Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Device Manager, version 7.2

Dernière modification : 2025-08-11

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

© 2022–2025 Cisco Systems, Inc. Tous droits réservés.

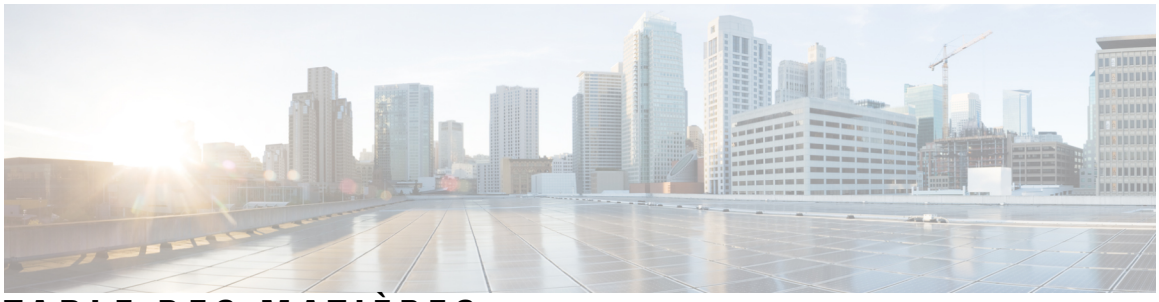
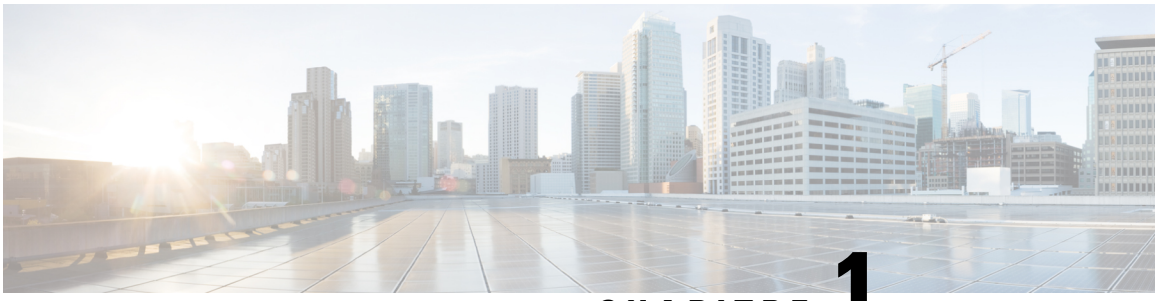


TABLE DES MATIÈRES



CHAPITRE 1

Pour commencer

Ce guide est-il pour vous?

Ce guide explique comment préparer et terminer une mise à niveau réussie de **Cisco Secure Firewall Threat Defense** avec un **Cisco Secure Firewall device manager** exécutant actuellement **Version 7.2**.

Les mises à niveau peuvent être majeures (A.x), de maintenance (A.x.y) ou de correctifs (A.x.y.z). Nous pouvons également fournir des correctifs rapides, qui sont des mises à jour mineures qui traitent de problèmes particuliers et urgents.

Ressources supplémentaires

Si vous mettez à niveau une autre plateforme ou un autre composant, effectuez une mise à niveau vers ou depuis une autre version ou utilisez un gestionnaire basé sur le nuage, consultez l'une de ces ressources.

Tableau 1 : Guides de mise à niveau pour Centre de gestion

Version actuelle de Centre de gestion	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 Défense contre les menaces avec Centre de gestion

Version actuelle de Centre de gestion	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 Défense contre les menaces avec Gestionnaire d'appareil

Version actuelle de Défense contre les menaces	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 : 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 centre de gestion	Notes de mise à jour du correctif Cisco Secure Firewall Threat Defense/Firepower

Version	Composant	Guide
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

Planification de votre 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 relatifs à la mise à niveau.

Tableau 5 : 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.
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 le micrologiciel sur le Firepower 4100/9300. Mettez à niveau FXOS sur le Firepower 4100/9300.

Phase de planification	Y compris :
Contrôle final	Vérifiez les configurations. Vérifiez la synchronisation NTP. Déployez des configurations. Exécutez la vérification de l'état de préparation. Vérifiez l'espace disque. Vérifiez les tâches en cours. Vérifiez l'intégrité et les communications dans le déploiement.

Historique des fonctionnalités de mise à niveau

Tableau 6 : Fonctionnalités de la version 7.0.0

Caractéristiques	Détails
Vérification de l'état de préparation à la mise à niveau pour les périphériques gérés par Firewall Device Manager.	Vous pouvez exécuter une vérification de l'état de préparation à la mise à niveau sur un ensemble de mise à niveau Firewall Threat Defense téléchargé avant de tenter de l'installer. La vérification de l'état de préparation vérifie que la mise à niveau est valide pour le système et que le système répond aux autres exigences nécessaires à l'installation du paquet. L'exécution d'une vérification de l'état de préparation à la mise à niveau vous permet d'éviter les échecs d'installation. Un lien pour exécuter la vérification de l'état de préparation à la mise à niveau a été ajouté à la section **System Upgrade (Mise à niveau du système)** de la page **Device (Périphérique)** > **Updates (Mises à jour)**.

Tableau 7 : Fonctionnalités de la version 6.7.0

Caractéristiques	Détails
Possibilité d'annuler une mise à niveau logicielle de Firewall Threat Defense ayant échoué et de revenir à la version précédente.	Si une mise à niveau logicielle majeure Firewall Threat Defense échoue ou ne fonctionne pas correctement, vous pouvez rétablir l'état du périphérique tel qu'il était lorsque vous avez installé la mise à niveau. Nous avons ajouté la possibilité de rétablir la mise à niveau au panneau de mise à niveau du système dans FDM. Lors d'une mise à niveau, l'écran de connexion FDM affiche l'état de la mise à niveau et vous donne la possibilité de l'annuler ou de revenir en arrière en cas d'échec de la mise à niveau. Dans l'API Firewall Threat Defense, nous avons ajouté les ressourcesCanCal Upgrade, RevertUPgrade, RetryUPgrade et UpgradeRevertInfo. Dans l'interface de ligne de commande Firewall Threat Defense, nous avons ajouté les commandes suivantes : **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.

Tableau 8 : Fonctionnalités de la version 6.2.0

Caractéristiques	Détails
Mettre à niveau le logiciel Firewall Threat Defense au moyen de Firewall Device Manager.	Vous pouvez installer les mises à niveau logicielles au moyen de Firewall Device Manager. Sélectionnez **Périphérique** > **Mettre à jour**.

Pour de l'assistance

Guides de mise à niveau

Dans les déploiements de centre de gestion, le centre de gestion doit exécuter une version de maintenance (le troisième chiffre) identique ou plus récente que celle de ses périphériques gérés. Pour la mise à niveau, commencez par le centre de gestion, puis passez aux périphériques. Utilisez le guide de mise à niveau de la version que vous utilisez *actuellement*, et non celui de votre version cible.

Tableau 9 : Guides de mise à niveau

Plateforme	Guide de mise à niveau	Lien
Centre de gestion	Version du centre de gestion que vous utilisez *actuellement*.	https://cisco.com/go/fmc-upgrade
Threat Defense avec centre de gestion	Version du centre de gestion que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fmc-upgrade
Threat Defense avec gestionnaire de périphérique	Version de Threat Defense que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fdm-upgrade
Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage).	https://cisco.com/go/ftd-cdfmc-upgrade

Guides d'installation

Si vous ne pouvez pas ou ne souhaitez pas effectuer de mise à niveau, vous pouvez installer les versions majeures et de maintenance les plus récentes. C'est ce que l'on appelle la *recréation d'image*. Cette procédure ne peut pas s'appliquer à un correctif. Installez la version majeure ou de maintenance appropriée, puis appliquez le correctif. Si vous procédez à une recréation d'image vers une version antérieure de Threat Defense sur un périphérique FXOS, une recréation d'image complète est nécessaire, y compris pour les périphériques où le système d'exploitation et le logiciel sont combinés.

