

Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Dernière modification : 2025-11-10

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2018–2025 Cisco Systems, Inc. Tous droits réservés.

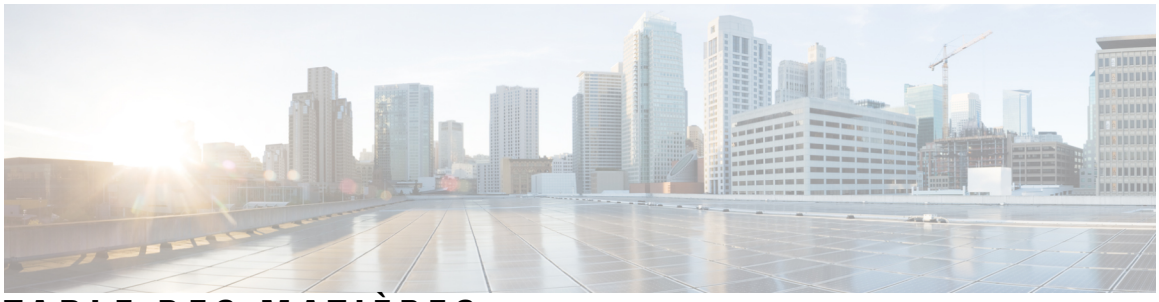


TABLE DES MATIÈRES

CHAPITRE 1 **Pour commencer** 1

Ce guide est-il pour vous? 1

Historique des fonctionnalités de mise à niveau 4

CHAPITRE 2 **Planification de votre mise à niveau** 9

Upgrade Planning Phases (Phases de planification de la mise à niveau) 9

Renseignements sur la version actuelle et le modèle 10

Chemins de mise à niveau 11

Chemins de mise à niveau : Cisco Firepower Management Center 12

Chemin de mise à niveau : Firepower 4100/9300 avec périphériques logiques FTD 15

Chemin de mise à niveau : autres appareils Cisco Firepower Threat Defense 18

Chemins de mise à niveau : Firepower de série 7000/8000 20

Chemin de mise à niveau : ASA FirePOWER 22

Chemin de mise à niveau : ASA pour ASA FirePOWER 25

Chemin de mise à niveau : NGIPSv 29

Mises à niveau qui ne répondent pas 31

Tests de temps et d'espace disque 32

Téléchargez les paquets de mise à niveau 34

Paquets logiciels Firepower 34

Prologiciels FXOS 36

Paquets ASA 37

Charger des paquets de mise à niveau logicielle Firepower 38

Charger vers Cisco Firepower Management Center 38

Charger du contenu vers un serveur interne (version 6.6.0 ou version ultérieure de FTD avec FMC) 38

Copier des données sur les périphériques gérés 40

Vérification de l'état de préparation du logiciel Firepower 41

Exécuter les vérifications de l'état de préparation avec FDM (FTD version 7.0.0 ou version ultérieure) 41

Exécuter les vérifications de préparation avec FMC (version 6.7.0 et versions ultérieures) 42

Exécuter des vérifications de l'état de préparation avec FMC (version 6.0.1–6.6.x) 43

CHAPITRE 3 **Mises à Niveau Cisco Firepower Management Center 45**

Liste de contrôle de mise à niveau : Firepower Management Center.contrôle 45

Mettre à niveau un élément autonome Cisco Firepower Management Center 49

Mettre à niveau les Firepower Management Center à haute disponibilité 51

CHAPITRE 4 **Mettre à niveau des dispositifs logiques FTD 53**

Liste de contrôle des mises à niveau : Firepower Threat Defense avec FMC 53

Mettre à niveau FXOS sur un Firepower 4100/9300 avec des périphériques logiques Firepower Threat Defense 58

Mettre à niveau FXOS : périphériques FTD en déploiement autonome et grappes intra-châssis 58

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intra-châssis FTD à l'aide de Firepower Chassis Manager 58

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intra-châssis FTD à l'aide de l'interface de ligne de commande de FXOS 60

Mettre à niveau FXOS : paires FTD à haute disponibilité 63

Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de Firepower Chassis Manager 63

Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de l'interface de ligne de commande de FXOS 66

Mettre à niveau FXOS : grappes FTD inter-châssis. 71

Mettre à niveau FXOS sur une grappe inter-châssis FTD à l'aide de Firepower Chassis Manager 71

Mettre à niveau FXOS sur une grappe inter-châssis FTD à l'aide de l'interface de ligne de commande de FXOS 74

Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0) 77

Mettre à niveau Firepower Threat Defense avec FMC (version 6.0.1–6.7.0) 81

CHAPITRE 5 **Mise à niveau de la série Firepower 7000/8000 et NGIPSv 85**

Liste de contrôle de mise à niveau : série Firepower 7000/8000 et NGIPSv avec FMC 85

Mise à niveau de la série Firepower 7000/8000 et NGIPSv avec FMC 89

CHAPITRE 6 **Mise à niveau d'ASA avec les services FirePOWER** 91

Liste de vérification de mise à niveau : ASA FirePOWER avec FMC 91

Mettre à niveau l'ASA 95

Mettre à niveau une unité autonome 95

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande 95

Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM 97

Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com 99

Mettre à niveau une paire de basculements actif/de secours 100

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande 101

Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM 103

Mettre à niveau une paire de basculements actif/actif 105

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande 105

Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM 108

Mettre à niveau une grappe ASA 110

Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de commande 110

Mettre à niveau une grappe ASA à l'aide d'ASDM 115

Mettre à niveau un module ASA FirePOWER avec FMC 118

CHAPITRE 7 **Désinstaller un correctif** 121

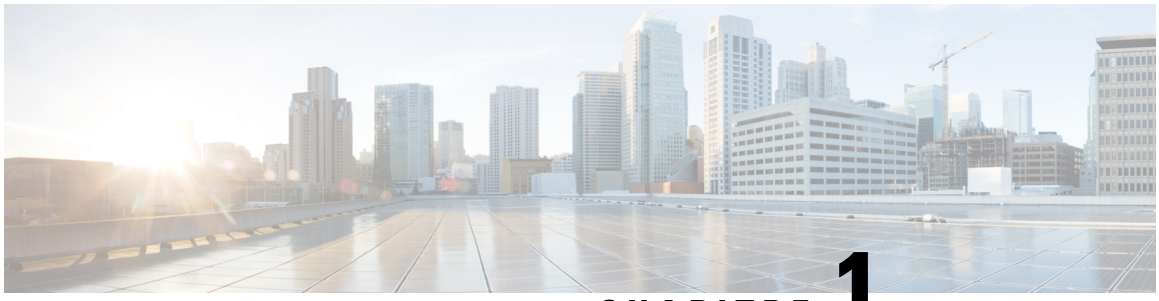
Correctifs qui prennent en charge la désinstallation 121

Ordre de désinstallation pour la haute disponibilité/évolutivité 124

Désinstaller les périphériques Threat Defense avec le FMC 126

Désinstaller les correctifs FMC autonomes 128

Désinstaller les correctifs de haute disponibilité FMC 129



CHAPITRE 1

Pour commencer

- Ce guide est-il pour vous?, à la page 1
- Historique des fonctionnalités de mise à niveau, à la page 4

Ce guide est-il pour vous?

Ce guide explique comment préparer et réussir une mise à niveau vers la **version 7.0.x ou une version antérieure** du Firepower, pour :

- Centre de gestion Firepower (FMC)
- Périphériques Firepower Threat Defense (FTD) avec FMC, y compris FXOS pour le Firepower 4100/9300
- Périphériques des séries 7000/8000 avec FMC
- Périphériques NGIPSv avec FMC
- Périphériques ASA FirePOWER avec FMC, y compris le système d'exploitation de l'ASA

Ressources supplémentaires

Si vous mettez à niveau une autre plateforme ou un autre composant, ou si vous effectuez une mise à niveau vers une version différente, consultez l'une de ces ressources.

Tableau 1 : Guides de mise à niveau pour FMC

Version actuelle de FMC	Guide
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Management Center, version 7.1
version 7.0 ou versions antérieures	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Tableau 2 : Guides de mise à niveau pour FTD avec FMC

Version actuelle de FMC	Guide
Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion Firewall livré dans le nuage
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Management Center, version 7.1
version 7.0 ou versions antérieures	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Tableau 3 : Guides de mise à niveau pour FTD avec FDM

Version actuelle de FTD	Guide
7.2+	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le gestionnaire des périphériques pour votre version
7.1	Guide de mise à niveau de Cisco Firepower Threat Defense pour Firepower Device Manager, version 7.1
version 7.0 ou versions antérieures	Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager pour votre version : *gestion du système* Pour les périphériques Firepower 4100/9300, consultez également les instructions de mise à niveau de FXOS dans Guide de mise à niveau de Cisco Firepower 4100/9300, FTD 6.0.1–7.0.x ou ASA 9.4(1)–9.16(x) avec FXOS 1.1.1–2.10.1.
Version 6.4 ou ultérieure, avec Security Cloud Control	Gestion des appareils FDM avec Pare-feu dans Security Cloud Control

Tableau 4 : Guides de mise à niveau pour NGIPS

Plateforme	Version actuelle du gestionnaire	Guide
Série Firepower 7000/8000 avec FMC	6.0.0–7.0.x	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0

Plateforme	Version actuelle du gestionnaire	Guide
NGIPSv avec FMC	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0
	7.2.6–7.2.x De la version 7.4.1 à la version 7.4.x	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
ASA FirePOWER avec FMC	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0
	7.2.6–7.2.x De la version 7.4.1 à la version 7.4.x	Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour le centre de gestion pour votre version
ASA FirePOWER avec ASDM	N'importe lequel	Guide de mise à niveau de Cisco Secure Firewall ASA

Tableau 5 : Mettre à niveau d'autres composants

Version	Composant	Guide
N'importe lequel	Périphériques logiques ASA sur le Firepower 4100/9300	Guide de mise à niveau de Cisco Secure Firewall ASA
Nouveaux	BIOS et micrologiciel pour FMC	Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower
Nouveaux	Micrologiciel pour le Firepower 4100/9300	CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS
Nouveaux	Image ROMMON pour l'ISA 3000	Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense

Historique des fonctionnalités de mise à niveau

Tableau 6 : Historique des mises à niveau FMC

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Les mises à niveau reportent les tâches planifiées.	6.4.0	N'importe lequel	Le processus de mise à niveau FMC reporte les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. **Remarque** Avant de commencer une mise à niveau, vous devez toujours vous assurer que les tâches en cours d'exécution sont terminées. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Notez que cette fonctionnalité est prise en charge pour toutes les mises à niveau *à partir d'* une version prise en charge. Cela comprend les correctifs pour la version 6.4.0.10 et ultérieures, la version 6.6.3 et les versions de maintenance ultérieures, et la version 6.7.0+. Cette fonctionnalité n'est pas prise en charge pour les mises à niveau *vers* une version prise en charge à partir d'une version non prise en charge.

Tableau 7 : Historique des mises à niveau des périphériques

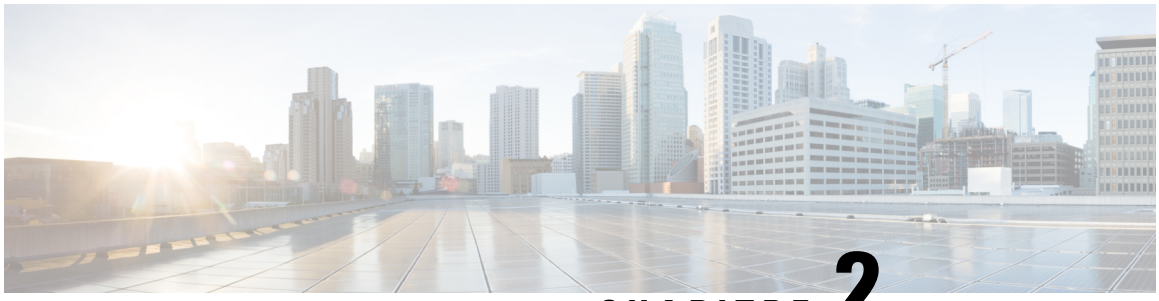
Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
L'amélioration des rapports d'état et de performance de la mise à niveau FTD.	7.0.0	7.0.0	Les mises à niveau de FTD sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Un nouvel onglet **Mises à niveau** dans le centre de messages fournit d'autres améliorations à l'état des mises à niveau et aux rapports d'erreurs.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Flux de travail de mise à niveau facile à suivre pour les périphériques FTD.	7.0.0	N'importe lequel	Une nouvelle page de mise à niveau des périphériques (**Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)**) fournit un assistant facile à suivre pour la mise à niveau des périphériques de version 6.4+ FTD. Il vous guide à travers les étapes préalables à la mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Pour commencer, utilisez la nouvelle action de **mise à niveau du logiciel Firepower** sur la page de gestion des périphériques **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Selection (Sélection)**. Pendant que vous continuez, le système affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante. Si vous quittez l'assistant, votre progression est conservée, bien que d'autres utilisateurs disposant d'un accès administrateur puissent réinitialiser, modifier ou continuer l'assistant. **Remarque** Vous devez toujours utiliser **System (Système)** > **Updates (mises à jour)** pour charger ou préciser l'emplacement des packages de mise à niveau Cisco FTD. Vous devez également utiliser la page System Updates pour mettre à niveau le FMC lui-même, ainsi que tous les périphériques non gérés par FTD. **Remarque** Dans la version 7.0, l'assistant n'affiche pas correctement les périphériques dans les grappes ou les paires à haute disponibilité. Même si vous devez sélectionner et mettre à niveau ces périphériques en tant qu'unité, l'assistant les affiche en tant que périphériques autonomes. L'état du périphérique et l'état de préparation aux mises à niveau sont évalués et signalés sur une base individuelle. Cela signifie qu'il est possible qu'une unité semble « passer » à l'étape suivante alors que l'autre ou les autres ne le font pas. Cependant, ces périphériques sont toujours regroupés. Exécuter une vérification de l'état de préparation sur l'un d'eux et l'appliquer à tous. Lancez la mise à niveau sur l'un d'eux, démarrez-la sur tous. Pour éviter d'éventuelles échecs chronophages de mise à niveau, *vérifiez* que tous les membres du groupe sont prêts à passer à l'étape suivante de l'assistant avant de cliquer sur **Next**(suivant).

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mettez à niveau davantage de périphériques FTD à la fois.	7.0.0	Tout (source) 6.7.0 (cible)	Le nombre de périphériques que vous pouvez mettre à niveau simultanément est désormais limité par la bande passante de votre réseau de gestion, et non par la capacité du système à gérer des mises à niveau simultanées. Auparavant, il était déconseillé de mettre à niveau plus de cinq périphériques à la fois. **Important** Seules les mises à niveau vers la version 6.7 ou ultérieure de Cisco FTD à l'aide l'assistant de mise à niveau constatent cette amélioration. Si vous mettez à niveau des périphériques vers une version antérieure de FTD, même si vous utilisez le nouvel assistant de mise à niveau, nous vous recommandons de vous limiter à cinq périphériques à la fois.
Procédez à la mise à niveau groupée de différents modèles de périphériques.	7.0.0	N'importe lequel	Vous pouvez désormais utiliser l'assistant de mise à niveau de Cisco FTD pour mettre en file d'attente et appeler des mises à niveau pour tous les modèles Cisco FTD en même temps, tant que le système a accès aux packages de mise à niveau appropriés. Auparavant, vous deviez choisir un forfait de mise à niveau, puis les périphériques à mettre à niveau à l'aide de ce forfait. Cela signifie que vous ne pouvez mettre à niveau plusieurs périphériques en même temps *que* s'ils partagent un ensemble de mise à niveau. Par exemple, vous pourriez mettre à niveau deux périphériques de la série Firepower 2100 en même temps, mais pas une série Firepower 2100 et une série 1000.
Les mises à niveau suppriment les fichiers PCAP pour économiser de l'espace disque.	6.7.0	6.7.0	Les mises à niveau suppriment désormais les fichiers PCAP stockés localement. Pour la mise à niveau, vous devez disposer de suffisamment d'espace disque libre, sinon la mise à niveau échoue.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Amélioration des rapports sur l'état de la mise à niveau de FTD et des options d'annulation et de nouvelle tentative.	6.7.0	6.7.0	Vous pouvez désormais afficher l'état des mises à niveau des périphériques FTD et des vérifications de l'état de préparation en cours sur la page de gestion des périphériques, ainsi qu'un historique de 7 jours des réussites et des échecs des mises à niveau. Le centre de messages fournit également des messages d'erreur et d'état améliorés. Une nouvelle fenêtre contextuelle d'état de mise à niveau, accessible en un seul clic à partir de la gestion des périphériques et du centre de messagerie, affiche des informations détaillées sur la mise à niveau, notamment le pourcentage/temps restant, l'étape spécifique de la mise à niveau, les données de réussite et d'échec, les journaux de mise à niveau, etc. Également dans cette fenêtre contextuelle, vous pouvez annuler manuellement les mises à niveau ayant échoué ou en cours (**Annuler la mise à niveau**), ou réessayer les mises à niveau qui ont échoué (**Réessayer la mise à niveau**). L'annulation d'une mise à niveau ramène le périphérique à l'état qu'il avait avant la mise à niveau. **Remarque** Pour pouvoir annuler manuellement ou réessayer une mise à niveau ayant échoué, vous devez désactiver la nouvelle option d'annulation automatique, qui apparaît lorsque vous utilisez la console FMC pour mettre à niveau un périphérique FTD : **Automatically cancel on upgrade failure and roll back to the previous version** (Annulation automatique en cas d'échec de la mise à jour et retour à la version précédente). Lorsque l'option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Écrans nouveaux ou modifiés : • **System (Système)** > **Update (Mise à niveau)** > **Product Updates (Mises à jour de produits)** > **Available Updates (Mises à jour disponibles)** > **icône Install (Installer)** pour le paquet de mise à niveau de Cisco FTD • **Périphériques** > **Gestion des périphériques** > **Mettre à niveau** • **Message Center (Centre de messages)** > **Tasks (Tâches)** Commandes CLI nouvelles ou modifiées : **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Obtenez les paquets de mise à niveau FTD à partir d'un serveur Web interne.	6.6.0	6.6.0	Les périphériques FTD peuvent désormais obtenir des paquets de mise à niveau à partir de votre propre serveur Web interne, plutôt que du FMC. Cela est particulièrement utile si la bande passante entre le FMC et ses périphériques est limitée. Cela permet également de gagner de la place sur le FMC. **Remarque** Cette fonctionnalité est prise en charge uniquement pour les périphériques FTD exécutant la version 6.6+. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.6, ni pour les périphériques FMC ou classique. Écrans nouveaux ou modifiés : nous avons ajouté une option – **Préciser la source des mises à jour logicielles** à la page où vous téléchargez les paquets de mise à niveau.
Copier les ensembles de mises à niveau sur les périphériques gérés avant la mise à niveau.	6.2.3	N'importe lequel	Vous pouvez maintenant copier (ou pousser) un paquet de mise à niveau de FMC vers un périphérique géré avant d'exécuter la mise à niveau elle-même. C'est utile, car vous pouvez pousser pendant les périodes de faible utilisation de la bande passante, en dehors de la fenêtre de maintenance de la mise à niveau. Lorsque vous poussez vers des périphériques à haute disponibilité, en grappe ou empilés, le système envoie d'abord l'ensemble de mise à niveau à l'ordinateur actif/contrôle/principal, puis à l'interface de secours/données/secondaire. Écrans nouveaux ou modifiés : **System (système)** > **Updates (mises à jour)**



CHAPITRE 2

Planification de votre mise à niveau

- Upgrade Planning Phases (Phases de planification de la mise à niveau), à la page 9
- Renseignements sur la version actuelle et le modèle, à la page 10
- Chemins de mise à niveau, à la page 11
- Mises à niveau qui ne répondent pas, à la page 31
- Tests de temps et d'espace disque, à la page 32
- Téléchargez les paquets de mise à niveau, à la page 34
- Charger des paquets de mise à niveau logicielle Firepower, à la page 38
- Vérification de l'état de préparation du logiciel Firepower, à la page 41

Upgrade Planning Phases (Phases de planification de la mise à niveau)

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs. Ce tableau résume le processus de planification des mises à niveau. Pour obtenir des listes de contrôle et des procédures détaillées, consultez les chapitres de mise à niveau

Remarque Avant la mise à niveau FXOS, si vous rencontrez la faute critique F1715 sur votre Firepower Chassis Manager ou dans la CLI FXOS avec le message `Adapter 1 on Security Module 1 requires a critical firmware upgrade` (L'adaptateur 1 sur le module de sécurité 1 nécessite une mise à niveau critique du microprogramme). Nous vous recommandons de mettre à niveau votre programme d'amorçage d'adaptateur, puis de poursuivre le processus de mise à niveau de FXOS. Pour des instructions détaillées de mise à niveau de l'adaptateur détaillé, consultez les notes de version de FXOS pour la version respective.

Tableau 8 : Phases de planification de la mise à niveau

Phase de planification	Y compris :
Planification et faisabilité	Évaluez votre déploiement. Planifiez votre chemin de mise à niveau. Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Vérifiez l'accès à l'appareil. Vérifiez la bande passante. Planifiez des périodes de maintenance.
Sauvegardes	Sauvegardez le logiciel. Sauvegardez FXOS sur le Firepower 4100/9300. Sauvegardez ASA pour ASA FirePOWER.
Progiciels de mise à niveau	Téléchargez les paquets de mise à niveau à partir de Cisco. Chargez les paquets de mise à niveau sur le système.
Mises à niveau associées	Mettez à niveau l'hébergement virtuel dans les déploiements virtuels. Mettez à niveau FXOS sur le Firepower 4100/9300. Mettez à niveau ASA pour ASA FirePOWER.
Contrôle final	Vérifiez les configurations. Vérifiez la synchronisation NTP. Vérifiez l'espace disque. Déployez des configurations. Exécutez la vérification de l'état de préparation. Vérifiez les tâches en cours. Vérifiez l'intégrité et les communications dans le déploiement.

Renseignements sur la version actuelle et le modèle

Utilisez ces commandes pour trouver la version actuelle et les renseignements sur le modèle pour votre déploiement,

Tableau 9 :

Composant	Renseignements
Cisco Firepower Management Center	Sur le FMC, choisissez **Aide** > **À propos**.

Composant	Renseignements
Périphériques gérés par Firepower	Dans le FMC, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
FXOS pour Firepower 4100/9300	Firepower Chassis Manager : choisissez **Aperçu**. Interface de ligne de commande de FXOS : pour la version, utilisez la commande **show version**. Pour le modèle, saisissez **scope chassis 1**, puis **show inventory**.
Système d'exploitation ASA pour Pare-feu ASA avec services FirePOWER	Sur l'interface de ligne de commande d'ASA, utilisez la commande **show version**.
Environnement d'hébergement virtuel	Consultez la documentation correspondant à votre environnement d'hébergement virtuel.

Chemins de mise à niveau

Votre chemin de mise à niveau est un plan détaillé de ce que vous allez mettre à niveau et quand, y compris les environnements d'hébergement virtuel et les systèmes d'exploitation des appareils. Vous devez en tout temps maintenir la compatibilité de votre matériel, de vos logiciels, de votre système d'exploitation et de votre hébergement.



Astuces Ce guide couvre le Firepower 7.0.x et les versions antérieures. Voir la section Ce guide est-il pour vous?, à la page 1.

Qu'est-ce que j'ai?

Avant de mettre à niveau un appareil Firepower, déterminez l'état actuel de votre déploiement. n plus des informations sur la version et le modèle actuels, déterminez si vos périphériques sont configurés pour la haute disponibilité/l'évolutivité et s'ils sont déployés en mode passif, comme IPS, comme pare-feu, etc.

Consultez Renseignements sur la version actuelle et le modèle, à la page 10.

Où vais-je?

Maintenant que vous savez ce que vous avez, assurez-vous de pouvoir aller là où vous le souhaitez :

- Votre déploiement peut-il exécuter la version cible du Firepower?
- Vos appareils requièrent-ils une mise à niveau du système d'exploitation distincte avant de pouvoir exécuter la version cible du Firepower ? Vos appareils peuvent-ils exécuter le système d'exploitation cible?
- Vos appliances virtuelles requièrent-elles une mise à niveau de l'environnement d'hébergement avant de pouvoir exécuter la version cible du Firepower ?

Pour obtenir des réponses à toutes ces questions, consultez l'une des ressources suivantes :

- Guide de compatibilité de Cisco Secure Firewall Management Center

- Guide de compatibilité de Cisco Secure Firewall Threat Defense
- Guide de compatibilité des appareils de Cisco Firepower Classic

Comment y arriver?

Après avoir confirmé que vos appareils peuvent exécuter la version cible, assurez-vous qu'une mise à niveau directe est possible :

- Une mise à niveau logicielle directe de Firepower est-elle possible?
- Une mise à niveau directe de FXOS est-elle possible pour le Firepower 4100/9300?
- Une mise à niveau directe de l'ASA est-elle possible, pour l'ASA avec les services FirePOWER?

Pour obtenir des réponses à toutes ces questions, consultez les chemins de mise à niveau fournis dans ce guide.

Astuces Les chemins de mise à niveau qui requièrent des versions intermédiaires peuvent prendre du temps. Surtout dans les déploiements Firepower de grande envergure où vous devez alterner les mises à niveau des FMC et des périphériques, pensez à recréer l'image des anciens périphériques au lieu de les mettre à niveau. Tout d'abord, retirez les périphériques du FMC. Ensuite, mettez à niveau le FMC, réinitialisez les périphériques et ajoutez-les au FMC.

Puis-je maintenir la compatibilité du déploiement?

