ou un redémarrage ordonné.

Vous pouvez également arrêter Firewall Management Center à l'aide de la commande **system shutdown** depuis l'interface CLI Firewall Management Center.

Astuces Pour les appareils virtuels, consultez la documentation de votre plateforme virtuelle. Pour VMware en particulier, les options d'alimentation personnalisées font partie des outils VMware.

Mise en garde N'éteignez pas l'unité Firewall Management Center à l'aide du bouton d'alimentation; cette action peut entraîner une perte de données. L'utilisation de l'interface Web ou de la commande **shutdown** prépare le système à être éteint et redémarré en toute sécurité, sans perte de données de configuration.

Procédure

Étape 1 Connectez-vous à votre centre de gestion, puis choisissez **Système** (⚙) > **Configuration** > **Processus**.

Étape 2 Effectuez l'une des opérations suivantes :

- **Arrêtez le Firewall Management Center** pour lancer l'arrêt ordonné de Firewall Management Center.
- **Redémarrez le Firewall Management Center** pour arrêter et redémarrer Firewall Management Center de façon ordonnée.
- **Redémarrez la console du Firewall Management Center** pour relancer les processus de communication, de base de données et de serveur HTTP. Cette action est généralement utilisée lors du dépannage et peut entraîner la réapparition des hôtes supprimés dans la cartographie du réseau.

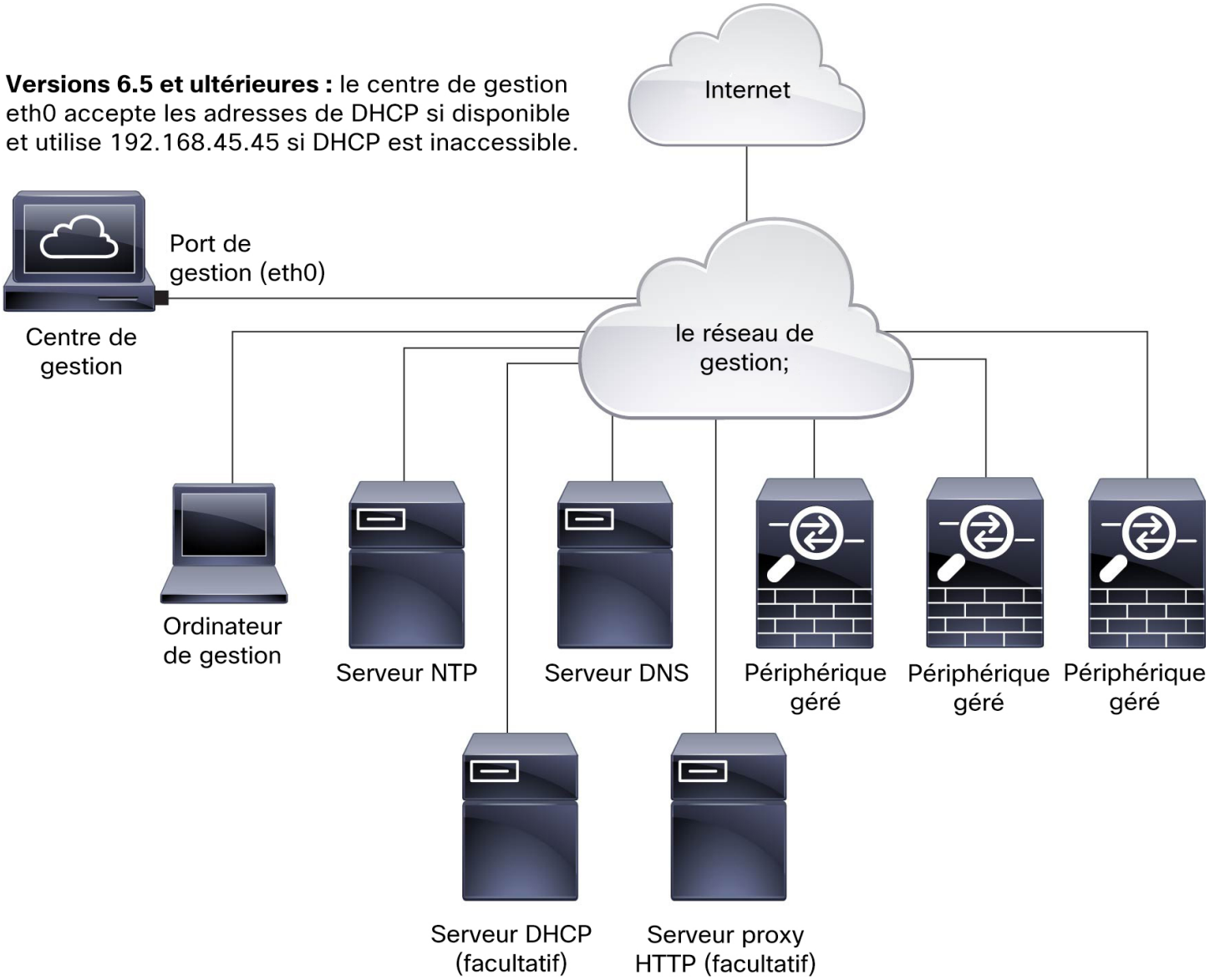
Installer le Centre de gestion pour les versions 6.5 et ultérieures

Suivez ces instructions pour installer le Firewall Management Center qui exécutera les versions 6.5 et ultérieures.

Passer en revue le déploiement du réseau pour les versions 6.5 et ultérieures

Pour déployer le Firewall Management Center, vous avez besoin d'informations sur l'environnement dans lequel il fonctionnera. La figure suivante montre un exemple de configuration réseau pour un déploiement de pare-feu.

Illustration 3 : Exemple de déploiement du réseau



Par défaut, le Firewall Management Center se connecte à votre réseau de gestion local par l'intermédiaire de son interface de gestion (eth0). Par cette connexion, le Firewall Management Center communique avec un ordinateur de gestion; appareils gérés; des services tels que DHCP, DNS, NTP; et Internet.

Le Firewall Management Center nécessite un accès Internet pour prendre en charge les services de licences Smart, Secure Firewall Threat Intelligence Director, et de défense contre les programmes malveillants. Selon les services fournis par votre réseau de gestion local, le Firewall Management Center peut également nécessiter un accès Internet pour atteindre un serveur NTP ou DNS. Vous pouvez configurer votre réseau pour fournir un accès Internet au Firewall Management Center directement ou via un appareil pare-feu.

Vous pouvez charger les mises à jour du logiciel système, ainsi que celles de la base de données des vulnérabilités (VDB), de la base de données de géolocalisation (GeoDB) et des règles d'intrusion directement

sur le Firewall Management Center à partir d'une connexion Internet ou d'un ordinateur local qui a préalablement téléchargé ces mises à jour depuis Internet.

Pour établir la connexion entre le Firewall Management Center et l'un de ses appareils gérés, vous avez besoin de l'adresse IP d'au moins un des appareils : le Firewall Management Center ou l'appareil géré. Nous vous recommandons d'utiliser les deux adresses IP, si elles sont disponibles. Cependant, vous ne pouvez connaître qu'une seule adresse IP. Par exemple, les appareils gérés peuvent utiliser des adresses privées derrière un NAT, de sorte que vous ne connaissez que l'adresse Firewall Management Center. Dans ce cas, vous pouvez spécifier l'adresse Firewall Management Center sur l'appareil géré ainsi qu'un mot de passe unique à usage unique de votre choix appelé ID NAT. Sur le Firewall Management Center, vous spécifiez le même ID NAT pour identifier l'appareil géré.

Le processus d'installation et de configuration initial décrit dans ce document suppose que le Firewall Management Center aura accès à Internet. Si vous déployez un Firewall Management Center dans un environnement isolé, consultez le Guide d'administration Cisco Secure Firewall Management Center pour votre version pour connaître les autres méthodes que vous pouvez utiliser pour prendre en charge certaines fonctionnalités telles que la configuration d'un serveur mandataire pour les communications HTTP ou l'utilisation d'un serveur satellite de logiciels Smart pour les licences Smart. Dans un déploiement où le Firewall Management Center dispose d'un accès Internet, vous pouvez charger les mises à jour du logiciel système, ainsi que de la base de données des vulnérabilités (VDB), de la base de données de géolocalisation (GeoDB) et des règles de prévention des intrusions directement sur le Firewall Management Center à partir d'une connexion Internet. Mais si le Firewall Management Center n'a pas accès à Internet, le Firewall Management Center peut charger ces mises à jour à partir d'un ordinateur local qui les a précédemment téléchargées depuis Internet. En outre, dans un déploiement isolé, vous pouvez utiliser le Firewall Management Center pour servir de l'heure aux appareils de votre déploiement.

Configuration réseau initiale pour les centres de gestion utilisant les versions 6.5 et ultérieures :

- Interface de gestion

  Par défaut, Firewall Management Center recherche un serveur DHCP local pour l'adresse IP, le masque réseau et la passerelle par défaut à utiliser pour l'interface de gestion (eth0). Si le Firewall Management Center ne parvient pas à atteindre un serveur DHCP, il utilise l'adresse IPv4 par défaut 192.168.45.45, le masque de réseau 255.255.255.0 et la passerelle 192.168.45.1. Lors de la configuration initiale, vous pouvez accepter ces valeurs par défaut ou spécifier des valeurs différentes.

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

  Si vous choisissez d'utiliser l'adressage IPv6 pour l'interface de gestion, vous devez le configurer par le biais de l'interface Web après avoir terminé la configuration initiale.

- DNS Server(s) [Serveur(s) DNS]

  Spécifiez les adresses IP pour un maximum de deux serveurs DNS. Si vous utilisez une licence d'évaluation, vous pouvez choisir de ne pas utiliser DNS. (Lors de la configuration initiale, vous pouvez également fournir un nom d'hôte et un domaine pour faciliter les communications entre le Firewall

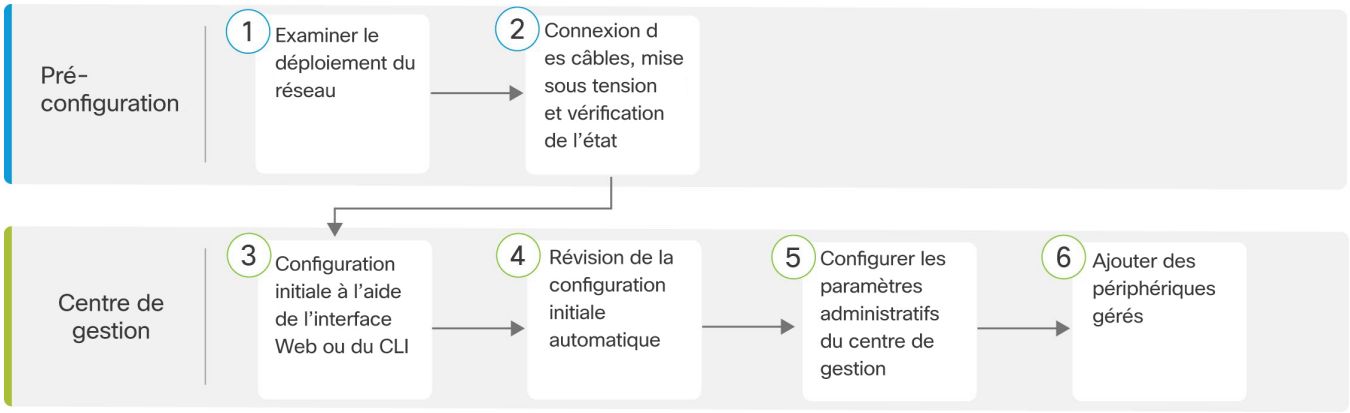
Management Center et d'autres hôtes par DNS; vous pouvez configurer des domaines supplémentaires après avoir terminé la configuration initiale.)

- Serveur(s) NTP

  La synchronisation de l'heure système sur votre Firewall Management Center et ses appareils gérés est essentielle au bon fonctionnement de votre système; le réglage de la synchronisation de l'heure Firewall Management Center est nécessaire lors de la configuration initiale. Vous pouvez accepter la valeur par défaut (0.sourcefire.pool.ntp.org et 1.sourcefire.pool.ntp.org comme serveurs NTP principal et secondaire, respectivement), ou fournir des noms de domaine complets ou des adresses IP pour un ou deux serveurs NTP de confiance accessibles à partir de votre réseau. (Si vous n'utilisez pas DNS, vous ne pouvez pas utiliser les noms de domaine complets pour spécifier les serveurs NTP.)

Procédure de bout en bout pour installer le Centre de gestion pour les versions 6.5 et ultérieures

Consultez les tâches suivantes pour déployer et configurer un Firewall Management Center qui exécutera les versions 6.5 et ultérieures.



1	Pré-configuration	Passer en revue le déploiement du réseau pour les versions 6.5 et ultérieures, à la page 6
2	Pré-configuration	État de vérification de l'alimentation des câbles de connexion pour les versions 6.5 et ultérieures, à la page 10
3	Centre de gestion	Utilisez l'un des éléments suivants : • Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures, à la page 12 • Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17
4	Centre de gestion	Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 20
5	Centre de gestion	Configurer les paramètres d'administration du centre de gestion, à la page 32
6	Centre de gestion	Ajouter des périphériques gérés au centre de gestion, à la page 43

État de vérification de l'alimentation des câbles de connexion pour les versions 6.5 et ultérieures

Cette procédure fait référence aux ports du panneau arrière du Cisco Firepower Management Center 1600, 2600 et 4600.

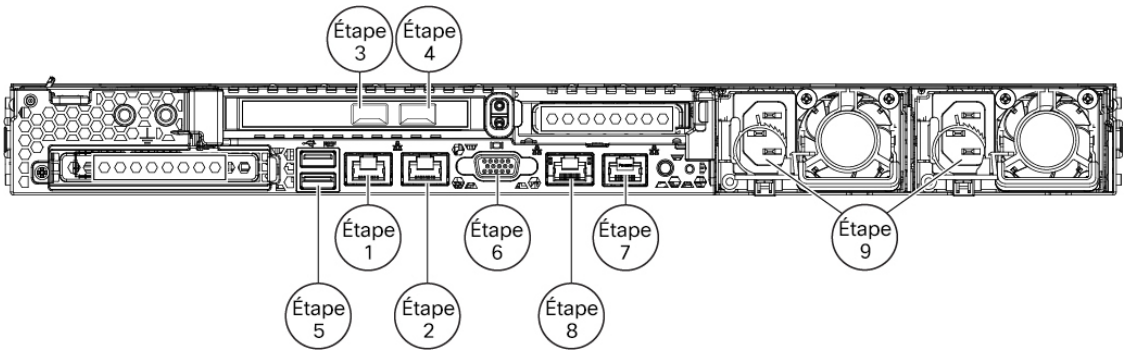
Les blocs d'alimentation CA ont une mise à la terre interne ; aucune mise à la terre de châssis supplémentaire n'est requise lorsque les cordons d'alimentation CA pris en charge sont utilisés. Pour en savoir plus sur les cordons d'alimentation pris en charge, consultez Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Nous recommandons d'établir une connexion secondaire pour assurer un accès alternatif au Firewall Management Center à des fins de dépannage, en cas de panne réseau ou d'autres problèmes empêchant l'accès à l'interface Web Firewall Management Center. Vous pouvez établir une ou plusieurs des trois connexions répertoriées ci-dessous ; Les messages de la console apparaîtront dans la sortie que vous sélectionnez dans l'interface Web Firewall Management Center sous **System (système)** > **Configuration** > **Console Configuration (configuration de console)**.

- Connectez un clavier et un moniteur au Firewall Management Center, comme décrit aux étapes 5 et 6. (Le Firewall Management Center envoie des messages de console au port VGA par défaut.)
- Connectez un ordinateur local au port série Firewall Management Center, comme décrit à l'étape 7. (Pour utiliser cette connexion, consultez Configuration de l'accès série, à la page 45.)
- Connectez le port CIMC Firewall Management Center à un réseau local accessible à partir d'un ordinateur local sur lequel vous exécuterez un utilitaire IPMI pour la gestion en service réduit, comme décrit à l'étape 8. (Pour utiliser cette connexion, consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46.)

Après avoir monté le châssis en rack, suivez ces étapes pour connecter les câbles, mettre l'appareil sous tension et vérifier la connectivité. Utilisez l'illustration suivante pour identifier les ports du panneau arrière.

Illustration 4 : Connexions des câbles



Avant de commencer

Important Lisez le document d'informations sur la sécurité, la conformité et la réglementation avant d'installer le châssis Firewall Management Center.

- Montez le périphérique en rack, comme décrit dans le Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Procédure

Étape 1 Interface de gestion eth0 (étiquetée « 1 » sur le panneau arrière) : à l'aide d'un câble Ethernet, connectez l'interface eth0 au réseau de gestion par défaut accessible à partir de votre ordinateur de gestion. Cette interface est l'interface de gestion par défaut et est activée par défaut. Vérifiez que le voyant DEL de liaison est activé pour l'interface réseau sur l'ordinateur local et pour l'interface de gestion Firewall Management Center.

Vous pouvez utiliser cette connexion pour configurer les paramètres réseau et effectuer la configuration initiale en utilisant HTTPS. Vous pouvez également utiliser cette connexion pour effectuer une gestion de routine et pour gérer les périphériques à partir de l'interface Web Firewall Management Center.

Étape 2 (Facultatif) interface de gestion eth1 (étiquetée « 2 » sur le panneau arrière) : connectez cette interface de gestion au même réseau ou à un réseau différent de vos autres interfaces de gestion en fonction des besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Étape 3 (Facultatif) Interface de gestion eth2 : Installez n'importe quel émetteur-récepteur SFP+ pris en charge par Firewall Management Centeret le câble dans cette interface SFP+ de 10-Gigabit Ethernet au besoin. Vous pouvez connecter cette interface au même réseau ou à un réseau différent de vos autres interfaces de gestion selon les besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Chaque émetteur-récepteur SFP+ pris en charge par le Firewall Management Center (SFP-10G-SR and SFP-10G-LR) possède une mémoire série interne EEPROM dans laquelle sont codées les informations relatives à la sécurité. Ce codage nous permet de déterminer et de valider que l'émetteur-récepteur SFP répond aux exigences du châssis.