Tableau 10 : Guides d'installation

Plateforme	Guide d'installation	Lien
Matériel du centre de gestion	Guide de démarrage du modèle de centre de gestion matériel.	https://cisco.com/go/fmc-install

Plateforme	Guide d'installation	Lien
Centre de gestion virtuel	Guide de démarrage du centre de gestion virtuel.	https://cisco.com/go/fmcv-quick
Threat Defense - Matériel	Guide de démarrage ou de recréation d'image relatif à votre modèle de périphérique.	https://cisco.com/go/ftd-quick
Threat Defense - Virtuel	Guide de démarrage de votre version virtuelle de Threat Defense.	https://cisco.com/go/ftdv-quick
FXOS pour Cisco Firepower 4100/9300	Guide de configuration de votre version de FXOS, chapitre *Gestion des images*.	https://cisco.com/go/firepower9300-config
FXOS pour Cisco Firepower 1000/2100 et Secure Firewall 3100	Guide de dépannage, chapitre *Procédures de récréation d'image*.	Guide de dépannage Cisco FXOS pour le Firepower 1000/2100 et Secure Firewall 3100/4200 avec Firepower Threat Defense

Autres ressources en ligne

Cisco fournit des ressources en ligne suivantes pour télécharger de la documentation, des logiciels et des outils, pour rechercher des bogues et pour ouvrir des demandes de service. Utilisez ces ressources pour installer et configurer le logiciel Cisco, ainsi que pour résoudre les problèmes techniques.

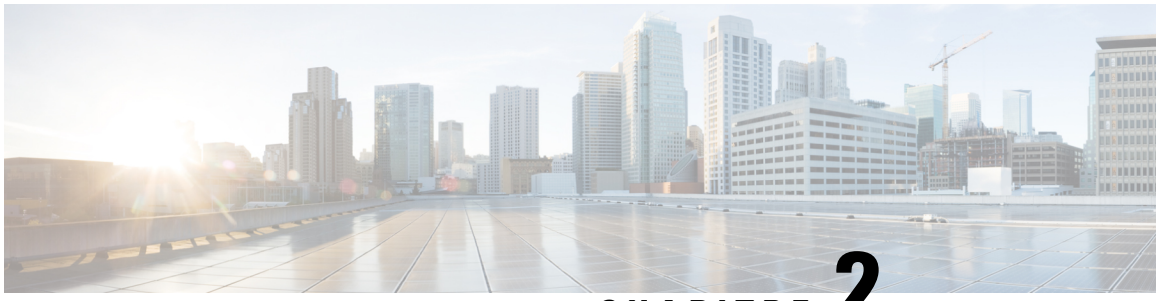
- Documentation : https://cisco.com/go/threatdefense-72-docs
- Site d'assistance et de téléchargement Cisco : https://cisco.com/c/en/us/support/index.html
- Outil de recherche de bogues de Cisco : https://tools.cisco.com/bugsearch/
- Service de notification de Cisco : https://cisco.com/cisco/support/notifications.html

Vous devez posséder un identifiant utilisateur et un mot de passe sur Cisco.com pour pouvoir accéder à la plupart des outils du Site d'assistance et de téléchargement Cisco.

Communiquez avec Cisco

Si vous ne pouvez pas résoudre un problème à l'aide des ressources en ligne répertoriées ci-dessus, communiquez avec :Centre d'assistance technique Cisco (TAC)

- Courriel Centre d'assistance technique Cisco (TAC) : tac@cisco.com
- Composez le Centre d'assistance technique Cisco (TAC) (Amérique du Nord) : 1.408.526.7209 ou 1.800.553.2447
- Appelez le Centre d'assistance technique Cisco (TAC) (monde entier) : Contacts d'assistance Cisco dans le monde



CHAPITRE 2

Configuration système requise

Ce document comprend la configuration système requise pour Version 7.2.

PlateformesDéfense contre les menaces

Les périphériquesThreat Defense surveillent le trafic réseau et décident s'il faut autoriser ou bloquer un trafic spécifique en fonction d'un ensemble défini de règles de sécurité. Pour en savoir plus sur les méthodes de gestion des périphériques, consultez Gestion du Défense contre les menaces, à la page 9. Pour des informations générales sur la compatibilité, consultez Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Matériel Défense contre les menaces

Le matériel Version 7.2défense contre les menaces est proposé en divers débits, capacités d'évolutivité et tailles.

Tableau 11 : Matériel Version 7.2 Défense contre les menaces

Plateforme	Compatibilité Centre de gestion		Compatibilité Gestionnaire d'appareil		Notes
	Déployé par le client	Envoyé par nuage	Gestionnaire d'appareil uniquement	Gestionnaire d'appareil + CDO	
Firepower 1010E, 1010, 1120, 1140, 1150	OUI	OUI	OUI	OUI	Firepower 1010E nécessite la version 7.2.3 ou ultérieures.
Firepower 2110, 2120, 2130, 2140	OUI	OUI	OUI	OUI	—
Secure Firewall3110, 3120, 3130, 3140	OUI	OUI	OUI	OUI	—

Plateforme	Compatibilité Centre de gestion		Compatibilité Gestionnaire d'appareil		Notes
	Déployé par le client	Envoyé par nuage	Gestionnaire d'appareil uniquement	Gestionnaire d'appareil + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300 : modules SM-24, SM-36 et SM-44 Firepower 9300 : modules SM-40, SM-48 et SM-56	OUI	OUI	OUI	OUI	nécessite la version FXOS 2.12.0.31 ou ultérieure. Nous vous recommandons d'utiliser le micrologiciel le plus récent. Consultez la section CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS.
ISA 3000	OUI	OUI	OUI	OUI	Peut nécessiter une mise à jour de ROMMON. Consultez la section Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense.

Défense contre les menaces virtuelles

Les implémentations de Version 7.2 défense contre les menaces virtuelles prennent en charge le Smart Software Licensing à plusieurs niveaux de performance, en fonction des exigences de débit et des limites des sessions VPN d'accès à distance. Les options vont de FTDv5 (100 Mbit/s/50 sessions) à FTDv100 (16 Gbit/s/10 000 sessions). Pour en savoir plus sur les instances prises en charge, les débits et les autres exigences d'hébergement, consultez le *guide de démarrage* approprié.

Tableau 12 : Plateformes Version 7.2 Défense contre les menaces virtuelles

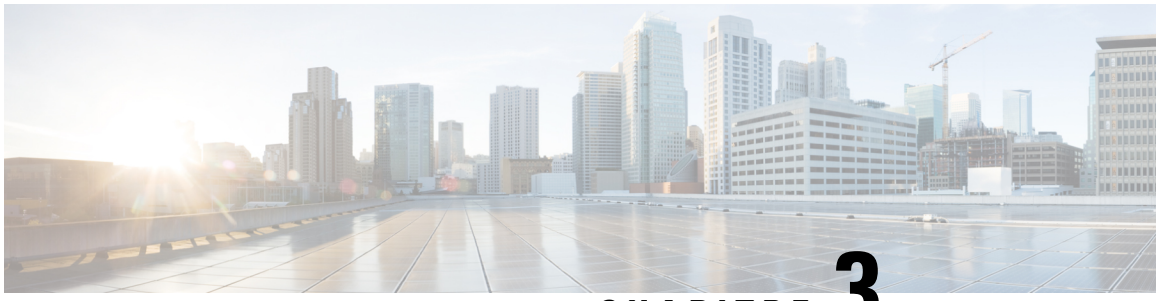
Plateforme du périphérique	Compatibilité Centre de gestion		Compatibilité Gestionnaire d'appareil	
	Déployé par le client	Envoyé par nuage	Gestionnaire d'appareil uniquement	Gestionnaire d'appareil + CDO
Nuage public				
Amazon Web Services (AWS)	OUI	OUI	OUI	OUI
Microsoft Azure	OUI	OUI	OUI	OUI
Google Cloud Platform (GCP)	OUI	OUI	OUI	OUI