Vous devez en tout temps maintenir la compatibilité de votre matériel, de vos logiciels et de votre système d'exploitation :

- Puis-je maintenir la compatibilité des versions du Firepower entre le FMC et ses périphériques gérés : Guide de compatibilité de Cisco Secure Firewall Management Center.
- Puis-je maintenir la compatibilité de FXOS avec les périphériques logiques pour le Firepower 4100/9300: Compatibilité FXOS de Cisco Firepower 4100/9300.
- Puis-je maintenir la compatibilité de l'ASA avec les modules ASA FirePOWER, pour l'ASA avec les services FirePOWER : Compatibilité de Cisco Secure Firewall ASA.

Chemins de mise à niveau : Cisco Firepower Management Center

Ce tableau fournit des chemins de mise à niveau pour le FMC, y compris le FMCv.

Recherchez votre version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version reprise dans la colonne de droite.

Remarque Si votre version actuelle est publiée après une date postérieure à celle de votre version cible, vous ne pourrez peut-être pas mettre à niveau comme prévu. Dans ces cas, la mise à niveau échoue rapidement et affiche une erreur expliquant qu'il existe des incompatibilités d'entrepôts de données entre les deux versions. Les notes de mise à jour de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Tableau 10 : Mises à niveau directes de FMC

Version actuelle	Version cible
7.0.0 7.0.x Dernière prise en charge de FMC 1000, 2500 et 4500	Une des versions suivantes : → de la version 7.1.0 à la version 7.4.x → toute version de maintenance 7.0.x ultérieure **Remarque** En raison d'incompatibilités avec le magasin de données, vous ne pouvez pas mettre à niveau de la version 7.0.4+ à la version 7.1.0. Nous vous recommandons de mettre à niveau directement vers la version 7.2+.
6.7.0 6.7.x	Une des versions suivantes : → de la version 7.0.0 à la version 7.2.x → toute version de maintenance 6.7.x ultérieure
6.6.0 6.6.x Dernière prise en charge de FMC 2000 et 4000.	Une des versions suivantes : → de la version 6.7.0 à la version 7.2.x → toute version de maintenance 6.6.x ultérieure **Remarque** En raison d'incompatibilités avec l'entrepôt de données, vous ne pouvez pas passer de la version 6.6.5 ou d'une version ultérieure à la version 6.7.0. Nous vous recommandons de mettre à niveau directement vers la version 7.0.0+.
6.5.0	De la version 6.6.0 à la version 7.1.x
6.4.0 Dernière prise en charge de FMC 750, 1500 et 3500.	Une des versions suivantes : → de la version 6.6.0 à la version 7.0.x → 6.5.0
6.3.0	Une des versions suivantes : → de la version 6.6.0 à la version 6.7.x → 6.5.0 → 6.4.0
6.2.3	Une des versions suivantes : → 6.6.x → 6.5.0 → 6.4.0 → 6.3.0

Version actuelle	Version cible
6.2.2	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3
6.2.1	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Une des versions suivantes : → 6.1.0
6.0.0	Une des versions suivantes : → 6.0.1 Requiert un paquet de préinstallation : notes de mise à jour du système Firepower version 6.0.1 – préinstallation.
5.4.1.1	Une des versions suivantes : → 6.0.0 Requiert un paquet de préinstallation : notes de mise à jour du système FireSIGHT version 6.0.0 – préinstallation.

Chemin de mise à niveau : Firepower 4100/9300 avec périphériques logiques FTD

Ce tableau présente les chemins de mise à niveau pour le Firepower 4100/9300 avec des périphériques logiques FTD, gérés par un Firepower Management Center.

Remarque Si vous mettez à niveau un châssis Firepower 9300 avec FTD *et* ASA fonctionnant sur des modules distincts, consultez Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x ou ASA 9.4(1)–9.16(x) avec FXOS 1.1.1–2.10.1.

Recherchez votre combinaison de version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau vers n'importe quelle combinaison de version reprise dans la colonne de droite. Il s'agit d'un processus en plusieurs étapes : d'abord la mise à niveau de FXOS, puis la mise à niveau des périphériques logiques.

Notez que ce tableau répertorie uniquement les combinaisons de versions spécialement qualifiées de Cisco. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez *brièvement* une combinaison prise en charge, mais non recommandée, dans laquelle FXOS est « en avance » sur les périphériques logiques. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez Compatibilité FXOS de Cisco Firepower 4100/9300.

Tableau 11 : Chemins de mise à niveau : Firepower 4100/9300 avec périphériques logiques FTD

Versions actuelles	Versions cibles
FXOS 2.9.1 avec FTD 6.7.0/6.7.x	→ FXOS 2.10.1 avec FTD 7.0.0/7.0.x
FXOS 2.8.1 avec FTD 6.6.0/6.6.x	Une des versions suivantes : → FXOS 2.10.1 avec FTD 7.0.0/7.0.x → FXOS 2.9.1 avec FTD 6.7.x
FXOS 2.7.1 avec FTD 6.5.0	Une des versions suivantes : → FXOS 2.10.1 avec FTD 7.0.0/7.0.x → FXOS 2.9.1 avec FTD 6.7.0/6.7.x → FXOS 2.8.1 avec FTD 6.6.0/6.6.x
FXOS 2.6.1 avec FTD 6.4.0	Une des versions suivantes : → FXOS 2.10.1 avec FTD 7.0.0/7.0.x → FXOS 2.9.1 avec FTD 6.7.0/6.7.x → FXOS 2.8.1 avec FTD 6.6.0/6.6.x → FXOS 2.7.1 avec FTD 6.5.0

Versions actuelles	Versions cibles
FXOS 2.4.1 avec FTD 6.3.0	Une des versions suivantes : → FXOS 2.9.1 avec FTD 6.7.0/6.7.x → FXOS 2.8.1 avec FTD 6.6.0/6.6.x → FXOS 2.7.1 avec FTD 6.5.0 → FXOS 2.6.1 avec FTD 6.4.0
FXOS 2.3.1 avec FTD 6.2.3	Une des versions suivantes : → FXOS 2.8.1 avec FTD 6.6.0/6.6.x → FXOS 2.7.1 avec FTD 6.5.0 → FXOS 2.6.1 avec FTD 6.4.0 → FXOS 2.4.1 avec FTD 6.3.0
FXOS 2.2.2 avec FTD 6.2.2	Une des versions suivantes : → FXOS 2.6.1 avec FTD 6.4.0 → FXOS 2.4.1 avec FTD 6.3.0 → FXOS 2.3.1 avec FTD 6.2.3
FXOS 2.2.2 avec FTD 6.2.0	Une des versions suivantes : → FXOS 2.6.1 avec FTD 6.4.0 → FXOS 2.4.1 avec FTD 6.3.0 → FXOS 2.3.1 avec FTD 6.2.3 → FXOS 2.2.2 avec FTD 6.2.2
FXOS 2.2.1 avec FTD 6.2.0	→ FXOS 2.2.2 avec FTD 6.2.0 (mise à niveau de FXOS *uniquement*) Une autre option consiste à effectuer une mise à niveau vers FXOS 2.2.2 avec FTD 6.2.2, qui est une combinaison recommandée. Toutefois, si vous prévoyez de faire évoluer votre déploiement, ne vous en préoccupez pas. Maintenant que vous utilisez FXOS 2.2.2, vous pouvez effectuer une mise à niveau complète vers FXOS 2.6.1 avec FTD 6.4.0.
FXOS 2.1.1 avec FTD 6.2.0	→ FXOS 2.2.1 avec FTD 6.2.0 (mise à niveau de FXOS *uniquement*)
FXOS 2.0.1 avec FTD 6.1.0	→ FXOS 2.1.1 avec FTD 6.2.0
FXOS 1.1.4 avec FTD 6.0.1	→ FXOS 2.0.1 avec FTD 6.1.0

Mise à niveau de FXOS avec des périphériques logiques FTD en grappes ou en paires à haute disponibilité

Dans les déploiements de Firepower Management Center, vous mettez à niveau des périphériques logiques FTD en grappe et à haute disponibilité en tant qu'unité. Cependant, vous mettez à niveau FXOS sur chaque châssis indépendamment.

Tableau 12 : Commande de mise à niveau FXOS + FTD

Déploiement	Commande de mise à niveau
Périphérique autonome Grappe, unités sur le même châssis (Firepower 9300 uniquement)	**1.** Mettez à niveau FXOS. **2.** Mettre à niveau FTD.
Haute disponibilité	Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. **1.** Mettez à niveau FXOS sur l'unité de secours. **2.** Changez de rôle. **3.** Mettez à niveau FXOS sur le nouveau périphérique de secours. **4.** Mettre à niveau FTD.
Grappe, unités sur différents châssis (version 6.2 ou version ultérieure)	Pour réduire au minimum les perturbations, mettez toujours à niveau un châssis d'unités de données. Par exemple, pour une grappe à deux châssis : **1.** Mettez à niveau FXOS sur le châssis de l'unité de données. **2.** Basculez le module de contrôle sur le châssis que vous venez de mettre à niveau. **3.** Mettez à niveau FXOS sur le nouveau châssis d'unités de données. **4.** Mettre à niveau FTD.

Avec les anciennes versions, les mises à niveau transparente ont des exigences supplémentaires.

Tableau 13 : Mises à niveau transparente dans les versions antérieures

Scénario	Détails
Mise à niveau de périphériques à haute disponibilité ou en grappe et vous utilisez actuellement l'un des éléments suivants : • FXOS de la version 1.1.4.x à la version 2.2.1.x • FXOS de la version 2.2.2.17 à la version 2.2.2.68 • FXOS de la version 2.3.1.73 à la version 2.3.1.111 Avec : • FTD de la version 6.0.1 à la version 6.2.2.x	En raison de corrections de bogues dans la fonction de déchargement de flux, certaines combinaisons de FXOS et FTD ne prennent pas en charge le déchargement de flux; consultez le Guide de compatibilité de Cisco Firepower. Pour effectuer une mise à niveau transparente, vous devez toujours exécuter une combinaison compatible. Si votre chemin de mise à niveau comprend la mise à niveau de FXOS vers la version 2.2.2.91, 2.3.1.130 ou une version ultérieure (y compris FXOS 2.4.1.x, 2.6.1.x, etc.), utilisez ce chemin : 1. Mettre à niveau FTD vers la version 6.2.2.2 ou une version ultérieure. 2. Mettez à niveau FXOS vers la version 2.2.2.91, 2.3.1.130 ou une version ultérieure. 3. Mettez à niveau FTD vers votre version finale. Par exemple, si vous utilisez FXOS 2.2.2.17 avec FTD 6.2.2.0 et que vous souhaitez effectuer une mise à niveau vers FXOS 2.6.1 avec FTD 6.4.0, vous pouvez : 1. Mettre à niveau FTD vers la version 6.2.2.5. 2. Mettre à niveau FXOS vers la version 2.6.1. 3. Mettre à niveau FTD vers la version 6.4.0.
Mise à niveau de périphériques à haute disponibilité vers la version 6.1.0 de FTD	Requiert un paquet de préinstallation. Pour en savoir plus, consultez les notes de mise à jour du système Firepower version 6.1.0 – préinstallation.

Remarque sur les rétrogradations

La rétrogradation des images FXOS n'est pas officiellement prise en charge. La seule méthode prise en charge par Cisco pour rétrograder une version d'image FXOS consiste à effectuer une recréation d'image complète de l'appareil.

Chemin de mise à niveau : autres appareils Cisco Firepower Threat Defense

Ce tableau fournit des chemins de mise à niveau pour les périphériques FTD gérés par un FMC, où vous n'avez pas à mettre à jour le système d'exploitation : Firepower 1000/2100, ASA 5500-X, ISA 3000 et Firepower Threat Defense Virtual.

Recherchez votre version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version reprise dans la colonne de droite.

Tableau 14 : Chemins de mise à niveau : Firepower 1000/2100, ASA 5500-X, ISA 3000 et Firepower Threat Defense Virtual avec FMC

Version actuelle	Version cible
7.0.0 7.0.x Dernière prise en charge de FTD pour ASA 5508-X et 5516-X.	→ toute version de maintenance 7.0.x ultérieure
6.7.0 6.7.x	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → toute version de maintenance 6.7.x ultérieure
6.6.0 6.6.x Dernière prise en charge de FTD pour les ASA 5525-X, 5545-X et 5555-X.	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → toute version de maintenance 6.6.x ultérieure
6.5.0	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x
6.4.0 Dernière prise en charge de FTD pour ASA 5515-X.	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0
6.3.0	Une des versions suivantes : → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0
6.2.3 Dernière prise en charge de FTD pour la série ASA 5506-X.	Une des versions suivantes : → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0 → 6.3.0

Version actuelle	Version cible
6.2.2	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Série Firepower 2100 uniquement.	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	→ 6.1.0

Chemins de mise à niveau : Firepower de série 7000/8000

Ce tableau fournit les chemins de mise à niveau pour les périphériques Firepower de la série 7000/8000, gérés par un FMC.

Recherchez votre version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version reprise dans la colonne de droite.

Tableau 15 : Chemins de mise à niveau : Firepower de série 7000/8000 avec FMC

Version actuelle	Version cible
6.4.0	Aucun. La version 6.4.0 est la dernière version majeure pour les périphériques Firepower de la série 7000/8000.

Version actuelle	Version cible
6.3.0	Une des versions suivantes : → 6.4.0
6.2.3	Une des versions suivantes : → 6.4.0 → 6.3.0
6.2.2	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Aucune prise en charge sur cette plateforme.	—
6.2.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Une des versions suivantes : → 6.1.0
6.0.0	Une des versions suivantes : → 6.0.1
5.4.0.2	Une des versions suivantes : → 6.0.0 Requiert un paquet de préinstallation : notes de mise à jour du système FireSIGHT version 6.0.0 – préinstallation.

Chemin de mise à niveau : ASA FirePOWER

Ce tableau fournit les chemins de mise à niveau pour les Module ASA FirePOWER, gérés par un FMC.

Recherchez votre version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version reprise dans la colonne de droite.

Si vous le souhaitez, vous pouvez également mettre à niveau l'ASA. Il existe une large compatibilité entre les versions d'ASA et de ASA FirePOWER. Cependant, la mise à niveau vous permet de profiter de nouvelles fonctionnalités et de la résolution de certains problèmes. Pour les chemins de mise à niveau ASA, consultez Chemin de mise à niveau : ASA pour ASA FirePOWER, à la page 25.

Tableau 16 : Chemins de mise à niveau : ASA FirePOWER avec FMC

Version actuelle	Version cible
7.0.0 7.0.x Dernière prise en charge d'ASA FirePOWER sur n'importe quelle plateforme.	→ toute version de maintenance 7.0.x ultérieure
6.7.0 6.7.x	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → toute version de maintenance 6.7.x ultérieure
6.6.0 6.6.x Dernière prise en charge d'ASA FirePOWER pour les ASA 5525-X, 5545-X et 5555-X.	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → toute version de maintenance 6.6.x ultérieure
6.5.0	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x
6.4.0 Dernière prise en charge d'ASA FirePOWER pour la série ASA 5585-X et l'ASA 5515-X.	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0

Version actuelle	Version cible
6.3.0	Une des versions suivantes : → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0
6.2.3 Dernière prise en charge d'ASA FirePOWER pour la série ASA 5506-X et l'ASA 5512-X.	Une des versions suivantes : → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 Aucune prise en charge sur cette plateforme.	—
6.2.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Une des versions suivantes : → 6.1.0
6.0.0	Une des versions suivantes : → 6.0.1

Version actuelle	Version cible
5.4.0.2 ou 5.4.1.1	Une des versions suivantes : → 6.0.0 Requiert un paquet de préinstallation : notes de mise à jour du système FireSIGHT version 6.0.0 – préinstallation.

Mise à niveau d'ASA

Il existe une large compatibilité entre les versions d'ASA et de ASA FirePOWER. Cependant, la mise à niveau vous permet de profiter de nouvelles fonctionnalités et de la résolution de certains problèmes. Pour en savoir plus sur la compatibilité, consultez Compatibilité de Cisco Secure Firewall ASA.

Vous mettez à niveau l'ASA sur chaque périphérique indépendamment, même si vous avez configuré des paires de mise en grappe ou de basculements ASA. Le moment exact où vous mettez à niveau le module ASA FirePOWER (avant ou après le rechargement de l'ASA) dépend de votre déploiement. Ce tableau décrit l'ordre de mise à niveau d'ASA pour les déploiements autonomes et à haute disponibilité/évolutivité. Pour plus de renseignements sur les instructions, consultez Mettre à niveau l'ASA, à la page 95.

Tableau 17 : Commande de mise à niveau ASA + ASA FirePOWER

Déploiement d'ASA	Commande de mise à niveau
Périphérique autonome	**1.** Mettez à niveau l'ASA, y compris le rechargement. **2.** Mettez à niveau ASA FirePOWER.
Basculement de l'ASA : actif/de secours	Mettez toujours à niveau l'unité de secours. **1.** Mettez à niveau l'ASA sur l'unité de secours, mais ne rechargez pas l'unité. **2.** Mettez à niveau ASA FirePOWER sur l'unité de secours. **3.** Rechargez l'ASA sur l'unité de secours. **4.** Effectuez le basculement. **5.** Mettez à niveau l'ASA sur le nouveau périphérique de secours. **6.** Mettez à niveau ASA FirePOWER sur le nouveau périphérique de secours. **7.** Rechargez l'ASA sur la nouvelle unité de secours.

Déploiement d'ASA	Commande de mise à niveau
Basculement de l'ASA : actif/actif	Activez les deux groupes de basculement sur l'unité que vous ne mettez pas à niveau. **1.** Activez les deux groupes de basculement sur l'unité principale. **2.** Mettez à niveau l'ASA sur l'unité secondaire, mais ne rechargez pas l'unité. **3.** Mettez à niveau ASA FirePOWER sur l'unité secondaire. **4.** Rechargez l'ASA sur l'unité secondaire. **5.** Activez les deux groupes de basculement sur l'unité secondaire. **6.** Mettez à niveau l'ASA sur l'unité principale, mais ne rechargez pas l'unité. **7.** Mettez à niveau ASA FirePOWER sur l'unité principale. **8.** Rechargez ASA sur l'unité principale.
Grappe ASA	Désactivez la mise en grappe sur chaque unité avant d'effectuer la mise à niveau. Mettez à niveau une unité à la fois, en laissant l'unité de contrôle pour la fin. **1.** Sur une unité de données, désactivez la mise en grappe. **2.** Mettez à niveau l'ASA sur cette unité de données, mais ne rechargez pas l'unité. **3.** Mettez à niveau ASA FirePOWER sur l'unité. **4.** Rechargez l'ASA. **5.** Réactivez la mise en grappe. Attendez que l'unité rejoigne la grappe. **6.** Répétez l'opération pour chaque unité de données. **7.** Sur une unité de contrôle, désactivez la mise en grappe. Attendez qu'un nouveau contrôle prenne le relais. **8.** Mettez à niveau l'ASA sur l'ancienne unité de contrôle, mais ne rechargez pas l'unité. **9.** Mettez à niveau ASA FirePOWER sur l'ancienne unité de contrôle. **10.** Réactivez la mise en grappe.

Chemin de mise à niveau : ASA pour ASA FirePOWER

Ce tableau fournit des chemins de mise à niveau pour l'ASA sur l'ASA avec les services FirePOWER. Il existe une large compatibilité entre les versions d'ASA et de ASA FirePOWER. Cependant, la mise à niveau vous permet de profiter de nouvelles fonctionnalités et de la résolution de certains problèmes.

Recherchez votre version actuelle d'ASA dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers les versions cibles énumérées. Les versions recommandées sont en **gras**.

Tableau 18 : Chemins de mise à niveau : ASA pour ASA FirePOWER

Version actuelle	Version cible
9.15(x) Dernière prise en charge d'ASA FirePOWER sur n'importe quelle plateforme, avec la version 7.0.x du Firepower.	→ **9.16(x)**
9.14(x) Dernière prise en charge d'ASA FirePOWER pour l'ASA 5525-X, l'ASA 5545-X et l'ASA 5555-X, avec la version 6.6.x du Firepower.	Une des versions suivantes : → **9.16(x)** → **9.15(x)**
9.13(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)**
9.12(x) Dernière prise en charge d'ASA FirePOWER pour l'ASA 5515-X et l'ASA 5585-X, avec la version 6.4.0 du Firepower.	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)**
9.10(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x)

Version actuelle	Version cible
9.9(x) Dernière prise en charge d'ASA FirePOWER pour la série ASA 5506-X et l'ASA 5512-X, avec la version 6.2.3 du Firepower.	Une des versions suivantes : → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x)
9.8(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

Version actuelle	Version cible
9.6(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Version actuelle	Version cible
9.3(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	Une des versions suivantes : → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

Chemin de mise à niveau : NGIPSv

Ce tableau fournit les chemins de mise à niveau pour le NGIPSv, géré par un FMC.

Recherchez votre version actuelle dans la colonne de gauche. Vous pouvez effectuer une mise à niveau directement vers n'importe quelle version reprise dans la colonne de droite.

Tableau 19 : Chemins de mise à niveau : NGIPSv avec FMC

Version actuelle	Version cible
7.0.0 7.0.x Dernière prise en charge de NGIPSv.	→ toute version de maintenance 7.0.x ultérieure

Version actuelle	Version cible
6.7.0 6.7.x	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → toute version de maintenance 6.7.x ultérieure
6.6.0 6.6.x	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → toute version de maintenance 6.6.x ultérieure
6.5.0	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x
6.4.0	Une des versions suivantes : → version 7.0.0 ou toute version de maintenance 7.0.x → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0
6.3.0	Une des versions suivantes : → version 6.7.0 ou toute version de maintenance 6.7.x → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0
6.2.3	Une des versions suivantes : → version 6.6.0 ou toute version de maintenance 6.6.x → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Une des versions suivantes : → 6.4.0 → 6.3.0
6.2.1 Aucune prise en charge sur cette plateforme.	—

Version actuelle	Version cible
6.2.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Une des versions suivantes : → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Une des versions suivantes : → 6.1.0
6.0.0	Une des versions suivantes : → 6.0.1
5.4.1.1	Une des versions suivantes : → 6.0.0 Requiert un paquet de préinstallation : notes de mise à jour du système FireSIGHT version 6.0.0 – préinstallation.

Mises à niveau qui ne répondent pas

Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image..

Mise à niveau de périphérique classique ou FMC ne répondant pas

Ne pas redémarrer une mise à niveau en cours. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez le Centre d'assistance technique Cisco (TAC)

Mise à niveau FTD sans réponse

Pour les mises à niveau majeures et de maintenance, vous pouvez annuler manuellement les mises à niveau en cours ou ayant échoué, et réessayer les mises à niveau qui ont échoué. Dans FMC, utilisez la fenêtre contextuelle Upgrade Status (état de la mise à niveau), accessible à partir de l'onglet Mise à niveau sur la page de gestion des périphériques et à partir du centre de messages. Vous pouvez également utiliser la CLI FTD.

Remarque Par défaut, FTD revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« auto-cancel ») (Annulation automatique). Pour pouvoir annuler manuellement ou réessayer une mise à niveau qui a échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.

Cette fonctionnalité n'est pas prise en charge pour les correctifs ou pour les mises à niveau à partir de la version 6.6 et des versions antérieures.

Tests de temps et d'espace disque

À titre de référence, nous fournissons des rapports sur les tests de temps et d'espace disque réalisés en interne pour les mises à niveau logicielles de FMC et de périphériques. Pour les rapports réels, consultez les notes de mise à jour de votre version cible.

Tests de temps

Nous signalons la durée de test *la plus lente* de toutes les mises à niveau logicielles testées sur une plateforme ou une série particulière. Votre mise à niveau prendra probablement plus de temps que les délais fournis pour plusieurs raisons, comme l'explique le tableau suivant. Nous vous recommandons de suivre et d'enregistrer vos propres délais de mise à niveau afin de pouvoir les utiliser comme références futures.

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas, à la page 31.

Tableau 20 : Conditions de test de temps pour les mises à niveau logicielles

Condition	Détails
Déploiement	Les délais de mise à niveau des périphériques sont basés sur des tests réalisés dans des déploiements FMC. Les délais de mise à niveau bruts pour les périphériques gérés à distance et localement sont similaires, compte tenu de conditions similaires.
Versions	Pour les versions majeures et de maintenance, nous testons les mises à niveau à partir de toutes les versions majeures précédentes admissibles. Pour les correctifs, nous testons les mises à niveau à partir de la version de base. Le délai de mise à niveau augmente généralement si votre mise à niveau ignore des versions.
Modèles	Dans la plupart des cas, nous effectuons les tests sur les modèles les plus bas de gamme de chaque série, et parfois sur plusieurs modèles d'une même série.

Condition	Détails
Appliances virtuelles	Nous testons avec les paramètres par défaut pour la mémoire et les ressources. Cependant, notez que le temps de mise à niveau dans les déploiements virtuels dépend fortement du matériel.
Disponibilité élevée/évolutivité	Sauf indication contraire, nous testons sur des périphériques autonomes. Dans une configuration à haute disponibilité ou en grappe, les périphériques sont mis à niveau un par un afin de préserver la continuité des opérations, chaque périphérique fonctionnant en mode maintenance pendant sa mise à niveau. Par conséquent, la mise à niveau d'une paire de périphériques ou d'une grappe complète prend plus de temps que la mise à niveau d'un périphérique autonome.
Configurations	Nous testons sur des appareils avec une configuration et une charge de trafic minimales. Le délai de mise à niveau peut augmenter en fonction de la complexité de vos configurations, de la taille des bases de données d'événements et de l'incidence de la mise à niveau sur ces éléments. Par exemple, si vous utilisez de nombreuses règles de contrôle d'accès et que la mise à niveau doit apporter des modifications générales à la façon dont ces règles sont stockées, la mise à niveau peut prendre plus de temps.
Composants	Nous signalons *uniquement* les durées nécessaires à la mise à niveau du logiciel et au redémarrage ultérieur. Cela n'inclut pas le temps pour les mises à niveau des systèmes d'exploitation, le transfert des paquets de mise à niveau, les vérifications de la préparation, les mises à jour de la VDB et des règles de prévention des intrusions (SRU/LSP), ni le déploiement des configurations.