Remarque
Seuls les émetteurs-récepteurs SFP+ prenant en charge Firewall Management Center sont compatibles avec les interfaces de 10 Go. Cisco TAC pourrait refuser de fournir de l'assistance pour tout problème d'interopérabilité résultant de l'utilisation d'un émetteur-récepteur SFP de tiers non testé.

Étape 4 (Facultatif) Interface de gestion eth3 : Installez n'importe quel émetteur-récepteur SFP+ pris en charge par Firewall Management Centeret le câble approprié dans cette interface Ethernet 10 Gigabits SFP+ au besoin. Vous pouvez connecter cette interface au même réseau ou à un réseau différent de vos autres interfaces de gestion selon les besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Chaque émetteur-récepteur SFP+ pris en charge par le Firewall Management Center (SFP-10G-SR and SFP-10G-LR) possède une mémoire série interne EEPROM dans laquelle sont codées les informations relatives à la sécurité. Ce codage nous permet de déterminer et de valider que l'émetteur-récepteur SFP répond aux exigences du châssis.

Remarque
Seuls les émetteurs-récepteurs SFP+ prenant en charge Firewall Management Center sont compatibles avec les interfaces de 10 Go. Cisco TAC pourrait refuser de fournir de l'assistance pour tout problème d'interopérabilité résultant de l'utilisation d'un émetteur-récepteur SFP de tiers non testé.

Étape 5 (Facultatif) Port USB : connectez un clavier au port USB.

Vous pouvez utiliser cette connexion et un moniteur connecté au port VGA pour configurer les paramètres réseau et effectuer la configuration initiale au niveau de l'interface de ligne de commande (CLI) ; voir Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17.

Étape 6 (Facultatif) Port VGA : branchez un moniteur sur le port VGA.

Le Firewall Management Center envoie par défaut les messages de console au port VGA. Vous pouvez utiliser cette connexion et un clavier connecté à un port USB pour configurer les paramètres réseau et effectuer la configuration initiale au niveau de l'interface de ligne de commande ; voir Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17.

Étape 7 (Facultatif) Utilisez le câble de console RJ-45 à DB-9 fourni avec le périphérique (numéro de pièce Cisco 72-3383-XX) pour connecter un ordinateur local au port série Firewall Management Center. (Vous aurez peut-être besoin d'un adaptateur DB-9 à USB pour vous connecter à l'ordinateur local.) Vous pouvez utiliser cette connexion pour l'accès série (voir Configuration de l'accès série, à la page 45) et pour configurer les paramètres réseau et effectuer la configuration initiale au niveau de l'interface de ligne de commande (voir Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17).

Étape 8 (Facultatif) Utilisez un câble Ethernet pour connecter le port CIMC à un réseau local accessible à partir d'un ordinateur sur lequel vous exécuterez une utilitaire IPMI pour la gestion en service réduit. Consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46 pour obtenir de plus amples renseignements.

Étape 9 Bloc d'alimentation : utilisez l'un des cordons d'alimentation pris en charge pour connecter les blocs d'alimentation du châssis à votre source d'alimentation. Pour en savoir plus sur les cordons d'alimentation pris en charge, consultez Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Remarque
Nous vous recommandons de connecter les deux blocs d'alimentation sur le Firewall Management Center pour assurer une protection de la redondance . L'appareil génère une alerte d'intégrité si un seul bloc d'alimentation est connecté.

Étape 10 Alimentation : appuyez sur le bouton d'alimentation à l'avant du châssis et vérifiez que le voyant d'état d'alimentation est allumé.

Étape 11 Vérification : utilisez le diagramme dans Voyants DEL du panneau avant et leurs états , à la page 2 pour vérifier que les voyants DEL du panneau avant indiquent un bon état.

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

Si vous avez un accès HTTPS à l'adresse IP Firewall Management Center (de l'adresse obtenue de DHCP ou de l'adresse par défaut 192.168.45.45), vous pouvez effectuer la configuration initiale en utilisant HTTPS sur l'interface Web de l'appareil. Si vous devez définir manuellement l'adresse IP Firewall Management Center, consultez Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17.

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

- Le premier écran vous force à modifier le mot de passe de l'utilisateur **admin** à partir de la valeur par défaut de **Admin123**.
- Le deuxième écran présente le contrat de licence d'utilisateur final (CLUF) que vous devez accepter avant d'utiliser l'appareil.
- Le troisième écran vous permet de modifier les paramètres réseau de l'interface de gestion des appareils. Cette page est préremplie avec les paramètres actuels, que vous pouvez modifier.

  Si vous configurez un périphérique après l'avoir restauré aux valeurs par défaut (voir À propos du processus de restauration, à la page 55) et que vous n'avez pas supprimé les paramètres de licence et de réseau du périphérique, les invites seront préremplies avec les valeurs conservées.
- L' assistant effectue la validation des valeurs que vous saisissez dans cet écran pour confirmer les éléments suivants :
  - Correction syntaxique
  - Compatibilité des valeurs saisies (par exemple, adresse IP et passerelle compatibles, ou DNS fourni lorsque les serveurs NTP sont précisés à l'aide de FQDN)
  - Connectivité réseau entre le Firewall Management Center et les serveurs DNS et NTP

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

  Le système n'effectue pas de tests de connectivité si vous saisissez des valeurs de configuration qui conduiraient à couper la connexion existante entre le Firewall Management Center et le navigateur. Dans ce cas, l' assistant n'affiche aucune information sur l'état de connectivité pour le DNS ou le NTP.
- Après avoir terminé les trois écrans, une boîte de dialogue contextuelle s'affiche et vous permet de configurer rapidement et facilement les licences Smart.

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

Avant de commencer

- .Installez le Firewall Management Center comme décrit dans État de vérification de l'alimentation des câbles de connexion pour les versions 6.5 et ultérieures, à la page 10.
- Assurez-vous que les informations suivantes sont nécessaires pour que le On-Prem Firewall Management Center communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4.

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

n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.

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

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

Désactivez toutes les autres connexions réseau sur cet ordinateur.

Procédure

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

La page d'ouverture de session s'affiche.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Remarque

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

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

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

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

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

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

Prochaine étape

- Si vous avez modifié les paramètres réseau lors de la configuration initiale, vous devez vous reconnecter au Firewall Management Center en utilisant les nouvelles informations réseau.
- Le système affiche une fenêtre contextuelle qui vous permet de configurer rapidement et facilement les licences Smart. L'utilisation de cette boîte de dialogue est facultative; si votre Firewall Management Center gère des périphériques Cisco Firewall Threat Defense et que vous connaissez bien les licences Smart, utilisez cette boîte de dialogue. Sinon, ignorez cette boîte de dialogue et consultez la section « Licences » dans le Guide d'administration Cisco Secure Firewall Management Center de votre version.
- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 20 .
- Une fois que vous avez terminé l'assistant de configuration initial et désactivé la boîte de dialogue de licences Smart, le système affiche la page de gestion des périphériques, décrite dans le *Guide de configuration des périphériques de Cisco Secure Firewall Management Center*. Établissez la configuration de base pour votre On-Prem Firewall Management Center, comme décrit dans Configurer les paramètres d'administration du centre de gestion, à la page 32.
- Vous pouvez éventuellement configurer le Firewall Management Center pour l'accès en série sur LAN ou en service réduit, comme décrit dans Configurer l'accès secondaire au centre de gestion, à la page 45.

Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures

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

Avant de commencer

- .Installez le Firewall Management Center comme décrit dans État de vérification de l'alimentation des câbles de connexion pour les versions 6.5 et ultérieures, à la page 10.
- Assurez-vous que les informations suivantes sont nécessaires pour que le Firewall Management Center Virtual communique sur votre réseau de gestion :
  - Une adresse IP de gestion IPv4.

    L'interface On-Prem Firewall Management Center est préconfigurée pour accepter une adresse IP4 attribuée par DHCP. Consultez votre administrateur système pour déterminer l'IP attribuée par DHCP à l'adresse MAC On-Prem Firewall Management Center. Dans les scénarios où aucun DHCP n'est disponible, l'interface On-Prem Firewall Management Center utilise l'adresse IPv4 192.168.45.45.
  - Un masque réseau et une passerelle par défaut (si vous n'utilisez pas DHCP).
- Connectez-vous au On-Prem Firewall Management Center en utilisant l'une des trois méthodes suivantes :
  - Établissez une connexion SSH en utilisant l'adresse IP de gestion IPv4.
  - Clavier USB et moniteur VGA connectés au On-Prem Firewall Management Center pour l'accès à la console.
  - Ordinateur local relié au port série On-Prem Firewall Management Center avec un câble console RJ-45 vers DB-9.

  Utilisez SSH pour vous connecter au On-Prem Firewall Management Center en utilisant l'adresse IP de gestion IPv4.

Procédure

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

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

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

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

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

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

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

Étape 5 Répondez aux invites pour configurer les paramètres réseau.

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

- Si vous configurez un périphérique après l'avoir restauré aux valeurs par défaut (voir À propos du processus de restauration, à la page 55) et que vous n'avez pas supprimé les paramètres de licence et de réseau du périphérique, les invites seront préremplies avec les valeurs conservées.
- Appuyez sur **Enter** (Entrée) à une invite pour accepter la valeur par défaut.
- Pour le nom d'hôte, indiquez un nom de domaine complet (`<hostname>.<domain>`) ou le nom d'hôte. Ce champ est obligatoire.
- Si vous utilisez DHCP, vous devez utiliser la réservation DHCP, de sorte que l'adresse attribuée ne change pas. Si l'adresse DHCP change, l'enregistrement du périphérique échouera car la configuration réseau On-Prem Firewall Management Center n'est pas synchronisée. Pour récupérer après un changement d'adresse DHCP, connectez-vous à On-Prem Firewall Management Center (en utilisant le nom d'hôte ou la nouvelle adresse IP) et accédez à **System (Système)** > **Configuration** > **Management Interfaces (Interfaces de gestion)**pour réinitialiser le réseau.
- Si vous choisissez de configurer IPv4 manuellement, le système vous demandera l'adresse IPv4, le masque réseau et la passerelle par défaut.
- La configuration d'un serveur DNS est facultative ; pour spécifier aucun serveur DNS, saisissez **`None`** (aucun). Sinon, spécifiez les adresses IPv4 pour un ou deux serveurs DNS. Si vous spécifiez deux adresses, séparez-les par une virgule. (Si vous spécifiez plus de deux serveurs DNS, le système ignore les entrées supplémentaires.) Si votre On-Prem Firewall Management Center n'a pas d'accès Internet, vous ne pouvez pas utiliser de DNS en dehors de votre réseau local.

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

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

Exemple :

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

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

Exemple :

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

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

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

Exemple :