Plateforme du périphérique	Compatibilité Centre de gestion		Compatibilité Gestionnaire d'appareil	
	Déployé par le client	Envoyé par nuage	Gestionnaire d'appareil uniquement	Gestionnaire d'appareil + CDO
Oracle Cloud Infrastructure (OCI)	OUI	OUI	—	—
Nuage privé				
Cisco Hyperflex	OUI	OUI	OUI	OUI
Machine virtuelle basée sur le noyau (KVM)	OUI	OUI	OUI	OUI
Nutanix Enterprise Cloud	OUI	OUI	OUI	OUI
OpenStack	OUI	OUI	—	—
VMware vSphere/VMware ESXi 6.5, 6.7 ou 7.0	OUI	OUI	OUI	OUI

Gestion du Défense contre les menaces

Vous pouvez utiliser gestionnaire d'appareil pour gérer localement un seul périphérique défense contre les menaces . La plupart des modèles prennent en charge la gestion locale.

Si vous le souhaitez, ajoutez Cisco Security Cloud Control pour gérer à distance plusieurs périphériques défense contre les menaces , au lieu de centre de gestion. Bien que certaines configurations nécessitent toujours gestionnaire d'appareil, Security Cloud Control vous permet d'établir et de maintenir des politiques de sécurité cohérentes dans votre déploiement de défense contre les menaces .



CHAPITRE 3

Directives relatives aux mises à niveau logicielles

Pour plus de commodité, ce document duplique les directives relatives aux mises à niveau logicielles critiques et spécifiques aux versions publiées dans les notes de mise à jour défense contre les menaces . Pour connaître les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300, consultez Directives de mise à niveau pour le châssis Firepower 4100/9300, à la page 17.

Important Vous devez quand même lire les notes de mise à jour, qui peuvent contenir des informations supplémentaires essentielles et spécifiques à la version. Par exemple, les fonctionnalités nouvelles et obsolètes peuvent nécessiter des modifications de configuration avant ou après la mise à niveau, ou même empêcher la mise à niveau. Des problèmes connus (bogues ouverts) peuvent influer sur la mise à niveau.

Version minimale pour la mise à niveau

Version minimale pour la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers Version 7.2, y compris les versions de maintenance, comme suit.

Tableau 13 : Version minimale pour la mise à niveau vers Version 7.2

Plateforme	Version minimale
Firewall Threat Defense	6.6 FXOS 2.12.0.31 est requis pour les périphériques Firepower 4100/9300. Dans la plupart des cas, nous vous recommandons d'utiliser la dernière version de FXOS dans chaque version principale. Pour vous aider à prendre une décision, consultez Notes de mise à jour de Cisco Firepower 4100/9300 FXOS, 2.12.

Version minimale pour les correctifs.

Les correctifs modifient *uniquement* le quatrième chiffre . Vous ne pouvez pas effectuer de mise à niveau directement vers un correctif à partir d'une version majeure ou d'une version de maintenance précédente.

Directives de mise à niveau pour Version 7.2

Ces listes de contrôle fournissent des directives de mise à niveau nouvelles et/ou déjà publiées qui peuvent vous concerner.

Tableau 14 : Directives de mise à niveau pour Défense contre les menaces avec Gestionnaire d'appareil Version 7.2

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
TOUJOURS VÉRIFIER				
	Version minimale pour la mise à niveau, à la page 11	N'importe lequel	N'importe lequel	N'importe lequel
	Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version, pour les fonctionnalités nouvelles et obsolètes qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions entre votre version actuelle et la version cible.	N'importe lequel	N'importe lequel	N'importe lequel
	Cisco Secure Firewall Threat Defense Notes de mise à jour, dans le chapitre *Bogues ouverts et résolus*, pour les bogues qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions des notes de mise à jour entre votre version actuelle et la version cible.	N'importe lequel	N'importe lequel	N'importe lequel
	Directives de mise à niveau pour le châssis Firepower 4100/9300, à la page 17	Firepower 4100/9300	N'importe lequel	N'importe lequel

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
DIRECTIVES SUPPLÉMENTAIRES POUR LES DÉPLOIEMENTS SPÉCIFIQUES				
	Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides, à la page 13	Firepower 1010	De la version 6.4.0 à la version 6.6.x	6.7+

Échec de la mise à niveau : ports de commutation du Firepower 1010 avec des identifiants VLAN non valides

Déploiements : Firepower 1010

Mise à niveau à partir de : de la version 6.4 à la version 6.6

Directement vers : version 6.7 et versions ultérieures

Pour le Firepower 1010, les mises à niveau de défense contre les menaces vers la version 6.7 ou une version ultérieure échoueront si vous avez configuré des ports de commutation avec un identifiant de VLAN compris entre 3968 et 4047. Ces identifiants sont destinés à un usage interne uniquement.

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..

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. Utilisez le panneau de mise à niveau du système ou l'interface de ligne de commande défense contre les menaces . Notez que cette fonctionnalité est uniquement prise en charge pour les mises à niveau *à partir de* (et non vers) la version 6.7.0 ou ultérieure.

Remarque Par défaut, défense contre les menaces 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, 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.

Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces

Mises à niveau logicielles

Le trafic est abandonné pendant la mise à niveau. Dans un déploiement à haute disponibilité, vous pouvez minimiser les perturbations en mettant à niveau les périphériques un à la fois.

Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique achève son redémarrage après la mise à niveau.

Restauration logicielle (versions majeures et de maintenance)

Le trafic est abandonné pendant la restauration. Dans le cadre d'un déploiement à haute disponibilité, la restauration est plus efficace lorsque les deux unités sont restaurées simultanément. Le flux de trafic et l'inspection reprennent lorsque la première unité est remise en ligne.

Déploiement des modifications de configuration

Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Il ne redémarre pas pendant d'autres déploiements, sauf si, avant le déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

Temps et espace disque

Délai de mise à niveau

Nous vous recommandons de suivre et d'enregistrer vos propres délais de mise à niveau afin de pouvoir les utiliser comme références futures. Le tableau suivant répertorie certaines éléments qui peuvent influer sur le délai de mise à niveau.

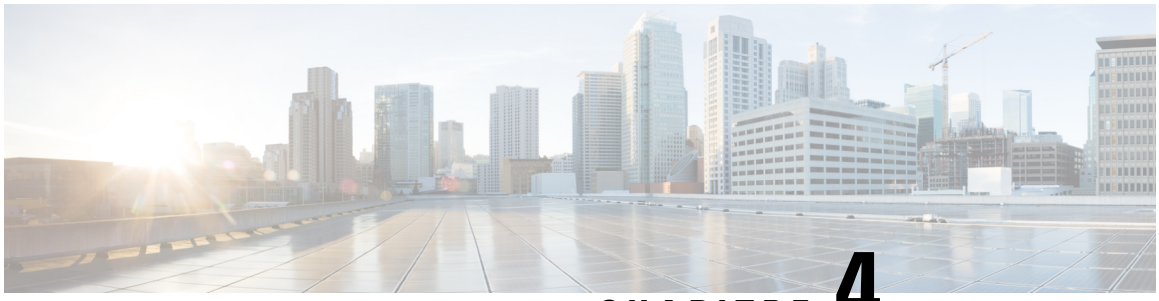
Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système 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, voir Dépannage des mises à niveau de Threat Defense , à la page 55.