Tests d'espace disque

Nous signalons l'espace disque *le plus* utilisé de toutes les mises à niveau logicielles testées sur une plateforme ou une série particulière. Cela inclut l'espace nécessaire pour copier le paquet de mise à niveau sur le périphérique.

Nous signalons également l'espace nécessaire sur le FMC (dans / Volume ou /var) pour le paquet de mise à niveau de périphérique. Si vous avez un serveur interne pour les paquets de mise à niveau FTD ou si vous utilisez FDM, ignorez ces valeurs.

Lorsque nous signalons des estimations d'espace disque pour un emplacement particulier (par exemple, /var ou /ngfw), nous signalons l'estimation d'espace disque pour la partition montée à cet emplacement. Sur certaines plateformes, ces emplacements peuvent se trouver sur la même partition.

Sans suffisamment d'espace disque libre, la mise à niveau échoue.

Tableau 21 : Vérification de l'espace disque

Plateforme	Commande
FMC	Choisissez **System (Système)** > **Monitoring (Surveillance)** > **Statistics (Statistiques)** et sélectionnez le FMC. Sous Disk Usage (Utilisation du disque), développez les informations de By partition (Par partition).

Plateforme	Commande
FTD avec FMC	Choisissez **System (Système)** > **Monitoring (Surveillance)** > **Statistics (Statistiques)** et sélectionnez le périphérique que vous souhaitez vérifier. Sous Disk Usage (Utilisation du disque), développez les informations de By partition (Par partition).

Téléchargez les paquets de mise à niveau

Téléchargez les paquets de mise à niveau à partir de Site d'assistance et de téléchargement Cisco avant de commencer la mise à niveau. Selon la mise à niveau, vous devez placer les paquets sur votre ordinateur local ou sur un serveur auquel le périphérique peut accéder. Les listes de contrôle et les procédures de ce guide expliquent vos choix.



Remarque Les téléchargements nécessitent un identifiant et un contrat de service Cisco.com.

Paquets logiciels Firepower

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco.

- Cisco Firepower Management Center, y compris Cisco Firepower Management Center Virtual : https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (ISA 3000) : https://www.cisco.com/go/isa3000-software
- Firepower Threat Defense (tous les autres modèles, y compris Cisco Firepower Threat Defense) : https://www.cisco.com/go/ftd-software
- Série FirePOWER 7000 : https://www.cisco.com/go/7000series-software
- Série FirePOWER 8000 : https://www.cisco.com/go/8000series-software
- ASA avec services FirePOWER (série ASA 5500-X) : https://www.cisco.com/go/asa-firepower-sw
- ASA avec services FirePOWER (série ISA 3000 : https://www.cisco.com/go/isa3000-software
- NGIPSv : https://www.cisco.com/go/ngipsv-software

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez le modèle de votre appareil, puis accédez à la page de téléchargement logiciel correspondant à votre version actuelle. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables.

Astuces Un Cisco Firepower Management Center avec accès à Internet peut télécharger certains correctifs et versions de maintenance directement à partir de Cisco, quelque temps après qu'ils soient disponibles pour le téléchargement manuel. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs.

Vous utilisez le même ensemble de mises à niveau pour tous les modèles d'une famille ou d'une série. Les noms des fichiers des paquets de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif rapide) et la version du logiciel. Les versions de maintenance utilisent le type de paquet « mise à niveau ».

Par exemple :

- Paquet : `Cisco_Firepower_Mgmt_Center_Upgrade--999.sh.REL.tar`
- Platforme : Firepower Management Center
- Type de paquet : mise à niveau
- Version et build : -999
- Extensions de fichier : sh.REL.tar

Afin que le système vérifie que vous utilisez les bons fichiers, les paquets de mise à niveau Version 6.2.1+ sont des archives tar *signées* (.tar). Ne décompressez pas les paquets signés (.tar). Et n'envoyez pas les paquets de mise à niveau par courriel.

Remarque Une fois que vous avez chargé un paquet de mise à niveau signé, l'interface graphique Cisco Firepower Management Center peut prendre plusieurs minutes pour se charger, pendant que le système vérifie le paquet. Supprimez les paquets signés une fois que vous n'en avez plus besoin pour accélérer l'affichage.

Paquets de mise à niveau du logiciel Firepower

Tableau 22 :

Plateforme	Versions	Ensemble
FMC/FMCv	6.3.0 et les versions ultérieures	Cisco_Firepower_Mgmt_Center
	De 5.4.0 à 6.2.3	Sourcefire_3D_Defense_Center_S3
Série Firepower 1000	N'importe lequel	Cisco_FTD_SSP-FP1K
Série Firepower 2100	N'importe lequel	Cisco_FTD_SSP-FP2K

Plateforme	Versions	Ensemble
Firepower 4100/9300	N'importe lequel	Cisco_FTD_SSP
Gamme ASA 5500-X avec FTD ISA 3000 avec FTD FTDv	N'importe lequel	Cisco_FTD
Série Firepower 7000/8000 Modèles AMP	De 6.3.0 à 6.4.0	Cisco_Firepower_NGIPS_Appliance
	De 5.4.0 à 6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	N'importe lequel	Cisco_Network_Sensor
NGIPSv	6.3.0 et les versions ultérieures	Cisco_Firepower_NGIPS_Virtual
	6.2.2 à 6.2.3	Sourcefire_3D_Device_VMware
	De 5.4.0 à 6.2.0	Sourcefire_3D_Device_Virtual64_VMware

Prologiciels FXOS

Les paquets FXOS pour les périphériques Firepower 4100/9300 sont disponibles sur le Site d'assistance et de téléchargement Cisco.

- Firepower 4100 : http://www.cisco.com/go/firepower4100-software
- Firepower 9300 : http://www.cisco.com/go/firepower9300-software

Pour trouver des progiciels FXOS, sélectionnez ou recherchez votre modèle d'appareil Firepower, puis accédez à la page de téléchargement de Firepower Extensible Operating System pour obtenir la version cible.

Remarque Si vous prévoyez d'utiliser l'interface de ligne de commande pour mettre à niveau FXOS, copiez le paquet de mise à niveau sur un serveur auquel Firepower 4100/9300 peut accéder en utilisant le protocole SCP, SFTP, TFTP ou FTP.

Tableau 23 : Paquets FXOS pour Firepower 4100/9300

Type de package	Ensemble
Image FXOS	fxos-k9.*version*.**SPA**

Type de package	Ensemble
Récupération (démarrage)	fxos-k9-**kickstart**.*version***.SPA**
Récupération (gestionnaire)	fxos-k9-**manager**.*version***.SPA**
Récupération (système)	fxos-k9-**system**.*version***.SPA**
Bases d'informations de gestion (MIB)	fxos-**mibs**-fp9k-fp4k.*version***.zip**
Micrologiciel : Firepower 4100	fxos-k9-fpr4k-**firmware**.*version***.SPA**
Micrologiciel : Firepower 9300	fxos-k9-fpr9k-**firmware**.*version***.SPA**

Paquets ASA

Le logiciel ASA est disponible sur le Site d'assistance et de téléchargement Cisco.

- ASA avec services FirePOWER (série ASA 5500-X) : https://www.cisco.com/go/asa-firepower-sw
- ASA avec services FirePOWER (série ISA 3000 : https://www.cisco.com/go/isa3000-software

Pour trouver un logiciel ASA, sélectionnez ou recherchez le modèle de votre appliance Firepower, puis accédez à la page de téléchargement appropriée et sélectionnez une version.

Remarque Si vous utilisez l'assistant de mise à niveau ASDM, vous n'avez pas besoin de prétélécharger le logiciel. Sinon, téléchargez sur votre ordinateur local. Pour les mises à niveau CLI, vous devez ensuite copier le logiciel sur un serveur auquel le périphérique peut accéder par l'intermédiaire de tout protocole pris en charge par la commande ASA **copy**, y compris HTTP, FTP et SCP.

Tableau 24 : Logiciel pour ASA

Télécharger la page	Type de logiciel	Ensemble
Logiciel pour dispositifs de sécurité adaptatifs (ASA)	Mise à niveau ASA et ASDM	asa*version*-**lfbff-k8.SPA** pour les ASA 5506-X, ASA 5508-X, ASA 5516-X et ISA 3000.
		asa*version*-**smp-k8.bin** pour les ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X et ASA 5585-X.
Gestionnaire d'appareils de sécurité adaptables (ASA)	Mise à niveau ASDM seulement	asdm-*version***.bin**
Module d'extension API REST d'appareils de sécurité adaptables	API REST ASA	asa-restapi-*version*-**lfbff-k8.SPA**

Charger des paquets de mise à niveau logicielle Firepower

Pour mettre à niveau le logiciel Firepower, le paquet de mise à niveau doit se trouver sur le périphérique.

Charger vers Cisco Firepower Management Center

Utilisez cette procédure pour charger manuellement les paquets de mise à niveau logicielle Firepower sur le Cisco Firepower Management Center, pour lui-même et les périphériques qu'il gère.

Avant de commencer

Si vous mettez à niveau le périphérique de secours Cisco Firepower Management Center dans une paire à haute disponibilité, suspendez la synchronisation.

Pour des déploiements FMC à haute disponibilité, vous devez charger le paquet de mise à niveau FMC sur les deux homologues, en suspendant la synchronisation avant de transférer le paquet sur le paquet de secours. Pour limiter les interruptions de la synchronisation à haute disponibilité, vous pouvez transférer le paquet vers l'homologue actif pendant l'étape de préparation de la mise à niveau, et vers l'homologue de secours dans le cadre du processus de mise à niveau lui-même, après avoir suspendu la synchronisation.

Procédure

Étape 1 Sur l'interface Web Cisco Firepower Management Center, choisissez **Système** > **Mises à jour**.

Étape 2 Cliquez sur **Charger la mise à jour**.

Astuces
Sélectionnez les paquets de mise à niveau disponibles pour le téléchargement direct par le Cisco Firepower Management Center quelque temps après que la version puisse être téléchargée manuellement. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. Si votre Cisco Firepower Management Center dispose d'un accès à Internet, vous pouvez plutôt cliquer sur **Télécharger les mises à jour** pour télécharger *tous* les paquets admissibles pour votre déploiement, ainsi que la dernière VDB, si nécessaire.

Étape 3 (version 6.6.0 ou version ultérieure) Pour l'**Action**, cliquez sur le bouton radio **Charger le paquet de mise à jour du logiciel local**.

Étape 4 Cliquez sur **Choisir le fichier**.

Étape 5 Accédez au paquet et cliquez sur **Charger**.

Charger du contenu vers un serveur interne (version 6.6.0 ou version ultérieure de FTD avec FMC)

À partir de la version 6.6.0, les périphériques Firepower Threat Defense peuvent obtenir des paquets de mise à niveau à partir d'un serveur Web interne, plutôt que du FMC. Cela est particulièrement utile si la bande passante entre le FMC et ses périphériques est limitée. Cela permet également de gagner de la place sur le FMC.

Remarque Cette fonctionnalité est prise en charge uniquement pour les périphériques FTD exécutant la version 6.6.0+. Elle n'est pas prise en charge pour les mises à niveau *vers* la version 6.6.0, ni pour les périphériques FMC ou classique.

Pour configurer cette fonctionnalité, vous enregistrez un pointeur (URL) à l'emplacement d'un paquet de mise à niveau sur le serveur Web. Le processus de mise à niveau obtiendra ensuite le paquet de mise à niveau du serveur Web au lieu du FMC. Vous pouvez également utiliser FMC pour copier le paquet avant d'effectuer la mise à niveau.

Répétez cette procédure pour chaque paquet de mise à niveau FTD. Vous ne pouvez configurer qu'un seul emplacement par paquet de mise à niveau.

Avant de commencer

- Téléchargez les paquets de mise à niveau appropriés à partir de Site d'assistance et de téléchargement Cisco et copiez-les sur un serveur Web interne auquel vos périphériques FTD peuvent accéder.
- Pour les serveurs Web sécurisés (HTTPS), procurez-vous le certificat numérique du serveur (format PEM). Vous devriez pouvoir obtenir le certificat de l'administrateur du serveur. Vous pouvez également utiliser votre navigateur ou un outil comme OpenSSL, pour afficher les détails du certificat du serveur et exporter ou copier le certificat.

Procédure

Étape 1 Sur l'interface Web de FMC, choisissez **Système** > **Mises à jour**.

Étape 2 Cliquez sur **Charger la mise à jour**.

Choisissez cette option même si vous ne chargez rien. La page suivante vous demandera de fournir une URL.

Étape 3 Pour l'**action**, cliquez sur le bouton radio **Préciser la source des mises à jour logicielles**.

Étape 4 Saisissez une **URL source** pour le paquet de mise à niveau.

Fournissez le protocole (HTTP/HTTPS) et le chemin complet. Par exemple :

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif rapide) ainsi que la version du Firepower à laquelle vous passez. Assurez-vous de saisir le bon nom de fichier.

Étape 5 Pour les serveurs HTTPS, fournissez un **certificat d'autorité de certification**.

Il s'agit du certificat numérique du serveur que vous avez obtenu plus tôt. Copiez et collez le bloc de texte entier, y compris les lignes BEGIN CERTIFICATE et END CERTIFICATE.

Étape 6 Cliquez sur **Save** (enregistrer).

Vous êtes renvoyé à la page Mises à jour de produits. Les paquets de mise à niveau chargés et les URL des paquets de mise à niveau sont listés ensemble, mais étiquetés distinctement.

Copier des données sur les périphériques gérés

Pour mettre à niveau le logiciel Firepower, le paquet de mise à niveau doit se trouver sur le périphérique. Dans la mesure du possible, nous vous recommandons d'utiliser cette procédure pour copier (*pousser*) les paquets sur les périphériques gérés avant de lancer la mise à niveau de ces derniers.

Remarque Pour les périphériques Firepower 4100/9300, nous vous recommandons (et parfois demandons) de copier le paquet de mise à niveau Cisco Firepower Threat Defense avant de commencer la mise à niveau FXOS associée requise.

La prise en charge varie selon la version du Firepower :

- La version 6.2.2 et les versions antérieures ne prennent pas en charge la copie préalable à la mise à niveau.

  Lorsque vous démarrez une mise à niveau de périphérique, le système copie le paquet de mise à niveau de Cisco Firepower Management Center sur le périphérique en tant que première tâche.

- La version 6.2.3 ajoute la possibilité de copier manuellement les paquets de mise à niveau sur le périphérique à partir de Cisco Firepower Management Center.

  Cette action réduit la durée de la période de maintenance de votre mise à niveau.

- La version 6.6.0 ajoute la possibilité de copier manuellement les paquets de mise à niveau d'un serveur Web interne sur les périphériques Cisco Firepower Threat Defense.

  Cela est utile si la bande passante entre le Cisco Firepower Management Center et ses périphériques Cisco Firepower Threat Defense est limitée. Cela permet également de gagner de la place sur le Cisco Firepower Management Center.

- La version 7.0.0 présente un nouveau flux de travail de mise à niveau Cisco Firepower Threat Defense qui vous invite à copier le paquet de mise à niveau sur les périphériques Cisco Firepower Threat Defense.

  Si votre Cisco Firepower Management Center exécute la version 7.0.0 ou une version ultérieure, nous vous recommandons d'utiliser la page de mise à niveau de périphérique pour copier le paquet de mise à niveau sur les périphériques FTD ; voir Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 77. Vous devez toujours utiliser cette procédure pour copier les paquets de mise à niveau dans les anciens déploiements et sur les périphériques classiques (Firepower 7000/8000, ASA FirePOWER et NGIPSv).

Notez que lorsque vous copiez manuellement, chaque périphérique obtient le paquet de mise à niveau de la source : le système ne copie pas les paquets de mise à niveau entre les unités membres de la grappe, de la pile ou de la haute disponibilité.

Avant de commencer

Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).

Procédure

Étape 1 Sur l'interface Web Cisco Firepower Management Center, choisissez **Système** > **Mises à jour**.

Étape 2 Placez le paquet de mise à niveau où le périphérique peut y accéder.

- Cisco Firepower Management Center : chargez manuellement ou récupérez directement le paquet sur le FMC.
- Serveur Web interne (Cisco Firepower Threat Defense version 6.6.0 ou version ultérieure) : chargez-le sur un serveur Web interne et configurez les périphériques Cisco Firepower Threat Defense pour obtenir le paquet de ce serveur.

Étape 3 Cliquez sur l'icône **Push** (Pousser) (version 6.5.0 ou version antérieure) ou **Push or Stage update** (Pousser la mise à jour ou lui attribuer une étape) (version 6.6.0 et versions ultérieures) à côté du paquet de mise à niveau que vous souhaitez pousser, puis choisissez les périphériques de destination.

Si les périphériques dans lesquels vous souhaitez pousser le paquet de mise à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

Étape 4 Pousser le paquet

- Cisco Firepower Management Center : cliquez sur **Pousser**.
- Serveur Web internet : cliquez sur **Télécharger la mise à jour vers le périphérique à partir de la source**.

Vérification de l'état de préparation du logiciel Firepower

Les vérifications de l'état de préparation évaluent la préparation d'un périphérique Firepower à une mise à niveau logicielle.Si l'appareil échoue au contrôle de l'état de préparation, corrigez les problèmes et relancez ce dernier. Si le contrôle de l'état de préparation révèle des problèmes que vous ne pouvez pas résoudre, nous vous recommandons de ne pas démarrer la mise à niveau.

Le temps nécessaire pour exécuter une vérification de l'état de préparation varie en fonction du modèle d'appareil et de la taille de la base de données. Les versions ultérieures ont également des vérifications plus rapides de l'état de préparation.

Exécuter les vérifications de l'état de préparation avec FDM (FTD version 7.0.0 ou version ultérieure)

Si votre FMC exécute la version 7.0.0 ou une version ultérieure, nous vous recommandons d'utiliser la page de mise à niveau de périphérique pour vérifier l'état de préparation des périphériques FTD ; voir Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 77.

Consultez les en-têtes suivantes si vous :

- Exécutez des vérifications de préparation sur le FMC lui-même.
- Exécutez des vérifications de préparation sur les périphériques gérés, et votre FMC exécute la version 6.7.x.
- Exécutez des vérifications de préparation sur les appareils gérés, et votre FMC exécute la version 6.6.x ou antérieure.

Exécuter les vérifications de préparation avec FMC (version 6.7.0 et versions ultérieures)

Cette procédure est valide pour les FMC exécutant *actuellement* la version 6.7.0 ou une version ultérieure et leurs périphériques gérés, y compris les périphériques exécutant d'anciennes versions (6.3.0-6.6.x) et les périphériques Cisco FTD dans les déploiements à haute disponibilité et évolutivité .



Important Si votre FMC exécute la version 7.0.0 ou une version ultérieure, nous vous recommandons d'utiliser la page de mise à niveau de périphérique pour pour vérifier l'état de préparation des périphériques FTD ; voir Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 77. Vous devez toujours utiliser cette procédure pour exécuter des vérifications de la préparation sur le FMC et sur tous les périphériques Classic.

Avant de commencer

- Mettez à niveau le FMC au moins à la version 6.7.0. Si votre FMC exécute actuellement une version plus ancienne, consultez Exécuter des vérifications de l'état de préparation avec FMC (version 6.0.1–6.6.x), à la page 43.
- Chargez le paquet de mise à niveau dans le FMC, pour l'appliance que vous voulez vérifier. Si vous voulez vérifier des périphériques FTD version 6.6.0 et versions ultérieures, vous pouvez aussi indiquer l'emplacement du paquet de mise à niveau sur un serveur web interne. Ceci est requis parce que les vérifications de l'état de préparation sont incluses dans les paquets de mise à niveau.
- (Facultatif) Si vous mettez à niveau un périphérique Classic vers n'importe quelle version, ou un périphérique Cisco FTD vers la version 6.3.0.1-6.6.x, copiez le paquet de mise à niveau sur le périphérique. Cela peut réduire le temps nécessaire pour exécuter la vérification de la disponibilité. Si vous mettez à niveau un périphérique Cisco FTD à la version 6.7.0 et ultérieures, vous pouvez ignorer cette étape. Bien que nous vous recommandions toujours de pousser le package de mise à niveau sur le périphérique avant de commencer la mise à niveau, vous n'avez plus à le faire avant d'exécuter la vérification de l'état de préparation.

Procédure

Étape 1 Sur l'interface Web de FMC, choisissez **Système** > **Mises à jour**.

Étape 2 Sous Mises à jour disponibles, cliquez sur l'icône **Install** (Installer) à côté du paquet de mise à niveau approprié.

Le système affiche une liste des périphériques admissibles, ainsi que leurs résultats de vérification de compatibilité préalables à la mise à niveau. À partir de la version 6.7.0, les périphériques Cisco FTD doivent réussir certaines vérifications de base avant que vous puissiez exécuter la vérification de préparation la plus complexe. Cette pré-vérification permet de détecter les problèmes qui *entraîneront* l'échec de votre mise à niveau, mais nous les détectons désormais plus tôt et vous empêchons de continuer.

Étape 3 Sélectionnez les périphériques que vous souhaitez vérifier et cliquez sur **Launch Readiness Check** (Lancer la vérification de l'état de préparation).

Si vous ne pouvez pas sélectionner un appareil autrement admissible, assurez-vous qu'il a réussi ses vérifications de compatibilité. Vous devrez peut-être mettre à niveau un système d'exploitation ou déployer des modifications de configuration .

Étape 4 Surveillez l'état de préparation de la mise à jour dans le Message Center (Centre de messages).

Si la vérification échoue, le Centre de messages fournit des journaux d'échec.

Prochaine étape

Sur la page **System (Système)** > **Updates (Mises à jour)**, cliquez sur **Readiness Checks** (Vérifications de préparation) pour voir l'état des vérifications pour votre déploiement FTD (en cours et échouées). Vous pouvez également utiliser cette page pour réexécuter facilement les vérifications après un échec.

Exécuter des vérifications de l'état de préparation avec FMC (version 6.0.1–6.6.x)

Cette procédure est valide pour les FMC exécutant *actuellement* la version 6.0.1–6.6.x, et leurs périphériques gérés autonomes.

Remarque Pour les périphériques en grappe, les périphériques empilés et les périphériques en paire à haute accessibilité, vous pouvez exécuter la vérification de l'état de préparation à partir de l'interface Shell Linux, également appelée *mode expert*. Pour exécuter la vérification, vous devez d'abord pousser ou copier le paquet de mise à niveau au bon emplacement sur chaque périphérique, puis utiliser cette commande : `sudo install_update.pl --detach --readiness-check /var/sf/updates/upgrade_package_name`. Pour en savoir plus sur les instructions, communiquez le Centre d'assistance technique Cisco (TAC).

Avant de commencer

- (Version 6.0.1) Si vous voulez exécuter des vérifications de l'état de préparation lors d'une mise à niveau de la version 6.0.1 → 6.1.0, installez d'abord le paquet de pré-installation de la version 6.1. Vous devez le faire pour le FMC et les périphériques gérés. Reportez-vous aux notes de mise à jour du système Firepower version 6.1.0 – préinstallation.
- Chargez le paquet de mise à niveau dans le FMC, pour l'appliance que vous voulez vérifier. Si vous voulez vérifier des périphériques FTD version 6.6.x, vous pouvez aussi indiquer l'emplacement du paquet de mise à niveau sur un serveur web interne. Ceci est requis parce que les vérifications de l'état de préparation sont incluses dans les paquets de mise à niveau.
- (Facultatif, version 6.2.3+) Envoyez le paquet de mise à niveau vers le périphérique géré. Cela peut réduire le temps requis pour exécuter la vérification.
- Déployez les configurations vers les périphériques gérés dont les configurations ne sont pas à jour. Sinon, la vérification de l'état de préparation peut échouer.

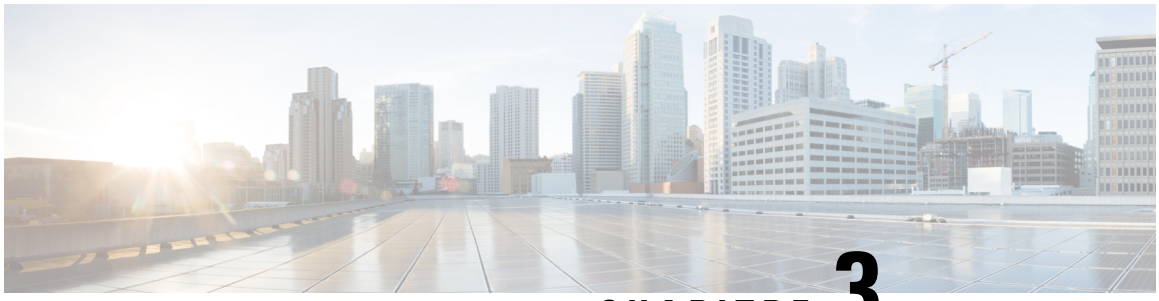
Procédure

Étape 1 Sur l'interface web de FMC, choisissez **System (Système)** > **Updates (Mises à jour)**.

Étape 2 Cliquez sur l'icône **Install** (Installer) à côté du paquet de mise à niveau approprié.

Étape 3 Sélectionnez les périphériques que vous souhaitez vérifier et cliquez sur **Launch Readiness Check** (Lancer la vérification de l'état de préparation).

Étape 4 Surveillez la progression de la vérification de l'état de préparation dans le centre de messages.



CHAPITRE 3

Mises à Niveau Cisco Firepower Management Center

- Liste de contrôle de mise à niveau : Firepower Management Center.contrôle, à la page 45
- Mettre à niveau un élément autonome Cisco Firepower Management Center, à la page 49
- Mettre à niveau les Firepower Management Center à haute disponibilité, à la page 51

Liste de contrôle de mise à niveau : Firepower Management Center.contrôle

Terminez cette liste de contrôle avant de mettre à niveau un FMC, y compris FMCv. Si vous mettez à niveau une paire à haute disponibilité, remplissez la liste de contrôle pour chaque homologue.