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

Updated network configuration.
```

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

Prochaine étape

- Vous pouvez vous connecter à l'interface Web Firewall Management Center en utilisant les informations sur le réseau que vous venez de configurer.

- Passez en revue les activités de maintenance hebdomadaires que le On-Prem Firewall Management Center configure automatiquement dans le cadre du processus de configuration initial. Ces activités sont conçues pour maintenir votre système à jour et vos données sauvegardées. Voir Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 20 .
- Vous pouvez éventuellement configurer le On-Prem Firewall Management Center pour l'accès en série sur LAN ou en service réduit, comme décrit dans Configurer l'accès secondaire au centre de gestion, à la page 45.

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

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

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

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

- Mises à jour hebdomadaires de GeoDB

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

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

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

  Cette tâche télécharge uniquement les correctifs et mises à jour urgentes (hotfix) pour la version actuellement exécutée par vos appliances ; il vous revient d'installer les mises à jour téléchargées par

cette tâche. Voir le *Guide de mise à niveau de Cisco On-Prem Firewall Management Center* pour obtenir plus d'information.

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

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

- Mise à jour de la base de données de vulnérabilités

  Dans les versions 6.6 et ultérieures, le On-Prem Firewall Management Center télécharge et installe la dernière mise à jour de la base de données des vulnérabilités (VDB) à partir du site d'assistance de Cisco. Il s'agit d'une opération unique. Vous pouvez observer l'état de cette mise à jour à l'aide de l'interface Web du centre de messages. Pour maintenir votre système à jour, si votre On-Prem Firewall Management Center a accès à Internet, nous vous recommandons de planifier des tâches pour effectuer des téléchargements et des installations de mises à jour automatiques récurrentes de la VDB, comme décrit dans Guide d'administration Cisco Secure Firewall Management Center pour votre version.

- Mise à jour quotidienne des règles d'intrusion

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

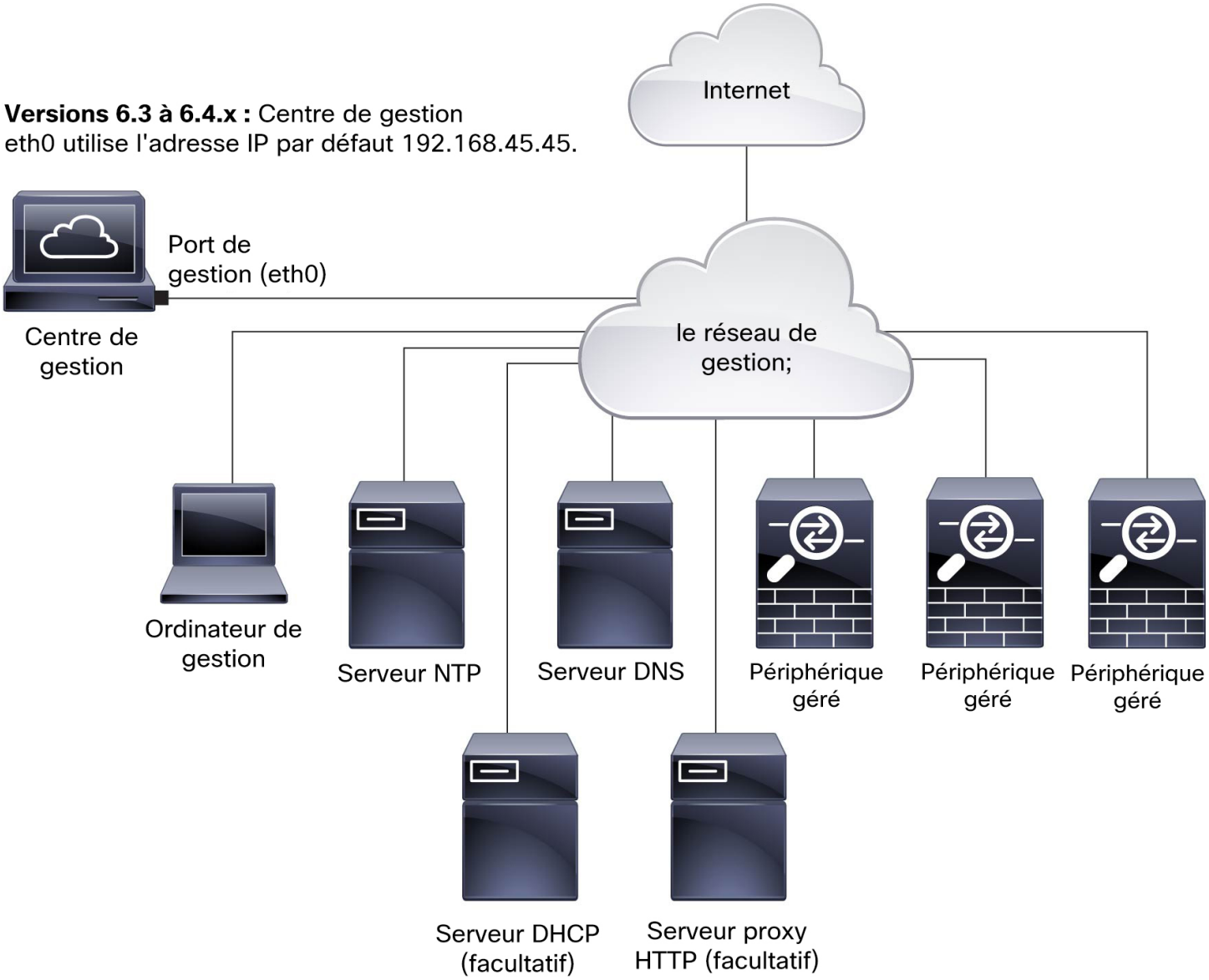
Installer le Centre de gestion pour les versions de logiciel 6.3 - 6.4

Suivez ces instructions pour installer le Firewall Management Center qui exécutera les versions 6.3 - 6.4.

Passer en revue le déploiement du réseau pour les versions 6.3-6.4

Pour déployer le Firewall Management Center, vous avez besoin d'informations sur l'environnement dans lequel il fonctionnera. La figure suivante montre un exemple de configuration réseau pour un déploiement de pare-feu.

Illustration 5 : Exemple de déploiement du réseau



Par défaut, le Firewall Management Center se connecte à votre réseau de gestion local par l'intermédiaire de son interface de gestion (eth0). Par cette connexion, le Firewall Management Center communique avec un ordinateur de gestion; appareils gérés; des services tels que DHCP, DNS, NTP; et Internet.

Le Firewall Management Center nécessite un accès Internet pour prendre en charge les licences Smart, le directeur de renseignements sur les menaces et les services de défense contre les programmes malveillants. Selon les services fournis par votre réseau de gestion local, le Firewall Management Center peut également nécessiter un accès Internet pour atteindre un serveur NTP ou DNS. Vous pouvez configurer votre réseau pour fournir un accès Internet au Firewall Management Center directement ou via un appareil pare-feu.

Vous pouvez charger les mises à jour du logiciel système, ainsi que celles de la base de données des vulnérabilités (VDB), de la base de données de géolocalisation (GeoDB) et des règles d'intrusion directement

sur le Firewall Management Center à partir d'une connexion Internet ou d'un ordinateur local qui a préalablement téléchargé ces mises à jour depuis Internet.

Pour établir la connexion entre le Firewall Management Center et l'un de ses appareils gérés, vous avez besoin de l'adresse IP d'au moins un des appareils : le Firewall Management Center ou l'appareil géré. Nous vous recommandons d'utiliser les deux adresses IP, si elles sont disponibles. Cependant, vous ne pouvez connaître qu'une seule adresse IP. Par exemple, les appareils gérés peuvent utiliser des adresses privées derrière un NAT, de sorte que vous ne connaissez que l'adresse Firewall Management Center. Dans ce cas, vous pouvez spécifier l'adresse Firewall Management Center sur l'appareil géré ainsi qu'un mot de passe unique à usage unique de votre choix appelé ID NAT. Sur le Firewall Management Center, vous spécifiez le même ID NAT pour identifier l'appareil géré.

Le processus d'installation et de configuration initial décrit dans ce document suppose que le Firewall Management Center aura accès à Internet. Si vous déployez le Firewall Management Center dans un environnement isolé, consultez le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version pour connaître les autres méthodes que vous pouvez utiliser pour prendre en charge certaines fonctionnalités, telles que la configuration d'un proxy pour les communications HTTP ou l'utilisation d'un serveur satellite de logiciels Smart pour la gestion des licences Smart. Dans un déploiement où le Firewall Management Center dispose d'un accès Internet, vous pouvez charger les mises à jour du logiciel système, ainsi que de la base de données des vulnérabilités (VDB), de la base de données de géolocalisation (GeoDB) et des règles de prévention des intrusions directement sur le Firewall Management Center à partir d'une connexion Internet. Mais si le Firewall Management Center n'a pas accès à Internet, le Firewall Management Center peut charger ces mises à jour à partir d'un ordinateur local qui les a précédemment téléchargées depuis Internet. En outre, dans un déploiement isolé, vous pouvez utiliser le Firewall Management Center pour servir de l'heure aux appareils de votre déploiement.

Configuration réseau initiale pour les Firewall Management Center utilisant les versions 6.3 - 6.4 :

- Interface de gestion

  L'interface Firewall Management Center (eth0) utilise l'adresse IPv4 par défaut 192.168.45.45, le masque réseau 255.255.255.0 et la passerelle 192.168.45.1. Lors de la configuration initiale, vous pouvez accepter ces valeurs par défaut ou spécifier des valeurs différentes.

  Si vous choisissez d'utiliser l'adressage IPv6 pour l'interface de gestion, vous avez la possibilité d'utiliser la configuration automatique du routeur ou vous devez fournir l'adresse IPv6, la longueur du préfixe et la passerelle. Si votre réseau utilise DNS, lors de la configuration initiale, vous pouvez fournir un nom d'hôte pour identifier le Firewall Management Center.

- DNS Server(s) [Serveur(s) DNS]

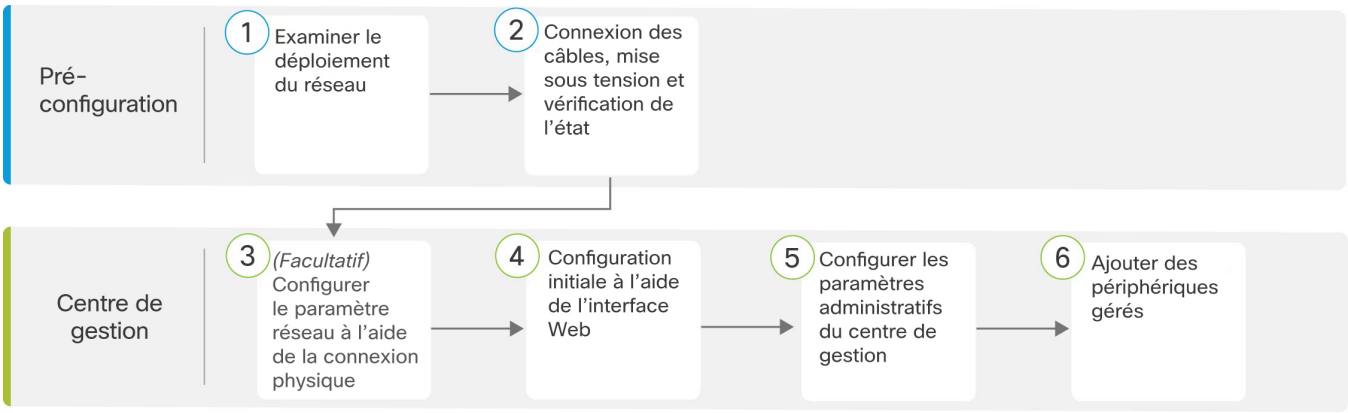
  Si votre réseau utilise le DNS, vous pouvez spécifier les adresses IP d'un maximum de trois serveurs DNS lors de la configuration initiale. Si vous utilisez une licence d'évaluation, vous pouvez choisir de ne pas utiliser DNS. (Lors de la configuration initiale, vous pouvez également fournir un nom d'hôte et un domaine pour faciliter les communications entre le Firewall Management Center et d'autres hôtes par DNS; vous pouvez configurer des domaines supplémentaires après avoir terminé la configuration initiale.)

- Serveur(s) NTP

  La synchronisation de l'horloge système sur votre Firewall Management Center et ses périphériques gérés est essentielle au bon fonctionnement de votre système. La configuration de la synchronisation de l'heure n'est pas nécessaire lors de la configuration initiale, mais nous vous recommandons de configurer votre Firewall Management Center pour utiliser des serveurs NTP fiables. Lors de la configuration initiale, vous aurez besoin des noms d'hôte ou des adresses IP de ces serveurs NTP.

Procédure de bout en bout pour installer Centre de gestion pour exécuter les versions logicielles 6.3 - 6.4

Consultez les tâches suivantes pour déployer et configurer le Firewall Management Center qui exécutera les versions 6.3 - 6.4.



1	Pré-configuration	Passer en revue le déploiement du réseau pour les versions 6.3-6.4, à la page 21
2	Pré-configuration	État de vérification de l'alimentation des câbles de connexion pour les versions 6.3 à 6.4, à la page 24
3	Centre de gestion	(Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27
4	Centre de gestion	Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4, à la page 28
5	Centre de gestion	Configurer les paramètres d'administration du centre de gestion, à la page 32
6	Centre de gestion	Ajouter des périphériques gérés au centre de gestion, à la page 43

État de vérification de l'alimentation des câbles de connexion pour les versions 6.3 à 6.4

Cette procédure fait référence aux ports du panneau arrière du Cisco Firepower Management Center 1600, 2600 et 4600.

Les blocs d'alimentation CA ont une mise à la terre interne ; aucune mise à la terre de châssis supplémentaire n'est requise lorsque les cordons d'alimentation CA pris en charge sont utilisés. Pour en savoir plus sur les cordons d'alimentation pris en charge, consultez Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

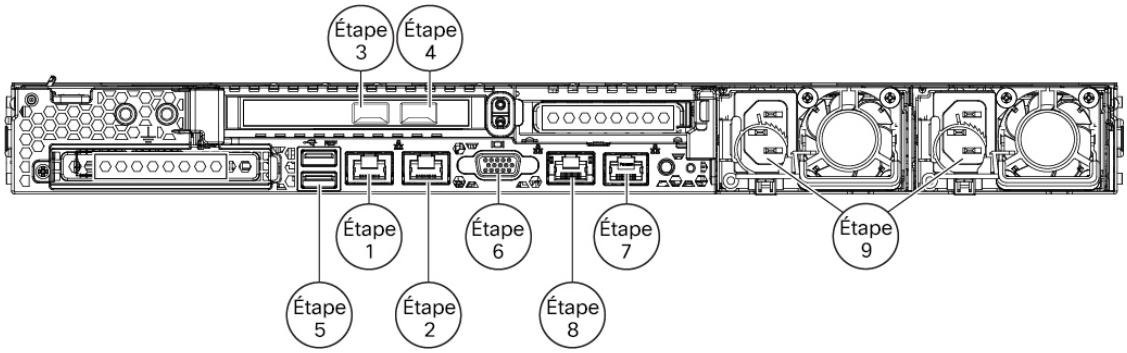
Nous recommandons d'établir une connexion secondaire pour assurer un accès alternatif au Firewall Management Center à des fins de dépannage, en cas de panne réseau ou d'autres problèmes empêchant l'accès à l'interface Web Firewall Management Center. Vous pouvez établir une ou plusieurs des trois connexions répertoriées ci-dessous ; Les messages de la console apparaîtront dans la sortie que vous sélectionnez dans

l'interface Web Firewall Management Center sous **System (système)** > **Configuration** > **Console Configuration (configuration de console)**.

- Connectez un clavier et un moniteur au Firewall Management Center, comme décrit aux étapes 5 et 6. (Le Firewall Management Center envoie des messages de console au port VGA par défaut.)
- Connectez un ordinateur local au port série Firewall Management Center, comme décrit à l'étape 7. (Pour utiliser cette connexion, consultez Configuration de l'accès série, à la page 45.)
- Connectez le port CIMC Firewall Management Center à un réseau local accessible à partir d'un ordinateur local sur lequel vous exécuterez un utilitaire IPMI pour la gestion en service réduit, comme décrit à l'étape 8. (Pour utiliser cette connexion, consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46.)

Après avoir monté le châssis en rack, suivez ces étapes pour connecter les câbles, mettre l'appareil sous tension et vérifier la connectivité. Utilisez l'illustration suivante pour identifier les ports du panneau arrière.

Illustration 6 : Connexions des câbles



Avant de commencer

Important Lisez le document d'informations sur la sécurité, la conformité et la réglementation avant d'installer le châssis Firewall Management Center.

- Montez le périphérique en rack, comme décrit dans le Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Procédure

Étape 1 Interface de gestion eth0 (étiquetée « 1 » sur le panneau arrière) : à l'aide d'un câble Ethernet, connectez l'interface eth0 au réseau de gestion par défaut accessible à partir de votre ordinateur de gestion. Cette interface est l'interface de gestion par défaut et est activée par défaut. Vérifiez que le voyant DEL de liaison est activé pour l'interface réseau sur l'ordinateur local et pour l'interface de gestion Firewall Management Center.

Vous pouvez utiliser cette connexion pour configurer les paramètres réseau et effectuer la configuration initiale en utilisant HTTPS. Vous pouvez également utiliser cette connexion pour effectuer une gestion de routine et pour gérer les périphériques à partir de l'interface Web Firewall Management Center.

Étape 2 (Facultatif) interface de gestion eth1 (étiquetée « 2 » sur le panneau arrière) : connectez cette interface de gestion au même réseau ou à un réseau différent de vos autres interfaces de gestion en fonction des besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Étape 3 (Facultatif) Interface de gestion eth2 : Installez n'importe quel émetteur-récepteur SFP+ pris en charge par Firewall Management Centeret le câble dans cette interface SFP+ de 10-Gigabit Ethernet au besoin. Vous pouvez connecter cette interface au même réseau ou à un réseau différent de vos autres interfaces de gestion selon les besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Chaque émetteur-récepteur SFP+ pris en charge par le Firewall Management Center (SFP-10G-SR and SFP-10G-LR) possède une mémoire série interne EEPROM dans laquelle sont codées les informations relatives à la sécurité. Ce codage nous permet de déterminer et de valider que l'émetteur-récepteur SFP répond aux exigences du châssis.

Remarque
Seuls les émetteurs-récepteurs SFP+ prenant en charge Firewall Management Center sont compatibles avec les interfaces de 10 Go. Cisco TAC pourrait refuser de fournir de l'assistance pour tout problème d'interopérabilité résultant de l'utilisation d'un émetteur-récepteur SFP de tiers non testé.

Étape 4 (Facultatif) Interface de gestion eth3 : Installez n'importe quel émetteur-récepteur SFP+ pris en charge par Firewall Management Centeret le câble approprié dans cette interface Ethernet 10 Gigabits SFP+ au besoin. Vous pouvez connecter cette interface au même réseau ou à un réseau différent de vos autres interfaces de gestion selon les besoins de votre réseau. Pour en savoir plus sur les interfaces de gestion, consultez le Guide d'administration Cisco Secure Firewall Management Center et sur la topologie du réseau, consultez le Guide de configuration Cisco Secure Firewall Management Center Device.

Chaque émetteur-récepteur SFP+ pris en charge par le Firewall Management Center (SFP-10G-SR and SFP-10G-LR) possède une mémoire série interne EEPROM dans laquelle sont codées les informations relatives à la sécurité. Ce codage nous permet de déterminer et de valider que l'émetteur-récepteur SFP répond aux exigences du châssis.

Remarque
Seuls les émetteurs-récepteurs SFP+ prenant en charge Firewall Management Center sont compatibles avec les interfaces de 10 Go. Cisco TAC pourrait refuser de fournir de l'assistance pour tout problème d'interopérabilité résultant de l'utilisation d'un émetteur-récepteur SFP de tiers non testé.

Étape 5 (Facultatif) Port USB : connectez un clavier au port USB.

Vous pouvez utiliser cette connexion et un moniteur connecté au port VGA pour configurer les paramètres réseau du Firewall Management Center avant d'effectuer la configuration initiale en utilisant l'interface Web ; voir (Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27.

Étape 6 (Facultatif) Port VGA : branchez un moniteur sur le port VGA.

Le Firewall Management Center envoie par défaut les messages de console au port VGA. Vous pouvez utiliser cette connexion et un clavier connecté à un port USB pour configurer les paramètres réseau pour le Firewall Management Center avant d'effectuer la configuration initiale à l'aide de l'interface Web ; voir (Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27.

Étape 7 (Facultatif) Utilisez le câble de console RJ-45 à DB-9 fourni avec le périphérique (numéro de pièce Cisco 72-3383-XX) pour connecter un ordinateur local au port série Firewall Management Center. (Vous aurez peut-être besoin d'un adaptateur DB-9 à USB pour vous connecter à l'ordinateur local.) Vous pouvez utiliser cette connexion pour l'accès série (voir Configuration de l'accès série, à la page 45) et pour configurer les paramètres réseau du Firewall Management Center avant d'effectuer la configuration initiale à l'aide de l'interface Web ; voir (Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27.

Étape 8 (Facultatif) Utilisez un câble Ethernet pour connecter le port CIMC à un réseau local accessible à partir d'un ordinateur sur lequel vous exécutez une utilitaire IPMI pour la gestion en service réduit. Consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46 pour de plus amples renseignements.

Étape 9 Bloc d'alimentation : utilisez l'un des cordons d'alimentation pris en charge pour connecter les blocs d'alimentation du châssis à votre source d'alimentation. Pour plus d'information sur les cordons pris en charge, consultez le Guide d'installation du matériel Cisco Firepower Management Center 1600, 2600 et 4600.

Remarque
Nous vous recommandons de connecter les deux blocs d'alimentation sur le Firewall Management Center pour assurer une protection de la redondance . L'appareil génère une alerte d'intégrité si un seul bloc d'alimentation est connecté.

Étape 10 Alimentation : appuyez sur le bouton d'alimentation à l'avant du châssis et vérifiez que le voyant d'état d'alimentation est allumé.

Étape 11 Vérification : utilisez le diagramme dans Voyants DEL du panneau avant et leurs états , à la page 2 pour vérifier que les voyants DEL du panneau avant indiquent un bon état.

(Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4

Vous pouvez utiliser un clavier USB et un moniteur VGA connectés directement au périphérique pour accéder à l'interface Shell Linux et exécuter un script pour établir la configuration de réseau pour le périphérique. Lorsque vous effectuez cette tâche, reportez-vous au schéma du Fonctionnalités du panneau arrière, à la page 1 pour identifier les ports du panneau arrière.

Procédure

Étape 1 Si vous ne l'avez pas encore fait, connectez le moniteur au port VGA et le clavier à l'un des ports USB à l'arrière du châssis.

Étape 2 Accédez à l'interface Shell Linux sur le Firewall Management Center en utilisant **admin** comme nom d'utilisateur et **Admin123** comme mot de passe. (Les mots de passe sont sensibles à la casse.) Suivez les étapes adaptées à votre version ; consultez Accéder à la CLI ou au Shell Linux sur le On-Prem Firewall Management Center, à la page 5.

Étape 3 Exécutez le script suivant pour configurer les paramètres réseau Firewall Management Center : **sudo /usr/local/sf/bin/configure-network**.

Étape 4 Répondez aux invites pour fournir les informations de configuration IPv4 et (facultatif) IPv6 pour votre appareil.

Étape 5 La dernière invite vous donne la possibilité de confirmer les paramètres.

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

Passez en revue les paramètres que vous avez saisis :

- 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.

Étape 6 Après avoir accepté les paramètres, saisissez **exit** (sortir) pour vous déconnecter de l'interface Shell.

Prochaine étape

Terminez le processus de configuration comme décrit dans Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4, à la page 28.

Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4

Pour tous les Firewall Management Center, vous devez terminer le processus de configuration en vous connectant à l'interface Web Firewall Management Center et en sélectionnant les options de configuration initiale sur une page de configuration. À tout le moins, vous devez changer le mot de passe administrateur, préciser les paramètres réseau (si ce n'est pas déjà fait) et accepter le contrat de licence d'utilisateur final (CLUF).

Procédure

Étape 1 Dirigez votre navigateur vers https://*mgmt_ip*/, où *mgmt_ip* est l'adresse IP de l'interface Firewall Management Center :

- Pour le Firewall Management Center 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/.
- Si vous avez configuré l'adresse IP Firewall Management Center sur une connexion physique (voir (Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27), utilisez un ordinateur de votre réseau de gestion pour accéder à l'adresse IP de l'interface Firewall Management Center.

Étape 2 Utilisez le nom d'utilisateur **admin** et le mot de passe **Admin123** pour vous connecter. (Les mots de passe sont sensibles à la casse.)

Étape 3 Dans la section **Change Password (modifier le mot de passe)** de la page Setup (configuration), modifiez le mot de passe des comptes admin. Le compte admin pour l'interface Web a des privilèges d'administrateur et ne peut pas être supprimé. Cisco vous 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 d'administrateur permettant d'accéder à Firewall Management Center par l'intermédiaire de l'interface Shell plutôt que d'accéder à Firewall Management Center à l'aide de l'interface Web ne sont pas

identiques et peuvent utiliser des mots de passe différents. Ce paramètre aligne les deux mots de passe admin sur la même valeur.

Étape 4 Les paramètres réseau du Firewall Management Center lui permettent de communiquer sur votre réseau de gestion. Configurez ces paramètres dans la section **Network Settings** (Paramètres réseau) de la page de configuration.

- Si vous avez déjà configuré les paramètres réseau pour l'accès au périphérique à l'aide d'un clavier et d'un moniteur, la section **Network Settings** (Paramètres réseau) de la page Setup (Configuration) peut être préremplie.
- Si les valeurs ne sont pas préremplies dans **Network Settings** (Paramètres réseau), ou si vous souhaitez modifier les valeurs préremplies, vous devez choisir le protocole de réseau de gestion. Le système offre une implémentation à double pile pour les environnements de gestion IPv4 et IPv6 ; vous pouvez spécifier IPv4, IPv6 ou les deux.

  Selon votre choix de protocole , la page de configuration affiche les champs dans lesquels 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 le Firewall Management Center. Vous pouvez également spécifier jusqu'à trois serveurs DNS, ainsi que le nom d'hôte et le domaine du périphérique.

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

Étape 5 (Facultatif) Dans la section **Time Settings** (paramètres d'heure) de la page de configuration, vous pouvez définir l'heure d'un Firewall Management Center de l'une des deux manières suivantes : manuellement ou à l'aide du protocole NTP (Network Time Protocol) d'un serveur NTP.

- Pour définir l'heure à l'aide du protocole NTP (Network Time Protocol), sélectionnez **Via NTP from** (Via NTP à partir de) et indiquez un ou plusieurs serveurs NTP auxquels Firewall Management Center peut accéder.
- Pour régler l'heure manuellement, sélectionnez **Manually** (Manuel) et saisissez l'heure actuelle dans les champs prévus à cet effet.

Pour choisir le fuseau horaire utilisé sur l'interface Web locale pour le compte d'administrateur, cliquez sur la valeur du fuseau horaire actuelle et choisissez un fuseau horaire dans la fenêtre contextuelle.

Remarque
L'utilisation d'un serveur NTP est essentielle pour assurer une bonne synchronisation de l'heure entre le Firewall Management Center et ses périphériques gérés. Si vous ne configurez pas de serveur NTP pendant le processus de configuration initial, nous vous recommandons fortement de le faire dès que possible. Consultez la section Time and Time Synchronization (Heure et synchronisation de l'heure) dans le Guide d'administration Cisco Secure Firewall Management Center de votre version pour obtenir de plus amples renseignements.

Étape 6 (Facultatif) Si vous prévoyez d'effectuer la détection et la prévention des intrusions dans votre déploiement, dans la section **RecurRING Rule Update Imports** (importations de mises à jour de règles récurrentes) de la page de configuration, nous vous recommandons de cocher **Enable Recurring Rule Update Imports from the Support Site** (Activer les importations de mise à jour des règles récurrentes à partir du site de soutien).

Vous pouvez spécifier la **fréquence d'importation**et configurer le système pour effectuer un **déploiement de stratégie** de prévention des intrusions après chaque mise à jour de règle. Pour exécuter une mise à jour des règles dans le cadre de la configuration initiale, cochez la case **Install Now** (Installer maintenant).

Le Cisco Talos Intelligence Group publie des mises à jour de règles d'intrusion au fur et à mesure que de nouvelles vulnérabilités sont découvertes. 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.

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.

Étape 7 (Facultatif) Si vous prévoyez d'effectuer une analyse liée à la géolocalisation dans votre déploiement, dans la section **Recurring Geolocation Updates** (Mises à jour récurrentes de géolocalisation) de la page de configuration, nous vous recommandons de cocher **Enable Recurring Weekly Updates from the Support Site** (Activer les mises à jour hebdomadaires récurrentes à partir du site d'assistance) et précisez l' **Update Start Time** (Heure de début de mise à jour) à l'aide des champs fournis. Pour effectuer une mise à jour de la GeoDB dans le cadre du processus de configuration initial, cochez la case **Install Now** (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.

Les On-Prem Firewall Management Center 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 Firewall Management Centercontient des informations pour prendre en charge cette fonctionnalité, telles que le fournisseur de services 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.

Étape 8 (Facultatif) Dans la section **Automatic Backups** (Sauvegardes automatiques) de la page de configuration, vous pouvez cocher **Enable Automatic Backups** (Activer les sauvegardes automatiques) pour créer une tâche planifiée qui effectue une sauvegarde hebdomadaire des configurations du Firewall Management Center qui peuvent être restaurées en cas de défaillance.

Étape 9 Vous utilisez le Firewall Management Center pour gérer les licences des périphériques qu'il gère. Le Firewall Management Center peut gérer les périphériques, quel que soit le type de licence dont ils ont besoin :

- Pour les périphériques séries 7000 et 8000, Pare-feu ASA avec services FirePOWERet NGIPSv, vous devez utiliser des licences Classic. Les périphériques qui utilisent des licences Classic sont parfois appelés périphériques Classic.

  Vous devez attribuer des licences Classic à vos périphériques gérés avant de pouvoir utiliser des fonctions sous licence. Vous pouvez ajouter une licence lors de la configuration initiale de Firewall Management Center, lorsque vous ajoutez un périphérique au Firewall Management Center ou en modifiant les propriétés générales du périphérique après l'ajout.

  Pour ajouter une licence Classic lors de la configuration initiale de votre Firewall Management Center, suivez les instructions dans (Facultatif) Ajouter des licences Classic lors de la configuration initiale (versions 6.3 - 6.4), à la page 31. Vous pouvez également ajouter des licences classiques après avoir terminé la configuration initiale, comme décrit dans Configurer les licences Classic, à la page 37.

- Pour les périphériques physiques et virtuels Cisco Secure Firewall Threat Defense, vous devez utiliser des licences Smart.

Si vous prévoyez de gérer des périphériques qui utilisent Cisco Gestion des licences Smart Software, vous devez ajouter des licences Smart après avoir terminé la configuration initiale, comme décrit dans Configurer les licences Smart, à la page 34.

Le Guide d'administration Cisco Secure Firewall 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.

Étape 10 Lisez attentivement le **contrat de licence de l'utilisateur final** ; si vous acceptez de vous conformer à ses dispositions, cochez la case **J'ai lu et accepté le contrat de licence de l'utilisateur final**.

Étape 11 Assurez-vous que toutes les informations que vous avez fournies sont correctes, puis cliquez sur **Apply** (Appliquer).

Le Firewall Management Center applique votre configuration en fonction de vos sélections, vous connecte à l'interface Web en tant qu'utilisateur admin (qui a le rôle d'administrateur) et affiche la page du tableau de bord de résumé.

Remarque
Si votre environnement réseau utilise NAT, le navigateur peut expirer en essayant d'atteindre le Firewall Management Center en utilisant l'adresse configurée sur la page de configuration initiale. Dans ce cas, saisissez la bonne adresse dans la fenêtre d'adresse du navigateur et réessayez.

Étape 12 Si vous vous êtes connecté directement à l'interface de gestion de l'appareil à l'aide d'un câble Ethernet, une fois que vous avez cliqué sur **Apply** (Appliquer), vous serez déconnecté de Firewall Management Center, car son adresse IP a été modifiée. Déconnectez l'ordinateur et connectez l'interface Firewall Management Center au réseau de gestion. Pour effectuer les autres procédures du guide, utilisez un navigateur sur un ordinateur du réseau de gestion pour accéder à l'interface graphique Firewall Management Center à l'adresse IP ou au nom d'hôte que vous venez de configurer.

Étape 13 Vérifiez que la configuration initiale a réussi en surveillant l'onglet **Tasks** (Tâches) dans le centre de messages.

Prochaine étape

- Effectuez les activités décrites dans Configurer les paramètres d'administration du centre de gestion, à la page 32.
- Vous pouvez également configurer le Firewall Management Center pour l'accès en série ou en service réduit (LOM) ; voir Configurer l'accès secondaire au centre de gestion, à la page 45.

(Facultatif) Ajouter des licences Classic lors de la configuration initiale (versions 6.3 - 6.4)

Vous utilisez le Firewall Management Center pour gérer les licences Classic de séries 7000 et 8000, Pare-feu ASA avec services FirePOWERet NGIPSv.

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 de Firewall Management Center (comme décrit dans la procédure ci-dessous), lorsque vous ajoutez un périphérique à Firewall Management Centerou en modifiant les propriétés générales du périphérique après avoir ajouté le périphérique.

Avant de commencer

Avant d'ajouter une licence Classic à Firewall 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, contactez le Centre d'assistance technique Cisco (TAC).

Procédure

Étape 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).

Étape 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.

Étape 3 Suivez les instructions à l'écran pour générer une ou plusieurs licence qui vous seront envoyées par courriel.

Étape 4 Collez la ou les licences dans la zone de validation et cliquez sur **Add/Verify** (Ajouter/vérifier).

Configurer les paramètres d'administration du centre de gestion

Après avoir terminé le processus de configuration initiale de Firewall Management Center et vérifié sa réussite, nous vous recommandons d'effectuer diverses tâches administratives qui faciliteront la gestion de votre déploiement. Vous devez également effectuer toutes les tâches que vous avez ignorées lors de la configuration initiale, par exemple l'octroi de licences. Établissez ces configurations en utilisant le compte **admin** par défaut ou un autre compte avec accès administrateur.

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 d'administration Cisco Secure Firewall Management Center de votre version de logiciel.

Connexion à l'interface Web du centre de gestion en tant qu'administrateur

Si vous ne vous êtes pas encore connecté à l'interface Web Firewall Management Center pour effectuer la configuration initiale, vous devez le faire pour configurer les paramètres administratifs Firewall Management Center. Utilisez le compte **admin** par défaut ou, si vous avez déjà créé des comptes utilisateurs supplémentaires, utilisez un compte avec un accès administrateur.

Les utilisateurs sont limités à une seule session active. Si vous essayez de vous connecter avec un compte d'utilisateur qui a déjà une session active, le système vous invite à mettre fin à l'autre session ou à vous connecter sous un autre utilisateur.

Dans un environnement NAT où plusieurs Firewall Management Center partagent la même adresse IP et sont différenciés par des numéros de port :

- Chaque Firewall Management Center ne peut prendre en charge qu'une seule session de connexion à la fois.
- Pour accéder à différents Firewall Management Center, utilisez un navigateur différent à chaque connexion (par exemple, Firefox et Chrome) ou réglez le navigateur en mode de navigation privée ou masquée.

Procédure

Étape 1 Dirigez votre navigateur vers **https://***ipaddress_or_hostname/*, où *ipaddress* ou *hostname* correspond à votre Firewall Management Center.

Étape 2 Dans les champs **Nom d'utilisateur** et **Mot de passe**, saisissez votre nom d'utilisateur et mot de passe.

Étape 3 Cliquez sur **Ouvrir une session**.

Créer des comptes utilisateurs individuels

Après avoir terminé la configuration initiale, le seul utilisateur d'interface Web sur le système est l'utilisateur **admin**, qui a le rôle et l'accès administrateur. Les utilisateurs ayant ce rôle ont un accès complet au menu et à la configuration du système. Nous vous recommandons de limiter l'utilisation du compte **admin** (et du rôle d'administrateur) pour des raisons de sécurité et d'audit.

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

Le système inclut dix rôles utilisateur prédéfinis conçus pour divers administrateurs et analystes de l'interface Web. La création d'un compte distinct pour chaque personne qui utilise le système permet à votre organisation non seulement de vérifier les actions et les modifications effectuées par chaque utilisateur, mais aussi de limiter le rôle ou les rôles d'accès d'utilisateur associés à chaque personne. Cela est particulièrement important sur le Firewall Management Center, 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. Consultez les Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version pour connaître les descriptions des rôles d'utilisateur.

Pour en savoir plus sur les comptes d'utilisateurs authentifiés de l'extérieur ou les comptes d'utilisateurs dans les déploiements multidomaine, consultez le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

Procédure

Étape 1 Choisissez **Utilisateurs** > **système**.

Étape 2 Dans l'onglet **Utilisateurs**, cliquez sur **Créer un utilisateur**.

Étape 3 Saisissez un **nom d'utilisateur** et fournissez ou choisissiez des valeurs pour les caractéristiques du compte d'utilisateur.

Étape 4 Cliquez sur **Enregistrer**.

Configurer les paramètres de temps

La synchronisation de l'horloge système sur votre Firewall Management Center et ses périphériques gérés est essentielle au bon fonctionnement de votre système. Nous vous recommandons de préciser les serveurs NTP dans votre réseau lors de la configuration initiale de Firewall Management Center, mais en cas d'échec, vous pouvez ajouter un serveur NTP une fois la configuration initiale terminée.

Si votre Firewall Management Center ne parvient pas à atteindre un serveur NTP, consultez le Guide d'administration Cisco Secure Firewall Management Center pour votre version afin de connaître d'autres moyens de configurer l'heure de votre déploiement de pare-feu.

Procédure

Étape 1 Choisissez **System (système)** > **Configuration** > **Time Synchronization (synchronisation)**.

Étape 2 Désactivez l'option **Heure de service via NTP**.

Étape 3 Choisissez **Via NTP** pour l'option **Régler mon horloge**.

Étape 4 Pour les versions 6.3 - 6.4 :cliquez sur **Ajouter** et saisissez le nom d'hôte ou l'adresse IP d'un serveur NTP accessible à partir de votre Firewall Management Center. Cliquez ensuite sur **Enregistrer**.

Pour les versions 6.5 et ultérieures : cliquez sur **Ajouter** et saisissez le nom d'hôte ou l'adresse IP d'un serveur NTP accessible à partir de votre Firewall Management Center. Cliquez ensuite sur **Ajouter**, puis sur **Enregistrer**.

Configurer les licences Smart

Le Firewall Management Center lui-même ne requiert pas de licences, mais si vous prévoyez de gérer des appareils Cisco Firewall Threat Defense, vous devez créer un compte Smart si vous n'en possédez pas déjà un et acheter les licences Smart dont vous avez besoin pour prendre en charge la détection des menaces et des programme malveillant et de filtrage d'URL. Consultez https://software.cisco.com/smartaccounts/setup#accountcreation-account. Pour en savoir plus, consultez https://www.cisco.com/c/en/us/buy/smart-accounts.html.

Les appareils Firewall Threat Defense sont livrés avec une licence de base qui vous permet de :

- configurer vos périphériques Cisco Firewall Threat Defense pour effectuer la commutation et le routage (y compris le relais DHCP et la NAT).
- configurer des périphériques Cisco Firewall Threat Defense en tant que paire à haute disponibilité
- configurer les modules de sécurité en tant que grappe dans un châssis Firepower 9300 (mise en grappe intra-châssis).
- configurer des périphériques Firepower 9300 ou Firepower 4100 exécutant Cisco Firewall Threat Defense en tant que grappe (mise en grappe intra-châssis)
- mettre en œuvre le contrôle des utilisateurs et des applications en ajoutant des conditions d'utilisateurs et d'applications aux règles de contrôle d'accès

Les fonctionnalités de détection des menaces et des programmes malveillants et de filtrage d'URL nécessitent des licences facultatives supplémentaires. Lorsque vous planifiez votre déploiement, déterminez le nombre de périphériques Cisco Firewall Threat Defense que le Firewall Management Center gérera et les fonctionnalités dont vous devez obtenir une licence pour chacun.

Remarque Ce document fournit une version simplifiée des instructions pour la configuration des licences Smart, qui sera utile pour les clients déjà familiarisés avec le processus. Si vous découvrez Smart Licensing, ou si vous devez le configurer pour un déploiement isolé, des périphériques en HA, grappes, multilocation ou des fonctions soumises à contrôle d'exportation, consultez le Guide d'administration Cisco Secure Firewall Management Center de votre version.

Pour les versions 6.5 et ultérieures : si vous possédez déjà un compte Smart, si vous avez acheté des licences et que vous connaissez bienSmart Licensing, vous pouvez utiliser la boîte de dialogue que le système affiche après avoir terminé l'assistant de configuration initial. Sinon, après avoir terminé l'assistant, vous pouvez utiliser le même processus de configuration de licence que pour les versions 6.3 - 6.4.