Tableau 15 : Remarques concernant le délai de mise à niveau

Éléments à prendre en compte	Détails
Versions	Le délai de mise à niveau augmente généralement si votre mise à niveau ignore des versions.
Modèles	Le délai de mise à niveau augmente généralement avec les modèles inférieurs.
Appliances virtuelles	Le délai de mise à niveau dans les déploiements virtuels dépend fortement du matériel.
Haute disponibilité	Dans une configuration à haute disponibilité, 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 prend plus de temps que la mise à niveau d'un périphérique autonome.
Configurations	Le délai de mise à niveau peut augmenter en fonction de la complexité de vos configurations et de l'incidence de la mise à niveau. 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	Vous pourriez avoir besoin de plus de temps pour effectuer des mises à niveau de systèmes d'exploitation ou d'hébergement virtuel, des transferts de paquets de mise à niveau, des vérifications de l'état de préparation, des mises à jour de la VDB et des règles de prévention des intrusions (SRU/LSP), du déploiement de la configuration et d'autres tâches connexes.

Espace disque à mettre à niveau

Pour mettre à niveau, le paquet de mise à niveau doit se trouver sur le périphérique. Les vérifications de l'état de préparation doivent indiquer si vous disposez d'un espace disque suffisant pour effectuer la mise à niveau. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Pour vérifier l'espace disque, utilisez la commande **show disk** de l'interface de ligne de commande.



CHAPITRE 4

Mettre à niveau le châssis sur le Firepower 4100/9300

Notes de mise à jour de Cisco Firepower 4100/9300 FXOS, 2.12

Progiciels de mise à niveau pour FXOS

les images FXOS et les mises à jour de micrologiciel sont disponibles sur le Site d'assistance et de téléchargement Cisco :

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

Pour trouver la bonne image FXOS, sélectionnez ou recherchez votre modèle d'appareil et parcourez la page de téléchargement de *Firepower Extensible Operating System* correspondant à la version FXOS souhaitée. L'image FXOS est répertoriée avec les paquets de récupération et de MIB. Si vous devez mettre à niveau le micrologiciel, ces paquets se trouvent sous *All Releases (Toutes les versions) > Firmware (Micrologiciel)*.

Les paquets sont les suivants :

- Image Firepower 4100/9300 FXOS : fxos-k9.*fxos_version*.SPA
- Micrologiciel de la gamme Firepower 4100 : fxos-k9-fpr4k-firmware.*firmware_version*.SPA
- Micrologiciel Firepower 9300 : fxos-k9-fpr9k-firmware.*firmware_version*.SPA

Directives de mise à niveau pour le châssis Firepower 4100/9300

Pour les périphériques Firepower 4100/9300, les mises à niveau défense contre les menaces majeures nécessitent également une mise à niveau du châssis (FXOS et micrologiciel). La version de maintenance et

les correctifs l'exigent occasionnellement, mais vous pouvez toujours effectuer une mise à niveau vers la dernière version pour profiter des problèmes résolus.

Tableau 16 : Directives de mise à niveau pour le châssis Firepower 4100/9300

Directives	Détails
Mises à niveau de FXOS.	FXOS 2.12.0.31+ est requis pour exécuter la défense contre les menaces Version 7.2 sur Firepower 4100/9300. Vous pouvez effectuer une mise à niveau vers toute version FXOS ultérieure dès la version FXOS 2.2.2. Pour connaître les directives de mise à niveau critiques et spécifiques aux versions, les fonctionnalités nouvelles et obsolètes, ainsi que les bogues ouverts et résolus, consultez le Notes de version Cisco Firepower 4100/9300 FXOS.
Mises à niveau du micrologiciel.	Les mises à niveau de FXOS 2.14.1 et ultérieures comprennent le micrologiciel. Si vous effectuez une mise à niveau vers une version FXOS antérieure, consultez le CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS.
Délai de mise à niveau.	La mise à niveau du châssis peut prendre jusqu'à 45 minutes et peut affecter le flux de trafic et l'inspection. Pour en savoir plus, consultez Flux de trafic et inspection pour les mises à niveau de châssis, à la page 18.
Ordre de mise à niveau du châssis avec Défense contre les menaces haute disponibilité/évolutivité.	Dans les déploiements à haute disponibilité, vous pouvez mettre à niveau FXOS sur chaque châssis indépendamment. Pour réduire au minimum les perturbations, mettez à niveau FXOS un châssis à la fois. Vous devez également mettre à niveau les périphériques défense contre les menaces à la fois. Pour en savoir plus, consultez Ordre de mise à niveau pour FXOS avec Défense contre les menaces haute disponibilité, à la page 23.
Ordre de mise à niveau du châssis avec les périphériques logiques Défense contre les menaces et ASA.	Si vous avez des périphériques logiques défense contre les menaces *et* ASA configurés sur Firepower 9300, utilisez les procédures de ce chapitre pour mettre à niveau FXOS et défense contre les menaces . Assurez-vous que la mise à niveau de FXOS ne provoque pas d'incompatibilité avec l'un ou l'autre type de périphérique logique; voir Chemin de mise à niveau pour FXOS avec Défense contre les menaces et ASA, à la page 21. Pour les procédures de mise à niveau d'ASA, consultez le Guide de mise à niveau de Cisco Secure Firewall ASA.
Mise à niveau du châssis sans périphérique logique.	Si vous n'avez pas configuré de périphérique logique, utilisez les procédures du présent chapitre pour mettre à niveau FXOS sur des périphériques défense contre les menaces autonomes, en ne tenant pas compte des instructions sur les périphériques logiques. Ou effectuez une réimage complète du châssis en fonction de la version FXOS dont vous avez besoin.

Flux de trafic et inspection pour les mises à niveau de châssis

La mise à niveau de FXOS redémarre le châssis. Pour les mises à niveau FXOS vers la version 2.14.1+ qui incluent des mises à niveau du micrologiciel, le périphérique redémarre deux fois, une fois pour FXOS et une autre pour le micrologiciel.

Même dans les déploiements à disponibilité, vous pouvez mettre à niveau FXOS sur chaque châssis indépendamment. Pour réduire au minimum les perturbations, mettez à niveau un châssis à la fois.Pour plus de renseignements, consultez Ordre de mise à niveau pour FXOS avec Défense contre les menaces haute disponibilité, à la page 23.

Tableau 17 : Flux de trafic et inspection : mises à niveau de FXOS

Défense contre les menacesDéploiement	Comportement du trafic	Méthode
Autonomes	Abandonné.	—
Haute disponibilité	Non affecté.	**Bonnes pratiques :** mettez à jour FXOS sur le système en veille, changez les pairs actifs, mettez à niveau le nouveau système en veille.
	Abandonné jusqu'à ce qu'un pair soit en ligne.	Mettez à niveau FXOS sur le pair actif avant que le système en veille ait terminé la mise à niveau.

Chemins de mise à niveau pour FXOS

Choisissez le chemin de mise à niveau qui correspond à votre déploiement.

Chemin de mise à niveau pour FXOS avec Défense contre les menaces

Ce tableau fournit le chemin de mise à niveau pour défense contre les menaces sur le Firepower 4100/9300.