Remarque En tout temps pendant le processus, assurez-vous de maintenir la communication et l'intégrité de déploiement. *Ne redémarrez pas* une mise à niveau FMC en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez le Centre d'assistance technique Cisco (TAC)

Planification et faisabilité

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

Tableau 25 :

✓	Action/Vérification
	Planifiez votre chemin de mise à niveau. Cela est particulièrement important pour les déploiements de plusieurs appareils, les mises à niveau multisauts ou les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement, tout en maintenant la compatibilité de déploiement. Sachez toujours quelle mise à niveau vous venez d'effectuer et laquelle vous allez effectuer ensuite. **Remarque** Dans les déploiements de FMC, vous mettez généralement à niveau le FMC, puis ses périphériques gérés. Cependant, dans certains cas, vous devrez peut-être d'abord mettre à niveau les périphériques. Consultez Chemins de mise à niveau, à la page 11.
	Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par les notes de mise à jour, qui contiennent des renseignements essentiels et précis sur la version, notamment les avertissements de mise à niveau, les changements de comportement, les fonctionnalités nouvelles et obsolètes, ainsi que les problèmes connus.
	Vérifiez la bande passante. Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Dans les déploiements de FMC, si vous transférez un ensemble de mise à niveau vers un périphérique géré au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau ou même entraîner son expiration. Dans la mesure du possible, copiez les paquets de mise à niveau sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance. Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que la mise à niveau est susceptible de prendre. Tenez également compte des tâches que vous *devez* effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Par exemple, n'attendez pas la période de maintenance pour copier les paquets de mise à niveau sur les périphériques, exécuter des vérifications de la préparation, effectuer des sauvegardes, etc.

Progiciels de mise à niveau

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco.

Tableau 26 :

✓	Action/Vérification
	Téléverser le paquet de mise à niveau Pour des déploiements FMC à haute disponibilité, vous devez charger le paquet de mise à niveau FMC sur les deux homologues, en suspendant la synchronisation avant de transférer le paquet sur le paquet de secours. Pour limiter les interruptions de la synchronisation à haute disponibilité, vous pouvez transférer le paquet vers l'homologue actif pendant l'étape de préparation de la mise à niveau, et vers l'homologue de secours dans le cadre du processus de mise à niveau lui-même, après avoir suspendu la synchronisation. Consultez Charger vers Cisco Firepower Management Center, à la page 38.

Sauvegardes

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système.

La sauvegarde et la restauration peuvent être des processus complexes. Vous ne voulez sauter aucune étape ou ignorer les problèmes de sécurité ou de licence. Pour en savoir plus sur les exigences, les directives, les limitations et les bonnes pratiques en matière de sauvegarde et de restauration, consultez le guide de configuration de votre déploiement.

Mise en garde Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau.

Tableau 27 :

✓	Action/Vérification
	Sauvegardez. Sauvegarder avant et après la mise à niveau : • Avant la mise à niveau : si une mise à niveau échoue de manière catastrophique, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement. • Après la mise à niveau : cela crée un instantané de votre déploiement nouvellement mis à niveau. Dans les déploiements de FMC, nous vous recommandons de sauvegarder le FMC après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde FMC sache que ses périphériques ont été mis à niveau.

Mises à niveau associées

Étant donné que les mises à niveau de systèmes d'exploitation et d'environnements d'hébergement peuvent avoir une incidence sur le flux de trafic et l'inspection, effectuez-les pendant une période de maintenance.

Tableau 28 :

✓	Action/Vérification
	Mettez à niveau l'hébergement virtuel. Si nécessaire, mettez à niveau l'environnement d'hébergement. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau de FMC majeure.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à effectuer la mise à niveau.

Tableau 29 :

✓	Action/Vérification
	Vérifiez les configurations. Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP. Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. La désynchronisation peut entraîner l'échec de la mise à niveau. Dans les déploiements de FMC, le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, mais il convient de toujours vérifier manuellement. Pour vérifier l'heure : • FMC : choisissez **Système > Configuration > Temps**. • Périphériques : utilisez la commande **show time** de l'interface de ligne de commande.
	Vérifiez l'espace disque. Exécutez une vérification de l'espace disque pour la mise à niveau logicielle. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Consultez le chapitre *Mettre à niveau le logiciel* dans les Notes de version de Cisco Firepower de votre version cible.

✓	Action/Vérification
	Déployez des configurations. Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Dans certains déploiements, la mise à niveau peut être bloquée si vous avez des configurations obsolètes. Dans les déploiements FMC à haute disponibilité, il vous suffit de procéder au déploiement à partir de l'homologue actif. Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre Snort, ce qui interrompt l'inspection du trafic et, selon la façon dont votre périphérique gère le trafic, peut interrompre le trafic jusqu'à la fin du redémarrage. Consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.
	Exécutez la vérification de l'état de préparation. Si votre FMC exécute la version 6.1.0 ou une version ultérieure, nous recommandons de vérifier la compatibilité et l'état de préparation. Ces vérifications évaluent votre degré de préparation à une mise à niveau logicielle. Consultez Vérification de l'état de préparation du logiciel Firepower, à la page 41.
	Vérifiez les tâches en cours. Assurez-vous que les tâches essentielles, y compris le déploiement final, sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Nous vous recommandons également de vérifier les tâches qui sont programmées pour s'exécuter pendant la mise à niveau et de les annuler ou de les reporter. **Remarque** Dans certains déploiements, les mises à niveau reportent automatiquement les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. Cette fonctionnalité est actuellement prise en charge pour les FMC exécutant la version 6.4.0.10 et les versions ultérieures, la version 6.6.3 et les versions de maintenance ultérieures ainsi que la version 6.7.0 et les versions ultérieures. Notez que cette fonctionnalité est prise en charge pour toutes les mises à niveau *à partir d'* une version prise en charge. Cette fonctionnalité n'est pas prise en charge pour les mises à niveau *vers* une version prise en charge à partir d'une version non prise en charge.

Mettre à niveau un élément autonome Cisco Firepower Management Center

Utilisez cette procédure pour mettre à niveau un Cisco Firepower Management Center autonome, y compris Cisco Firepower Management Center Virtual.

⚠

Mise en garde N’apportez *pas* et ne déployez pas de modifications de configuration, ne redémarrez pas le système manuellement ou ne l’éteignez pas pendant la mise à niveau du FMC. Ne redémarrez *pas* une mise à niveau en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez le Centre d’assistance technique Cisco (TAC)

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.

Procédure

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

Étape 2 Cliquez sur l’icône Installer à côté du paquet de mise à niveau que vous souhaitez utiliser, puis choisissez FMC.

Étape 3 Cliquez sur **Installer** pour commencer la mise à niveau.

Confirmez que vous souhaitez procéder à la mise à niveau et redémarrez le système.

Étape 4 Surveillez la progression de la vérification préalable jusqu’à ce que vous soyez déconnecté. Évitez d’apporter des modifications à la configuration pendant ce temps.

Étape 5 Reconnectez-vous quand vous le pouvez.

- Mise à niveau mineures (correctifs et correctifs rapides) : vous pouvez vous connecter une fois la mise à niveau et le redémarrage terminés.
- Mises à niveau majeures et mises à niveau de maintenance : vous pouvez vous connecter avant la fin de la mise à niveau. Le système affiche une page que vous pouvez utiliser pour surveiller la progression de la mise à niveau et afficher le journal de cette dernière ainsi que les éventuels messages d’erreur. Vous êtes à nouveau déconnecté une fois la mise à niveau terminée et le système redémarre. Après le redémarrage, reconnectez-vous.

Étape 6 Si vous y êtes invité, passez en revue le contrat de licence de l’utilisateur final (CLUF) et acceptez-le.

Étape 7 Vérifiez la réussite de la mise à niveau.

Si le système ne vous informe pas de la réussite de la mise à niveau lorsque vous vous connectez, choisissez **Aide** > **À propos** pour afficher les informations sur la version actuelle du logiciel.

Étape 8 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d’assistance et de téléchargement Cisco est plus récent que la version en cours d’exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 9 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 10 Redéployez les configurations.

Redéployez les configurations sur *tous* les périphériques gérés. Si vous ne les déployez pas sur un périphérique, la mise à niveau ultérieure de ce dernier risque d'échouer et vous devrez peut-être le réinitialiser.

Mettre à niveau les Firepower Management Center à haute disponibilité

Utilisez cette procédure pour mettre à niveau le logiciel Firepower sur les FMC dans une paire à haute disponibilité.

Vous mettez à niveau les homologues un à la fois. Une fois que la synchronisation est interrompue, mettez d'abord à niveau l'unité de secours, puis l'unité active. Lorsque le périphérique de secours commence les vérifications préalables, son état passe de « de secours » à « actif », de sorte que les deux homologues sont actifs. Cet état temporaire s'appelle *split-brain* (déconnexion cérébrale) et *n'est pas* pris en charge, sauf lors de la mise à niveau. N'effectuez ni ne déployez *pas* de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale) Vos modifications seront perdues après le redémarrage de la synchronisation.

⚠

Mise en garde N'apportez *pas* et ne déployez pas de modifications de configuration, ne redémarrez pas le système manuellement ou ne l'éteignez pas pendant la mise à niveau du FMC. Ne redémarrez *pas* une mise à niveau en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez le Centre d'assistance technique Cisco (TAC)

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau pour les deux homologues. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.

Procédure

Étape 1 Suspendez la synchronisation.

a) Choisissez **Intégration** > **système**.
b) Sous l'onglet **High Availability**, cliquez sur **Suspendre la synchronisation**.

Étape 2 Chargez le paquet de mise à niveau vers l'unité de secours.

Pour des déploiements FMC à haute disponibilité, vous devez charger le paquet de mise à niveau FMC sur les deux homologues, en suspendant la synchronisation avant de transférer le paquet sur le paquet de secours. Pour limiter les interruptions de la synchronisation à haute disponibilité, vous pouvez transférer le paquet vers l'homologue actif pendant l'étape de préparation de la mise à niveau, et vers l'homologue de secours dans le cadre du processus de mise à niveau lui-même, après avoir suspendu la synchronisation.

Étape 3 Mettez à niveau les homologues un à la fois : d'abord l'homologue de secours, puis l'homologue actif.

Suivez les instructions dans Mettre à niveau un élément autonome Cisco Firepower Management Center, à la page 49, en vous arrêtant après avoir vérifié la réussite de la mise à jour sur chaque homologue. En résumé, pour chaque homologue :

a) Sur la page **Système** > **Mises à jour**, installez la mise à niveau.
b) Surveillez la progression jusqu'à ce que vous soyez déconnecté, puis reconnectez-vous lorsque vous le pouvez (cela se produit deux fois pour les mises à niveau majeures).
c) Vérifiez la réussite de la mise à niveau.

N'effectuez ni ne déployez *pas* de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale)

Étape 4 Redémarrez la synchronisation.

a) Connectez-vous au FMC que vous souhaitez utiliser comme homologue actif.
b) Choisissez **Système** > **Intégration**.
c) Sous l'onglet **Haute disponibilité**, cliquez sur **Rendez-moi actif**.
d) Attendez que la synchronisation redémarre et que l'autre FMC passe en mode de secours.

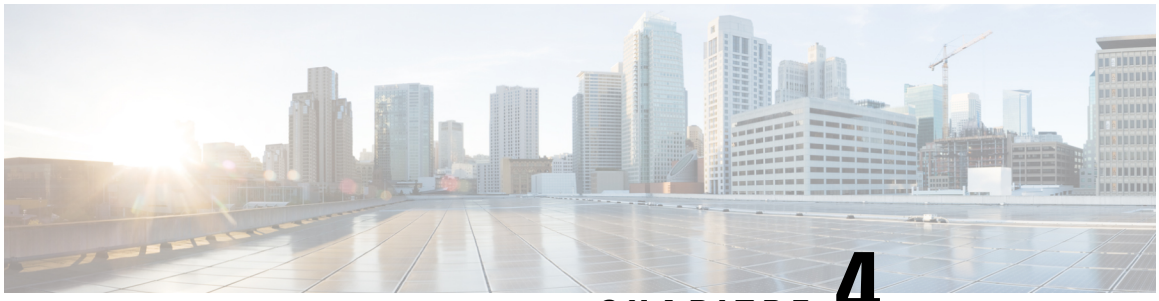
Étape 5 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d'assistance et de téléchargement Cisco est plus récent que la version en cours d'exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 6 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 7 Redéployez les configurations.

Redéployez les configurations sur *tous* les périphériques gérés. Si vous ne les déployez pas sur un périphérique, la mise à niveau ultérieure de ce dernier risque d'échouer et vous devrez peut-être le réinitialiser.



CHAPITRE 4

Mettre à niveau des dispositifs logiques FTD

- Liste de contrôle des mises à niveau : Firepower Threat Defense avec FMC, à la page 53
- Mettre à niveau FXOS sur un Firepower 4100/9300 avec des périphériques logiques Firepower Threat Defense, à la page 58
- Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 77
- Mettre à niveau Firepower Threat Defense avec FMC (version 6.0.1–6.7.0), à la page 81

Liste de contrôle des mises à niveau : Firepower Threat Defense avec FMC

Terminez cette liste de contrôle avant d'effectuer la mise à niveau de Cisco Firepower Threat Defense.

Remarque En tout temps pendant le processus, assurez-vous de maintenir la communication et l'intégrité de déploiement.

Dans la plupart des cas, ne redémarrez *pas* une mise à niveau en cours. Cependant, avec les mises à niveau majeures et de maintenance de FTD *à partir de* la version 6.7.0, vous pouvez annuler manuellement les mises à niveau échouées ou en cours, et réessayer les mises à niveau. Utilisez la fenêtre contextuelle État de la mise à niveau, accessible à partir de la page Gestion des périphériques et du Centre de messagerie, ou utilisez l'interface de ligne de commande de FTD. Veuillez notez que, par défaut, FTD revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« annulation automatique »). Pour pouvoir annuler *manuellement* ou réessayer une mise à niveau ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Veuillez noter que l'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Si vous avez épuisé toutes les options ou si votre déploiement ne prend pas en charge l'annulation/les nouveaux essais, communiquez avec le Centre d'assistance technique Cisco (TAC).

Planification et faisabilité

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

Tableau 30 :

✓	Action/Vérification
	Planifiez votre chemin de mise à niveau. Cela est particulièrement important pour les déploiements de plusieurs appareils, les mises à niveau multisauts ou les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement, tout en maintenant la compatibilité de déploiement. Sachez toujours quelle mise à niveau vous venez d'effectuer et laquelle vous allez effectuer ensuite. **Remarque** Dans les déploiements de FMC, vous mettez généralement à niveau le FMC, puis ses périphériques gérés. Cependant, dans certains cas, vous devrez peut-être d'abord mettre à niveau les périphériques. Consultez Chemins de mise à niveau, à la page 11.
	Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par les notes de mise à jour, qui contiennent des renseignements essentiels et précis sur la version, notamment les avertissements de mise à niveau, les changements de comportement, les fonctionnalités nouvelles et obsolètes, ainsi que les problèmes connus.
	Vérifiez l'accès à l'appareil. Les périphériques peuvent cesser de transmettre du trafic pendant la mise à niveau (en fonction de la configuration des interfaces) ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique . Dans les déploiements de FMC, vous devriez également pouvoir accéder à l'interface de gestion FMC sans traverser le périphérique.
	Vérifiez la bande passante. Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Dans les déploiements de FMC, si vous transférez un ensemble de mise à niveau vers un périphérique géré au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau ou même entraîner son expiration. Dans la mesure du possible, copiez les paquets de mise à niveau sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance. Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que la mise à niveau est susceptible de prendre. Tenez également compte des tâches que vous *devez* effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Par exemple, n'attendez pas la période de maintenance pour copier les paquets de mise à niveau sur les périphériques, exécuter des vérifications de la préparation, effectuer des sauvegardes, etc.

Progiciels de mise à niveau

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco.

Tableau 31 :

✓	Action/Vérification
	Chargez le paquet de mise à niveau sur le FMC ou sur le serveur Web interne. Dans la version 6.6.0 et les versions ultérieures, vous pouvez configurer un serveur Web interne au lieu du FMC comme source des paquets de mise à niveau de FTD. Cela est utile si vous disposez d'une bande passante limitée entre le FMC et ses périphériques, et permet de gagner de la place sur le FMC. Consultez Charger du contenu vers un serveur interne (version 6.6.0 ou version ultérieure de FTD avec FMC), à la page 38.
	Copiez le paquet de mise à niveau sur le périphérique. Dans la mesure du possible, nous vous recommandons de copier (*push*) (pousser) les paquets sur les périphériques gérés avant de lancer la mise à niveau de ces derniers : • La version 6.2.2 et les versions antérieures ne prennent pas en charge la copie préalable à la mise à niveau. • La version 6.2.3 vous permet de copier manuellement les paquets de mise à niveau à partir du FMC. • La version 6.6.0 ajoute la possibilité de copier manuellement les paquets de mise à niveau d'un serveur Web interne. • La version 7.0.0 ajoute un flux de travail de mise à niveau de FTD qui vous invite à copier les paquets de mise à niveau. **Remarque** Pour les périphériques Firepower 4100/9300, nous vous recommandons (et parfois demandons) de copier le paquet de mise à niveau avant de commencer la mise à niveau FXOS associée requise. Consultez Copier des données sur les périphériques gérés, à la page 40.

Sauvegardes

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système.

La sauvegarde et la restauration peuvent être des processus complexes. Vous ne voulez sauter aucune étape ou ignorer les problèmes de sécurité ou de licence. Pour en savoir plus sur les exigences, les directives, les limitations et les bonnes pratiques en matière de sauvegarde et de restauration, consultez le guide de configuration de votre déploiement.



Mise en garde Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau.

Tableau 32 :

✓	Action/Vérification
	Sauvegardez FTD. Utilisez le FMC pour sauvegarder les périphériques. Certaines plateformes et configurations de FTD ne prennent pas en charge la sauvegarde. Nécessite la version 6.3.0 ou ultérieure. Sauvegarder avant et après la mise à niveau : • Avant la mise à niveau : si une mise à niveau échoue de manière catastrophique, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement. • Après la mise à niveau : cela crée un instantané de votre déploiement nouvellement mis à niveau. Dans les déploiements de FMC, nous vous recommandons de sauvegarder le FMC après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde FMC sache que ses périphériques ont été mis à niveau.
	Sauvegardez FXOS sur le Firepower 4100/9300. Utilisez Firepower Chassis Manager ou l'interface de ligne de commande de FXOS pour exporter les configurations des châssis avant et après la mise à niveau, y compris les paramètres de configuration des périphériques logiques et de la plateforme.

Mises à niveau associées

Étant donné que les mises à niveau de systèmes d'exploitation et d'environnements d'hébergement peuvent avoir une incidence sur le flux de trafic et l'inspection, effectuez-les pendant une période de maintenance.

Tableau 33 :

✓	Action/Vérification
	Mettez à niveau l'hébergement virtuel. Si nécessaire, mettez à niveau l'environnement d'hébergement pour les appliances virtuelles. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau de périphérique majeure.
	Mettez à niveau FXOS sur le Firepower 4100/9300. Si nécessaire, mettez à niveau FXOS avant de mettre à niveau FTD. Il s'agit généralement d'une exigence pour les mises à niveau majeures, mais très rare pour les versions de maintenance et les correctifs. Pour éviter les interruptions du flux de trafic et de l'inspection, mettez à niveau FXOS dans les paires à haute disponibilité FTD et les grappes interchâssis, *un châssis à la fois*. **Remarque** Avant de mettre à niveau FXOS, assurez-vous de lire toutes les directives de mise à niveau et de planifier les changements de configuration. Commencez par les notes de mise à jour de FXOS : Notes de version Cisco Firepower 4100/9300 FXOS.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à effectuer la mise à niveau.

Tableau 34 :

✓	Action/Vérification
	Vérifiez les configurations. Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP. Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. La désynchronisation peut entraîner l'échec de la mise à niveau. Dans les déploiements de FMC, le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, mais il convient de toujours vérifier manuellement. Pour vérifier l'heure : • FMC : choisissez **Système > Configuration > Temps**. • Périphériques : utilisez la commande **show time** de l'interface de ligne de commande.
	Vérifiez l'espace disque. Exécutez une vérification de l'espace disque pour la mise à niveau logicielle. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Consultez le chapitre *Mettre à niveau le logiciel* dans les Notes de version de Cisco Firepower de votre version cible.
	Déployez des configurations. Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Dans certains déploiements, la mise à niveau peut être bloquée si vous avez des configurations obsolètes. Dans les déploiements FMC à haute disponibilité, il vous suffit de procéder au déploiement à partir de l'homologue actif. Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre Snort, ce qui interrompt l'inspection du trafic et, selon la façon dont votre périphérique gère le trafic, peut interrompre le trafic jusqu'à la fin du redémarrage. Consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.
	Exécutez la vérification de l'état de préparation. Si votre FMC exécute la version 6.1.0 ou une version ultérieure, nous recommandons de vérifier la compatibilité et l'état de préparation. Ces vérifications évaluent votre degré de préparation à une mise à niveau logicielle. La version 7.0.0 introduit un nouveau flux de travail de mise à niveau de FTD vous invite à effectuer ces vérifications. Consultez Vérification de l'état de préparation du logiciel Firepower, à la page 41.

✓	Action/Vérification
	Vérifiez les tâches en cours. Assurez-vous que les tâches essentielles sur le périphérique, y compris le déploiement final, sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Nous vous recommandons également de vérifier les tâches qui sont programmées pour s'exécuter pendant la mise à niveau et de les annuler ou de les reporter.

Mettre à niveau FXOS sur un Firepower 4100/9300 avec des périphériques logiques Firepower Threat Defense

Sur le Firepower 4100/9300, vous mettez à niveau FXOS sur chaque châssis indépendamment, même si vous avez configuré des grappes inter-châssis Firepower ou des paires à haute accessibilité. Vous pouvez utiliser la CLI FXOS ou le Firepower Chassis Manager.

La mise à niveau de FXOS redémarre le châssis. Selon votre déploiement, le trafic peut être abandonné ou traverser le réseau sans inspection ; consultez Cisco Firepower Notes de mise à jour de votre version.

Mettre à niveau FXOS : périphériques FTD en déploiement autonome et grappes intra-châssis

Pour un périphérique logique Firepower Threat Defense autonome ou pour une grappe intra-châssis Cisco FTD (unités sur le même châssis), mettez d'abord à niveau l'offre groupée de plateforme FXOS, puis mettez à niveau les périphériques logiques Cisco FTD . Utilisation le Cisco Firepower Management Center pour mettre à niveau des périphériques en grappe en tant qu'unité.

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intra-châssis FTD à l'aide de Firepower Chassis Manager

La section décrit le processus de mise à niveau pour les types de périphériques suivants :

- Un châssis Firepower 4100 configuré avec un périphérique logique FTD et ne faisant pas partie d'une paire de basculement ou d'une grappe inter-châssis.
- Un châssis Firepower 9300 configuré avec un ou plusieurs périphériques logiques FTD autonomes ne faisant pas partie d'une paire de basculement ou d'une grappe inter-châssis.
- Un châssis Firepower 9300 configuré avec des périphériques logiques FTD dans une grappe intra-châssis.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.

Procédure

Étape 1 Dans Firepower Chassis Manager, choisissez **System (Système)** > **Updates (Mises à jour)**.
La page Available Updates (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications disponibles sur le châssis.

Étape 2 Chargez la nouvelle image groupée de la plateforme :

a) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).
b) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
c) Cliquez sur **Upload** (charger).
L'image sélectionnée est téléchargée sur le Châssis Firepower 4100/9300 .
d) Pour certaines images logicielles, vous recevrez un contrat de licence d'utilisateur final après le téléchargement de l'image. Suivez les messages-guides du système pour accepter le contrat de licence d'utilisateur final.

Étape 3 Une fois que la nouvelle image groupée de plateforme a été chargée, cliquez sur **Upgrade** (Mise à niveau) de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Étape 4 Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation, ou cliquez sur **No** (Non) pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 5 Firepower Chassis Manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide du Interface de ligne de commande FXOS :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

```
Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
```

Étape 6 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intra-châssis FTD à l'aide de l'interface de ligne de commande de FXOS

La section décrit le processus de mise à niveau FXOS pour les types de périphériques suivants :

- Un châssis Firepower 4100 configuré avec un périphérique logique FTD et ne faisant pas partie d'une paire de basculement ou d'une grappe inter-châssis.
- Un châssis Firepower 9300 configuré avec un ou plusieurs périphériques FTD autonomes ne faisant pas partie d'une paire de basculement ou d'une grappe inter-châssis.
- Un châssis Firepower 9300 configuré avec des périphériques logiques FTD dans une grappe intra-châssis.

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.
- Collectez les informations suivantes dont vous aurez besoin pour télécharger l'image logicielle sur le Châssis Firepower 4100/9300 :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

Étape 1 Connectez-vous à l'Interface de ligne de commande FXOS.

Étape 2 Téléchargez la nouvelle image groupée de la plateforme sur le Châssis Firepower 4100/9300 :

a) Entrez en mode micrologiciel :

Firepower-chassis-a # **scope firmware**

b) Téléchargez l'image de l'offre logicielle groupée de la plateforme FXOS :

Firepower-chassis-a /firmware # **download image** *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) Pour surveiller le processus de téléchargement :

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 3 Si nécessaire, revenez au mode micrologiciel :

Firepower-chassis-a /firmware/download-task # **up**

Étape 4 Passez en mode d'installation automatique :

Firepower-chassis-a /firmware # **scope auto-install**

Étape 5 Installez l'ensemble de la plateforme FXOS :

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez, par exemple, la version 2.3(1.58).