Pour les versions 6.3 - 6.4 : ajoutez Smart Licensing après avoir terminé la configuration initiale. Pour chaque licence :

- Obtenez un jeton d'enregistrement de licence de produit pour Smart Licensing depuis Cisco Smart Software Manager (CSSM). Consultez le guide de démarrage pour votre périphérique afin de déterminer les numéros de licence disponibles pour ce dernier.
- Utilisez le jeton pour enregistrer le Firewall Management Center sur CSSM.
- Lorsque vous ajoutez un Cisco Firewall Threat Defense géré au Firewall Management Center, attribuez la licence au périphérique.

Obtenir un jeton d'enregistrement de licence de produit pour des licences Smart

Avant de commencer

- Créez un compte Smart et achetez le nombre et les types de licence dont vous avez besoin. Consultez https://software.cisco.com/smartaccounts/setup#accountcreation-account. Pour en savoir plus, consultez https://www.cisco.com/c/en/us/buy/smart-accounts.html.
- Vérifiez que les licences apparaissent dans votre compte Smart.
- Assurez-vous d'avoir les informations d'authentification pour vous connecter à Cisco Smart Software Manager.

Procédure

Étape 1 Accédez à https://software.cisco.com.

Étape 2 Cliquez sur **Smart Software Licensing** (dans la section License).

Étape 3 Connectez-vous à Cisco Smart Software Manager.

Étape 4 Cliquez sur **Inventory** (inventaire).

Étape 5 Cliquez sur **General** (Général).

Étape 6 Cliquez sur **New Token** (nouveau jeton).

Étape 7 Dans le champ **Description**, saisissez un nom qui identifie de manière unique et claire le Firewall Management Center pour lequel vous utiliserez ce jeton.

Étape 8 Saisissez un délai d'expiration inférieur ou égal à 365 jours. Cela détermine le temps dont vous disposez pour enregistrer le jeton dans un Firewall Management Center.

Étape 9 Cliquez sur **Créer le jeton**.

Étape 10 Localisez votre nouveau jeton dans la liste et cliquez sur **Actions**, puis sélectionnez **Copier** ou **Télécharger**.

Étape 11 Conservez votre jeton dans un emplacement sûr jusqu'à ce que vous soyez prêt à le saisir dans votre Firewall Management Center.

Prochaine étape

Continuez avec Enregistrer des licences Smart, à la page 36.

Enregistrer des licences Smart

Avant de commencer

- Assurez-vous que Firewall Management Center peut atteindre le serveur Cisco Smart Software Manager (CSSM) à l'adresse tools.cisco.com:443.
- Assurez-vous que Firewall Management Center a établi une connexion avec un serveur NTP. Lors de l'enregistrement, un échange de clé a lieu entre le serveur NTP et Cisco Smart Software Manager. L'heure doit donc être synchronisée pour un enregistrement correct.

  Si vous déployez Cisco Firewall Threat Defense sur un châssis Firepower 4100/9300, vous devez configurer le NTP sur le châssis Firepower en utilisant le même serveur NTP pour le châssis que pour Firewall Management Center.
- Générez le jeton d'enregistrement de licence de produit nécessaire à partir de CSSM. Consultez Obtenir un jeton d'enregistrement de licence de produit pour des licences Smart, à la page 35, y compris les conditions préalables. Assurez-vous que le jeton est accessible à partir de la machine à partir de laquelle vous accéderez à votre Firewall Management Center.

Procédure

Étape 1 Choisissez **Système** > **Licences** > **Licences Smart** > **Enregistrer**.

Étape 2 Collez le jeton que vous avez généré à partir de CSSM dans le champ **Product Instance Registration Token** (jeton d'enregistrement d'instance de produit). Vérifiez qu'il n'y a ni espace ni ligne vide au début ou à la fin du texte.

Étape 3 décidez si vous souhaitez envoyer les données d'utilisation à Cisco.

- **Enable Cisco Success Network** (Activer Cisco Success Network) est activé par défaut. Vous pouvez cliquer sur **des exemples de données** pour voir le type de données collectées par Cisco. Pour vous aider à prendre votre décision, lisez le bloc d'informations relatif au Cisco Success Network.
- **Pour les versions 6.5 et ultérieures : l'assistance proactive Cisco est activée** par défaut. Vous pouvez passer en revue le type de données que Cisco recueille en cliquant sur le lien au-dessus de la case. Pour

vous aider à prendre votre décision, lisez le bloc d'informations sur les dépistages d'assistance de Cisco (Cisco Support Diagnostics).

Remarque

- Lorsque cette option est activée, les diagnostics d'assistance Cisco sont activés dans les appareils Cisco Firewall Threat Defense lors du prochain cycle de synchronisation. La synchronisation de Firewall Management Center avec Cisco Firewall Threat Defense s'exécute une fois toutes les 30 minutes.
- Lorsque cette option est activée, Cisco Support Diagnostics sera automatiquement activé pour tout nouveau Cisco Firewall Threat Defense enregistré dans cet Firewall Management Center ultérieurement.

Étape 4 Cliquez sur **Apply Changes** (appliquer les modifications).

Prochaine étape

Lorsque vous ajoutez les appareils gérés par Cisco Firewall Threat Defense à Firewall Management Center, sélectionnez les licences appropriées à attribuer à ces appareils. Consultez Ajouter des périphériques gérés au centre de gestion, à la page 43.

Configurer les licences Classic

Le Firewall Management Center lui-même ne nécessite pas de licences, mais les périphériques séries 7000 et 8000, ASA FirePOWERet NGIPSv nécessitent que vous achètiez et activiez des licences Classic avant de pouvoir utiliser les fonctionnalités sous licence de ces périphériques. Les périphériques qui utilisent des licences Classic sont parfois appelés périphériques Classic.

Vous gérez les licences Classic à l'aide du portail d'enregistrement des licences de produit Cisco à l'adresse https://cisco.com/go/license. Consultez https://slexui.cloudapps.cisco.com/SWIFT/LicensingUI/Quickstart pour obtenir des renseignements sur l'utilisation du portail. Vous aurez besoin des identifiants de votre compte pour accéder à ces liens.

Remarque Ce document fournit une version simplifiée des instructions pour la configuration des licences Classic, utile pour les clients déjà familiarisés avec le processus. Si vous découvrez les licences Classic, ou si vous devez les configurer pour un déploiement isolé du réseau (air-gapped) ou multi-détenteurs, consultez le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version.

Si votre système exécute la version 6.5 ou version ultérieure : vous devez ajouter des licences pour les périphériques Classic gérés au Firewall Management Center après avoir terminé l'assistant de configuration initial de Firewall Management Center, comme décrit dans Générer une licence Classic et l'ajouter au centre de gestion, à la page 38 ou dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version.

Si votre système exécute les versions 6.3 - 6.4 : nous vous recommandons d'acheter des licences Classic avant de commencer le processus de configuration initiale de Firewall Management Center et d'ajouter les licences au Firewall Management Center comme décrit dans (Facultatif) Ajouter des licences Classic lors de la configuration initiale (versions 6.3 - 6.4), à la page 31. Si vous choisissez d'ajouter des licences après avoir terminé la configuration initiale, suivez les instructions dans Générer une licence Classic et l'ajouter au centre

de gestion, à la page 38 ou dans le Guide d'administration Cisco Secure Firewall Management Center de votre version.

Si vous n'ajoutez pas de licences Classic lors de la configuration initiale de Firewall Management Center, vous devez ajouter des licences pour les périphériques Classic gérés après avoir terminé la configuration initiale de Firewall Management Center. Si vous ajoutez des licences pendant ou après le processus de configuration initiale de Firewall Management Center, vous pouvez attribuer des licences à des périphériques classiques gérés lorsque vous enregistrez ces périphériques sur Firewall Management Centerou après les avoir enregistrés sur Firewall Management Center en modifiant les propriétés générales du périphérique. Pour en savoir plus, consultez les Guide d'administration Cisco Secure Firewall Management Center pour votre version.

Pour ajouter des licences traditionnelles après avoir terminé la configuration initiale, pour chaque licence :

- Générer une licence classique et l'ajouter au Firewall Management Center
- Attribuer la licence à un périphérique Classic géré.

Générer une licence Classic et l'ajouter au centre de gestion

Avant de commencer

- Confirmez que vous avez accès au portail d'enregistrement des licences de produit Cisco à l'adresse https://cisco.com/go/license.
- Passez en revue les informations sur les types de licences Classic dans le Guide d'administration Cisco Secure Firewall Management Center pour votre version afin de déterminer de quel type de licence Classic vous avez besoin et si vous devez également acheter des abonnements de service pour les fonctionnalités que vous prévoyez d'utiliser.
- Achetez une clé d'autorisation de produit (PAK) pour chaque licence et les abonnements de service, le cas échéant.

Procédure

Étape 1 Choisissez **Système** > **Licences** > **Licences traditionnelles** > **Add New License** (Ajouter une nouvelle licence).

Étape 2 Notez la valeur du champ **License Key** (clé de licence) en haut de la boîte de dialogue **Add Function License** (Ajouter une licence de fonction).

Étape 3 Cliquez sur **Get License** (Obtenir une licence) pour ouvrir le portail d'enregistrement de licences Cisco.

Étape 4 Générez une licence à partir de la clé PAK dans le portail d'enregistrement de licences. Pour en savoir plus, consultez https: //slexui.cloudapps.cisco.com/SWIFT/LicensingUI/home. Cette étape nécessite la clé PAK que vous avez reçue au cours du processus d'achat, ainsi que la clé de licence pour Firewall Management Center.

Étape 5 Copiez le texte de la licence provenant de l'écran du portail d'enregistrement de licences ou du courriel que le portail d'enregistrement de licences vous envoie.

Important
Le bloc de texte de licence dans le portail ou le message courriel peut inclure plusieurs licences. Chaque licence est délimitée par une ligne BEGIN LICENSE et une ligne END LICENSE. Veillez à ne copier et coller qu'une seule licence à la fois.

Étape 6 Revenez à la page **Add Function License** (ajouter une licence de fonctionnalité) dans l'interface Web de Firewall Management Center.

Étape 7 Collez le texte de la licence dans le champ **License** (Licence).

Étape 8 Cliquez sur **Verify Licence** (Vérifier la licence).

Étape 9 Cliquez sur **Submit Licence** (Envoyer la licence)

Prochaine étape

Lorsque vous ajoutez des périphériques gérés classiques à Firewall Management Center, sélectionnez les licences appropriées à appliquer aux périphériques. Consultez Ajouter des périphériques gérés au centre de gestion, à la page 43.

Planifier les mises à jour et les sauvegardes du système

Pour la version 6.5 et ultérieure :

Dans le cadre du processus de configuration initiale, le Firewall Management Center établit les mises à jour automatiques suivantes :

- Mises à jour hebdomadaires de GeoDB.
- Téléchargements hebdomadaires des mises à jour logicielles de Firewall Management Center. (L'installation de ces mises à jour est de votre responsabilité; consultez le Guide d'administration Cisco Secure Firewall Management Center pour obtenir de plus amples renseignements.)
- Sauvegardes hebdomadaires de la configuration Firewall Management Center.

Pour la version 6.6 et ultérieure :

Le Firewall Management Center établit en outre les mises à jour automatiques suivantes dans le cadre du processus de configuration initiale :

- Mise à jour unique de la base de données sur les vulnérabilités.
- Mises à jour quotidiennes des règles d'intrusion.

Ces mises à jour automatiques sont décrites dans le Passer en revue la configuration initiale automatique pour les versions 6.5 et ultérieures, à la page 20. Vous pouvez observer l'état de ces configurations à l'aide du centre de messages de l'interface Web. Si la configuration de l'une de ces mises à jour échoue, pour maintenir votre système à jour, nous vous recommandons fortement de les configurer vous-même, comme décrit dans les sections suivantes. Dans le cas des mises à jour de VDB, le système installe automatiquement la dernière mise à jour de VDB uniquement; nous vous recommandons de planifier des mises à jour automatiques régulières de la VDB.

Pour les versions 6.3 - 6.4 :

Après avoir terminé la configuration initiale du Firewall Management Center, pour maintenir votre système à jour, nous vous recommandons fortement de configurer les activités de mise à jour décrites dans les sections suivantes.

Planifier les mises à jour hebdomadaires de GeoDB

La base de données de géolocalisation Cisco (GeoDB) est une base de données contenant des informations géographiques (pays, ville, coordonnées) et des données relatives aux connexions (fournisseur d'accès à

Internet, nom de domaine, type de connexion) associées à des adresses IP routables. Lorsque votre système détecte des renseignements GeoDB correspondant à une adresse IP détectée, vous pouvez afficher les informations de géolocalisation associées à cette adresse IP.

Pour afficher des détails de géolocalisation autres que le pays ou le continent, vous devez installer GeoDB sur votre système. Cisco publie des mises à jour périodiques de la base de données GeoDB; pour optimiser la précision des recherches GeoDB, nous vous recommandons de toujours utiliser la dernière mise à jour de GeoDB sur votre système.

Avant de commencer

Assurez-vous que le Firewall Management Center peut accéder à Internet.

Procédure

Étape 1 Sélectionner **Système** > **Mises à jour** > **Mises à jour de géolocalisation**

Étape 2 Sous **Recurring Geolocation Updates**(mises à jour récurrentes de la géolocalisation), cochez l'option **Enable Recurring Weekly Updates from the Support Site**(activer les mises à jour hebdomadaires récurrentes à partir du site d'assistance).

Étape 3 Spécifiez l'**heure de début de la mise à jour**.

Étape 4 Cliquez sur **Enregistrer**.

Planifier des mises à jour logicielles hebdomadaires

Suivez ces instructions pour créer une tâche hebdomadaire planifiée afin de télécharger automatiquement les dernières mises à jour logicielles Firewall Management Center de Cisco. La mise à jour de votre logiciel Firewall Management Center garantit des performances optimales. L'installation des mises à jour après leur téléchargement est de votre responsabilité. Consultez le guide de mise à niveau Cisco Firepower Management Center pour obtenir des instructions d'installation.

Avant de commencer

Assurez-vous que le Firewall Management Center peut accéder à Internet.

Procédure

Étape 1 Choisissez **Système** > **Outils** > **Planification**, puis cliquez sur **Ajouter une tâche**.

Étape 2 Dans la liste **Job Type** (type de tâche), sélectionnez **Télécharger la dernière mise à jour**.

Étape 3 Indiquez que vous souhaitez planifier une tâche **récurrente**, puis définissez une planification hebdomadaire en choisissant les valeurs appropriées pour les champs **Commencer le**, **Répéter toutes les**, **Exécuter à** et **Répéter le**.

Étape 4 Saisissez un **nom de tâche**, puis cochez la case **Logiciel** à côté de **Mettre à jour les éléments**.

Étape 5 Cliquez sur **Enregistrer**.

Planifier des sauvegardes hebdomadaires de la configuration du centre de gestion

Pour faciliter la restauration de votre configuration du Firewall Management Center en cas de défaillance catastrophique du système, nous vous recommandons de planifier des sauvegardes périodiques du système.

Avant de commencer

Assurez-vous que le Firewall Management Center peut accéder à Internet.

Procédure

Étape 1 Sélectionnez **Système** > **Outils** > **Sauvegarde et restauration**, puis cliquez sur **Backup Profiles** (Profils de sauvegarde).

Étape 2 Cliquez sur **Create Profile** (Créer un profil)

Étape 3 Saisissez un **nom**, choisissez **Sauvegarder la configuration**, puis cliquez sur **Enregistrer en tant que nouveau**.

Étape 4 Choisissez **Système** > **Outils** > **Planification**, puis cliquez sur **Ajouter une tâche**.

Étape 5 Dans la liste **Job Type** (type de tâche), sélectionnez **Backup** (Sauvegarde).

Étape 6 Indiquez que vous souhaitez planifier une tâche **récurrente**, puis définissez une planification hebdomadaire en choisissant les valeurs appropriées pour les champs **Commencer le**, **Répéter toutes les**, **Exécuter à** et **Répéter le**.

Étape 7 Saisissez un nom de tâche, puis choisissez **Management Center** à côté de **Type de sauvegarde**.

Étape 8 Pour **Profil de sauvegarde**, choisissez le profil que vous avez créé à l'étape 3.

Étape 9 Cliquez sur **Enregistrer**.

Configurer les mises à jour récurrentes des règles d'intrusion

À mesure que de nouvelles vulnérabilités sont connues, Cisco Talos Intelligence Group (Talos) publie des mises à jour des règles de prévention des intrusions que vous pouvez importer dans votre Firewall Management Center, puis les mettre en œuvre en déployant la configuration modifiée sur vos périphériques gérés. Ces mises à jour affectent les règles de prévention des intrusions, les règles de préprocesseur et les politiques qui utilisent les règles. Les mises à jour des règles de prévention des intrusions sont cumulatives, et Cisco vous recommande de toujours importer la dernière mise à jour.

Avant de commencer

Assurez-vous que le Firewall Management Center peut accéder à Internet.

Procédure

Étape 1 Choisissez **Système** > **Mises à jour** > **Mises à jour des règles**.

Étape 2 Cochez la case **Activer les importations de mise à jour de règles récurrentes à partir du site d'assistance**.

Étape 3 Choisissez des valeurs pour déterminer la **fréquence d'importation**.

Étape 4 Cochez la case **Déployer les politiques mises à jour sur les appareils ciblés une fois la mise à jour des règles terminée**.

Étape 5 Cliquez sur **Enregistrer**.

Planifier les téléchargements et les mises à jour de VDB

La base de données sur les vulnérabilités de Cisco (VDB) est une base de données contenant les vulnérabilités connues auxquelles les hôtes peuvent être sensibles, ainsi que les empreintes digitales pour les systèmes d'exploitation, les clients et les applications. Le système utilise la VDB pour déterminer si un hôte particulier augmente le risque de compromission.

Utilisez ces instructions pour planifier des téléchargements et des installations automatiques réguliers de la dernière mise à jour de VDB. Le Cisco Talos Intelligence Group (Talos) n'envoie pas de mises à jour périodiques de la VDB plus d'une fois par jour. Nous vous recommandons fortement de toujours conserver la dernière mise à jour de VDB sur votre Firewall Management Center.

Lorsque vous automatisez les mises à jour de VDB, vous devez automatiser deux étapes distinctes :

- Téléchargement de la mise à jour de la VDB en cours.
- Installer la mise à jour de VDB