Notez que si votre version actuelle défense contre les menaces 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 de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Ce tableau répertorie nos combinaisons de versions spécialement qualifiées. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez brièvement une combinaison prise en charge, mais non recommandée, dans laquelle le système d'exploitation est « en avance » sur le logiciel du périphérique. Assurez-vous que la mise à niveau de FXOS ne vous rend pas compatible avec des périphériques logiques. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Tableau 18 : Défense contre les menaces Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Threat Defense 7.3	→ FXOS 2.13 avec toute version ultérieure de Threat Defense 7.3.x

Versions actuelles	Versions cibles
FXOS 2.12 avec Threat Defense 7.2 Dernière prise en charge de Firepower 4110, 4120, 4140, 4150. Dernière prise en charge de l'appareil Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Threat Defense 7.2.x
FXOS 2.11.1 avec Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Threat Defense 7.1.x
FXOS 2.10.1 avec Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Threat Defense 7.0.x **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+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.
FXOS 2.9.1 avec Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Threat Defense 6.7.x

Versions actuelles	Versions cibles
FXOS 2.8.1 avec Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Threat Defense 6.6.x
FXOS 2.7.1 avec Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec Threat Defense 6.6.x

Chemin de mise à niveau pour FXOS avec Défense contre les menaces et ASA

Ce tableau indique les chemins de mise à niveau pour le Firepower 9300 avec des périphériques logiques défense contre les menaces et ASA exécutés sur des modules distincts.

Remarque Le présent document ne contient pas de procédures de mise à niveau des périphériques logiques ASA. Pour ceux-ci, consultez le Guide de mise à niveau de Cisco Secure Firewall ASA.

Notez que si votre version actuelle défense contre les menaces 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 de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Ce tableau répertorie nos combinaisons de versions spécialement qualifiées. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez brièvement une combinaison prise en charge, mais non recommandée, dans laquelle le système d'exploitation est « en avance » sur le logiciel du périphérique. Assurez-vous que la mise à niveau de FXOS ne vous rend pas compatible avec des périphériques logiques (y compris les périphériques ASA). Si vous devez sauter plusieurs versions, c'est généralement défense contre les menaces qui posera une limite : FXOS et ASA peuvent généralement effectuer des mises à niveau plus étendues en une seule fois. Après avoir atteint la version FXOS cible, le type de périphérique logique que vous mettez à niveau en premier n'a pas d'importance. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense

Tableau 19 : Mises à niveau directes de Défense contre les menaces et ASA sur le Firepower 9300

Versions actuelles	Versions cibles
FXOS 2.13 avec : • Threat Defense 7.3 • ASA 9.19(x)	→ FXOS 2.13 avec ASA 9.19(x) et toute version ultérieure de Threat Defense 7.3.x
FXOS 2.12 avec : • Threat Defense 7.2 • ASA 9.18(x) Dernière prise en charge de l'appareil Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.	Une des versions suivantes : → FXOS 2.13 avec ASA 9.19(x) et Threat Defense 7.3.x → FXOS 2.12 avec ASA 9.18(x) et toute version ultérieure de Threat Defense 7.2.x
FXOS 2.11.1 avec : • Threat Defense 7.1 • ASA 9.17(x)	→ FXOS 2.13 avec ASA 9.19(x) et Threat Defense 7.3.x → FXOS 2.12 avec ASA 9.18(x) et Threat Defense 7.2.x → FXOS 2.11.1 avec ASA 9.17(x) toute version ultérieure de Threat Defense 7.1.x
FXOS 2.10.1 avec : • Threat Defense 7.0 • ASA 9.16(x)	Une des versions suivantes : → FXOS 2.13 avec ASA 9.19(x) et Threat Defense 7.3.x → FXOS 2.12 avec ASA 9.18(x) et Threat Defense 7.2.x → FXOS 2.11.1 avec ASA 9.17(x) et Threat Defense 7.1.x → FXOS 2.10.1 avec ASA 9.16(x) toute version ultérieure de Threat Defense 7.0.x **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+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Versions actuelles	Versions cibles
FXOS 2.9.1 avec : • Threat Defense 6.7 • ASA 9.15(x)	Une des versions suivantes : → FXOS 2.12 avec ASA 9.18(x) et Threat Defense 7.2.x → FXOS 2.11.1 avec ASA 9.17(x) et Threat Defense 7.1.x → FXOS 2.10.1 avec ASA 9.16(x) et Threat Defense 7.0.x → FXOS 2.9.1 avec ASA 9.15(x) et toute version ultérieure de Threat Defense 6.7.x
FXOS 2.8.1 avec : • Threat Defense 6.6 • ASA 9.14(x)	Une des versions suivantes : → FXOS 2.12 avec ASA 9.18(x) et Threat Defense 7.2.x → FXOS 2.11.1 avec ASA 9.17(x) et Threat Defense 7.1.x → FXOS 2.10.1 avec ASA 9.16(x) et Threat Defense 7.0.x → FXOS 2.9.1 avec ASA 9.15(x) et Threat Defense 6.7.x → FXOS 2.8.1 avec ASA 9.14(x) et toute version ultérieure de Threat Defense 6.6.x
FXOS 2.7.1 avec : • Threat Defense 6.5 • ASA 9.13(x)	Une des versions suivantes : → FXOS 2.11.1 avec ASA 9.17(x) et Threat Defense 7.1.x → FXOS 2.10.1 avec ASA 9.16(x) et Threat Defense 7.0.x → FXOS 2.9.1 avec ASA 9.15(x) et Threat Defense 6.7.x → FXOS 2.8.1 avec ASA 9.14(x) et Threat Defense 6.6.x

Ordre de mise à niveau pour FXOS avec Défense contre les menaces haute disponibilité

Dans les déploiements à haute disponibilité, vous pouvez mettre à niveau FXOS sur chaque châssis indépendamment. Pour réduire au minimum les perturbations, mettez à niveau FXOS un châssis à la fois. Vous devez également mettre à niveau les périphériques défense contre les menaces à la fois.

Tableau 20 :

Défense contre les menacesDéploiement	Commande de mise à niveau
Autonomes	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau défense contre les menaces .

Défense contre les menacesDéploiement	Commande de mise à niveau
Haute disponibilité	Mettez à niveau FXOS sur les deux châssis avant de mettre à niveau défense contre les menaces . Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. Dans le scénario suivant, le périphérique A est le périphérique actif d'origine et le périphérique B est le périphérique de secours d'origine. **1.** Mettez à niveau FXOS sur le châssis avec le périphérique de secours (B). **2.** Changez de rôle. **3.** Mettez à niveau FXOS sur le châssis avec le nouveau périphérique de secours (A). **4.** Mettez à niveau défense contre les menaces avec le nouveau périphérique de secours (A). **5.** Changez de nouveau de rôle. **6.** Mettez à niveau défense contre les menaces sur le périphérique de secours d'origine (B).

Mettre à niveau FXOS avec Gestionnaire de châssis

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes à l'aide de Firepower Chassis Manager

Cette section décrit comment mettre à niveau l'offre groupée de la plateforme FXOS pour un Firepower 4100/9300 chassis autonome.

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

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

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 Firepower 4100/9300 chassis.
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 FXOS CLI :

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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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 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 Firepower 4100/9300 chassis.
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 FXOS CLI :

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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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 Firepower 4100/9300 chassis.
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 FXOS CLI :

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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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 avec l'interface de ligne de commande

Mettre à niveau FXOS pour les périphériques logiques FTD autonomes à l'aide de l'interface de ligne de commande de FXOS

Cette section décrit comment mettre à niveau l'offre groupée de la plateforme FXOS pour un Firepower 4100/9300 chassis autonome.

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

- Un châssis Firepower 4100 series configuré avec un périphérique logique FTD et ne faisant pas partie d'une paire de basculement.

- Un châssis Firepower 9300 configuré avec un ou plusieurs périphériques FTD autonomes ne faisant pas partie d'une paire de basculement.

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 Firepower 4100/9300 chassis :
  - 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 au FXOS CLI.

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

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** pour confirmer que vous souhaitez procéder à la vérification.

Étape 7 Saisissez **yes** 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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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 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 Firepower 4100/9300 chassis :
  - 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 FXOS CLI 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 Firepower 4100/9300 chassis :

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** pour confirmer que vous souhaitez procéder à la vérification.