Étape 6 Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Saisissez **yes** (oui) pour confirmer que vous souhaitez procéder à la vérification.

Étape 7 Saisissez **yes** (oui) pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 8 Pour superviser le processus de mise à niveau :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Étape 9 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Mettre à niveau FXOS : paires FTD à haute disponibilité

Dans les déploiements à haute disponibilité de Firepower Threat Defense , mettez à niveau l'offre groupée de plateformes FXOS sur *les deux châssis* avant de mettre à niveau l'un ou l'autre des périphériques logiques Cisco FTD . Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours.

Dans les déploiements de Firepower Management Center, vous mettez à niveau des périphériques logiques en tant qu'unité :

1. Mettez à niveau FXOS sur l'unité de secours.
2. Changez de rôle.
3. Mettez à niveau FXOS sur le nouveau périphérique de secours.
4. Mettez à niveau les périphériques logiques FTD.

Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de Firepower Chassis Manager

Si vous possédez des appareils de sécurité Firepower 9300 ou Firepower 4100 qui ont des périphériques logiques FTD configurés en tant que paire à haute accessibilité, utilisez la procédure suivante pour mettre à jour l'ensemble de la plateforme FXOS sur vos appareils de sécurité Firepower 9300 ou Firepower 4100 :

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.

Procédure

Étape 1 Connectez-vous à Firepower Chassis Manager sur l'appareil de sécurité Firepower qui contient le périphérique logique Firepower Threat Defense en *veille* :

Étape 2 Dans Firepower Chassis Manager, choisissez **System (Système)** > **Updates (Mises à jour)**.
La page Available Updates (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications disponibles sur le châssis.

Étape 3 Chargez la nouvelle image groupée de la plateforme :

a) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).
b) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
c) Cliquez sur **Upload** (charger).
L'image sélectionnée est téléchargée sur le Châssis Firepower 4100/9300 .
d) Pour certaines images logicielles, vous recevrez un contrat de licence d'utilisateur final après le téléchargement de l'image. Suivez les messages-guides du système pour accepter le contrat de licence d'utilisateur final.

Étape 4 Une fois que la nouvelle image groupée de plateforme a été chargée, cliquez sur **Upgrade** (Mise à niveau) de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Étape 5 Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation, ou cliquez sur **No** (Non) pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 6 Firepower Chassis Manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide du Interface de ligne de commande FXOS :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Étape 7 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Étape 8 Faites de l'unité que vous venez de mettre à niveau l'unité *active* afin que le trafic flux de trafic vers l'unité mise à niveau :

a) Connectez-vous à Cisco Firepower Management Center.
b) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
c) À côté de la paire à haute accessibilité pour laquelle vous souhaitez changer de pair actif, cliquez sur l'icône Switch Active Peer (Changer de pair actif) ().
d) Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.

Étape 9 Connectez-vous à Firepower Chassis Manager sur l'appareil de sécurité Firepower qui contient le nouveau périphérique logique Firepower Threat Defense en *veille* :

Étape 10 Dans Firepower Chassis Manager, choisissez **System (Système)** > **Updates (Mises à jour)**.
La page Available Updates (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications disponibles sur le châssis.

Étape 11 Chargez la nouvelle image groupée de la plateforme :

a) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).
b) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
c) Cliquez sur **Upload** (charger).
L'image sélectionnée est téléchargée sur le Châssis Firepower 4100/9300 .
d) Pour certaines images logicielles, vous recevrez un contrat de licence d'utilisateur final après le téléchargement de l'image. Suivez les messages-guides du système pour accepter le contrat de licence d'utilisateur final.

Étape 12 Une fois que la nouvelle image groupée de plateforme a été chargée, cliquez sur **Upgrade** (Mise à niveau) de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Étape 13 Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation, ou cliquez sur **No** (Non) pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants. Le processus de mise à niveau peut prendre jusqu'à 30 minutes.

Étape 14 Firepower Chassis Manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide du Interface de ligne de commande FXOS :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
```

```
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Étape 15 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Étape 16 Faites de l'unité que vous venez de mettre à niveau l'unité *active* comme elle l'était avant la mise à niveau :

a) Connectez-vous à Cisco Firepower Management Center.
b) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
c) À côté de la paire à haute accessibilité pour laquelle vous souhaitez changer de pair actif, cliquez sur l'icône Switch Active Peer (Changer de pair actif) ( ).
d) Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.

Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de l'interface de ligne de commande de FXOS

Si vous possédez des appareils de sécurité Firepower 9300 ou Firepower 4100 qui ont des périphériques logiques FTD configurés en tant que paire à haute accessibilité, utilisez la procédure suivante pour mettre à jour l'ensemble de la plateforme FXOS sur vos appareils de sécurité Firepower 9300 ou Firepower 4100 :

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.
- Collectez les informations suivantes dont vous aurez besoin pour télécharger l'image logicielle sur le Châssis Firepower 4100/9300 :

- L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
- Nom complet du fichier image.

Procédure

Étape 1 Connectez-vous à Interface de ligne de commande FXOS sur l'appareil de sécurité Firepower qui contient le périphérique logique Firepower Threat Defense en *veille* :

Étape 2 Téléchargez la nouvelle image groupée de la plateforme sur le Châssis Firepower 4100/9300 :

a) Entrez en mode micrologiciel :

Firepower-chassis-a # **scope firmware**

b) Téléchargez l'image de l'offre logicielle groupée de la plateforme FXOS :

Firepower-chassis-a /firmware # **download image** *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*
- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname***:***port-num/path/image_name*

c) Pour surveiller le processus de téléchargement :

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 3 Si nécessaire, revenez au mode micrologiciel :

Firepower-chassis-a /firmware/download-task # **up**

Étape 4 Passez en mode d'installation automatique :

Firepower-chassis-a /firmware # **scope auto-install**

Étape 5 Installez l'ensemble de la plateforme FXOS :

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez; par exemple, la version 2.3(1.58).

Étape 6 Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Saisissez **yes** (oui) pour confirmer que vous souhaitez procéder à la vérification.

Étape 7 Saisissez **yes** (oui) pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 8 Pour superviser le processus de mise à niveau :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Étape 9 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.

d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Étape 10 Faites de l'unité que vous venez de mettre à niveau l'unité *active* afin que le trafic flux de trafic vers l'unité mise à niveau :

a) Connectez-vous à Cisco Firepower Management Center.
b) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
c) À côté de la paire à haute accessibilité pour laquelle vous souhaitez changer de pair actif, cliquez sur l'icône Switch Active Peer (Changer de pair actif) ( ).
d) Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.

Étape 11 Connectez-vous à l'Interface de ligne de commande FXOS sur l'appareil de sécurité Firepower qui contient le nouveau périphérique logique Firepower Threat Defense en *veille* :

Étape 12 Téléchargez la nouvelle image groupée de la plateforme sur le Châssis Firepower 4100/9300 :

a) Entrez en mode micrologiciel :

Firepower-chassis-a # **scope firmware**

b) Téléchargez l'image de l'offre logicielle groupée de la plateforme FXOS :

Firepower-chassis-a /firmware # **download image** *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*
- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname***:***port-num/path/image_name*

c) Pour surveiller le processus de téléchargement :

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
```

```
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 13 Si nécessaire, revenez au mode micrologiciel :

Firepower-chassis-a /firmware/download-task # **up**

Étape 14 Passez en mode d'installation automatique :

Firepower-chassis-a /firmware # **scope auto-install**

Étape 15 Installez l'ensemble de la plateforme FXOS :

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez; par exemple, la version 2.3(1.58).

Étape 16 Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Saisissez **yes** (oui) pour confirmer que vous souhaitez procéder à la vérification.

Étape 17 Saisissez **yes** (oui) pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 18 Pour superviser le processus de mise à niveau :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Étape 19 Une fois que tous les composants ont bien été mis à niveau, saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.
b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` pour tous les périphériques logiques installés sur le châssis.

Étape 20 Faites de l'unité que vous venez de mettre à niveau l'unité *active* comme elle l'était avant la mise à niveau :

a) Connectez-vous à Cisco Firepower Management Center.
b) Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
c) À côté de la paire à haute accessibilité pour laquelle vous souhaitez changer de pair actif, cliquez sur l'icône Switch Active Peer (Changer de pair actif) ( ).
d) Cliquez sur **Yes** (oui) pour faire immédiatement du périphérique en veille le périphérique actif dans la paire à haute disponibilité.

Mettre à niveau FXOS : grappes FTD inter-châssis.

Pour les grappes FTD inter-châssis (unités sur différents châssis), mettez à niveau le bundle FXOS sur *tous* les châssis avant de mettre à niveau les périphériques logiques FTD. Pour réduire au minimum les perturbations, mettez toujours à niveau FXOS sur un châssis d'unités de données. Utilisez ensuite le Cisco Firepower Management Center pour mettre à niveau les périphériques logiques en tant qu'unité.

Par exemple, pour une grappe à deux châssis :

1. Mettez à niveau FXOS sur le châssis de l'unité de données.
2. Basculez le module de contrôle sur le châssis que vous venez de mettre à niveau.
3. Mettez à niveau FXOS sur le nouveau châssis d'unités de données.
4. Mettez à niveau les périphériques logiques FTD.

Mettre à niveau FXOS sur une grappe inter-châssis FTD à l'aide de Firepower Chassis Manager

Si vous possédez des appareils de sécurité Firepower 9300 ou Firepower 4100 ayant des périphériques logiques FTD configurés en tant que grappe inter-châssis, utilisez la procédure suivante pour mettre à jour l'ensemble de la plateforme FXOS sur vos appareils de sécurité Firepower 9300 ou Firepower 4100 :

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.

Procédure

Étape 1 Saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Connectez-vous à l'Interface de ligne de commande FXOS sur le châssis n° 2 (il doit s'agir d'un châssis qui n'a pas d'unité de contrôle).
b) Entrez **top**.
c) Entrez **scope ssa**.
d) Entrez **show slot**.
e) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
f) Entrez **show app-instance**.
g) Vérifiez que l'état d'exploitation est `en ligne` et que l'état de grappe est `en grappe` pour tous les périphériques logiques installés sur le châssis. Vérifiez également que la bonne version du logiciel FTD est affichée comme version en cours d'exécution.

Important
Vérifiez que l'unité de contrôle ne se trouve pas sur ce châssis. Il ne doit y avoir aucune instance de Firepower Threat Defense ayant le rôle de grappe défini sur `Master` (Maître).

h) Pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300 ou pour le moteur de sécurité sur un appareil Firepower 4100, vérifiez que la version FXOS est correcte :

scope server 1/*slot_id*, où *slot_id* est 1 pour un moteur de sécurité Firepower 4100.

show version.

Étape 2 Connectez-vous au Firepower Chassis Manager sur le châssis n° 2 (il doit s'agir d'un châssis qui n'a pas d'unité de contrôle).

Étape 3 Dans Firepower Chassis Manager, choisissez **System (Système)** > **Updates (Mises à jour)**.
La page Available Updates (Mises à jour disponibles) affiche une liste des images de l'ensemble de la plateforme FXOS et des applications disponibles sur le châssis.

Étape 4 Chargez la nouvelle image groupée de la plateforme :

a) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).
b) Cliquez sur **Choose File** (choisir un fichier) pour accéder à l'image à télécharger et la sélectionner.
c) Cliquez sur **Upload** (charger).
L'image sélectionnée est téléchargée sur le Châssis Firepower 4100/9300 .
d) Pour certaines images logicielles, vous recevrez un contrat de licence d'utilisateur final après le téléchargement de l'image. Suivez les messages-guides du système pour accepter le contrat de licence d'utilisateur final.

Étape 5 Une fois que la nouvelle image groupée de plateforme a été chargée, cliquez sur **Upgrade** (Mise à niveau) de l'ensemble de la plateforme FXOS vers laquelle vous souhaitez effectuer la mise à niveau.

Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Étape 6 Cliquez sur **Yes** (Oui) pour confirmer que vous souhaitez poursuivre l'installation, ou cliquez sur **No** (Non) pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 7 Firepower Chassis Manager ne sera pas disponible pendant la mise à niveau. Vous pouvez surveiller le processus de mise à niveau à l'aide du Interface de ligne de commande FXOS :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

d) Entrez **top**.
e) Entrez **scope ssa**.
f) Entrez **show slot**.
g) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
h) Entrez **show app-instance**.
i) Vérifiez que l'état d'exploitation est `en ligne`, que l'état de grappe est `en grappe` et que le rôle de grappe est `esclave` pour tous les périphériques logiques installés sur le châssis.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #
```

```
FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

Étape 8 Définissez l'un des modules de sécurité sur le châssis 2 comme contrôle.

Après avoir configuré l'un des modules de sécurité du châssis 2 pour le contrôle, le châssis 1 ne contient plus l'unité de contrôle et peut maintenant être mis à niveau.

Étape 9 Répétez les étapes 1 à 7 pour tous les autres châssis de la grappe.

Étape 10 Pour rétablir le rôle de contrôle au châssis 1, définissez l'un des modules de sécurité du châssis 1 comme contrôle.

Mettre à niveau FXOS sur une grappe inter-châssis FTD à l'aide de l'interface de ligne de commande de FXOS

Si vous possédez des appareils de sécurité Firepower 9300 ou Firepower 4100 avec des périphériques logiques FTD configurés en tant que grappe inter-châssis, utilisez la procédure suivante pour mettre à jour l'ensemble de la plateforme FXOS sur vos appareils de sécurité Firepower 9300 ou Firepower 4100 :

Avant de commencer

Avant de commencer votre mise à niveau, assurez-vous d'avoir déjà effectué ce qui suit :

- Téléchargez l'offre logicielle groupée de la plateforme FXOS vers laquelle vous effectuez la mise à niveau.
- Sauvegardez vos configurations FXOS et FTD.
- Collectez les informations suivantes dont vous aurez besoin pour télécharger l'image logicielle sur le Châssis Firepower 4100/9300 :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

Étape 1 Connectez-vous à l'Interface de ligne de commande FXOS sur le châssis n° 2 (il doit s'agir d'un châssis qui n'a pas d'unité de contrôle).

Étape 2 Saisissez les commandes suivantes pour vérifier l'état des modules de sécurité/du moteur de sécurité et de toutes les applications installées :

a) Entrez **top**.

b) Entrez **scope ssa**.
c) Entrez **show slot**.
d) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
e) Entrez **show app-instance**.
f) Vérifiez que l'état d'exploitation est `en ligne` et que l'état de grappe est `en grappe` pour tous les périphériques logiques installés sur le châssis. Vérifiez également que la bonne version du logiciel FTD est affichée comme version en cours d'exécution.

Important
Vérifiez que l'unité de contrôle ne se trouve pas sur ce châssis. Il ne doit y avoir aucune instance de Firepower Threat Defense ayant le rôle de grappe défini sur `Master` (Maître).

g) Pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300 ou pour le moteur de sécurité sur un appareil Firepower 4100, vérifiez que la version FXOS est correcte :

scope server 1/*slot_id*, où *slot_id* est 1 pour un moteur de sécurité Firepower 4100.

show version.

Étape 3 Téléchargez la nouvelle image groupée de la plateforme sur le Châssis Firepower 4100/9300 :

a) Entrez **top**.
b) Entrez en mode micrologiciel :

Firepower-chassis-a # **scope firmware**

c) Téléchargez l'image de l'offre logicielle groupée de la plateforme FXOS :

Firepower-chassis-a /firmware # **download image** *URL*

Précisez l'URL du fichier en cours d'importation à l'aide de l'une des syntaxes suivantes :

- **ftp**://*username@hostname/path/image_name*
- **scp**://*username@hostname/path/image_name*
- **sftp**://*username@hostname/path/image_name*
- **tftp**://*hostname***:***port-num/path/image_name*

d) Pour surveiller le processus de téléchargement :

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Exemple :

L'exemple suivant copie une image à l'aide du protocole SCP :

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
```

```
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Étape 4 Si nécessaire, revenez au mode micrologiciel :

Firepower-chassis-a /firmware/download-task # **up**

Étape 5 Passez en mode d'installation automatique :

Firepower-chassis /firmware # **scope auto-install**

Étape 6 Installez l'ensemble de la plateforme FXOS :

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number est le numéro de version de l'ensemble de la plateforme FXOS que vous installez — par exemple, la version 2.3(1.58).

Étape 7 Le système vérifiera d'abord le paquet que vous souhaitez installer. Il vous informera de toute incompatibilité entre les applications actuellement installées et le paquet de plateforme FXOS indiqué. Il vous avertira également que toutes les sessions existantes seront terminées et que le système devra être redémarré dans le cadre de la mise à niveau.

Saisissez **yes** (oui) pour confirmer que vous souhaitez procéder à la vérification.

Étape 8 Saisissez **yes** (oui) pour confirmer que vous souhaitez poursuivre l'installation ou saisissez **no** pour annuler l'installation.

Le système décompresse l'ensemble et met à niveau/recharge les composants.

Étape 9 Pour superviser le processus de mise à niveau :

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.
c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.

Remarque
Après la mise à niveau du composant FPRM, le système redémarrera puis poursuivra la mise à niveau des autres composants.

d) Entrez **top**.
e) Entrez **scope ssa**.
f) Entrez **show slot**.
g) Vérifiez que l'état d'administration est `OK` et que l'état d'exploitation est `en ligne` pour le moteur de sécurité sur un appareil Firepower 4100 ou pour tous les modules de sécurité installés sur un Appareils Cisco Firepower de série 9300.
h) Entrez **show app-instance**.
i) Vérifiez que l'état d'exploitation est `en ligne`, que l'état de grappe est `en grappe` et que le rôle de grappe est `esclave` pour tous les périphériques logiques installés sur le châssis.

Exemple :