Prévoyez suffisamment de temps entre les tâches pour que le processus se termine. Par exemple, si vous planifiez une tâche pour installer une mise à jour et que la mise à jour n'a pas été complètement téléchargée, la tâche d'installation échouera. Toutefois, si la tâche d'installation planifiée se répète tous les jours, la mise à jour de VDB téléchargée sera installée lors de l'exécution de la tâche le jour suivant.

Mise en garde Lorsqu'une mise à jour de VDB comprend des modifications applicables aux appareils gérés, le premier déploiement manuel ou planifié après l'installation d'une nouvelle mise à jour de VBD peut entraîner un petit nombre de paquets abandonnés sans inspection. En outre, le déploiement de certaines configurations redémarre le processus Snort, qui interrompt l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez le Guide d'administration Cisco Secure Firewall Management Center correspondant à votre version pour plus d'information.

Avant de commencer

Assurez-vous que le Firewall Management Center peut accéder à Internet.

Procédure

Étape 1 Choisissez **Système** > **Outils** > **Planification**, puis cliquez sur **Ajouter une tâche**.

Étape 2 Dans la liste **Job Type** (type de tâche), sélectionnez **Télécharger la dernière mise à jour**.

Étape 3 Indiquez que vous souhaitez planifier une tâche **récurrente**, puis définissez une planification hebdomadaire en choisissant les valeurs appropriées pour les champs **Commencer le**, **Répéter toutes les**, **Exécuter à** et **Répéter le**.

Étape 4 Saisissez un **nom de tâche**, puis cochez la case **Base de données des vulnérabilités** à côté de **Mettre à jour les éléments**.

Étape 5 Cliquez sur **Enregistrer**.

Étape 6 Choisissez **Système** > **Outils** > **Planification**, puis cliquez sur **Ajouter une tâche**.

Étape 7 Dans la liste **Job Type** (type de tâche), sélectionnez **Install Latest Update (installation de la dernière mise à jour**).

Étape 8 Indiquez que vous souhaitez planifier une tâche **récurrente**, puis définissez une planification hebdomadaire en choisissant les valeurs appropriées pour les champs **Commencer le**, **Répéter toutes les**, **Exécuter à** et **Répéter le**.

Étape 9 Saisissez un **nom de tâche**, puis cochez la case **Base de données des vulnérabilités** à côté de **Mettre à jour les éléments**.

Étape 10 Cliquez sur **Enregistrer**.

Ajouter des périphériques gérés au centre de gestion

Pour chaque périphérique géré, suivez ces instructions pour établir un déploiement simple qui n'inclut pas la multilocation, les grappes ou la haute disponibilité. Pour configurer un déploiement à l'aide de l'une de ces fonctionnalités, consultez le Guide de configuration Cisco Secure Firewall Management Center Device de votre version.

Avant de commencer

- Effectuez les activités de configuration spécifiques au périphérique et configurez celui-ci pour la gestion à distance, comme décrit dans le guide de démarrage de ce dernier.

Important Assurez-vous de noter la clé d'enregistrement que vous utilisez pour le périphérique.

- Si votre environnement utilise NAT, notez l'ID de NAT utilisé lors de la configuration de l'appareil.
- Si votre environnement utilise DNS, notez le nom d'hôte qui se résout en une adresse IP valide pour le périphérique. Si votre environnement utilise le DHCP pour attribuer les adresses IP, utilisez un nom d'hôte pour identifier le périphérique plutôt qu'une adresse IP.
- Si votre environnement n'utilise pas DNS, vous avez besoin de l'adresse IP du périphérique.
- Déterminez quelles licences sont nécessaires pour le périphérique géré et ajoutez-les au Firewall Management Center ; vous ajouterez la ou les licences au périphérique géré au cours du processus d'ajout au Firewall Management Center. Consultez Configurer les licences Smart, à la page 34 et Configurer les licences Classic, à la page 37.
- Vous devez affecter une politique de contrôle d'accès au périphérique géré au moment de l'ajouter au Firewall Management Center. Les instructions ci-dessous comprennent une procédure pour établir une politique de contrôle d'accès de base à cette fin.

Procédure

Étape 1 Choisissez **Devices (appareils)** > **Device Management (gestion d'appareil)** > **Add (ajouter)** > **Add Device (ajouter un périphérique)**.

Étape 2 Dans le champ **Host** (hôte), saisissez l'adresse IP ou le nom d'hôte du périphérique que vous souhaitez ajouter.

Le nom d'hôte du périphérique est le nom complet de domaine ou le nom qui se résout par le DNS local en une adresse IP valide. Utilisez un nom d'hôte plutôt qu'une adresse IP si votre réseau utilise DHCP pour attribuer des adresses IP.

Dans un environnement NAT, vous n'avez peut-être pas besoin de préciser l'adresse IP ou le nom d'hôte du périphérique, si vous avez déjà spécifié l'adresse IP ou le nom d'hôte de Firewall Management Center lorsque vous avez configuré le périphérique pour qu'il soit géré par Firewall Management Center.

Étape 3 Dans le champ **Display Name**(Nom d'affichage), saisissez le nom du périphérique tel qu'il doit apparaître dans l'interface Web Firewall Management Center.

Étape 4 Dans le champ Registration Key (clé d'enregistrement), saisissez la clé d'enregistrement que vous avez utilisée lors de la configuration du périphérique pour qu'il soit géré par Firewall Management Center. (Cette clé d'enregistrement est un secret partagé à usage unique que vous avez créé lorsque vous avez identifié à l'origine ce Firewall Management Center sur le périphérique.)

Étape 5 Choisissez une **Access Control Policy** (politique de contrôle d'accès) initiale. Sauf si vous avez déjà une politique personnalisée que vous savez que vous devez utiliser, choisissez **Create new policy** (créer une nouvelle politique) et **Block all traffic** (bloquer tout le trafic). Vous pourrez modifier cela plus tard pour autoriser le trafic ; consultez le Guide de configuration Cisco Secure Firewall Management Center Device correspondant à votre version pour plus d'information.

Si le périphérique est incompatible avec la politique que vous choisissez, le déploiement échouera. 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. Consultez le Guide de configuration Cisco Secure Firewall Management Center Device correspondant à votre version pour plus d'information. Après avoir résolu le problème à l'origine de l'échec, déployez manuellement les configurations sur le périphérique.

Étape 6 Choisissez la licence à appliquer au périphérique.

Pour les périphériques classiques, notez que les licences de contrôle, de Cisco Secure Firewall Threat Defense Malware Defense, et Secure Firewall Threat Defense URL Filtering nécessitent une licence de Protection.

Étape 7 Si vous avez utilisé un ID NAT lors de la configuration du périphérique , développez la section **Advanced** (Avancé) et saisissez le même ID NAT dans le champ **Unique NAT ID** (ID NAT unique).

Étape 8 Cliquez sur **Register** (Inscrire).

Cela peut prendre jusqu'à deux minutes pour que le Firewall Management Center vérifie les pulsations du périphérique et établisse la communication.

Configurer l'accès secondaire au centre de gestion

Après avoir terminé le processus de configuration initiale, vous pouvez établir d'autres moyens d'accéder à Firewall Management Center en effectuant l'une des opérations suivantes :

- Vous pouvez configurer le Firewall Management Center pour l'accès direct d'un ordinateur local à son port série. Avant de configurer le Firewall Management Center pour l'accès série, redirigez la sortie de la console vers le port série.
- Vous pouvez configurer le Firewall Management Center pour un accès Lights-Out Management (LOM) à l'aide d'une connexion Serial over LAN (SOL) sur l'interface CIMC . Cela vous permet d'effectuer un nombre limité de tâches de maintenance sans avoir d'accès physique au périphérique.

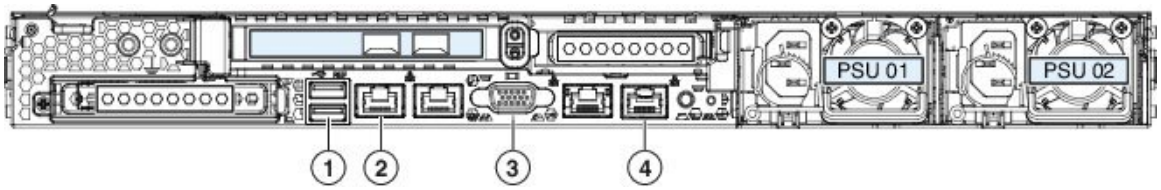
Configuration de l'accès série

Avant de commencer

- Terminer le processus de configuration initiale approprié à votre version :
  - Pour les versions 6.5 et ultérieures, consultez Installer le Centre de gestion pour les versions 6.5 et ultérieures, à la page 6.
  - Pour les versions 6.3 - 6.4, consultez Installer le Centre de gestion pour les versions de logiciel 6.3 - 6.4, à la page 21.
- Installez un logiciel d'émulation de terminal (p. ex., HyperTerminal ou XModem) sur l'ordinateur local pour interagir avec le Firewall Management Center.
- Redirigez la sortie de la console vers le port série. Consultez Rediriger la sortie de la console, à la page 49.

Procédure

Étape 1 Localisez le port série sur le panneau arrière Firewall Management Center, élément 4 dans le schéma ci-dessous.



Étape 2 Utilisez le câble de console RJ-45 à DB-9 fourni avec le périphérique (numéro de pièce Cisco 72-3383-XX) pour connecter un ordinateur local au port série Firewall Management Center.

Étape 3 Utilisez un logiciel d'émulation de terminal comme HyperTerminal ou XModem sur l'ordinateur local pour interagir avec le Firewall Management Center. Paramétrez l'émulateur à 9600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt, aucun contrôle de flux.

Configurer Lights-Out Management (Gestion en service réduit)

La fonction Lights-Out Management (LOM) vous permet d'effectuer un ensemble limité d'actions sur le Firewall Management Center à l'aide d'une connexion Serial over LAN (SOL). Vous pouvez effectuer des tâches limitées, par exemple afficher le numéro de série du châssis ou surveiller des conditions telles que la vitesse et la température du ventilateur, en utilisant une interface de ligne de commande sur une connexion de gestion hors bande. Notez que vous pouvez utiliser Lights-Out Management sur l'interface CIMC uniquement.

Si vous devez rétablir les valeurs par défaut de Firewall Management Center et que vous n'avez pas d'accès physique au périphérique, vous pouvez utiliser Lights-Out Management (LOM) pour effectuer le processus de restauration.

Mise en garde processus de restauration réinitialise les paramètres LOM sur le périphérique; vous ne pouvez pas accéder à un appareil nouvellement restauré à l'aide de LOM. Lors de la restauration d'un périphérique 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 périphérique après la restauration.

Remarque D'autres périphériques de pare-feu prennent également en charge LOM. 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 Firewall Management Center pour configurer LOM sur un périphérique de pare-feu. 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 Firewall Management Center ne transfère pas cette capacité aux utilisateurs sur les périphériques de pare-feu.

Pour en savoir plus sur Lights-Out Management, consultez « Remote Console Access Management » (Gestion de l'accès à la console à distance) dans le Guide d'administration Cisco Secure Firewall Management Center de votre version.

Avant de commencer

- Installez un utilitaire IMPI (Intelligent Platform Management Interface) sur votre ordinateur local. Consultez Installation de l'utilitaire IPMI, à la page 47 pour de plus amples renseignements.
- Déterminez quelles commandes sont nécessaires pour accéder à un appareil à l'aide de l'outil IPMI. Consultez Commandes LOM, à la page 47 pour de plus amples renseignements.
- Établissez une connexion du port CIMC à un réseau local accessible à partir d'un ordinateur sur lequel vous exécuterez l'utilitaire IPMI. Consultez l'étape 8 de État de vérification de l'alimentation des câbles de connexion pour les versions 6.3 à 6.4, à la page 24 ou État de vérification de l'alimentation des câbles de connexion pour les versions 6.5 et ultérieures, à la page 10, selon votre version.

Procédure

Étape 1 Activez LOM pour le Firewall Management Center. Consultez Activer la gestion en service réduit, à la page 48.

Étape 2 Activez LOM pour les utilisateurs qui utiliseront la fonctionnalité. Consultez Activer les utilisateurs de gestion en service réduit, à la page 49.

Étape 3 Utilisez un utilitaire IPMI tiers pour accéder au Firewall Management Center.

Installation de l'utilitaire IPMI

Vous utilisez un utilitaire IPMI tiers sur votre ordinateur pour créer une connexion SOL avec le périphérique. IPMItool est standard avec de nombreuses distributions Linux , mais sur les systèmes Mac et Windows, vous devez installer un utilitaire.

Si votre ordinateur exécute Mac OS, installez IPMItool. 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/ et 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/.

Commandes LOM

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.

Tableau 1 : 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 *IP_address*	**-N** *IP_address*	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* (mot de passe)	Pour ipmiutil uniquement, spécifie le mot de passe d'un compte LOM autorisé.

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
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, entrez la commande en dernier : **ipmitool -I lanplus -H** *IP_address* -U *username command* (commande) • Pour ipmiutil, saisissez d'abord la commande **ipmiutil** *command* (commande) **-V4 -J3 -N** *IP_address* **-U** *username* **-P** *password* (mot de passe)

Pour obtenir la liste complète des commandes LOM prises en charge par le système, consultez le Guide d'administration Cisco Secure Firewall Management Center.

Activer la gestion en service réduit

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Avant de commencer

- Installez un utilitaire IMPI (Intelligent Platform Management Interface) sur votre ordinateur local. Consultez Installation de l'utilitaire IPMI, à la page 47 pour de plus amples renseignements.
- Déterminez quelles commandes sont nécessaires pour accéder à un appareil à l'aide de l'outil IPMI. Consultez Commandes LOM, à la page 47 pour de plus amples renseignements.
- Établissez une connexion du port CIMC à un réseau local accessible à partir d'un ordinateur sur lequel vous exécuterez l'utilitaire IPMI. Consultez l'étape 8 de État de vérification de l'alimentation des câbles de connexion pour les versions 6.3 à 6.4, à la page 24 ou , selon votre version.
- Désactivez le protocole Spanning Tree (STP) sur tout équipement de commutation tiers connecté à l'interface de gestion du périphérique.

Procédure

Étape 1 Dans l'interface Web Firewall Management Center, choisissez **Système** > **Configuration**, puis cliquez sur **Console Configuration** (Configuration de la console).

Étape 2 Pour **Console**, choisissez **Lights Out Management** (gestion en service réduit).

Étape 3 Choisissez la **configuration** d'adresse pour le système (**DHCP** ou **manuel**)

Étape 4 Si vous avez choisi la configuration manuelle, saisissez les paramètres IPv4 nécessaires :

- Saisissez **l'adresse IP** à utiliser pour LOM.

  Remarque
  L'adresse IP du LOM doit être différente de l'adresse IP de l'interface de gestion Firewall Management Center et se trouver dans le même sous-réseau.

- Saisissez le **masque de réseau** pour le système.
- Saisissez la **passerelle par défaut** pour le système.

Étape 5 Cliquez sur **Enregistrer**.

Prochaine étape

Vous devez explicitement accorder des autorisations de gestion en service réduit (LOM) aux utilisateurs qui utilisent la fonctionnalité. Consultez Activer les utilisateurs de gestion en service réduit, à la page 49.

Activer les utilisateurs de gestion en service réduit

Avant de commencer

Les utilisateurs LOM doivent respecter les 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 LOM d'un utilisateur est identique au mot de passe système de cet utilisateur et doit être conforme aux exigences de mot de passe décrites pour les utilisateurs LOM dans le Guide d'administration Cisco Secure Firewall Management Center.
- Les On-Prem Firewall Management Center peuvent avoir jusqu'à treize utilisateurs LOM.

Procédure

Étape 1 Dans l'interface Web Firewall Management Center, sélectionnez **Utilisateurs** > **système** et sous l'onglet **Users** (Utilisateurs), modifiez un utilisateur existant pour ajouter des autorisations LOM ou créez un nouvel utilisateur que vous utiliserez pour l'accès LOM au périphérique.

Étape 2 Sous **User Role Configuration** (Configuration du rôle d'utilisateur), cochez la case **Administrator** (Administrateur) si elle n'est pas déjà cochée.

Étape 3 Cochez la case **Allow Lights-Out Management Access** (Autoriser l'accès à la gestion en service réduit).

Rediriger la sortie de la console

Par défaut, les Firewall Management Center envoient des messages sur l'état d'initialisation ou *init*, au port VGA. Si vous souhaitez utiliser le port série physique pour accéder à la console, nous vous recommandons de rediriger la sortie de la console vers le port série après avoir terminé la configuration initiale. Vous pouvez le faire à partir de l'interface Web ou de l'interface Shell.

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

Vous devez être un utilisateur administrateur pour effectuer cette procédure.

Avant de commencer

Terminer le processus de configuration initiale approprié à votre version :

- Pour les versions 6.5 et ultérieures, consultez Installer le Centre de gestion pour les versions 6.5 et ultérieures, à la page 6.
- Pour les versions 6.3 - 6.4, consultez Installer le Centre de gestion pour les versions de logiciel 6.3 - 6.4, à la page 21.
- Désactivez le protocole Spanning Tree (STP) sur tout équipement de commutation tiers connecté à l'interface de gestion du périphérique.

Procédure

Étape 1 Choisissez **Système** > **Configuration**.

Étape 2 Choisissez **Configuration de la console**.

Étape 3 Sélectionnez une option d'accès à la console à distance :

- Choisissez **VGA** pour utiliser le port VGA du périphérique . (Il s'agit du paramètre par défaut.)
- Choisissez **Port série physique** pour utiliser le port série de l'appareil.

Étape 4 Cliquez sur **Enregistrer**.

Utiliser le shell pour rediriger la sortie de la console

Avant de commencer

Terminer le processus de configuration initiale approprié à votre version :

- Pour les versions 6.5 et ultérieures, consultez Installer le Centre de gestion pour les versions 6.5 et ultérieures, à la page 6.
- Pour les versions 6.3 - 6.4, consultez Installer le Centre de gestion pour les versions de logiciel 6.3 - 6.4, à la page 21.

Procédure

Étape 1 Utilisez les informations d'authentification **admin** de l'interface de ligne de commande Firewall Management Center pour accéder au shell Linux sur le Firewall Management Center à l'aide de la méthode appropriée pour votre version; voir Accéder à la CLI ou au Shell Linux sur le On-Prem Firewall Management Center, à la page 5.

Étape 2 À l'invite, définissez la sortie de la console en entrant l'une des commandes suivantes :

- Pour diriger les messages de la console vers le port VGA : `sudo /usr/local/sf/bin/configure_console.sh vga`
- Pour diriger les messages de la console vers le port série physique : `sudo /usr/local/sf/bin/configure_console.sh serial`

Étape 3 Pour mettre en œuvre vos modifications, redémarrez l'appareil en saisissant `sudo reboot`.

Préconfigurer les centres de gestion