Étape 7 Saisissez **yes** 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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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 FXOS CLI 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 Firepower 4100/9300 chassis :

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** pour confirmer que vous souhaitez procéder à la vérification.

Étape 17 Saisissez **yes** 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 :

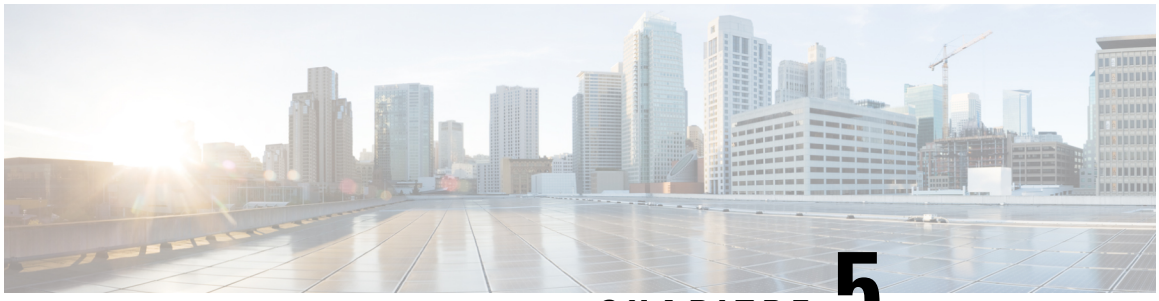
```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

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 series ou pour tous les modules de sécurité installés sur un Firepower 9300 appliance.
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.



CHAPITRE 5

Mise à niveau Défense contre les menaces

Liste de contrôle des mises à niveau pour Défense contre les menaces

Planification et faisabilité

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

✓	Action/Vérification	Détails
	Évaluez votre déploiement.	Comprendre où vous êtes détermine comment vous atteindrez votre objectif. En plus des informations sur la version et le modèle actuels, déterminez si votre déploiement est configuré pour une haute disponibilité
	Planifiez votre chemin de mise à niveau.	Cela est particulièrement important pour les déploiements à haute disponibilité, les mises à niveau multisauts et les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement. Les mises à niveau peuvent être majeures (A.x), de maintenance (A.x.y) ou de correctifs (A.x.y.z). Voir : • Chemins de mise à niveau pour Défense contre les menaces, à la page 43 • Chemins de mise à niveau pour FXOS, à la page 19

✓	Action/Vérification	Détails
	Lisez 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 celles-ci : • Directives relatives aux mises à niveau logicielles, à la page 11, pour les directives relatives aux mises à niveau critiques et spécifiques aux versions. • Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version, pour les fonctionnalités nouvelles et obsolètes qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions entre votre version actuelle et la version cible. • Cisco Secure Firewall Threat Defense Notes de mise à jour, dans le chapitre *Bogues ouverts et résolus*, pour les bogues qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions des notes de mise à jour entre votre version actuelle et la version cible. Si vous disposez d'un contrat d'assistance, vous pouvez utiliser l'outil de recherche de bogues pour obtenir des listes de bogues à jour. • Notes de version Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.
	Vérifiez l'accès à l'appareil.	Les périphériques peuvent arrêter de transmettre le trafic pendant la mise à niveau ou en cas d'échec de celle-ci. 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 .
	Vérifiez la bande passante.	Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Chaque fois que cela est possible, chargez les paquets de mise à niveau à l'avance. Si vous transférez un ensemble de mise à niveau vers un périphérique au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).

✓	Action/Vérification	Détails
	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 les mises à niveau sont susceptibles de prendre. Tenez compte des tâches que vous devez effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Voir : • Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces • Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces, à la page 14 • Flux de trafic et inspection pour les mises à niveau de châssis, à la page 18 • Tests de temps et d'espace disque

Sauvegardes

À l'exception des correctifs rapides, la mise à niveau supprime toutes les sauvegardes stockées sur le système. 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 :

- 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.

✓	Action/Vérification	Détails
	Sauvegardez défense contre les menaces .	Pour sauvegarder les configurations de défense contre les menaces , consultez le chapitre *Gestion du système* dans le Guide Cisco Secure Firewall Device Manager Configuration . Si vous avez un Firepower 9300 avec défense contre les menaces et des périphériques logiques ASA s'exécutant sur des modules distincts, utilisez ASDM ou l'interface de ligne de commande d'ASA pour sauvegarder les configurations et les autres fichiers critiques, en particulier s'il y a une migration de la configuration de l'ASA. Consultez le chapitre *Logiciels et configurations* du Guide de configuration des opérations générales de la gamme Cisco ASA.
	Sauvegardez FXOS sur le Firepower 4100/9300.	Utilisez le gestionnaire de châssis ou l'interface de ligne de commande de FXOS pour exporter les configurations des châssis, y compris les paramètres de configuration des périphériques logiques et de la plateforme. Consultez le chapitre *Importation et exportation de la configuration* du Guide de configuration de Cisco Firepower 4100/9300 FXOS.

Progiciels de mise à niveau

Le chargement des paquets de mise à niveau vers le système avant de commencer la mise à niveau peut réduire la durée de votre fenêtre de maintenance.

✓	Action/Vérification	Détails
	Téléchargez le paquet de mise à niveau à partir de Cisco et chargez-le sur le périphérique.	Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : Paquets de mise à niveau pour Défense contre les menaces, à la page 48. Pour la haute disponibilité de défense contre les menaces , vous devez charger le paquet de mise à niveau sur les deux unités.

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.

✓	Action/Vérification	Détails
	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 majeure.
	Mettez à niveau le micrologiciel sur le Firepower 4100/9300.	Nous vous recommandons d'utiliser le micrologiciel le plus récent. Consultez la section CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS.
	Mettez à niveau FXOS sur le Firepower 4100/9300.	La mise à niveau de FXOS est généralement requise pour les mises à niveau majeures, mais très rare pour les versions de maintenance et les correctifs. Pour minimiser les perturbations, mettez à niveau FXOS dans les paires à haute accessibilité défense contre les menaces et les grappes inter-châssis, . Consultez Mettre à niveau le châssis sur le Firepower 4100/9300, à la page 17.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à mettre à niveau le logiciel.

✓	Action/Vérification	Détails
	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. Pour vérifier l'heure, utilisez la commande **show time** de l'interface de ligne de commande.

✓	Action/Vérification	Détails
	Déployez des configurations.	Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Le déploiement peut affecter le flux de trafic et l'inspection; voir Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces, à la page 14.
	Exécutez la vérification de l'état de préparation.	La réussite des vérifications de l'état de préparation réduit considérablement les risques d'échec de la mise à niveau. Consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 48.
	Vérifiez l'espace disque.	Les vérifications de l'état de préparation comprennent une vérification de l'espace disque. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Pour vérifier l'espace disque disponible sur le périphérique, utilisez la commande **show disk** de l'interface de ligne de commande.
	Vérifiez les tâches en cours.	Assurez-vous que les tâches essentielles 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 programmées pour s'exécuter lors de la mise à niveau et de les annuler ou de les reporter.

Chemins de mise à niveau pour Défense contre les menaces

Choisissez le chemin de mise à niveau qui correspond à votre déploiement.

Chemin de mise à niveau pour Défense contre les menaces avec FXOS

Ce tableau fournit le chemin de mise à niveau pour défense contre les menaces sur le Firepower 4100/9300.

Notez que si votre version actuelle défense contre les menaces 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 de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Ce tableau répertorie nos combinaisons de versions spécialement qualifiées. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez brièvement une combinaison prise en charge, mais non recommandée, dans laquelle le système d'exploitation est « en avance » sur le logiciel du périphérique. Assurez-vous que la mise à niveau de FXOS ne vous rend pas compatible avec des périphériques logiques. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Tableau 21 : Défense contre les menaces Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Threat Defense 7.3	→ FXOS 2.13 avec toute version ultérieure de Threat Defense 7.3.x
FXOS 2.12 avec Threat Defense 7.2 Dernière prise en charge de Firepower 4110, 4120, 4140, 4150. Dernière prise en charge de l'appareil Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Threat Defense 7.2.x
FXOS 2.11.1 avec Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Threat Defense 7.1.x
FXOS 2.10.1 avec Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Threat Defense 7.0.x **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+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Versions actuelles	Versions cibles