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
```

```
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81
In Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81
Not Applicable  None
FP9300-A /ssa #
```

Étape 10 Définissez l'un des modules de sécurité sur le châssis 2 comme contrôle.

Après avoir configuré l'un des modules de sécurité du châssis 2 pour le contrôle, le châssis 1 ne contient plus l'unité de contrôle et peut maintenant être mis à niveau.

Étape 11 Répétez les étapes 1 à 9 pour tous les autres châssis de la grappe.

Étape 12 Pour rétablir le rôle de contrôle au châssis 1, définissez l'un des modules de sécurité du châssis 1 comme contrôle.

Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0)

Le FMC fournit un assistant pour mettre à niveau FTD. Vous devez toujours utiliser la page Mises à jour du système (**Système > Mises à jour**) pour charger ou préciser l'emplacement des paquets de mise à niveau.

Vous devez également utiliser la page System Updates pour mettre à niveau le FMC lui-même, ainsi que tous les périphériques classiques plus anciens.

L'assistant vous guide à travers les étapes préalables à la mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Au fur et à mesure que vous continuez, l'assistant affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante.

Si vous quittez l'assistant, votre progression est conservée, bien que d'autres utilisateurs avec un accès administrateur puissent réinitialiser, modifier ou continuer le flux de travail (à moins que vous ne vous connectiez à un CAC, auquel cas votre progression est effacée 24 heures après votre déconnexion). Votre progression est également synchronisée entre les FMC à haute disponibilité.

Remarque Dans la version 7.0.x, la page de mise à niveau des périphériques n'affiche pas correctement les périphériques dans les grappes ou les paires à haute disponibilité. Même si vous devez sélectionner et mettre à niveau ces périphériques comme une unité, le flux de travail les affiche comme des périphériques autonomes. L'état du périphérique et l'état de préparation aux mises à niveau sont évalués et signalés sur une base individuelle. Cela signifie qu'il est possible qu'une unité semble « passer » à l'étape suivante alors que l'autre ou les autres ne le font pas. Cependant, ces périphériques sont toujours regroupés. Exécuter une vérification de l'état de préparation sur l'un d'eux et l'appliquer à tous. Lancez la mise à niveau sur l'un d'eux, démarrez-la sur tous.

Pour éviter d'éventuels échecs de mise à niveau qui prennent du temps, *vérifiez* que tous les membres du groupe sont prêts à passer à l'étape suivante du flux de travail avant de cliquer sur **Next**(Suivant).

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Cependant, avec les mises à niveau majeures et de maintenance *à partir de* la version 6.7.0, vous pouvez annuler manuellement les mises à niveau échouées ou en cours, et réessayer les mises à niveau. Utilisez la fenêtre contextuelle État de la mise à niveau, accessible à partir de la page Gestion des périphériques et du Centre de messagerie, ou utilisez l'interface de ligne de commande de FTD.

Veuillez notez que, par défaut, FTD revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« annulation automatique »). Pour pouvoir annuler *manuellement* ou réessayer une mise à niveau ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Veuillez noter que l'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Si vous avez épuisé toutes les options ou si votre déploiement ne prend pas en charge l'annulation/les nouveaux essais, communiquez avec le Centre d'assistance technique Cisco (TAC).

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.

Procédure

Sélectionnez les périphériques à mettre à niveau

Étape 1 Choisissez **Devices**(périphériques) Device Management (gestion des périphériques).

Étape 2 Sélectionnez les périphériques que vous souhaitez mettre à niveau.

Vous pouvez mettre à niveau plusieurs périphériques à la fois. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

Important
Pour des raisons de performances, si vous mettez à niveau un périphérique *vers* une version comprise entre la version 6.4.0.x et la version 6.6.x, nous vous recommandons *fortement* de ne pas mettre à niveau plus de cinq périphériques simultanément.

Étape 3 Dans le menu **Sélectionner une action** ou **Sélectionner une action en bloc** sélectionnez **Mettre à niveau le logiciel Firepower**.

La page de mise à niveau des périphériques apparaît, indiquant le nombre de périphériques que vous avez sélectionnés et vous invitant à sélectionner une version cible. La page comporte deux volets : la sélection du périphérique à gauche et les détails du périphérique à droite. Cliquez sur le lien d'un périphérique dans le volet de sélection de périphériques (par exemple, « `4 périphériques` ») pour afficher les détails du périphérique correspondant.

Notez que si un flux de travail de mise à niveau est déjà en cours, vous devez d'abord soit **fusionner les périphériques** (ajouter les nouveaux périphériques sélectionnés aux périphériques sélectionnés précédemment et continuer), soit **Réinitialiser** (éliminer les sélections précédentes et utiliser uniquement les nouveaux périphériques sélectionnés).

Étape 4 Vérifiez votre sélection de périphérique.

Pour sélectionner d'autres périphériques, revenez à la page de gestion des périphériques — votre progression ne sera pas perdue. Vous pouvez ajouter et supprimer des périphériques à votre sélection, ou cliquer sur **Reset** (Réinitialiser) pour effacer votre sélection de périphériques et recommencer.

Copiez les paquets de mise à niveau vers les périphériques.

Étape 5 Dans le menu **Mettre à niveau vers**, sélectionnez votre version cible.

Le système détermine lesquels de vos périphériques sélectionnés peuvent être mis à niveau vers cette version. Si des périphériques ne sont pas admissibles, vous pouvez cliquer sur le lien du périphérique pour en comprendre la raison. Vous n'avez pas besoin de supprimer des périphériques non admissibles si vous ne le souhaitez pas; ils ne seront tout simplement pas inclus à l'étape suivante.

Notez que les choix dans le menu **Upgrade to** correspondent aux ensembles de mise à niveau de périphériques disponibles pour le système. Si votre version cible ne figure pas dans cette liste, accédez à **Système >Mises à jour** et chargez ou précisez l'emplacement du bon paquet de mise à niveau.

Étape 6 Pour tous les périphériques qui ont encore besoin d'un paquet de mise à niveau, cliquez sur **Copier les paquetsde mise à niveau**, puis confirmez votre choix.

Pour mettre à niveau FTP, le paquet de mise à niveau du logiciel doit se trouver sur le périphérique. La copie du paquet de mise à niveau avant la mise à niveau réduit la durée de votre fenêtre de maintenance de mise à niveau.

Effectuer les vérifications finales de compatibilité et d'état de préparation, ainsi que d'autres vérifications..

Étape 7 Pour tous les périphériques qui doivent réussir la vérification de l'état de préparation, cliquez sur **Exécuter la vérification de l'état de préparation**, puis confirmez votre choix.

Bien que vous puissiez ignorer les vérifications en désactivant l'option **Exiger la réussite des contrôles de compatibilité et de préparation**, nous vous déconseillons de le faire. La réussite de tous les contrôles réduit considérablement les risques d'échec de la mise à niveau. Ne déployez *pas* de modifications, ne redémarrez pas ou n'éteignez pas manuellement un périphérique pendant l'exécution des vérifications de l'état de préparation. Si un dispositif échoue au contrôle de l'état de préparation, corrigez les problèmes et relancez ce dernier. Si le contrôle de l'état de préparation révèle des problèmes que vous ne pouvez pas résoudre, ne démarrez pas la mise à niveau. Communiquez plutôt avec le Centre d'assistance technique Cisco (TAC).

Notez que les vérifications de compatibilité sont automatiques. Par exemple, le système vous alerte immédiatement si vous devez mettre à niveau FXOS sur le Firepower 4100/9300 ou si vous devez effectuer le déploiement sur des périphériques gérés.

Étape 8 effectuer les dernières vérifications préalables à la mise à niveau.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales.

Étape 9 Si nécessaire, revenez à la page de mise à niveau des périphériques.

Votre progression aurait dû être préservée. Si ce n'est pas le cas, il se peut qu'une autre personne disposant d'un accès administrateur ait réinitialisé, modifié ou achevé le flux de travail.

Étape 10 Cliquez sur **Next** (suivant).

Effectuez une mise à niveau.

Étape 11 Vérifiez la sélection de votre périphérique et la version cible.

Étape 12 Choisissez les options de restauration.

Dans le cas des mises à niveau majeures et de maintenance, vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Avec cette option activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.

Cette option n'est pas prise en charge pour les correctifs.

Étape 13 Cliquez sur **Start Upgrade**(commencer la mise à niveau), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Vous pouvez surveiller la progression de la mise à niveau dans le centre de messagerie. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez le chapitre Mise à niveau du logiciel dans les notes de mise à jour.

Les périphériques peuvent redémarrer deux fois pendant la mise à niveau. Il s'agit du comportement attendu.

Confirmation de la réussite et achèvement des tâches postérieures à la mise à niveau.

Étape 14 Vérifiez la réussite de la mise à niveau.

Une fois la mise à niveau terminée, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 15 (Facultatif) Dans les déploiements à haute disponibilité et évolutivité, examinez les rôles des périphériques.

Le processus de mise à niveau modifie les rôles de chaque périphérique de manière à ce qu'il mette toujours à niveau un périphérique de secours ou une unité de données. Il ne ramène pas les périphériques aux rôles qu'ils avaient avant la mise à niveau. Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 16 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d'assistance et de téléchargement Cisco est plus récent que la version en cours d'exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 17 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 18 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Prochaine étape

(Facultatif) Effacez l'assistant en revenant à la page de mise à niveau des périphériques et en cliquant sur **Terminer**. Jusqu'à ce que vous fassiez cela, la page de mise à niveau des périphériques continue d'afficher les détails de la mise à niveau que vous venez d'effectuer.

Mettre à niveau Firepower Threat Defense avec FMC (version 6.0.1–6.7.0)

Utilisez cette procédure pour mettre à niveau le Cisco FTD en utilisant la page de mise à jour du système du FMC. Sur cette page, vous pouvez mettre à niveau plusieurs périphériques en même temps uniquement s'ils utilisent le même progiciel de mise à niveau. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure. Pour les mises à niveau de Cisco FTD vers la version 7.0.x, nous vous recommandons d'utiliser l' assistant de mise à niveau ; voir Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 77.
- Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.
- (Facultatif) Modifiez les rôles actif/de secours de vos paires de périphériques à haute disponibilité. Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur l'icône **Switch Active Peer** (Commuter l'homologue actif) à côté de la paire et confirmez votre choix.

  Le périphérique en attente dans une paire à haute disponibilité effectue la mise à niveau en premier. Les périphériques changent de rôle, puis le nouvel appareil en attente effectue la mise à niveau. Une fois la mise à niveau terminée, les rôles des périphériques restent commutés. Si vous souhaitez conserver les rôles actif/de secours, changez manuellement les rôles avant d'effectuer la mise à niveau. De cette façon, le processus de mise à niveau les rétablit.

Procédure

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

Étape 2 Cliquez sur l'icône Install (Installer) à côté du paquet de mise à niveau que vous voulez utiliser, puis choisissez les périphériques à mettre à niveau.

Si les périphériques que vous souhaitez mettre à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

Remarque
Nous vous recommandons *fortement* de mettre à niveau moins de cinq périphériques simultanément à partir de la page de mise à jour du système. Vous ne pouvez pas arrêter la mise à niveau tant que tous les périphériques sélectionnés n'ont pas terminé le processus. S'il y a un problème avec la mise à niveau d'un périphérique, tous les périphériques doivent terminer la mise à niveau avant que vous puissiez résoudre le problème.

Étape 3 (version 6.7.0 et versions ultéreures) Choisissez les options de restauration.

Dans le cas des mises à niveau majeures et de maintenance, vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Avec cette option activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. L'annulation automatique n'est pas prise en charge pour les correctifs.

Étape 4 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Certains périphériques peuvent redémarrer deux fois pendant la mise à niveau; il s'agit d'un comportement attendu. Le trafic est abandonné tout au long de la mise à niveau ou traverse le réseau sans inspection, en fonction de la configuration et du déploiement de vos périphériques. Pour en savoir plus, consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.

Étape 5 Surveillez l'avancement de la mise à niveau.

Mise en garde
Ne déployez *pas* de modifications, ne redémarrez pas ou n'éteignez pas manuellement un périphérique pendant l'exécution des vérifications de l'état de préparation.

Dans la plupart des cas, ne redémarrez *pas* une mise à niveau en cours. Cependant, avec les mises à niveau majeures et de maintenance de FTD *à partir de* la version 6.7.0, vous pouvez annuler manuellement les mises à niveau échouées ou en cours, et réessayer les mises à niveau. Utilisez la fenêtre contextuelle État de la mise à niveau, accessible à partir de la page Gestion des périphériques et du Centre de messagerie, ou utilisez l'interface de ligne de commande de FTD. Veuillez notez que, par défaut, FTD revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« annulation automatique »). Pour pouvoir annuler *manuellement* ou réessayer une mise à niveau ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Veuillez noter que l'annulation automatique n'est pas prise en charge pour les correctifs. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli. Si vous avez épuisé toutes les options ou si votre déploiement ne prend pas en charge l'annulation/les nouveaux essais, communiquez avec le Centre d'assistance technique Cisco (TAC).

Étape 6 Vérifiez la réussite de la mise à niveau.

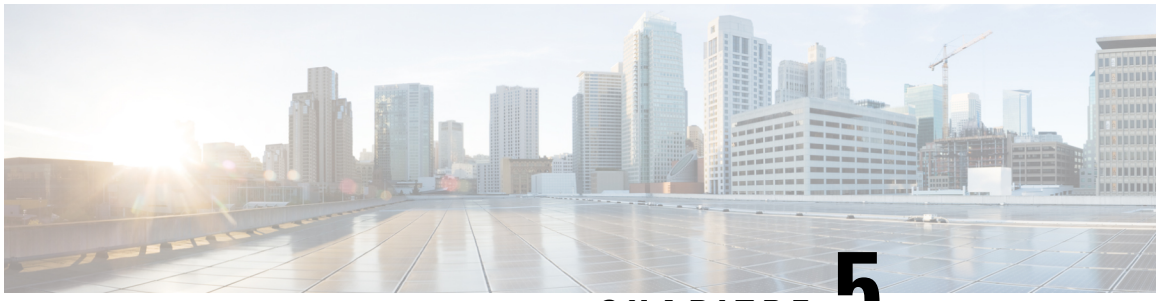
Une fois la mise à niveau terminée, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 7 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d'assistance et de téléchargement Cisco est plus récent que la version en cours d'exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 8 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 9 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.



CHAPITRE 5

Mise à niveau de la série Firepower 7000/8000 et NGIPSv

- Liste de contrôle de mise à niveau : série Firepower 7000/8000 et NGIPSv avec FMC, à la page 85
- Mise à niveau de la série Firepower 7000/8000 et NGIPSv avec FMC, à la page 89

Liste de contrôle de mise à niveau : série Firepower 7000/8000 et NGIPSv avec FMC

Remplissez cette liste de contrôle avant de mettre à niveau des périphériques Firepower 7000/8000 et NGIPSv.

Remarque En tout temps pendant le processus, assurez-vous de maintenir la communication et l'intégrité de déploiement. Ne redémarrez *pas* une mise à niveau de périphérique en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec le Centre d'assistance technique Cisco (TAC)

Planification et faisabilité

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

Tableau 35 :

✓	Action/Vérification
	Planifiez votre chemin de mise à niveau. Cela est particulièrement important pour les déploiements de plusieurs appareils, les mises à niveau multisauts ou les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement, tout en maintenant la compatibilité de déploiement. Sachez toujours quelle mise à niveau vous venez d'effectuer et laquelle vous allez effectuer ensuite. **Remarque** Dans les déploiements de FMC, vous mettez généralement à niveau le FMC, puis ses périphériques gérés. Cependant, dans certains cas, vous devrez peut-être d'abord mettre à niveau les périphériques. Consultez Chemins de mise à niveau, à la page 11.
	Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par les notes de mise à jour, qui contiennent des renseignements essentiels et précis sur la version, notamment les avertissements de mise à niveau, les changements de comportement, les fonctionnalités nouvelles et obsolètes, ainsi que les problèmes connus.
	Vérifiez l'accès à l'appareil. Les périphériques peuvent cesser de transmettre du trafic pendant la mise à niveau (en fonction de la configuration des interfaces) ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique . Dans les déploiements de FMC, vous devriez également pouvoir accéder à l'interface de gestion FMC sans traverser le périphérique.
	Vérifiez la bande passante. Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Dans les déploiements de FMC, si vous transférez un ensemble de mise à niveau vers un périphérique géré au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau ou même entraîner son expiration. Dans la mesure du possible, copiez les paquets de mise à niveau sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance. Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que la mise à niveau est susceptible de prendre. Tenez également compte des tâches que vous *devez* effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Par exemple, n'attendez pas la période de maintenance pour copier les paquets de mise à niveau sur les périphériques, exécuter des vérifications de la préparation, effectuer des sauvegardes, etc.

Progiciels de mise à niveau

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco.

Tableau 36 :

✓	Action/Vérification
	Chargez le paquet de mise à niveau vers le FMC. Consultez Charger vers Cisco Firepower Management Center, à la page 38.
	Copiez le paquet de mise à niveau sur le périphérique. Si votre instance de FMC utilise la version 6.2.3 ou une version ultérieure, nous vous recommandons de copier (*pousser*) les paquets sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez Copier des données sur les périphériques gérés, à la page 40.

Sauvegardes

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système.

La sauvegarde et la restauration peuvent être des processus complexes. Vous ne voulez sauter aucune étape ou ignorer les problèmes de sécurité ou de licence. Pour en savoir plus sur les exigences, les directives, les limitations et les bonnes pratiques en matière de sauvegarde et de restauration, consultez le guide de configuration de votre déploiement.



Mise en garde Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau.

Tableau 37 :

✓	Action/Vérification
	Savegardez les périphériques de séries 7000/8000. Utilisez le FMC pour sauvegarder les périphériques de la série 7000/8000. Les sauvegardes ne sont pas prises en charge pour NGIPSv. Sauvegarder avant et après la mise à niveau : • Avant la mise à niveau : si une mise à niveau échoue de manière catastrophique, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement. • Après la mise à niveau : cela crée un instantané de votre déploiement nouvellement mis à niveau. Dans les déploiements de FMC, nous vous recommandons de sauvegarder le FMC après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde FMC sache que ses périphériques ont été mis à niveau.

Mises à niveau associées

Étant donné que les mises à niveau de systèmes d'exploitation et d'environnements d'hébergement peuvent avoir une incidence sur le flux de trafic et l'inspection, effectuez-les pendant une période de maintenance.

Tableau 38 :

✓	Action/Vérification
	Mettez à niveau l'hébergement virtuel. Si nécessaire, mettez à niveau l'environnement d'hébergement pour les appliances virtuelles. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau de périphérique majeure.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à effectuer la mise à niveau.

Tableau 39 :

✓	Action/Vérification
	Vérifiez les configurations. Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP. Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. La désynchronisation peut entraîner l'échec de la mise à niveau. Dans les déploiements de FMC, le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, mais il convient de toujours vérifier manuellement. Pour vérifier l'heure : • FMC : choisissez **Système > Configuration > Temps**. • Périphériques : utilisez la commande **show time** de l'interface de ligne de commande.
	Vérifiez l'espace disque. Exécutez une vérification de l'espace disque pour la mise à niveau logicielle. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Consultez le chapitre *Mettre à niveau le logiciel* dans les Notes de version de Cisco Firepower de votre version cible.

✓	Action/Vérification
	Déployez des configurations. Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Dans certains déploiements, la mise à niveau peut être bloquée si vous avez des configurations obsolètes. Dans les déploiements FMC à haute disponibilité, il vous suffit de procéder au déploiement à partir de l'homologue actif. Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre Snort, ce qui interrompt l'inspection du trafic et, selon la façon dont votre périphérique gère le trafic, peut interrompre le trafic jusqu'à la fin du redémarrage. Consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.
	Exécutez la vérification de l'état de préparation. Si votre FMC exécute la version 6.1.0 ou une version ultérieure, nous recommandons de vérifier la compatibilité et l'état de préparation. Ces vérifications évaluent votre degré de préparation à une mise à niveau logicielle. Consultez Vérification de l'état de préparation du logiciel Firepower, à la page 41.
	Vérifiez les tâches en cours. Assurez-vous que les tâches essentielles sur le périphérique, y compris le déploiement final, sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Nous vous recommandons également de vérifier les tâches qui sont programmées pour s'exécuter pendant la mise à niveau et de les annuler ou de les reporter.

Mise à niveau de la série Firepower 7000/8000 et NGIPSv avec FMC

Utilisez cette procédure pour mettre à niveau les périphériques Firepower 7000/8000 Series et NGIPSv. Vous pouvez mettre à niveau plusieurs périphériques à la fois s'ils utilisent le même paquet de mise à niveau. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.

Procédure

Étape 1 (Facultatif) Modifiez les rôles actif/de secours de vos paires de périphériques à haute disponibilité qui effectuent la commutation/le routage.

Si vos paires à haute disponibilité sont déployées pour effectuer *uniquement* un contrôle d'accès, les périphériques actifs sont mis à niveau en premier. Une fois la mise à niveau terminée, les périphériques actifs et de secours conservent leurs anciens rôles.

Cependant, dans un déploiement routé ou commuté, c'est le périphérique de secours qui est d'abord mis à niveau. Les périphériques changent de rôle, puis le nouvel appareil en attente effectue la mise à niveau. Une fois la mise à niveau terminée, les rôles des périphériques restent commutés. Si vous souhaitez conserver les rôles actif/de secours, changez manuellement les rôles avant d'effectuer la mise à niveau. De cette façon, le processus de mise à niveau les rétablit.

Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur l'icône **Switch Active Peer** (Commuter l'homologue actif) à côté de la paire et confirmez votre choix.

Étape 2 Choisissez **Système** > **Mises à jour**.

Étape 3 Cliquez sur l'icône Install (Installer) à côté du paquet de mise à niveau que vous voulez utiliser, puis choisissez les périphériques à mettre à niveau.

Si les périphériques que vous souhaitez mettre à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

Remarque
Nous vous recommandons *fortement* de mettre à niveau moins de cinq périphériques simultanément à partir de la page de mise à jour du système. Vous ne pouvez pas arrêter la mise à niveau tant que tous les périphériques sélectionnés n'ont pas terminé le processus. S'il y a un problème avec la mise à niveau d'un périphérique, tous les périphériques doivent terminer la mise à niveau avant que vous puissiez résoudre le problème.

Étape 4 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Le trafic est abandonné tout au long de la mise à niveau ou traverse le réseau sans inspection, en fonction de la configuration et du déploiement de vos périphériques. Pour en savoir plus, consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.

Étape 5 Surveillez l'avancement de la mise à niveau.

Mise en garde
Ne déployez *pas* de modifications, ne redémarrez pas ou n'éteignez pas manuellement un périphérique pendant l'exécution des vérifications de l'état de préparation. Ne redémarrez *pas* une mise à niveau de périphérique en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec le Centre d'assistance technique Cisco (TAC)

Étape 6 Vérifiez la réussite de la mise à niveau.

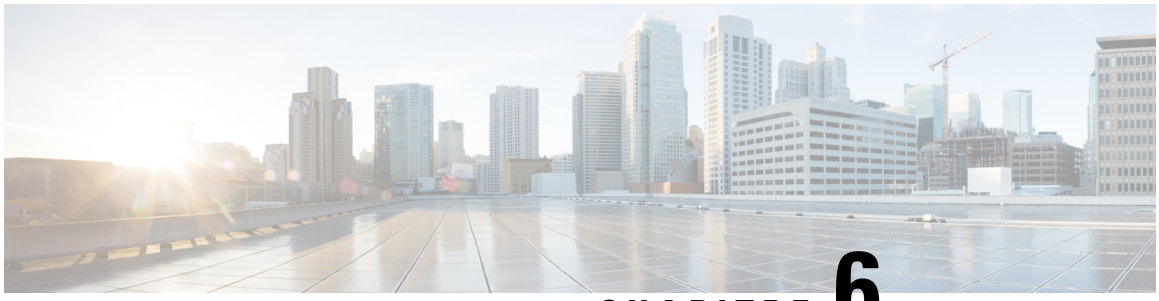
Une fois la mise à niveau terminée, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 7 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d'assistance et de téléchargement Cisco est plus récent que la version en cours d'exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 8 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 9 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.



CHAPITRE 6

Mise à niveau d'ASA avec les services FirePOWER

- Liste de vérification de mise à niveau : ASA FirePOWER avec FMC, à la page 91
- Mettre à niveau l'ASA, à la page 95
- Mettre à niveau un module ASA FirePOWER avec FMC, à la page 118

Liste de vérification de mise à niveau : ASA FirePOWER avec FMC

Terminez cette liste de contrôle avant d'effectuer la mise à niveau Pare-feu ASA avec services FirePOWER.

Remarque En tout temps pendant le processus, assurez-vous de maintenir la communication et l'intégrité de déploiement. *Ne pas* redémarrer une mise à niveau ASA FirePOWER en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec le Centre d'assistance technique Cisco (TAC)

Planification et faisabilité

Une planification et une préparation rigoureuses peuvent vous aider à éviter les erreurs.

Tableau 40 :

✓	Action/Vérification
	Planifiez votre chemin de mise à niveau. Cela est particulièrement important pour les déploiements de plusieurs appareils, les mises à niveau multisauts ou les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement, tout en maintenant la compatibilité de déploiement. Sachez toujours quelle mise à niveau vous venez d'effectuer et laquelle vous allez effectuer ensuite. **Remarque** Dans les déploiements de FMC, vous mettez généralement à niveau le FMC, puis ses périphériques gérés. Cependant, dans certains cas, vous devrez peut-être d'abord mettre à niveau les périphériques. Consultez Chemins de mise à niveau, à la page 11.
	Lisez *toutes* les directives de mise à niveau et prévoyez les modifications de configuration. Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par les notes de mise à jour, qui contiennent des renseignements essentiels et précis sur la version, notamment les avertissements de mise à niveau, les changements de comportement, les fonctionnalités nouvelles et obsolètes, ainsi que les problèmes connus.
	Vérifiez l'accès à l'appareil. Les périphériques peuvent cesser de transmettre du trafic pendant la mise à niveau (en fonction de la configuration des interfaces) ou en cas d'échec de la mise à niveau. Avant d'effectuer la mise à niveau, assurez-vous que le trafic en provenance de votre emplacement n'a pas à traverser le périphérique lui-même pour accéder à l'interface de gestion du périphérique . Dans les déploiements de FMC, vous devriez également pouvoir accéder à l'interface de gestion FMC sans traverser le périphérique.
	Vérifiez la bande passante. Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Dans les déploiements de FMC, si vous transférez un ensemble de mise à niveau vers un périphérique géré au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau ou même entraîner son expiration. Dans la mesure du possible, copiez les paquets de mise à niveau sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance. Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que la mise à niveau est susceptible de prendre. Tenez également compte des tâches que vous *devez* effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Par exemple, n'attendez pas la période de maintenance pour copier les paquets de mise à niveau sur les périphériques, exécuter des vérifications de la préparation, effectuer des sauvegardes, etc.

Progiciels de mise à niveau

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco.

Tableau 41 :

✓	Action/Vérification
	Chargez le paquet de mise à niveau vers le FMC. Consultez Charger vers Cisco Firepower Management Center, à la page 38.
	Copiez le paquet de mise à niveau sur le périphérique. Si votre instance de FMC utilise la version 6.2.3 ou une version ultérieure, nous vous recommandons de copier (*pousser*) les paquets sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. Consultez Copier des données sur les périphériques gérés, à la page 40.

Sauvegardes

La reprise après sinistre est un élément essentiel de tout plan de maintenance de système.

La sauvegarde et la restauration peuvent être des processus complexes. Vous ne voulez sauter aucune étape ou ignorer les problèmes de sécurité ou de licence. Pour en savoir plus sur les exigences, les directives, les limitations et les bonnes pratiques en matière de sauvegarde et de restauration, consultez le guide de configuration de votre déploiement.



Mise en garde Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau.

Tableau 42 :

✓	Action/Vérification
	Sauvegardez l'ASA. Utilisez ASDM ou l'interface de ligne de commande d'ASA pour sauvegarder les configurations et les autres fichiers critiques avant et après la mise à niveau, en particulier s'il y a une migration de la configuration de l'ASA.

Mises à niveau associées

Étant donné que les mises à niveau de systèmes d'exploitation et d'environnements d'hébergement peuvent avoir une incidence sur le flux de trafic et l'inspection, effectuez-les pendant une période de maintenance.

Tableau 43 :

✓	Action/Vérification
	Mettez à niveau l'ASA. Si vous le souhaitez, mettez à niveau l'ASA. Il existe une large compatibilité entre les versions d'ASA et de ASA FirePOWER. Cependant, la mise à niveau vous permet de profiter de nouvelles fonctionnalités et de la résolution de certains problèmes. Pour les périphériques ASA autonomes, mettez à niveau le module ASA FirePOWER juste *après* avoir mis à niveau l'ASA et rechargé l'unité. Dans le cas des grappes ASA et des paires de basculements, pour éviter les interruptions du flux de trafic et de l'inspection, mettez entièrement à niveau ces périphériques *un à la fois*. Mettez à niveau le module ASA FirePOWER juste *avant* de recharger chaque unité pour mettre à niveau l'ASA. **Remarque** Avant de mettre à niveau ASA, assurez-vous de lire toutes les directives de mise à niveau et de planifier les changements de configuration. Commencez par les notes de mise à jour de l'ASA : Notes de version de Cisco ASA.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à effectuer la mise à niveau.

Tableau 44 :

✓	Action/Vérification
	Vérifiez les configurations. Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP. Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. La désynchronisation peut entraîner l'échec de la mise à niveau. Dans les déploiements de FMC, le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, mais il convient de toujours vérifier manuellement. Pour vérifier l'heure : • FMC : choisissez **Système > Configuration > Temps**. • Périphériques : utilisez la commande **show time** de l'interface de ligne de commande.
	Vérifiez l'espace disque. Exécutez une vérification de l'espace disque pour la mise à niveau logicielle. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Consultez le chapitre *Mettre à niveau le logiciel* dans les Notes de version de Cisco Firepower de votre version cible.

✓	Action/Vérification
	Déployez des configurations. Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Dans certains déploiements, la mise à niveau peut être bloquée si vous avez des configurations obsolètes. Dans les déploiements FMC à haute disponibilité, il vous suffit de procéder au déploiement à partir de l'homologue actif. Lorsque vous déployez, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection. En outre, le déploiement de certaines configurations redémarre Snort, ce qui interrompt l'inspection du trafic et, selon la façon dont votre périphérique gère le trafic, peut interrompre le trafic jusqu'à la fin du redémarrage. Consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.
	Désactivez l'API REST ASA sur les anciens périphériques. Avant de mettre à niveau un module ASA FirePOWER exécutant *actuellement* la version 6.3.0 ou une version antérieure, assurez-vous que l'API REST ASA est désactivée. Sinon, la mise à niveau peut échouer. À partir de l'interface de ligne de commande d'ASA : `no rest api agent`. Vous pouvez la réactiver après la mise à niveau : `rest-api agent`.
	Exécutez la vérification de l'état de préparation. Si votre FMC exécute la version 6.1.0 ou une version ultérieure, nous recommandons de vérifier la compatibilité et l'état de préparation. Ces vérifications évaluent votre degré de préparation à une mise à niveau logicielle. Consultez Vérification de l'état de préparation du logiciel Firepower, à la page 41.
	Vérifiez les tâches en cours. Assurez-vous que les tâches essentielles sur le périphérique, y compris le déploiement final, sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Nous vous recommandons également de vérifier les tâches qui sont programmées pour s'exécuter pendant la mise à niveau et de les annuler ou de les reporter.

Mettre à niveau l'ASA

Utilisez les procédures de cette section pour mettre à niveau ASA et ASDM pour les déploiements autonomes, de basculement ou de mise en grappe.

Mettre à niveau une unité autonome

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau l'unité autonome.

Mettre à niveau une unité autonome à l'aide de l'interface de ligne de commande

Cette section décrit comment installer les images ASDM et ASA, et quand mettre à niveau le module ASA FirePOWER.

Avant de commencer

Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 En mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash.

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

Étape 2 Copiez l'image ASDM dans la mémoire flash.

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name* **disk***n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

Étape 3 Accédez au mode de configuration globale.

configure terminal

Exemple :

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Étape 4 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Exemple :

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Étape 5 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin/*]*nom_de_l_image_asa*

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Exemple :

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Étape 7 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin/*]*nom_de_l_image_asdm*

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Exemple :

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Étape 9 Rechargez l'ASA :

reload

Étape 10 Si vous mettez à niveau le module ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 11 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une unité autonome à partir de votre ordinateur local à l'aide d'ASDM

L'**outil de mise à niveau du logiciel à partir de l'ordinateur local** vous permet de charger un fichier image de votre ordinateur vers le système de fichiers flash pour mettre à niveau l'ASA.

Procédure

Étape 1 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 2 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 3 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 4 Dans le champ **Chemin d'accès au système de fichiers flash**, cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 5 Cliquez sur **Charger une image**.

Le processus de chargement peut prendre quelques minutes.

Étape 6 Vous êtes invité à définir cette image comme image ASDM. Cliquez sur **Yes** (Oui).

Étape 7 Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**.

Vous quittez l'outil **Mise à niveau**. **Remarque :** Vous enregistrerez la configuration, puis quitterez et vous reconnecterez à ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 8 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**. Vous pouvez également utiliser cette procédure pour charger d'autres types de fichiers.

Étape 9 Choisissez **Outils** > **Rechargement du système** pour recharger l'ASA.

Une nouvelle fenêtre s'affiche et vous demande de vérifier les détails du rechargement.

a) Cliquez sur le bouton radio **Enregistrer la configuration en cours d'enregistrement au moment du rechargement**.
b) Choisissez une heure de rechargement (par exemple, **Maintenant**, la valeur par défaut).
c) Cliquer sur **Planifier le rechargement**.

Une fois que le rechargement est en cours, une fenêtre **État du rechargement** s'affiche pour indiquer qu'un rechargement est en cours. Une option pour quitter ASDM est également fournie.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Étape 11 Si vous mettez à niveau un module ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande**et en entrant **no rest-api agent**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera. Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 12 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une unité autonome à l'aide de l'assistant ASDM Cisco.com

L'**assistant de mise à niveau du logiciel à partir de Cisco.com** vous permet de mettre à niveau automatiquement ASDM et ASA vers des versions plus récentes.

Dans cet assistant, vous pouvez effectuer les opérations suivantes :

- Choisissez un fichier image ASA ou un fichier image ASDM à mettre à niveau.

Remarque ASDM télécharge la dernière version de l'image, qui comprend le numéro de version. Par exemple, si vous téléchargez la version 9.9(1), le téléchargement peut inclure la version 9.9(1.2). Ce comportement est normal, vous pouvez donc procéder à la mise à niveau prévue.

- Passez en revue les modifications de mise à niveau que vous avez apportées.
- Téléchargez l'image ou les images et installez-les.
- Passez en revue l'état de l'installation.
- Si l'installation a réussi, rechargez l'ASA pour enregistrer la configuration et terminer la mise à niveau.

Avant de commencer

En raison d'une modification interne, l'assistant est uniquement pris en charge par ASDM 7.10(1) ou les versions ultérieures. De plus. Comme ASDM est rétrocompatible avec les versions d'ASA antérieures, vous pouvez mettre à niveau ASDM, quelle que soit la version d'ASA que vous utilisez.

Procédure

Étape 1 Choisissez **Outils** > **Vérifier la présence de mises à jour ASA/ASDM**.

En mode contexte multiple, accédez à ce menu à partir du système.

La boîte de dialogue **Authentification de Cisco.com** s'affiche.

Étape 2 Saisissez votre nom d'utilisateur et votre mot de passe Cisco.com, puis cliquez sur **Connexion**.

L'**assistant de mise à niveau Cisco.com** s'affiche.

Remarque
Si aucune mise à niveau n'est disponible, une boîte de dialogue s'affiche. Cliquez sur **OK** pour quitter l'assistant.

Étape 3 Cliquez sur **Suivant** pour afficher l'écran **Sélectionner un logiciel**.

La version d'ASA actuelle et la version d'ASDM s'affichent.

Étape 4 Pour mettre à niveau la version d'ASA et la version d'ASDM, procédez comme suit :

a) Dans la zone **ASA**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASA à laquelle vous souhaitez passer dans la liste déroulante.
b) Dans la zone **ASDM**, cochez la case **Mettre à niveau vers**, puis choisissez une version d'ASDM à laquelle vous souhaitez passer dans la liste déroulante.

Étape 5 Cliquez sur **Suivant** pour afficher l'écran **Passer en revue les modifications**.

Étape 6 Vérifiez les éléments suivants :

- Le fichier image ASA ou le fichier image ASDM que vous avez téléchargé est le bon.
- Le fichier image ASA ou le fichier image ASDM que vous souhaitez charger est le bon.
- La bonne image de démarrage ASA a été sélectionnée.

Étape 7 Cliquez sur **Suivant** pour lancer l'installation de la mise à niveau.

Vous pouvez ensuite afficher l'état de l'installation de la mise à niveau à mesure qu'elle progresse.

L'écran **Résultats** s'affiche, et fournit des détails supplémentaires, comme l'état de l'installation de la mise à niveau (réussite ou échec).

Étape 8 Si l'installation de la mise à niveau a réussi, pour que les versions de mise à niveau prennent effet, cochez la case **Enregistrer la configuration et recharger le périphérique maintenant** pour redémarrer l'ASA et le redémarrer ASDM.

Étape 9 Cliquez sur **Terminer** pour quitter l'assistant et enregistrer les modifications de configuration que vous avez apportées.

Remarque
Pour passer à la version ultérieure, le cas échéant, vous devez redémarrer l'assistant.

Étape 10 Après le rechargement de l'ASA, redémarrez ASDM.

Vous pouvez vérifier l'état de rechargement à partir d'un port de console, ou vous pouvez attendre quelques minutes et essayer de vous connecter à l'aide d'ASDM.

Étape 11 Si vous mettez à niveau un module ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande**et en entrant **no rest-api agent**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera. Vous pouvez la réactiver après la mise à niveau :

rest-api agent

Remarque
La série ASA 5506-X ne prend pas en charge l'API REST ASA si vous utilisez la version 6.0 du module FirePOWER ou une version ultérieure.

Étape 12 Mettez à niveau le module ASA FirePOWER.

Mettre à niveau une paire de basculements actif/de secours

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/de secours pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/de secours à l'aide de l'interface de ligne de commande

Pour mettre à niveau la paire de basculements actif/de secours, procédez comme suit.

Avant de commencer

- Exécutez ces étapes sur l'unité active. Pour l'accès SSH, connectez-vous à l'adresse IP active; l'unité active présente toujours cette adresse IP. Lorsque vous vous connectez à l'interface de ligne de commande, déterminez l'état de basculement en examinant l'invite d'ASA; vous pouvez configurer l'invite ASA pour afficher l'état et la priorité de basculement (principal ou secondaire), ce qui est utile pour déterminer à quelle unité vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show failover** pour afficher l'état et la priorité de cette unité (principale ou secondaire).
- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité active, en mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash de l'unité active :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

Étape 2 Copiez le logiciel sur l'unité de secours. Assurez-vous de définir le même chemin que pour l'unité active :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin
disk0:/asa941-smp-k8.bin
```