Vous pouvez préconfigurer votre Firewall Management Center à un emplacement de préconfiguration (un emplacement central pour préconfigurer ou mettre en place plusieurs appareils) en vue d'un déploiement à un emplacement cible (tout emplacement autre que l'emplacement de préconfiguration).

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

1. Installez le système sur l'appareil à l'emplacement de préconfiguration.
2. Arrêtez et expédiez l'appareil vers l'emplacement cible.
3. Déployez l'appareil à l'emplacement cible.

Remarque Conservez tous les matériaux d'emballage et incluez toute la documentation de référence ainsi que les cordons d'alimentation lors du réemballage de l'appareil.

Renseignements de préconfiguration requis

Avant de préconfigurer l'appareil, collectez les paramètres réseau, les licences et les autres informations pertinentes pour l'emplacement de stockage 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.

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

- Nouveau mot de passe (la configuration initiale nécessite la modification du mot de passe)
- Nom d'hôte de l'appareil
- Nom de domaine de l'appareil
- Adresse IP de gestion de l'appareil
- Masque réseau de l'appareil à l'emplacement cible
- Passerelle par défaut de l'appareil à l'emplacement cible
- Adresse IP du serveur DNS à l'emplacement de mise en place ou, s'il est accessible, de l'emplacement cible

- Adresse IP du serveur NTP à l'emplacement de rangement ou, si accessible, à l'emplacement cible

Renseignements facultatifs sur la préconfiguration

Vous pouvez modifier certaines configurations par défaut, notamment les suivantes :

- Le fuseau horaire (si vous choisissez de définir manuellement l'heure pour vos appareils)
- L'emplacement de stockage distant pour les sauvegardes automatiques
- L'adresse IP du LOM pour activer le LOM

Préconfigurer la gestion de l'heure

Procédure

Étape 1 Synchronisez l'heure avec un serveur NTP physique.

Étape 2 Définissez les adresses IP pour les serveurs DNS et NTP en utilisant l'une des méthodes suivantes :

- Si votre réseau à l'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 à l'emplacement cible.
- Si votre réseau à l'emplacement de mise en place ne peut pas accéder aux serveurs DNS et NTP de l'emplacement cible, utilisez les informations d'emplacement de mise en place et réinitialisez-le à l'emplacement cible.

Étape 3 Utilisez le fuseau horaire du déploiement cible si vous définissez l'heure sur l'appareil manuellement au lieu d'utiliser le protocole NTP. Pour en savoir plus, consultez les Guide d'administration Cisco Secure Firewall Management Center pour votre version.

Installer le système

Procédure

Étape 1 Utilisez les procédures d'installation appropriées à votre version :

- Pour les versions 6.5 et ultérieures, consultez le Installer le Centre de gestion pour les versions 6.5 et ultérieures, à la page 6
- Pour les versions 6.3 - 6.4, consultez Installer le Centre de gestion pour les versions de logiciel 6.3 - 6.4, à la page 21.

Étape 2 Pour plus d'informations sur l'installation du châssis, consultez le Guide d'installation du matériel (GIM) pour Cisco Firepower Management Center 1600, 2600 et 4600.

Préparer le centre de gestion pour l'expédition

Procédure

Étape 1 Éteignez en toute sécurité Firewall Management Center. Pour plus d'informations, consultez le Guide d'administration Cisco Secure Firewall Management Center.

Étape 2 Assurez-vous que votre appareil est préparé en toute sécurité pour l'expédition. Pour en savoir plus, consultez Considérations relatives à l'expédition, à la page 53.

Considérations relatives à 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 de l'appareil

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

Si vous avez des difficultés à vous connecter à l'appareil, 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 à l'appareil.
- 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. Pour en savoir plus, consultez les instructions de configuration initiale appropriées à votre version :
  - Pour les versions 6.5 et ultérieures, consultez Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures, à la page 12 ou Configuration initiale du centre de gestion à l'aide de l'interface de ligne de commande pour les versions 6.5 et ultérieures, à la page 17.
  - Pour les versions 6.3 - 6.4, consultez (Facultatif) Configurer les paramètres réseau à l'aide d'une connexion physique pour les versions logicielles 6.3 - 6.4, à la page 27 ou Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4, à la page 28.

- Confirmez que les ports de communication appropriés fonctionnent correctement. Pour en savoir plus sur la gestion des ports de pare-feu et les ports ouverts requis, consultez Guide d'administration Cisco Secure Firewall Management Center pour votre version.

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

Gestion du centre de gestion à l'aide de l'utilitaire de restauration du système

Le Firewall Management Center fournit un utilitaire de restauration du système que vous pouvez utiliser pour effectuer un certain nombre de fonctions de maintenance :

- Restaurez Firewall Management Center aux paramètres d'usine en utilisant une image ISO fournie par Cisco sur son site d'assistance. Consultez À propos du processus de restauration, à la page 55.
- Enregistrez un ensemble de configurations Firewall Management Center ou chargez une configuration Firewall Management Center enregistrée précédemment. Voir la section Enregistrer et charger les configurations du centre de gestion, à la page 67.
- Nettoyez le disque dur Firewall Management Center en toute sécurité pour vous assurer que son contenu n'est plus accessible. Consultez Effacer le disque dur, à la page 69.

Le menu de l'utilitaire de restauration

L'utilitaire de restauration pour Firewall Management Center utilise un menu interactif pour vous guider dans le processus de restauration.

Le menu affiche les options répertoriées dans le tableau suivant :

Tableau 2 : Options du menu de restauration

Option	Description	Pour plus de renseignements, consultez...
1 Configuration IP	Précisez les informations réseau concernant l'interface de gestion de l'appareil que vous souhaitez restaurer, afin que l'appareil puisse communiquer avec le serveur où vous avez placé l'image ISO et les fichiers de mise à jour.	Identifier l'interface de gestion de l'appareil, à la page 62
2 Choisir le protocole de transport	Précisez l'emplacement de l'image ISO que vous utiliserez pour restaurer l'appareil, ainsi que les informations d'authentification dont l'appareil a besoin pour télécharger le fichier.	Préciser l'emplacement de l'image ISO et la méthode de transport, à la page 63

Option	Description	Pour plus de renseignements, consultez...
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 de l'appareil à la version de base dans l'image ISO.	Sélectionner les mises à jour du logiciel système et des règles pendant la restauration, à la page 64
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.	Télécharger l'image ISO et les fichiers de mise à jour et monter l'image, à la page 65
5 Exécuter l'installation	Appelez le processus de restauration.	Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57
6 Enregistrer la configuration. 7 Charger la configuration	Enregistrez tout ensemble de configurations de restauration pour une utilisation ultérieure ou chargez un ensemble sauvegardé.	Enregistrer et charger les configurations du centre de gestion, à la page 67
8 Effacer le contenu du disque	Nettoyez le disque dur en toute sécurité pour vous assurer que son contenu n'est plus accessible.	Effacer le disque dur, à la page 69

Naviguez dans le menu à l'aide des touches fléchées. Pour sélectionner une option de menu, utilisez les touches fléchées **Haut** et **Bas**. Utilisez les touches fléchées **Droite** et **Gauche** pour basculer entre les boutons **OK** et **Annuler** en bas de la page.

Le menu présente deux options :

- 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 **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 **Entrée** lorsque le bouton **OK** est en surbrillance.

À propos du processus de restauration

L'image ISO que vous utilisez pour restaurer un périphérique dépend du moment où Cisco a introduit la prise en charge de ce modèle de périphérique. 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, 6.1 ou 6.2). Pour éviter d'installer une version incompatible du système, nous vous recommandons de toujours utiliser la dernière image ISO disponible pour votre appareil. 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. Gardez à l'esprit que seuls les Firewall Management Centernécessitent des mises à jour de règles.

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

Nous vous recommandons 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 d'administration Cisco Secure Firewall Management Center de votre version.

Avant de commencer à restaurer vos périphériques aux valeurs par défaut, prenez en compte les recommandations suivantes et le comportement attendu du système pendant le processus de restauration :

- Pour éviter de perturber le flux de trafic sur votre réseau, nous vous recommandons de restaurer vos périphériques pendant une fenêtre de maintenance ou à un moment où l'interruption a le moins d'impact sur votre déploiement.
- Nous vous recommandons 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 appareil aux valeurs par défaut entraîne la perte de presque toutes les données de configuration et d'événements sur le périphérique, y compris l'affichage de la console et les paramètres LOM. Bien que l'utilitaire de restauration puisse conserver la licence et les paramètres réseau du périphérique, vous devez effectuer toutes les autres tâches de configuration une fois le processus de restauration terminé.
- Pour restaurer le Firewall Management Center, 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.

Remarque Vous *ne pouvez pas* restaurer un périphérique à l'aide de son interface Web.

- Pour restaurer le Firewall Management Center, 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 (clé, vidéo et souris). Reportez-vous à la figure à Fonctionnalités du panneau arrière, à la page 1 pour identifier les ports USB et VGA. Si vous avez un KVM accessible à distance, vous pouvez restaurer des périphériques sans accès physique.
  - Serial Connection/ordinateur portable : vous pouvez utiliser le câble de console RJ-45 vers DP-9 fourni avec le périphérique (numéro de pièce Cisco 72-3383-XX) pour connecter un ordinateur au périphérique. Reportez-vous à la figure à Fonctionnalités du panneau arrière, à la page 1 pour identifier 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 Firewall Management Center en utilisant LOM avec une connexion 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.

Remarque Vous pouvez utiliser LOM uniquement sur l'interface CIMC (consultez le schéma à Fonctionnalités du panneau arrière, à la page 1). Pour restaurer le Firewall Management Center à l'aide de LOM, vous devez accorder l'autorisation LOM à l'utilisateur **admin**. Pour en savoir plus, consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46.

Mise en garde Lors de la restauration d'un périphérique aux paramètres d'usine à l'aide de LOM, sans accès physique au périphérique, vous ne pourrez pas y accéder après la restauration.

Remarque Les procédures de ce chapitre expliquent comment restaurer un périphérique sans l'éteindre. Cependant, si vous devez l'éteindre pour quelque raison que ce soit, utilisez de l'interface Web de l'appareil, la commande **system shutdown** (arrêt du système) de l'interface de ligne de commande Firewall Management Center ou la commande **shutdown -h now** (arrêt -h maintenant) de l'interface Shell du périphérique.

Restaurer un centre de gestion à ses paramètres d'usine par défaut

Cette rubrique fournit une description générale des tâches requises pour restaurer les paramètres d'usine par défaut du Firewall Management Center, ainsi que l'ordre dans lequel vous devez les effectuer.

Avant de commencer

Prenez connaissance du menu de restauration interactif de Firewall Management Center. Pour en savoir plus, consultez Le menu de l'utilitaire de restauration, à la page 54.

Procédure

Étape 1 Obtenez les fichiers de restauration et de mise à jour ISO. Consultez Obtenir l'image ISO de restauration et les fichiers de mise à jour, à la page 59.

Étape 2 Démarrez le processus de restauration en utilisant l'une de ces deux méthodes :

- Démarrer l'utilitaire de restauration à l'aide du KVM ou du port série physique, à la page 60
- Démarrer l'utilitaire de restauration à l'aide de Lights-Out Management, à la page 61 (Cela est utile si vous n'avez pas d'accès physique à l'appareil.)

Mise en garde
Lors de la restauration d'un appareil aux paramètres d'usine des à l'aide de LOM, si vous n'avez pas d'accès physique à l'appareil et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder à l'appareil après la restauration.

Étape 3 Utilisez le menu de restauration interactif pour identifier l'interface de gestion de l'appareil. Consultez Identifier l'interface de gestion de l'appareil, à la page 62.

Étape 4 Utilisez le menu de restauration interactif pour préciser l'emplacement de l'image ISO et la méthode de transport. Consultez Préciser l'emplacement de l'image ISO et la méthode de transport, à la page 63.

Étape 5 (Facultatif) Utilisez le menu de restauration interactif pour sélectionner les mises à jour de logiciel système ou de règles à inclure dans le processus de restauration. Consultez Sélectionner les mises à jour du logiciel système et des règles pendant la restauration, à la page 64.

Étape 6 (Facultatif) Enregistrez la configuration système que vous avez sélectionnée pour l'utiliser dans les activités de restauration futures. Consultez Enregistrer la configuration du centre de gestion, à la page 68.

Étape 7 Utilisez le menu de restauration interactif pour télécharger les fichiers ISO et de mise à jour, et monter l'image sur l'appareil. Consultez Télécharger l'image ISO et les fichiers de mise à jour et monter l'image, à la page 65.

Étape 8 Vous avez deux options en fonction de la version du logiciel à laquelle vous restaurez l'appareil :

- Si vous restaurez le système vers une version majeure différente, effectuez le processus de restauration en deux temps :

  1. La première passe met à jour l'image de restauration. Consultez Mettre à jour l'image de restauration, à la page 65.
  2. La deuxième passe installe la nouvelle version du logiciel système. Consultez Installer la nouvelle version du logiciel système, à la page 66.

- Si vous restaurez le système vers la même version principale, vous ne devez installer que la nouvelle version du logiciel système. Consultez Installer la nouvelle version du logiciel système, à la page 66.

Prochaine étape

La restauration de votre Firewall Management Center aux paramètres d'usine par défaut entraîne la perte de presque toutes les données de configuration et d'événement sur l'appareil, y compris les paramètres d'affichage de la console.

- Si vous n'avez pas supprimé la licence et les paramètres réseau de l'appareil, vous pouvez utiliser un ordinateur de votre réseau de gestion pour accéder directement à l'interface Web de l'appareil afin d'effectuer la configuration.

  Pour en savoir plus, consultez le processus de configuration approprié à votre version :

  - Pour les versions 6.5 et ultérieures, consultez Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures, à la page 12.
  - Pour les versions - 6.4x, consultez Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4, à la page 28.

- 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, consultez le processus de configuration approprié à votre version :

  - Pour les versions 6.5 et ultérieures, consultez Effectuer la configuration initiale au niveau de l'interface Web pour les versions 6.5 et ultérieures, à la page 12.
  - Pour les versions - 6.4x, consultez Configuration initiale Centre de gestion à l'aide de l'interface Web pour les versions logicielles 6.3 - 6.4, à la page 28.

- Si vous avez désenregistré Firewall Management Center de Cisco Smart Software Manager, enregistrez l'appareil sur Cisco Smart Software Manager. Choisissez **Système** > **Licences** > **Licences Smart** et cliquez sur l'icône de registre.

Remarque La restauration des valeurs d'usine de l'appareil réinitialise également les paramètres LOM. Après avoir terminé le processus de configuration initiale, effectuez l'une des opérations suivantes :

- Si vous souhaitez utiliser une connexion de série ou SOL/LOM pour accéder à la console de votre appareil, redirigez la sortie de la console; voir Rediriger la sortie de la console, à la page 49.
- Si vous souhaitez utiliser LOM, vous devez réactiver la fonctionnalité, ainsi qu'activer au moins un utilisateur LOM. Pour en savoir plus, consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46.

Obtenir l'image ISO de restauration et les fichiers de mise à jour

Avant de commencer

Cisco fournit des images ISO permettant de restaurer les paramètres d'usine d'origine des appareils. Avant de restaurer un appareil, procurez-vous l'image ISO correcte auprès du site d'assistance, comme décrit ici.

Procédure

Étape 1 En utilisant le nom d'utilisateur et le mot de passe de votre compte d'assistance, connectez-vous au site d'assistance à l'adresse https://sso.cisco.com/autho/forms/CDClogin.html.

Étape 2 Accédez à la section de téléchargement de logiciels à l'adresse : https://software.cisco.com/download/navigator.html.

Étape 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.

Étape 4 Recherchez l'image (l'image ISO) que vous souhaitez télécharger. Vous pouvez cliquer sur l'un des liens dans la partie gauche de la page pour afficher la section appropriée de la page.

Exemple :

Cliquez sur **6.3.0** pour afficher les images et les notes de mise à jour pour la version 6.3.0 du système.

Étape 5 Cliquez sur l'image ISO que vous souhaitez télécharger.
Le téléchargement du fichier commence.

Étape 6 Copiez les fichiers sur un serveur HTTP (Web), un serveur FTP ou un hôte SCP auquel l'appareil peut accéder sur son réseau de gestion.

Mise en garde
Ne transférez pas de fichiers ISO ou de mise à jour par courriel, car les fichiers 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.

Démarrer l'utilitaire de restauration à l'aide du KVM ou du port série physique

Pour Firewall Management Center, Cisco fournit un utilitaire de restauration sur un disque flash interne.

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 À l'aide de votre clavier/moniteur ou d'une connexion série, connectez-vous à l'interface Shell de l'appareil à l'aide du compte **admin**. Suivez les étapes adaptées à votre version ; consultez Accéder à la CLI ou au Shell Linux sur le On-Prem Firewall Management Center, à la page 5.

Étape 2 Redémarrez l'appareil; saisissez **sudo reboot**. Saisissez le mot de passe administrateur lorsque vous y êtes invité.

Remarque
Vous devez effectuer les étapes 3 et 4 rapidement pour éviter un redémarrage physique.