FXOS 2.9.1 avec Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Threat Defense 6.7.x
FXOS 2.8.1 avec Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Threat Defense 6.6.x
FXOS 2.7.1 avec Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec Threat Defense 6.6.x

Chemin de mise à niveau pour Défense contre les menaces sans FXOS

Ce tableau fournit le chemin de mise à niveau pour défense contre les menaces lorsque vous n'avez pas besoin de mettre à niveau le système d'exploitation. Cela comprend Cisco les séries Firepower 1000/2100, la série ASA-5500-X et l'ISA 3000.

Notez que si votre version actuelle défense contre les menaces 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 de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Tableau 22 : Mises à niveau directes de Défense contre les menaces

Version actuelle	Version cible
7.4	→ Toute version ultérieure à 7.4.x
7.3	Une des versions suivantes : → 7.4.x → Toute version ultérieure à 7.3.x

Version actuelle	Version cible
7.2	Une des versions suivantes : → 7.4.x → 7.3.x → Toute version ultérieure à 7.2.x **Remarque** Le Firepower 1010E, introduit dans la version 7.2.3, n'est pas pris en charge dans la version 7.3. L'assistance revient dans la version 7.4.1.
7.1	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → Toute version ultérieure à 7.1.x
7.0 Dernière prise en charge pour ASA 5508-X et 5516-X.	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Toute version ultérieure à 7.0.x **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+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Version actuelle	Version cible
6.7	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → Toute version ultérieure à 6.7.x
6.6 Dernière prise en charge pour ASA 5525-X, 5545-X et 5555-X.	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Toute version ultérieure à 6.6.x
6.5	Une des versions suivantes : → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Dernière prise en charge pour ASA 5515-X.	Une des versions suivantes : → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Une des versions suivantes : → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Dernière prise en charge pour la série ASA 5506-X.	Une des versions suivantes : → 6.6.x → 6.5 → 6.4 → 6.3

Paquets de mise à niveau pour Défense contre les menaces

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : https://www.cisco.com/go/ftd-software.

Vous utilisez le même ensemble de mises à niveau pour tous les modèles d'une famille ou d'une série. Pour trouver le bon modèle, sélectionnez ou recherchez votre modèle sur le Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Notez que les paquets de mise à niveau à sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Tableau 23 : Paquets de mise à niveau logicielle

Plateforme	Paquet de mise à niveau
Série Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Série Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Cisco Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Défense contre les menaces virtuelles	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar
ISA 3000 avec FTD	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar

Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces

Avant d'installer une mise à niveau, le système exécute une vérification de préparation pour s'assurer que la mise à niveau est valide pour le système et pour examiner les autres facteurs qui peuvent empêcher la réussite de la mise à niveau. Si la vérification de préparation échoue, vous devez résoudre les problèmes avant de relancer l'installation. Si la vérification a échoué, vous serez informé de l'échec la prochaine fois que vous tenterez l'installation, et vous aurez la possibilité de forcer l'installation si vous le souhaitez.

Vous pouvez également exécuter manuellement le test de préparation avant de lancer la mise à niveau, comme le décrit cette procédure.

Avant de commencer

Chargez l'ensemble de mises à niveau que vous souhaitez vérifier.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour (Updates).

La section **System Upgrade** (mise à niveau du système) affiche la version du logiciel en cours d'exécution et toute mise à jour que vous avez déjà téléchargée.

Étape 2 Consultez la section **Readiness Check** (vérification de l'état de préparation).

- Si la vérification de mise à niveau n'a pas encore été effectuée, cliquez sur le lien **Run Upgrade Readiness Check** (exécuter la vérification de l'état préparation aux mises à niveau). La progression de la vérification s'affiche dans cette zone. Le processus devrait prendre environ 20 secondes.
- Si la vérification de mise à niveau a déjà été exécutée, cette section indique si la vérification s'est soldée par une réussite ou un échec. En cas d'échec, cliquez sur **See Details** (Consulter les détails) pour consulter plus d'information au sujet de la vérification de l'état de préparation. Après avoir résolu les problèmes, relancez la vérification.

Étape 3 Si la vérification de l'état de préparation conduit à un échec, vous devez résoudre les problèmes avant d'installer la mise à niveau. Les informations détaillées comprennent de l'aide pour résoudre les problèmes signalés. À la suite d'un script d'échec, cliquez sur le lien **Show Recovery Message** (Afficher le message de récupération) pour afficher les informations.

Voici quelques problème courants :

- Incompatibilité de la version de FXOS - Sur les systèmes où vous installez les mises à niveau de FXOS séparément, comme le Firepower 4100/9300, un paquet de mise à niveau peut nécessiter une version minimale de FXOS différente de la version du logiciel défense contre les menaces que vous exécutez actuellement. Dans ce cas, vous devez d'abord mettre à niveau FXOS avant de pouvoir mettre à niveau le logiciel défense contre les menaces .
- Modèle de périphérique non pris en charge : l'ensemble de mise à niveau ne peut pas être installé sur ce périphérique. Vous avez peut-être téléchargé le mauvais paquet, ou l'appareil est un ancien modèle qui n'est tout simplement plus pris en charge par la nouvelle version du logiciel défense contre les menaces . Veuillez vérifier la compatibilité de l'appareil et télécharger un ensemble pris en charge, s'il en existe un.
- Espace disque insuffisant : Si l'espace disponible est insuffisant, essayez de supprimer les fichiers inutiles, comme les sauvegardes du système. Supprimez uniquement les fichiers que vous avez créés.

Mise à niveau Défense contre les menaces

Mise à niveau du système autonome Défense contre les menaces

Utilisez cette procédure pour mettre à niveau un périphérique autonome défense contre les menaces . Si vous devez mettre à jour FXOS, faites-le en premier. Pour mettre à niveau la défense contre les menaces haute disponibilité, voir Mise à de la haute disponibilité Défense contre les menaces, à la page 51.

Mise en garde Le trafic est abandonné pendant la mise à niveau. Même si le système semble inactif ou ne répond pas, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense , à la page 55.

Avant de commencer

Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 2 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Browse** (Parcourir) ou sur ,**Replace File** (Remplacer le fichier) pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Run Upgrade Immediately** (Exécuter la mise à niveau immédiatement) pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 3 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour plus de renseignements, consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 48

Étape 4 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continue** (Continuer) pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 5 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (sommaire du périphérique) affiche la version du logiciel actuellement exécutée.

Étape 6 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.
b) Apportez toutes les modifications de configuration requises après la mise à niveau.
c) Déployez.

Mise à de la haute disponibilité Défense contre les menaces

Utilisez cette procédure pour mettre à niveau des périphériques à haute disponibilité. Mettez-les à niveau un à la fois. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. C'est-à-dire que vous mettez à niveau le serveur de secours actuel, changez de rôle, puis mettez à niveau le nouveau serveur de secours. Si vous devez mettre à jour FXOS, faites-le sur les deux châssis avant de mettre à niveau défense contre les menaces sur l'un ou l'autre. Encore une fois, mettez toujours à niveau le serveur de secours.

⚠

Mise en garde N'apportez pas et n'utilisez pas de modifications de configuration sur une unité pendant que l'autre est en cours de mise à niveau, ou vers une paire de versions mixte. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense , à la page 55.

Avant de commencer

Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Connectez-vous à l'unité en veille.

Étape 2 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 3 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Browse** (Parcourir) ou sur ,**Replace File** (Remplacer le fichier) pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Run Upgrade Immediately** (Exécuter la mise à niveau immédiatement) pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 4 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour plus de renseignements, consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 48