Étape 3 Copiez l'image ASDM dans la mémoire flash de l'unité active :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name* **disk***n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-741.bin disk0:/asdm-741.bin
```

Étape 4 Copiez l'image ASDM sur l'unité de secours. Assurez-vous de définir le même chemin que pour l'unité active :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/asdm_image_name* **disk***n***:/**[*chemin/*]*asdm_image_name*

Exemple :

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

Étape 5 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 6 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

Exemple :

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 7 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 8 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act(config)# boot system disk0://asa941-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 9 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin*/]*nom_de_l_image_asdm*

Exemple :

```
asa/act(config)# asdm image disk0:/asdm-741.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 10 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 11 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Étape 12 Mettez à niveau le module ASA FirePOWER sur l'unité de secours.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée.

Étape 13 Rechargez l'unité de secours pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité de secours ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que l'unité de secours est à l'état de secours.

Étape 14 Forcez l'unité active à basculer vers l'unité de secours.

no failover active

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP principale, maintenant sur la nouvelle unité active/ancienne unité de secours.

Étape 15 Mettez à niveau le module ASA FirePOWER sur l'ancienne unité active.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée.

Étape 16 À partir de la nouvelle unité active, rechargez l'ancienne unité active (maintenant la nouvelle unité de secours).

failover reload-standby

Exemple :

```
asa/act# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'ancienne unité active, vous devez plutôt saisir la commande **reload** pour recharger l'ancienne unité active.

Mettre à niveau une paire de basculements actif/de secours à l'aide d'ASDM

Pour mettre à niveau la paire de basculements actif/de secours, procédez comme suit.

Avant de commencer

Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *de secours* en vous connectant à l'adresse IP de secours.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASDM, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 8 Connectez ASDM à l'unité *active* en vous connectant à l'adresse IP principale et chargez le logiciel ASDM en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité de secours.

Étape 9 Lorsque vous êtes invité à définir l'image comme image ASDM, cliquez sur **Oui**.

Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé pour l'unité de secours.

Étape 11 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 12 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité de secours.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Mettez à niveau le module ASA FirePOWER sur l'unité de secours.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité active.

Étape 15 Rechargez l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité de secours.

Étape 16 Après le rechargement de l'unité de secours, forcez l'unité active à basculer vers l'unité de secours en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à la nouvelle unité active.

Étape 17 Mettez à niveau le module ASA FirePOWER sur l'ancienne unité active.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours*. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité active.

Étape 18 Rechargez l'unité de secours (nouvelle) en sélectionnant **Surveillance** > **Propriétés** > **Basculement** > **État**, puis cliquez sur **Recharger l'unité de secours**.

Mettre à niveau une paire de basculements actif/actif

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la paire de basculements actif/actif pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une paire de basculements actif/actif à l'aide de l'interface de ligne de commande

Pour mettre à niveau deux unités dans une configuration de basculement actif/actif, procédez comme suit.

Avant de commencer

- Exécutez ces étapes sur l'unité principale.
- Effectuez ces étapes dans l'espace d'exécution du système.
- Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Procédure

Étape 1 Sur l'unité principale, en mode d'exécution privilégié, copiez le logiciel ASA dans la mémoire flash :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

Étape 2 Copiez le logiciel sur l'unité secondaire. Assurez-vous de définir le même chemin que pour l'unité principale :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[*/chemin*]*/nom_de_l_image_asa* **disk***n***:/**[*chemin/*]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin
```

```
disk0:/asa941-smp-k8.bin
```

Étape 3 Copiez l'image ASDM dans la mémoire flash de l'unité principale :

copy ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*asdm_image_name* **disk***n***:/**[*chemin*/]*asdm_image_name*

Exemple :

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-741.bin disk0:/asdm-741.bin
```

Étape 4 Copiez l'image ASDM sur l'unité secondaire. Assurez-vous de définir le même chemin que pour l'unité principale :

failover exec mate copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*asdm_image_name* **disk***n***:/**[*chemin*/]*asdm_image_name*

Exemple :

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

Étape 5 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y :

configure terminal

Étape 6 Affichez les images de démarrage actuelles configurées (jusqu'à 4) :

show running-config boot system

Exemple :

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 7 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 8 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/act/pri(config)# boot system disk0://asa941-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 9 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n*:/[*chemin*/]*nom_de_l_image_asdm*

Exemple :

```
asa/act/pri(config)# asdm image disk0:/asdm-741.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 10 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 11 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau échouera.

no rest-api agent

Étape 12 Activez les deux groupes de basculement sur l'unité principale :

failover active group 1

failover active group 2

Exemple :

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

Étape 13 Mettez à niveau le module ASA FirePOWER sur l'unité secondaire.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée.

Étape 14 Rechargez l'unité secondaire pour démarrer la nouvelle image :

failover reload-standby

Attendez que l'unité secondaire ait terminé le chargement. Utilisez la commande **show failover** pour vérifier que les deux groupes de basculement sont à l'état de secours.

Étape 15 Forcez les deux groupes de basculement à devenir actifs sur l'unité secondaire :

no failover active group 1

no failover active group 2

Exemple :

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
```

```
asa/stby/pri(config)#
```

Si vous êtes déconnecté de votre session SSH, reconnectez-vous à l'adresse IP du groupe de basculement 1, maintenant sur l'unité secondaire.

Étape 16 Mettez à niveau le module ASA FirePOWER sur l'unité principale.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée.

Étape 17 Rechargez l'unité principale :

failover reload-standby

Exemple :

```
asa/act/sec# failover reload-standby
```

Remarque
Si vous êtes connecté au port de console de l'unité principale, vous devez plutôt saisir la commande **reload** pour recharger l'unité principale.

Il se peut que vous soyez déconnecté de votre session SSH.

Étape 18 Si les groupes de basculement sont configurés avec la commande **preempt**, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé.

Mettre à niveau une paire de basculements actif/actif à l'aide d'ASDM

Pour mettre à niveau deux unités dans une configuration de basculement actif/actif, procédez comme suit.

Avant de commencer

- Effectuez ces étapes dans l'espace d'exécution du système.
- Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *secondaire* en vous connectant à l'adresse de gestion dans le groupe de basculement 2.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 3 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 4 Dans le champ **Chemin d'accès au fichier local**, saisissez le chemin d'accès local au fichier sur votre ordinateur ou cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 5 Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Étape 6 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Lorsque vous êtes invité à définir cette image comme image ASDM, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 7 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Lorsque vous êtes invité à définir cette image comme image ASA, cliquez sur **Non**. Vous quittez l'outil Mise à niveau.

Étape 8 Connectez ASDM à l'unité *principale* en vous connectant à l'adresse IP de gestion dans le groupe de basculement 1 et chargez le logiciel ASDM en utilisant le même emplacement de fichier que vous avez utilisé sur l'unité secondaire.

Étape 9 Lorsque vous êtes invité à définir l'image comme image ASDM, cliquez sur **Oui**.

Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Chargez le logiciel ASA en utilisant le même emplacement de fichier que vous avez utilisé pour l'unité secondaire.

Étape 11 Lorsque vous êtes invité à définir l'image comme image ASA, cliquez sur **Oui**.

Il vous est rappelé de recharger l'ASA pour utiliser la nouvelle image. Cliquez sur **OK**. Vous quittez l'outil Mise à niveau.

Étape 12 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur l'unité secondaire.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Activez les deux groupes de basculement sur l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité principale, puis cliquez sur **Faire passer en groupe actif**.

Étape 15 Mettez à niveau le module ASA FirePOWER sur l'unité secondaire.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité principale.

Étape 16 Rechargez l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Restez dans le volet **Système** pour surveiller le rechargement de l'unité secondaire.

Étape 17 Après le déploiement de l'unité secondaire, activez les deux groupes de basculement sur l'unité secondaire en sélectionnant **Surveillance** > **Basculement** > **Groupe de basculement #**, où **#** est le numéro du groupe de basculement que vous souhaitez déplacer dans l'unité secondaire, puis cliquez sur **Faire passer en groupe de secours**.

ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité secondaire.

Étape 18 Mettez à niveau le module ASA FirePOWER sur l'unité principale.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *de secours* du groupe de basculement 1 ou 2. Attendez que la mise à niveau soit terminée, puis reconnectez ASDM à l'unité secondaire.

Étape 19 Rechargez l'unité principale en sélectionnant **Surveillance** > **Basculement** > **Système**, puis cliquez sur **Recharger l'unité de secours**.

Étape 20 Si les groupes de basculement sont configurés avec la préemption activée, ils deviennent automatiquement actifs sur l'unité désignée une fois le délai de préemption écoulé. ASDM se reconnectera automatiquement à l'adresse IP du groupe de basculement 1 sur l'unité principale.

Mettre à niveau une grappe ASA

Utilisez l'interface de ligne de commande ou ASDM pour mettre à niveau la grappe ASA pour une mise à niveau sans temps d'arrêt.

Mettre à niveau une grappe ASA à l'aide de l'interface de ligne de commande

Pour mettre à niveau toutes les unités d'une grappe ASA, suivez les étapes suivantes. Cette procédure utilise le protocole FTP. Pour TFTP, HTTP ou d'autres types de serveurs, consultez la commande **copy** dans la référence de commande ASA.

Avant de commencer

- Exécutez ces étapes sur l'unité de contrôle. Si vous mettez également à niveau le module ASA FirePOWER, vous avez besoin d'un accès à la console ou à ASDM sur chaque unité de données. Vous pouvez configurer l'invite ASA pour afficher l'unité de la grappe et son état (contrôle ou données), ce qui est utile pour déterminer à quelle unité vous êtes connecté. Consultez la commande d'invite. Vous pouvez également saisir la commande **show cluster info** pour afficher le rôle de chaque unité.
- Vous devez utiliser le port de console; vous ne pouvez pas activer ni désactiver la mise en grappe à partir d'une connexion distante d'interface de ligne de commande.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.

Procédure

Étape 1 Sur l'unité de contrôle en mode d'exécution privilégié, copiez le logiciel ASA sur toutes les unités de la grappe.

cluster exec copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*nom_de_l_image_asa* **disk***n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa941-smp-k8.bin disk0:/asa941-smp-k8.bin
```

Étape 2 Copiez l'image ASDM sur toutes les unités de la grappe :

cluster exec copy /noconfirm ftp://[[*utilisateur*[**:***mot de passe*]**@**]*serveur*[/*chemin*]/*asdm_image_name* **disk***n***:/**[*chemin*/]*asdm_image_name*

Exemple :

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-741.bin
disk0:/asdm-741.bin
```

Étape 3 Si vous n'êtes pas déjà en mode de configuration globale, accédez-y maintenant.

configure terminal

Exemple :

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

Étape 4 Affichez les images de démarrage actuelles configurées (jusqu'à 4).

show running-config boot system

Exemple :

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

L'ASA utilise les images dans l'ordre indiqué; si la première image n'est pas disponible, l'image suivante est utilisée, et ainsi de suite. Vous ne pouvez pas insérer une nouvelle URL d'image en haut de la liste. Pour placer la nouvelle image en première position, vous devez supprimer toutes les entrées existantes et saisir les URL d'image dans l'ordre souhaité, en fonction des étapes suivantes.

Étape 5 Supprimez toutes les configurations d'image de démarrage existantes afin de pouvoir utiliser la nouvelle image de démarrage comme votre premier choix :

no boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

Étape 6 Définissez l'image ASA à démarrer (celle que vous venez de charger) :

boot system disk*n***:/**[*chemin*/]*nom_de_l_image_asa*

Exemple :

```
asa/unit1/master(config)# boot system disk0://asa941-smp-k8.bin
```

Répétez cette commande pour toutes les images de sauvegarde que vous souhaitez utiliser au cas où cette image ne serait pas disponible. Par exemple, vous pouvez réintroduire les images que vous avez précédemment supprimées.

Étape 7 Définissez l'image ASDM à utiliser (celle que vous venez de charger) :

asdm image disk*n***:/**[*chemin*/]*nom_de_l_image_asdm*

Exemple :