Étape 3 Supervisez le processus de redémarrage. Lorsque le menu de démarrage s'affiche, choisissez rapidement **Option 3** pour restaurer le système.

Remarque
Le menu de démarrage ne vous donne que quelques secondes pour effectuer votre sélection avant d'expirer. Si vous ratez votre fenêtre d'occasion, l'appareil lance le processus de redémarrage. Attendez que le redémarrage soit terminé et réessayez.

Étape 4 Le système vous invite à passer en mode d'affichage pour le menu interactif de l'utilitaire de restauration. Choisissez rapidement parmi :

- Pour une connexion de clavier et de moniteur, saisissez **1** et appuyez sur **Entrée**.
- Pour une connexion série, saisissez **2** et appuyez sur **Entrée**.

Si vous ne sélectionnez pas de mode d'affichage, l'utilitaire de restauration utilise l'option marquée d'un astérisque (*****).

Remarque
Le menu du mode d'affichage ne vous donne que quelques secondes pour effectuer votre sélection avant l'expiration. Si vous ratez votre fenêtre d'occasion et redémarrez accidentellement l'appareil en mode de restauration du système avec la mauvaise sélection de console, attendez la fin du redémarrage, puis éteignez l'appareil. (Vous devez utiliser le bouton d'alimentation pour éteindre l'appareil à ce moment-là, car le logiciel Firewall Management Center n'est pas en cours d'exécution.) Mettez ensuite l'unité Firewall Management Center sous tension et recommencez cette tâche.

Sauf s'il s'agit de la première restauration de l'appareil à 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.

Étape 5 Appuyez sur **Entrée** pour confirmer l'avis de droits d'auteur.

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

Si vous devez rétablir les valeurs par défaut de l'appareil et que vous n'avez pas d'accès physique à l'appareil, vous pouvez utiliser Lights-Out Management (LOM) pour effectuer le processus de restauration.

Remarque Le processus de restauration réinitialise les paramètres LOM de l'appareil; vous ne pouvez pas accéder à un appareil nouvellement restauré à l'aide de LOM.

Mise en garde Lors de la restauration d'un appareil aux paramètres d'usine des à l'aide de LOM, si vous n'avez pas d'accès physique à l'appareil et que vous supprimez la licence et les paramètres réseau, vous ne pourrez plus accéder à l'appareil après la restauration.

Avant de commencer

- Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.
- Vous devez activer la fonctionnalité LOM et vous devez accorder l'autorisation LOM à l'utilisateur admin. Pour en savoir plus, consultez Configurer Lights-Out Management (Gestion en service réduit), à la page 46 .

Procédure

Étape 1 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 admin sol activate**
- Pour ipmiutil, saisissez : **sudo ipmiutil sol -a -V4 -J3 -N *IP_address* -U admin -P *password***

L' *IP_address* est l'adresse IP de l'interface de gestion sur l'appareil et *password* est le mot de passe du compte admin. Notez qu'IPMItool vous invite à saisir le mot de passe après avoir exécuté la commande **sol activate**.

Étape 2 Redémarrez l'appareil en tant qu'utilisateur root; saisissez **sudo reboot**. Saisissez le mot de passe administrateur lorsque vous y êtes invité.

Étape 3 Supervisez le processus de redémarrage. Lorsque le menu de démarrage s'affiche, choisissez rapidement **Option 3** pour restaurer le système.

Remarque
Le menu de démarrage ne vous donne que quelques secondes pour effectuer votre sélection avant d'expirer. Si vous ratez votre fenêtre d'occasion, l'appareil lance le processus de redémarrage. Attendez que le redémarrage soit terminé et réessayez.

Étape 4 Le système vous invite à passer en mode d'affichage pour le menu interactif de l'utilitaire de restauration. Saisissez **2** et appuyez sur **Entrée** pour charger le menu de restauration interactif à l'aide du port série de l'appareil.

Si vous ne sélectionnez pas de mode d'affichage, l'utilitaire de restauration utilise l'option marquée d'un astérisque (*****).

Important
Le menu du mode d'affichage ne vous donne que quelques secondes pour effectuer votre sélection avant l'expiration. Si vous ratez votre fenêtre d'occasion et redémarrez accidentellement l'appareil en mode de restauration du système avec l'Option 1 (pour une connexion de clavier et de moniteur), vous devez obtenir un accès physique à l'appareil, attendre la fin du redémarrage, puis éteindre l'appareil. (Vous devez utiliser le bouton d'alimentation pour éteindre l'appareil à ce moment-là, car le logiciel Firewall Management Center n'est pas en cours d'exécution.) Mettez ensuite l'unité Firewall Management Center sous tension et recommencez cette tâche.

Sauf s'il s'agit de la première restauration de l'appareil à 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.

Étape 5 Appuyez sur **Entrée** pour confirmer l'avis de droits d'auteur.

Identifier l'interface de gestion de l'appareil

La première étape de l'exécution de l'utilitaire de restauration consiste à identifier l'interface de gestion sur l'appareil que vous souhaitez restaurer, afin que l'appareil puisse communiquer avec le serveur sur lequel vous avez copié l'image ISO et les fichiers de mise à jour.

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **1 Configuration IP**.

Étape 2 Choisissez l'interface de gestion de l'appareil (généralement eth0).

Étape 3 Choisissez 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.

Étape 4 Choisissez une méthode pour attribuer une adresse IP à l'interface de gestion :

- **Statique** : une série de pages vous invite à saisir manuellement l'adresse IP, le masque réseau ou la longueur du préfixe et la passerelle par défaut pour l'interface de gestion.
- **DHCP** : l'appareil détecte automatiquement l'adresse IP, le masque réseau ou la longueur du préfixe et la passerelle par défaut pour l'interface de gestion, puis affiche l'adresse IP.

Étape 5 Lorsque vous y êtes invité, confirmez vos paramètres.

Si vous y êtes invité, confirmez l'adresse IP attribuée à l'interface de gestion de l'appareil. Si vous utilisez LOM, n'oubliez pas que l'adresse IP de gestion de l'appareil n'est *pas* l'adresse IP LOM.

Préciser l'emplacement de l'image ISO et 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 l'appareil. Il s'agit de l'image ISO que vous avez téléchargée à partir du site d'assistance (voir Obtenir l'image ISO de restauration et les fichiers de mise à jour, à la page 59) et stockée sur un serveur Web, un serveur FTP ou un hôte compatible avec le protocole SCP.

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **2 Choisir le protocole de transport**.

Étape 2 Dans la page qui s'affiche, choisissez **HTTP**, **FTP** ou **SCP**.

Étape 3 Utilisez la série de pages présentées par l'utilitaire de restauration pour fournir les informations nécessaires pour le protocole que vous avez choisi; voir Configuration de téléchargement des fichiers de restauration, à la page 63.

Si vos informations sont correctes, l'appareil se connecte au serveur et affiche une liste des images ISO de Cisco à l'emplacement que vous avez spécifié.

Étape 4 Choisissez l'image ISO que vous souhaitez utiliser.

Étape 5 Lorsque vous y êtes invité, confirmez vos paramètres.

Configuration de téléchargement des fichiers de restauration

Avant de pouvoir identifier l'image ISO que vous utiliserez pour restaurer l'appareil, vous devez configurer l'adresse IP de gestion que le processus de restauration utilise pour télécharger les fichiers dont il a besoin. Le menu interactif sur le Firewall Management Center vous invite à saisir des informations pour terminer le téléchargement, comme indiqué dans le tableau suivant.

Tableau 3 : Informations nécessaires pour télécharger les fichiers de restauration

Pour utiliser...	Vous devez fournir...
HTTP	• Adresse IP du serveur Web • Chemin complet au répertoire de l'image ISO (par exemple, `/downloads/ISOs/`)

Pour utiliser...	Vous devez fournir...
FTP	• Adresse IP du serveur FTP • Chemin d'accès au répertoire de l'image ISO, par rapport au répertoire personnel de l'utilisateur dont vous souhaitez utiliser les informations d'identification (par exemple, `mydownloads/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 complet au répertoire de l'image ISO • Mot de passe pour le nom d'utilisateur que vous avez saisi plus tôt **Remarque** Avant de saisir votre mot de passe, vous pouvez être invité à ajouter le serveur SCP à la liste des hôtes de confiance. Vous devez accepter pour continuer.

Sélectionner les mises à jour du logiciel système et des règles pendant la restauration

Vous pouvez éventuellement utiliser l'utilitaire de restauration pour mettre à jour le logiciel système et les règles de prévention des intrusions après la restauration de l'appareil à la version de base dans l'image ISO. Gardez à l'esprit que seuls les Firewall Management Center 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 jusqu'à la dernière version majeure; les mises à jour de règles sont également cumulatives. Nous vous recommandons d'obtenir les dernières mises à jour disponibles pour votre appareil; voir Obtenir l'image ISO de restauration et les fichiers de mise à jour, à la page 59.

Si vous choisissez de ne pas mettre à jour l'appareil 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 mise à jour que vous souhaitez installer, ainsi que le chapitre Mise à jour du logiciel système dans Guide d'administration Cisco Secure Firewall Management Center.

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **3 Sélectionner les correctifs/mises à jour des règles**.

L'utilitaire de restauration utilise le protocole et l'emplacement que vous avez spécifiés dans la procédure précédente (voir Préciser l'emplacement de l'image ISO et la méthode de transport, à la page 63) pour récupérer

et afficher une liste de tous les fichiers de mise à jour de logiciel système 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.

Étape 2 Choisissez la mise à jour du logiciel système, le cas échéant, que vous souhaitez utiliser. Vous n'avez pas à choisir une mise à jour; appuyez sur **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 **Entrée** pour continuer.

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

Étape 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 **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 **Entrée** pour continuer.

Télécharger l'image ISO et les fichiers de mise à jour et monter l'image

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **4 Télécharger et monter l'ISO**.

Étape 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. Le système télécharge et monte les fichiers appropriés.

Mettre à jour l'image de restauration

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

Remarque Si vous restaurez un appareil à la même version majeure ou s'il s'agit de votre deuxième transmission directe du processus, n'utilisez pas ces instructions; voir Installer la nouvelle version du logiciel système, à la page 66.

Avant de commencer

Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **5 Exécuter l'installation**.

Étape 2 Lorsque vous y êtes invité (deux fois), confirmez que vous souhaitez redémarrer l'appareil.

Étape 3 Le système demande le mode d'affichage du menu interactif de l'utilitaire de restauration :

- Pour une connexion de clavier et de moniteur, saisissez **1** et appuyez sur Entrée.
- Pour une connexion série, saisissez **2** et appuyez sur **Entrée**.

Si vous ne sélectionnez pas de mode d'affichage, l'utilitaire de restauration utilise l'option marquée d'un astérisque (*****).

Sauf s'il s'agit de la première restauration de l'appareil à cette version majeure, l'utilitaire charge automatiquement la dernière configuration de restauration que vous avez utilisée. Pour continuer, confirmez les paramètres affichés dans la série de pages suivante.

Étape 4 Appuyez sur **Entrée** pour confirmer l'avis de droits d'auteur.

Prochaine étape

Effectuez les tâches de la deuxième étape du processus de restauration. Consultez Installer la nouvelle version du logiciel système, à la page 66.

Installer la nouvelle version du logiciel système

Effectuez les tâches suivantes si vous restaurez un appareil vers la même version majeure ou si c'est votre deuxième passage dans le processus de restauration en deux étapes.

Remarque Le processus de restauration réinitialise les paramètres d'affichage de la console au mode par défaut d'utilisation du port VGA.

Avant de commencer

- Assurez-vous d'avoir effectué les étapes précédentes appropriées dans le processus de restauration, comme décrit dans Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.
- Si vous effectuez cette tâche en tant que deuxième passe dans le processus de restauration du système en deux temps, vous devez d'abord télécharger et monter l'image ISO. Consultez Télécharger l'image ISO et les fichiers de mise à jour et monter l'image, à la page 65. (Si vous effectuez le processus de restauration en deux temps, ce sera la deuxième fois que vous téléchargerez et monterez l'image ISO.)

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **5 Exécuter l'installation**.

Étape 2 Confirmez que vous souhaitez restaurer l'appareil.

Étape 3 Choisissez si vous souhaitez supprimer la licence de l'appareil et les paramètres réseau.

Dans la plupart des cas, vous ne souhaitez pas supprimer ces paramètres; les conserver 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.

Mise en garde
Le processus de restauration réinitialise les paramètres LOM de l'appareil; vous ne pouvez pas accéder à un appareil nouvellement restauré à l'aide de LOM. Lors de la restauration d'un appareil aux paramètres d'usine des à l'aide de LOM, sans accès physique à l'appareil, vous ne pourrez pas y accéder après la restauration.

Étape 4 Saisissez votre confirmation finale que vous souhaitez restaurer l'appareil.

L'étape finale du processus de restauration commence. Une fois celle-ci terminée, si vous y êtes invité, confirmez que vous souhaitez redémarrer l'appareil.

Mise en garde
Assurez-vous de prévoir suffisamment de temps pour que le processus de restauration se termine. Sur les appareils 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 flash, 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 plutôt avec Centre d'assistance technique Cisco (TAC).

Remarque
Recréez toujours l'image de vos appareils pendant une fenêtre de maintenance.

Enregistrer et charger les configurations du centre de gestion

Vous pouvez utiliser l'utilitaire de restauration pour enregistrer une configuration si vous devez restaurer le Firewall Management Center. Bien que l'utilitaire de restauration enregistre automatiquement la dernière configuration utilisée, vous pouvez enregistrer plusieurs configurations, notamment les suivantes :

- Renseignements sur le réseau concernant l'interface de gestion de l'appareil. Pour en savoir plus, consultez Identifier l'interface de gestion de l'appareil, à la page 62.
- Emplacement de l'image ISO, ainsi que du protocole de transport et des informations d'authentification dont l'appareil a besoin pour télécharger le fichier. Pour en savoir plus, consultez Préciser l'emplacement de l'image ISO et la méthode de transport, à la page 63.
- Mises à jour du logiciel système et des règles de prévention des intrusions, le cas échéant, que vous souhaitez appliquer après la restauration de l'appareil à la version de base dans l'image ISO. Pour en savoir plus, consultez Sélectionner les mises à jour du logiciel système et des règles pendant la restauration, à la page 64.

Le système n'enregistre pas les mots de passe SCP. Si la configuration spécifie que l'utilitaire doit utiliser SCP pour transférer les fichiers ISO et d'autres fichiers vers l'appareil, vous devez vous authentifier de nouveau auprès du serveur pour terminer le processus de restauration.

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

Enregistrer la configuration du centre de gestion

Avant de commencer

Effectuez les étapes 1 à 5 de Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Procédure

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

L'utilitaire affiche les paramètres de la configuration que vous enregistrez.

Étape 2 Lorsque vous y êtes invité, confirmez que vous souhaitez enregistrer la configuration.

Étape 3 Lorsque vous y êtes invité, saisissez un nom pour la configuration.

Prochaine étape

Si vous souhaitez utiliser la configuration enregistrée pour effectuer une restauration du système, passez à l'étape 7 de Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Charger une configuration du centre de gestion enregistrée

Vous pouvez charger une configuration enregistrée précédemment pour restaurer le Firewall Management Center.

Procédure

Étape 1 Dans le menu principal de l'utilitaire de restauration, choisissez **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 l'appareil. Les autres options sont des configurations de restauration que vous avez enregistrées.

Étape 2 Choisissez la configuration que vous souhaitez utiliser.

L'utilitaire affiche les paramètres de la configuration que vous chargez.

Étape 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 de l'appareil.

Prochaine étape

Pour utiliser la configuration que vous venez de charger pour restaurer le système, passez à l'étape 7 de Restaurer un centre de gestion à ses paramètres d'usine par défaut, à la page 57.

Effacer le disque dur

Vous pouvez effacer en toute sécurité le disque dur sur Firewall Management Center pour vous assurer que son contenu ne peut plus être consulté. Par exemple, si vous devez retourner un appareil défectueux qui contient des données sensibles, vous pouvez utiliser cette fonctionnalité pour remplacer les données qu'il contient.

La séquence d'effacement du disque dur est conforme à la procédure DoD 5220.22-M pour l'intégrité des disques durs amovibles et non amovibles, qui nécessite le remplacement de tous les emplacements adressables par un caractère, son complément, un caractère aléatoire, puis une vérification. Consultez le document DoD pour connaître les contraintes supplémentaires.

Mise en garde L'effacement de votre disque dur entraîne la perte de toutes les données d'appareil, lequel devient alors inutilisable.

Vous pouvez effacer le disque dur à l'aide d'une option dans le menu interactif de l'appareil. Pour en savoir plus, consultez Le menu de l'utilitaire de restauration, à la page 54 .

Procédure

Étape 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 à l'appareil :

- Démarrer l'utilitaire de restauration à l'aide du KVM ou du port série physique, à la page 60
- Démarrer l'utilitaire de restauration à l'aide de Lights-Out Management, à la page 61

Étape 2 Dans le menu principal de l'utilitaire de restauration, choisissez **8 Effacer le contenu du disque**.

Étape 3 Lorsque vous y êtes invité, confirmez que vous souhaitez effacer le disque dur. Le processus peut prendre plusieurs heures; les disques durs plus volumineux prendront plus de temps.

À propos de la traduction

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

À propos de la traduction

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