```
asa/unit1/master(config)# asdm image disk0:/asdm-741.bin
```

Vous ne pouvez configurer qu'une seule image ASDM à utiliser, vous n'avez donc pas besoin de supprimer la configuration existante en premier lieu.

Étape 8 Enregistrez les nouveaux paramètres dans la configuration de démarrage :

write memory

Ces modifications de configuration sont automatiquement enregistrées sur les unités de données.

Étape 9 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA, sinon la mise à niveau du module ASA FirePOWER échouera.

no rest-api agent

Étape 10 Si vous mettez à niveau des modules ASA FirePOWER gérés par ASDM, vous devrez connecter ASDM aux adresses IP de gestion *individuelles*, vous devez donc noter les adresses IP de chaque unité.

show running-config interface *ID_d_interface_de_gestion*

Notez le nom de regroupement **cluster-pool** utilisé.

show ip[**v6**] **local pool** *nom_de_regroupement*

Notez les adresses IP de l'unité de grappe.

Exemple :

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

Étape 11 Mettez à niveau les unités de données.

Choisissez la procédure ci-dessous selon que vous mettez également à niveau des modules ASA FirePOWER. Les procédures ASA FirePOWER réduisent le nombre de rechargements de l'ASA lors de la mise à niveau du module ASA FirePOWER. Vous pouvez choisir d'utiliser la console de données ou ASDM pour ces procédures. Vous pouvez utiliser le module ASDM à la place de la console si vous n'avez pas accès à tous les ports de la console, mais que vous pouvez atteindre le module ASDM par le réseau.

Remarque
Pendant le processus de mise à niveau, n'utilisez jamais la commande **cluster master unit** pour forcer une unité de données à devenir l'unité de contrôle; vous pouvez causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez d'abord mettre à niveau et recharger toutes les unités de données, puis poursuivre cette procédure pour assurer une transition harmonieuse de l'unité de contrôle actuelle vers une nouvelle unité de contrôle.

Si aucune mise à niveau du module ASA FirePOWER ne vous est proposée :

a) Sur l'unité de contrôle, pour afficher les noms de membre, saisissez **cluster exec unit ?**, ou saisissez la commande **show cluster info**.

b) Rechargez une unité de données.

cluster exec unit *unité_de_données* **reload noconfirm**

Exemple :

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, saisissez **show cluster info**.

Si une mise à niveau du module ASA FirePOWER vous est proposée (à l'aide de la console de données) :

a) Connectez-vous au port de console d'une unité de données et passez en mode de configuration globale.

enable

configure terminal

Exemple :

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) Désactivez la mise en grappe.

cluster group *name*

no enable

N'enregistrez pas cette configuration; vous voulez que la mise en grappe soit activée lorsque vous rechargez le nœud. Vous devez désactiver la mise en grappe pour éviter plusieurs défaillances et renouvellements pendant le processus de mise à niveau; cette unité ne doit se joindre qu'une fois la mise à niveau et le rechargement terminés.

Exemple :

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) Mettez à niveau le module ASA FirePOWER sur cette unité de données.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *individuelle* que vous avez notée plus tôt. Attendez que la mise à niveau soit terminée.

d) Rechargez l'unité de données.

reload noconfirm

e) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, saisissez **show cluster info**.

Si une mise à niveau du module ASA FirePOWER vous est proposée (à l'aide d'ASDM) :

a) Connectez ASDM à l'adresse IP de gestion *individuelle* de cette unité de données que vous avez notée plus tôt.
b) Choisissez **Configuration** > **Device Management High Availability and Scalability (Gestion des périphériques Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de la grappe)** > **.**
c) Décochez la case **Participer à la grappe ASA**.

Vous devez désactiver la mise en grappe pour éviter plusieurs défaillances et renouvellements pendant le processus de mise à niveau; cette unité ne doit se joindre qu'une fois la mise à niveau et le rechargement terminés.

Ne décochez pas la case **Configurer les paramètres de grappe ASA**. Cette action efface toute la configuration de la grappe et désactive également toutes les interfaces, y compris l'interface de gestion à laquelle ASDM est connecté. Pour rétablir la connectivité dans ce cas, vous devez accéder à l'interface de ligne de commande au niveau du port de console.

Remarque
Certaines anciennes versions d'ASDM ne prennent pas en charge la désactivation de la grappe sur cet écran; dans ce cas, utilisez l'outil **Outils** > **Interface de ligne de commande**, cliquez sur le bouton radio **Ligne multiple**, puis entrez **cluster group** *nom* et **no enable**. Vous pouvez afficher le nom du groupe de grappes dans la zone **Home (Accueil)** > **Device Dashboard (Tableau de bord du périphérique)** > **Device Information (Renseignements sur le périphérique)** > **ASA Cluster (Grappe ASA)**.

d) Cliquez sur **Apply**.
e) Vous êtes invité à quitter ASDM. Reconnectez ASDM à la même adresse IP.
f) Mettez à niveau le module ASA FirePOWER.

Attendez que la mise à niveau soit terminée.

g) Dans ASDM, choisissez **Outils** > **Rechargement du système**.
h) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

i) Cliquer sur **Planifier le rechargement**.
j) Cliquez sur **Oui** pour poursuivre le rechargement.
k) Répétez l'opération pour chaque unité de données.

Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**de l'unité de contrôle.

Étape 12 Mettez à niveau l'unité de contrôle.

a) Désactivez la mise en grappe.

cluster group *name*

no enable

Attendez 5 minutes qu'une nouvelle unité de contrôle soit sélectionnée et que le trafic se stabilise.

N'enregistrez pas cette configuration; vous voulez que la mise en grappe soit activée lorsque vous rechargez le nœud.

Nous vous recommandons de désactiver manuellement la grappe sur l'unité de contrôle si possible afin qu'une nouvelle unité de contrôle puisse être choisie aussi rapidement et proprement que possible.

Exemple :

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either
enable clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Mettez à niveau le module ASA FirePOWER sur cette unité.

Pour un module ASA FirePOWER géré par ASDM, connectez ASDM à l'adresse IP de gestion *individuelle* que vous avez notée plus tôt. L'adresse IP de la grappe principale appartient maintenant à la nouvelle unité de contrôle. Cette ancienne unité de contrôle est toujours accessible sur son adresse IP de gestion individuelle.

Attendez que la mise à niveau soit terminée.

c) Rechargez cette unité.

reload noconfirm

Lorsque l'ancienne unité de contrôle rejoint la grappe, elle devient une unité de données.

Mettre à niveau une grappe ASA à l'aide d'ASDM

Pour mettre à niveau toutes les unités d'une grappe ASA, suivez les étapes suivantes.

Avant de commencer

- Exécutez ces étapes sur l'unité de contrôle. Si vous mettez également à niveau le module ASA FirePOWER, vous avez besoin d'un accès à ASDM sur chaque unité de données.
- Effectuez ces étapes dans l'espace d'exécution du système pour le mode contexte multiple.
- Placez les images ASA et ASDM sur votre ordinateur de gestion local.

Procédure

Étape 1 Lancez ASDM sur l'unité *de contrôle* en vous connectant à l'adresse IP principale de la grappe.

Cette adresse IP reste toujours avec l'unité de contrôle.

Étape 2 Dans la fenêtre d'application ASDM principale, choisissez **Outils** > **Mettre à niveau le logiciel à partir de l'ordinateur local**.

La boîte de dialogue **Mettre à niveau le logiciel à partir de l'ordinateur local** s'affiche.

Étape 3 Cliquez sur le bouton radio **All devices in the cluster** (Tous les périphériques de la grappe).

La boîte de dialogue **Mettre à niveau le logiciel** s'affiche.

Étape 4 Dans la liste déroulante **Image à charger**, sélectionnez **ASDM**.

Étape 5 Dans le champ **Chemin d'accès au fichier local**, cliquez sur **Parcourir les fichiers locaux** pour trouver le fichier sur votre ordinateur.

Étape 6 (Facultatif) Dans le champ **Chemin d'accès au système de fichiers flash**, saisissez le chemin d'accès au système de fichiers flash ou cliquez sur **Parcourir la mémoire flash** pour trouver le répertoire ou le fichier dans le système de fichiers flash.

Par défaut, ce champ est prérempli avec le chemin suivant : **disk0:/***filename*.

Étape 7 Cliquez sur **Charger une image**. Le processus de chargement peut prendre quelques minutes.

Étape 8 Vous êtes invité à définir cette image comme image ASDM. Cliquez sur **Yes** (Oui).

Étape 9 Il vous est rappellé de quitter ASDM et d'enregistrer la configuration. Cliquez sur **OK**.

Vous quittez l'outil Mise à niveau. **Remarque :** Vous enregistrerez la configuration et rechargerez ASDM *après* avoir mis à niveau le logiciel ASA.

Étape 10 Répétez ces étapes, en sélectionnant **ASA** dans la liste déroulante **Image à charger**.

Étape 11 Cliquez sur l'icône **Enregistrer** dans la barre d'outils pour enregistrer les modifications apportées à la configuration.

Ces modifications de configuration sont automatiquement enregistrées sur les unités de données.

Étape 12 Notez les adresses IP de gestion individuelles pour chaque unité dans la section **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)** afin de pouvoir connecter ASDM directement aux unités de données ultérieurement.

Étape 13 Si vous mettez à niveau des modules ASA FirePOWER, désactivez l'API REST ASA en sélectionnant **Outils** > **Interface de ligne de commande** et en saisissant **no rest-api enable**.

Si vous ne désactivez pas l'API REST, la mise à niveau du module ASA FirePOWER échouera.

Étape 14 Mettez à niveau les unités de données.

Choisissez la procédure ci-dessous selon que vous mettez également à niveau des modules ASA FirePOWER. La procédure ASA FirePOWER réduit le nombre de rechargements de l'ASA lors de la mise à niveau du module ASA FirePOWER.

Remarque
Pendant le processus de mise à niveau, ne modifiez jamais l'unité de contrôle à l'aide de la page **Surveillance** > **Grappe ASA** > **Résumé de la grappe** pour forcer une unité de données à devenir l'unité de contrôle; vous pouvez

causer des problèmes de connectivité au réseau et de stabilité de grappe. Vous devez d'abord recharger toutes les unités de données, puis poursuivre cette procédure pour assurer une transition harmonieuse de l'unité de contrôle actuelle vers une nouvelle unité de contrôle.

Si aucune mise à niveau du module ASA FirePOWER ne vous est proposée :

a) Sur l'unité de contrôle, choisissez **Outils** > **Rechargement du système**.
b) Choisissez un nom d'unité de données dans la liste déroulante **Périphérique**.
c) Cliquer sur **Planifier le rechargement**.
d) Cliquez sur **Oui** pour poursuivre le rechargement.
e) Répétez l'opération pour chaque unité de données.

   Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**.

Si une mise à niveau du module ASA FirePOWER vous est proposée :

a) Sur l'unité de contrôle, choisissez la section **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Members (Membres de la grappe)**.
b) Sélectionnez l'unité de données que vous souhaitez mettre à niveau, et cliquez sur **Supprimer**.
c) Cliquez sur **Apply**.
d) Quittez ASDM et connectez ASDM à l'unité de données en vous connectant à son adresse IP de gestion *individuelle* que vous avez notée plus tôt.
e) Mettez à niveau le module ASA FirePOWER.

   Attendez que la mise à niveau soit terminée.

f) Dans ASDM, choisissez **Outils** > **Rechargement du système**.
g) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

   Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

h) Cliquer sur **Planifier le rechargement**.
i) Cliquez sur **Oui** pour poursuivre le rechargement.
j) Répétez l'opération pour chaque unité de données.

   Pour éviter les interruptions de connexion et permettre au trafic de se stabiliser, attendez que chaque unité soit de nouveau opérationnelle et rejoigne la grappe (environ 5 minutes) avant de répéter ces étapes pour l'unité suivante. Pour savoir quand une unité rejoint la grappe, consultez le volet **Surveillance** > **Grappe ASA** > **Résumé de la grappe**.

Étape 15 Mettez à niveau l'unité de contrôle.

a) Dans ASDM, sur l'unité de contrôle, choisissez le volet **Configuration** > **Device Management (Gestion des périphériques)** > **High Availability and Scalability (Haute disponibilité et évolutivité)** > **ASA Cluster (Grappe ASA)** > **Cluster Configuration (Configuration de grappe)**.
b) Décochez la case **Participer à la grappe ASA**, puis cliquez sur **Appliquer**.

   Vous êtes invité à quitter ASDM.

c) Attendez jusqu'à 5 minutes qu'une nouvelle unité de contrôle soit sélectionnée et que le trafic se stabilise.

Lorsque l'ancienne unité de contrôle rejoint la grappe, elle devient une unité de données.

d) Reconnectez ASDM à l'ancienne unité de contrôle en vous connectant à son adresse IP de gestion *individuelle* que vous avez notée plus tôt.

   L'adresse IP de la grappe principale appartient maintenant à la nouvelle unité de contrôle. Cette ancienne unité de contrôle est toujours accessible sur son adresse IP de gestion individuelle.

e) Mettez à niveau le module ASA FirePOWER.

   Attendez que la mise à niveau soit terminée.

f) Choisissez **Outils** > **Rechargement du système**.

g) Cliquez sur le bouton radio **Recharger sans enregistrer la configuration en cours**.

   Il ne faut pas sauvegarder la configuration. Lorsque cette unité sera rechargée, vous voudrez que la mise en grappe soit activée sur cette unité.

h) Cliquer sur **Planifier le rechargement**.

i) Cliquez sur **Oui** pour poursuivre le rechargement.

   Vous êtes invité à quitter ASDM. Redémarrez ASDM sur l'adresse IP de la grappe principale. Vous vous reconnecterez à la nouvelle unité de contrôle.

Mettre à niveau un module ASA FirePOWER avec FMC

Utilisez cette procédure pour mettre à niveau un Module ASA FirePOWER géré par un FMC. Le moment où vous mettez à niveau le module dépend de la mise à niveau d'ASA et de votre déploiement d'ASA.

- Périphériques ASA autonomes : si vous mettez également à niveau l'ASA, mettez à niveau le Module ASA FirePOWER juste *après* avoir mis à niveau l'ASA et rechargé l'unité.
- Grappes ASA et paires de basculements : pour éviter les interruptions du flux de trafic et de l'inspection, mettez entièrement à niveau ces périphériques *un à la fois*. Si vous mettez également à niveau l'ASA, mettez à niveau le Module ASA FirePOWER juste *avant* de recharger chaque unité pour mettre à niveau l'ASA.

Pour en savoir plus, consultez Chemin de mise à niveau : ASA FirePOWER, à la page 22 et les procédures de mise à niveau de l'ASA.

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.

Procédure

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

Étape 2 Cliquez sur l'icône Install (Installer) à côté du paquet de mise à niveau que vous voulez utiliser, puis choisissez les périphériques à mettre à niveau.

Si les périphériques que vous souhaitez mettre à niveau ne sont pas répertoriés, vous avez choisi le mauvais paquet de mise à niveau.

Remarque
Nous vous recommandons *fortement* de mettre à niveau moins de cinq périphériques simultanément à partir de la page de mise à jour du système. Vous ne pouvez pas arrêter la mise à niveau tant que tous les périphériques sélectionnés n'ont pas terminé le processus. S'il y a un problème avec la mise à niveau d'un périphérique, tous les périphériques doivent terminer la mise à niveau avant que vous puissiez résoudre le problème.

Étape 3 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Le trafic est abandonné tout au long de la mise à niveau ou traverse le réseau sans inspection, en fonction de la configuration et du déploiement de vos périphériques. Pour en savoir plus, consultez le chapitre *Mettre à niveau le logiciel* dans le Notes de version de Cisco Firepower de votre version cible.

Étape 4 Surveillez l'avancement de la mise à niveau.

Mise en garde
Ne déployez *pas* de modifications, ne redémarrez pas ou n'éteignez pas manuellement un périphérique pendant l'exécution des vérifications de l'état de préparation. Ne redémarrez *pas* une mise à niveau de périphérique en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec le Centre d'assistance technique Cisco (TAC)

Étape 5 Vérifiez la réussite de la mise à niveau.

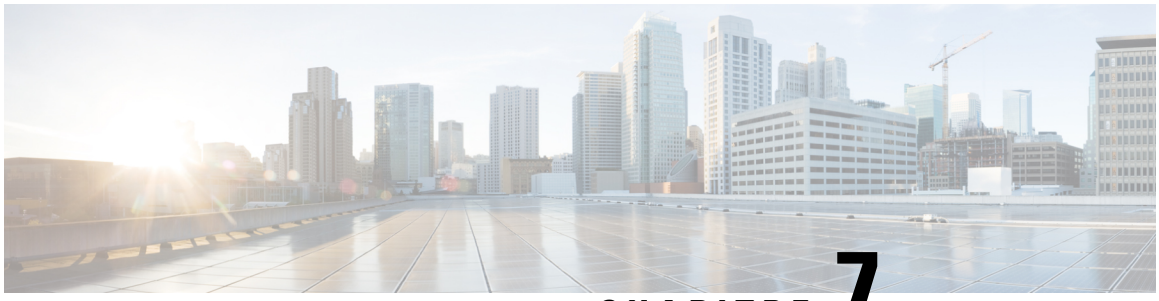
Une fois la mise à niveau terminée, choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** et confirmez que les périphériques que vous avez mis à niveau disposent de la bonne version de logiciel.

Étape 6 Mettez à jour les règles de prévention des intrusions (SRU/LSP) et la base de données des vulnérabilités (VDB).

Si le composant disponible sur Site d'assistance et de téléchargement Cisco est plus récent que la version en cours d'exécution, installez la version la plus récente. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 7 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 8 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.



CHAPITRE 7

Désinstaller un correctif

Vous pouvez désinstaller la plupart des correctifs. Si vous devez revenir à une version majeure ou de maintenance antérieure, vous devez effectuer une réinitialisation.

La désinstallation d'un correctif vous renvoie à la version à partir de laquelle vous avez mis à niveau et ne modifie pas les configurations. Étant donné que le FMC doit exécuter la même version ou une version plus récente que ses périphériques gérés, désinstallez d'abord les correctifs de ces périphériques. La désinstallation n'est pas prise en charge pour les correctifs rapides .

- Correctifs qui prennent en charge la désinstallation, à la page 121
- Ordre de désinstallation pour la haute disponibilité/évolutivité, à la page 124
- Désinstaller les périphériques Threat Defense avec le FMC, à la page 126
- Désinstaller les correctifs FMC autonomes , à la page 128
- Désinstaller les correctifs de haute disponibilité FMC, à la page 129

Correctifs qui prennent en charge la désinstallation

La désinstallation de correctifs spécifiques peut entraîner des problèmes, *même lorsque la désinstallation elle-même réussit*. Ces problèmes comprennent :

- Impossibilité de déployer les modifications de configuration après la désinstallation.
- Incompatibilités entre le système d'exploitation et le logiciel.
- Échec du FSIC (contrôle de l'intégrité du système de fichiers) lorsque le périphérique redémarre, si vous avez appliqué des correctifs avec la conformité des certifications de sécurité activée (mode CC/UCAPL).

⚠

Mise en garde Si la conformité aux certifications de sécurité est activée et que le FSIC échoue, le logiciel ne démarre pas, l'accès SSH à distance est désactivé et vous ne pouvez accéder au périphérique qu'à partir de la console locale. Dans ce cas, communiquez avec Centre d'assistance technique Cisco (TAC).

Correctifs de la version 7.0 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 7.0. La désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 45 : Correctifs de la version 7.0 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller		
	FTD/FTDv	ASA FirePOWER NGIPSv	FMC/FMCv
7.0.6.2 et ultérieures	7.0.6	7.0.6.1	7.0.6.1
7.0.6.1	7.0.6	—	—

Correctifs de la version 6.7 qui prennent en charge la désinstallation

La désinstallation est actuellement prise en charge pour tous les correctifs de la version 6.7.

Correctifs de la version 6.6 qui prennent en charge la désinstallation

La désinstallation est actuellement prise en charge pour tous les correctifs de la version 6.6.

Correctifs de la version 6.5 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 6.5. La désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 46 : Correctifs de la version 6.5.0 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller		
	FTD/FTDv	ASA FirePOWER NGIPSv	FMC/FMCv
6.5.0.2 et ultérieures	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

Correctifs de la version 6.4 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 6.4. La désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 47 : Correctifs de la version 6.4.0 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.4.0.5 et ultérieures	6.4.0.4	6.4.0.4	6.4.0.4
6.4.0.4	—	—	—
6.4.0.3	6.4.0	—	—
6.4.0.2	6.4.0	—	—
6.4.0.1	6.4.0	6.4.0	6.4.0

Correctifs de la version 6.3 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 6.3. La désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 48 : Correctifs de la version 6.3.0 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller
6.3.0.5	—
De la version 6.3.0.1 à la version 6.3.0.4	6.3.0

Correctifs de la version 6.2.3 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 6.2.3. La désinstallation vous ramène au niveau de correctif à partir duquel vous avez effectué la mise à niveau. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 49 : Correctifs de la version 6.2.3 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.2.3.16 et ultérieures	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	—	—	—

Version actuelle	Version la plus ancienne à désinstaller		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
De la version 6.2.3.12 à la version 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11
6.2.3.11	6.2.3	—	—
De la version 6.2.3.8 à la version 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7
6.2.3.7	6.2.3	—	—
De la version 6.2.3.1 à la version 6.2.3.6	6.2.3	6.2.3	6.2.3

Correctifs de la version 6.2.2 qui prennent en charge la désinstallation

Ce tableau répertorie les scénarios de désinstallation pris en charge pour les correctifs de la version 6.2.2. La désinstallation vous renvoie au correctif immédiatement précédent, même si vous avez effectué une mise à niveau à partir d'un correctif antérieur. Si la désinstallation vous amène plus loin que ce qui est pris en charge, nous vous recommandons de réinitialiser l'image, puis de la mettre à niveau au niveau de correctif souhaité.

Tableau 50 : Correctifs de la version 6.2.2 qui prennent en charge la désinstallation

Version actuelle	Version la plus ancienne à désinstaller
De la version 6.2.2.3 à la version 6.2.2.5	6.2.2.2
6.2.2.2	—
6.2.2.1	6.2.2

Ordre de désinstallation pour la haute disponibilité/évolutivité

Dans les déploiements à haute disponibilité/évolutivité, limitez les perturbations liées à la désinstallation d'un périphérique à la fois. Contrairement à la mise à niveau, le système ne le fait pas pour vous. Attendez que le correctif soit entièrement désinstallé d'une unité avant de passer à l'autre.

Tableau 51 : Ordre de désinstallation pour la haute disponibilité FMC

Configuration	Ordre de désinstallation
FMC Haute disponibilité	La synchronisation étant en pause, qui est un état appelé *split-brain* (déconnexion cérébrale), désinstallez des pairs à la fois. Ne pas effectuer ou déployer de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale) **1.** Suspendez la synchronisation (entrez dans l'état split-brain). **2.** Désinstallez du périphérique en veille. **3.** Désinstallez du périphérique actif. **4.** Redémarrez la synchronisation (sortez de l'état split-brain).

Tableau 52 : Ordre de désinstallation pour la haute disponibilité et les grappes FTD

Configuration	Ordre de désinstallation
FTD Haute disponibilité	Vous ne pouvez pas désinstaller un correctif des périphériques configurés pour la haute disponibilité. Vous devez d'abord interrompre la haute disponibilité. **1.** Rompre la haute accessibilité **2.** Désinstallez de l'ancien périphérique en veille. **3.** Désinstallez de l'ancien périphérique actif. **4.** Rétablissez la haute disponibilité.
grappe FTD	Désinstallez d'une unité à la fois, en laissant l'unité de contrôle pour la fin. Les unités en grappe fonctionnent en mode maintenance pendant que le correctif est désinstallé. **1.** Désinstallez des modules de données un à la fois. **2.** Faites de l'un des modules de données le nouveau module de contrôle. **3.** Désinstallez de l'ancien module de contrôle.

Tableau 53 : Ordre de désinstallation pour l'ASA avec les services FirePOWER dans les paires de basculement/grappes ASA

Configuration	Ordre de désinstallation
Paire de basculement ASA actif/veille, avec ASA FirePOWER	Désinstallez toujours du périphérique en veille. **1.** Désinstallez du module ASA FirePOWER sur le périphérique ASA en veille. **2.** Effectuez le basculement. **3.** Désinstallez du module ASA FirePOWER sur le nouveau périphérique ASA en veille.

Configuration	Ordre de désinstallation
Paire de basculement ASA actif/actif, avec ASA FirePOWER	Activez les deux groupes de basculement sur l'unité que vous ne désinstallez pas. **1.** Activez les deux groupes de basculement sur le périphérique ASA principal. **2.** Désinstallez du module ASA FirePOWER sur le périphérique ASA secondaire. **3.** Activez les deux groupes de basculement sur le périphérique ASA secondaire. **4.** Désinstallez du module ASA FirePOWER sur le périphérique ASA principal.
Grappe ASA, avec ASA FirePOWER	Désactivez la mise en grappe sur chaque unité avant d'effectuer la désinstallation. Désinstallez d'une unité à la fois, en laissant l'unité de contrôle pour la fin. **1.** Sur une unité de données, désactivez la mise en grappe. **2.** Désinstallez du module ASA FirePOWER sur cette unité. **3.** Réactivez la mise en grappe. Attendez que l'unité rejoigne la grappe. **4.** Répétez l'opération pour chaque unité de données. **5.** Sur une unité de contrôle, désactivez la mise en grappe. Attendez qu'une nouvelle unité de contrôle prenne le relais. **6.** Désinstallez du module ASA FirePOWER sur l'ancienne unité de contrôle. **7.** Réactivez la mise en grappe.

Désinstaller les périphériques Threat Defense avec le FMC

Utilisez l'interface Shell Linux (*mode expert*) pour désinstaller les correctifs. Vous devez avoir accès à l'interface Shell du périphérique en tant qu'utilisateur `administrateur` du périphérique ou en tant qu'autre utilisateur local avec accès à la configuration de l'interface de ligne de commande. Vous ne pouvez pas utiliser un compte d'utilisateur FMC. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.



Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Rompre les FTD les paires à haute accessibilité ; voir Ordre de désinstallation pour la haute disponibilité/évolutivité, à la page 124.

• Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Si les configurations du périphérique sont obsolètes, déployez maintenant à partir du FMC.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec. Assurez-vous que le déploiement et les autres tâches essentielles sont terminés. Les tâches en cours d'exécution au début de la désinstallation sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être reprises. Vous pouvez supprimer les messages d'état d'échec manuellement ultérieurement.

Étape 2 Accédez à l'interface de ligne de commande Firepower sur le périphérique Connectez-vous en tant qu'`administrateur` ou en tant qu'autre utilisateur de l'interface de ligne de commande avec accès à la configuration.

Vous pouvez vous connecter en SSH à l'interface de gestion du périphérique (nom de domaine ou adresse IP) ou utiliser la console. Si vous utilisez la console, certains périphériques utilisent l'interface de ligne de commande du système d'exploitation et nécessitent une étape supplémentaire pour accéder à l'interface de ligne de commande Firepower, comme indiqué dans le tableau ci-après.

Série Firepower 1000	`connect ftd`
Série Firepower 2100	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, puis `connect ftd` (première connexion uniquement)
ASA FirePOWER	`session sfr`

Étape 3 Utilisez la commande `expert` pour accéder à l'interface Shell Linux.

Étape 4 Vérifiez que le paquet de désinstallation se trouve dans le répertoire de mise à niveau.

```
ls /var/sf/updates
```

Les désinstallations de correctifs sont nommées comme les paquets de mise à niveau, mais ont `Patch_Uninstaller` au lieu de `Patch` dans le nom de fichier. Lorsque vous utilisez le correctif pour un périphérique, la désinstallation de ce correctif est automatiquement créée dans le répertoire de mise à niveau. Si le programme de désinstallation n'est pas présent, communiquez avec Centre d'assistance technique Cisco (TAC).

Étape 5 Exécutez la commande de désinstallation et saisissez votre mot de passe lorsque vous y êtes invité.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Mise en garde
Le système ne vous demande *pas* de confirmer. La saisie de cette commande démarre la désinstallation, qui comprend un redémarrage du périphérique. Les interruptions du flux de trafic et de l'inspection au cours d'une désinstallation sont identiques aux interruptions qui se produisent lors d'une mise à niveau. Assurez-vous d'être prêt. Remarque : l'utilisation de l'option `--detach` garantit que le processus de désinstallation n'est pas interrompu si votre session SSH expire, ce qui peut laisser le périphérique dans un état instable.

Étape 6 Surveillez la désinstallation jusqu'à ce que vous soyez déconnecté.

Pour une désinstallation dissociée, utilisez `tail` ou `tailf` pour afficher les journaux :

• FTD : `tail /ngfw/var/log/sf/update.status`

- ASA FirePOWER et NGIPSv : `tail /var/log/sf/update.status`

Sinon, surveillez la progression dans la console ou le terminal.

Étape 7 Vérifiez la réussite de la désinstallation.

Une fois la désinstallation terminée, vérifiez que les périphériques disposent de la bonne version du logiciel. Dans le FMC, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.

Étape 8 Dans les déploiements à haute disponibilité/évolutivité, répétez les étapes 2 à 6 pour chaque unité.

Pour les grappes, ne désinstallez jamais de l'unité de contrôle. Après avoir désinstallé de toutes les unités de données, faites de l'une d'elles le nouveau contrôle, puis désinstallez de l'ancien contrôle.

Étape 9 Redéployez les configurations.

Exception : Ne déployez pas sur des paires à haute accessibilité de version mixte ou des grappes de périphériques. Déployez avant de désinstaller le correctif du premier périphérique, mais pas à nouveau avant d'avoir désinstallé le correctif de tous les membres du groupe.

Prochaine étape

- Pour la haute disponibilité, rétablissez la haute disponibilité.
- Pour les grappes, si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Désinstaller les correctifs FMC autonomes

Nous vous recommandons d'utiliser l'interface Web pour désinstaller les correctifs FMC. Si vous ne pouvez pas utiliser l'interface Web , vous pouvez utiliser l'interface Shell Linux comme utilisateur `administrateur` de l'interface Shell ou en tant qu'utilisateur externe avec accès à l'interface Shell. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.

⚠

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Si la désinstallation place le FMC à un niveau de correctif inférieur à celui de ses périphériques gérés, désinstallez d'abord les correctifs de ces périphériques.
- Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Déployez vers les périphériques gérés dont les configurations ne sont pas à jour.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec.

Étape 2 Sous Available Updates (Mises à jour disponibles), cliquez sur l'icône **Install** (installer) à côté du paquet de mise à niveau, puis choisissez le FMC.

Les désinstallations de correctifs sont nommées comme les paquets de mise à niveau, mais ont `Patch_Uninstaller` au lieu de `Patch` dans le nom de fichier. Lorsque vous appliquez un correctif au FMC, la désinstallation de ce correctif est automatiquement créée dans le répertoire de mise à niveau. Si le programme de désinstallation n'est pas présent, communiquez avec Centre d'assistance technique Cisco (TAC).

Étape 3 Cliquez sur **Install (installer)**, puis confirmez que vous souhaitez désinstaller et redémarrer.

Vous pouvez surveiller la progression de la désinstallation dans le centre de messages jusqu'à ce que vous soyez déconnecté.

Étape 4 Reconnectez-vous quand vous le pouvez et vérifiez que la désinstallation a réussi.

Si le système ne vous informe pas de la réussite de la désinstallation lorsque vous vous connectez, choisissez **Help (Aide)** > **About (À propos)** pour afficher les informations sur la version actuelle du logiciel.

Étape 5 Déployez de nouveau les configurations sur tous les appareils gérés.

Désinstaller les correctifs de haute disponibilité FMC

Privilégiez l'interface Web pour désinstaller les correctifs FMC. Si vous ne pouvez pas utiliser l'interface Web , vous pouvez utiliser l'interface Shell Linux comme utilisateur `administrateur` de l'interface Shell ou en tant qu'utilisateur externe avec accès à l'interface Shell. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.

Désinstallez des pairs de haute disponibilité un à la fois. Une fois que la synchronisation est interrompue, désinstallez d'abord sur l'unité de secours, puis l'unité active. Lorsque le périphérique de secours commence la désinstallation, son état passe de « de secours » à « actif », de sorte que les deux homologues sont actifs. Cet état temporaire s'appelle *split-brain* (déconnexion cérébrale) et *n'est pas* pris en charge, sauf pendant une mise à niveau ou une désinstallation.



Mise en garde Ne pas effectuer ou déployer de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale) Vos modifications seront perdues après le redémarrage de la synchronisation. Le déploiement de pourrait placer le système dans un état inutilisable et nécessiter une recréation d'image. Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Si la désinstallation place les FMC à un niveau de correctif inférieur à celui de leurs périphériques gérés, désinstallez d'abord les correctifs sur les périphériques.
- Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Sur le FMC actif, déployez vers les périphériques gérés dont la configuration n'est pas à jour.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec.

Étape 2 Sur le FMC actif, suspendez la synchronisation.

a) Choisissez **System (Système)** ⚙) > **Integration (Intégration)**.
b) Sous l'onglet **High Availability**, cliquez sur **Suspendre la synchronisation**.

Étape 3 Désinstallez le correctif sur les homologues un à la fois : d'abord l'homologue de secours, puis l'homologue actif.

Suivez les instructions dans Désinstaller les correctifs FMC autonomes , à la page 128, mais omettez le déploiement initial et arrêtez-vous après avoir vérifié, pour chaque homologue, la réussite de la désinstallation. En résumé, pour chaque homologue :

a) Dans la page **System (Système)** > **Updates (Mises à jour)**, désinstallez le correctif.
b) Surveillez la progression jusqu'à ce que vous soyez déconnecté, puis reconnectez-vous lorsque vous le pouvez.
c) Vérifiez la réussite de la désinstallation.

Étape 4 Sur le FMC que vous souhaitez définir comme homologue actif, redémarrez la synchronisation.

a) Choisissez **System (Système)** ⚙) > **Integration (Intégration)**.
b) Sous l'onglet **High Availability (haute disponibilité)**, cliquez sur **Make-Me-Active** (Rendez-moi actif).
c) Attendez que la synchronisation redémarre et que l'autre FMC passe en mode veille.

Étape 5 Déployez de nouveau les configurations sur tous les appareils gérés.

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.