Étape 5 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continue** (Continuer) pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 6 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (Résumé du périphérique) affiche la version du logiciel actuellement exécutée et l'état de la haute disponibilité. Ne continuez pas tant que vous n'avez pas vérifié la réussite *et que* la haute disponibilité n'a pas été rétablie. Si la haute disponibilité reste suspendue après une mise à niveau réussie, consultez Dépannage des mises à niveau de Threat Defense , à la page 55.

Étape 7 Mettez à niveau la deuxième unité.

a) Changer de rôle, rendant cet appareil actif : sélectionnez **Device** > **High Availability**(haute disponibilité du périphérique), puis sélectionnez **Switch Mode** (changer de mode) dans le menu déroulant ( ). Attendez que l'état de l'unité passe à actif et confirmez que le trafic circule normalement. Déconnectez-vous.

b) Mise à niveau : répétez les étapes précédentes pour vous connecter au nouveau serveur de secours, téléverser le paquet, mettre à niveau le périphérique, surveiller la progression et vérifier la réussite.

Étape 8 Examiner les rôles des périphériques.

Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 9 Connectez-vous à l'unité active.

Étape 10 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.

b) Apportez toutes les modifications de configuration requises après la mise à niveau.

c) Déployez.

Surveilla des mises à niveau de Défense contre les menaces

Lorsque vous lancez la mise à niveau de défense contre les menaces , vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la progression globale de la mise à niveau. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, la page vous permet d'annuler manuellement ou de tenter de nouveau la mise à niveau.

Vous pouvez également vous connecter en SSH au périphérique et utiliser l'interface de ligne de commande : **show upgrade status**. Ajoutez le mot-clé **continuous** pour afficher les entrées de journal telles qu'elles sont créées et **detail** pour afficher des informations détaillées. Ajoutez les deux mots-clés pour obtenir des informations détaillées en continu.

Une fois la mise à niveau terminée, vous perdez l'accès à la page d'état et à l'interface de ligne de commande lorsque le périphérique redémarre.

ou nouvelle Défense contre les menaces mises à niveau

Utilisez la page d'état de la mise à niveau ou l'interface de ligne de commande pour annuler manuellement les mises à niveau majeures ou de maintenance qui ont échoué ou en cours, et pour réessayer les mises à niveau qui ont échoué :

- Page d'état de mise à niveau : cliquez sur **Cancel Upgrade** (Annuler la mise à niveau) pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez cliquer sur **Cancel Upgrade** (Annuler

la mise à niveau) pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou cliquer sur **Continue** (Continuer) pour réessayer la mise à niveau.

- CLI : Utilisez la commande **upgrade cancel** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez utiliser **upgrade cancel** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou utiliser **upgrade retry** pour réessayer la mise à niveau.

Remarque Par défaut, défense contre les menaces 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 ayant échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. Dans un déploiement à haute disponibilité, 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 et la nouvelle tentative ne sont pas prises en charge pour les correctifs. Pour en savoir plus sur la reprise d'une mise à niveau réussie, consultez , à la page 54.

Si une mise à niveau majeure ou de maintenance réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez revenir en arrière. Le rétablissement de défense contre les menaces ramène le logiciel à l'état qu'il avait avant la dernière mise à niveau majeure ou de maintenance; les modifications de configuration ultérieures à la mise à niveau ne sont pas conservées. Le rétablissement après l'application d'un correctif supprime également les correctifs. Notez que vous ne pouvez pas annuler des correctifs ou des correctifs rapides individuels.

La procédure suivante explique comment restaurer à partir de gestionnaire d'appareil. Si vous ne pouvez pas accéder à gestionnaire d'appareil, vous pouvez revenir à la ligne de commande défense contre les menaces dans une session SSH en utilisant la commande **upgrade revert**. Vous pouvez utiliser la commande **show upgrade revert-info** pour voir à quelle version le système retournera.

Avant de commencer

Si l'unité fait partie d'une paire à haute disponibilité, vous devez rétablir les deux unités. Idéalement, lancez la restauration sur les deux unités en même temps afin que la configuration puisse être restaurée sans problème de basculement. Ouvrez des sessions avec les deux unités et vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus. Notez que le trafic sera interrompu pendant la restauration, donc effectuez-la si possible en dehors des heures ouvrables.

Pour les châssis Firepower 4100/9300, les versions principales défense contre les menaces ont une version FXOS associée spécialement qualifiée et recommandée. Cela signifie qu'après avoir rétabli le logiciel défense contre les menaces , vous exécutez peut-être une version non recommandée de FXOS (trop récente). Bien que les nouvelles versions de FXOS soient rétrocompatibles avec les anciennes versions de défense contre les menaces , nous effectuons des tests avancés des combinaisons recommandées. Vous ne pouvez pas passer à une version antérieure de FXOS, donc si vous vous trouvez dans cette situation et que vous souhaitez exécuter une combinaison recommandée, vous devrez recréer l'image du périphérique.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour **(Updates)**.

Étape 2 Dans la section **System Upgrade** (mise à niveau du système), cliquez sur le lien **Revert Upgrade** (annuler la mise à niveau).

Une boîte de dialogue de confirmation s'affiche et affiche la version actuelle et la version à laquelle le système sera restauré. Si aucune version n'est disponible pour la restauration, il n'y a pas de lien **Annuler la mise à niveau**.

Étape 3 Si la version cible vous convient (et qu'une version est disponible), cliquez sur **Revert** (Restaurer).

Après avoir effectué le retour en arrière, vous devez réenregistrer le périphérique auprès du Smart Software Manager.

Dépannage des mises à niveau de Threat Defense

Dépannage général de la mise à niveau

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau 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 .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours; voir ou nouvelle Défense contre les menaces mises à niveau, à la page 53. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).

⚠

Mise en garde 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.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si vous continuez à rencontrer des problèmes et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être revenir à une version majeure ou de maintenance antérieure; voir , à la page 54. Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez la commande **Annuler automatiquement en cas d'échec de la mise à niveau...** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez ou nouvelle Défense contre les menaces mises à niveau, à la page 53. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Dépannage de la mise à niveau haute disponibilité

Ces problèmes sont spécifiques aux mises à niveau à haute disponibilité.

La mise à niveau ne commencera pas sans le déploiement des modifications non validées.

Si vous obtenez un message d'erreur indiquant que vous devez déployer toutes les modifications non validées, même s'il n'y en a pas, connectez-vous à l'unité active (n'oubliez pas que vous devriez mettre à niveau l'unité de secours), créez des modifications mineures et déployez. Ensuite, annulez la modification, redéployez et réessayez la mise à niveau sur le serveur de secours.

Si cela ne fonctionne pas et que les unités exécutent des versions logicielles différentes par rapport aux recommandations, changez de rôle pour rendre l'unité en veille active, puis suspendez la haute disponibilité. Vous pouvez ensuite effectuer le déploiement à partir de l'unité active/suspendue, reprendre la haute disponibilité, puis changer encore les rôles pour mettre l'unité active en veille à nouveau. La mise à niveau devrait alors fonctionner.

Le déploiement à partir de l'unité active échoue pendant la mise à niveau de secours ou provoque une erreur de synchronisation de l'application.

Cela peut se produire si vous déployez à partir de l'unité active tandis que l'unité de secours est en cours de mise à niveau, ce qui n'est pas pris en charge. Procédez à la mise à niveau malgré l'erreur. Après

avoir mis à niveau les deux unités, apportez les modifications de configuration requises et déployez à partir de l'unité active. L'erreur devrait être résolue.

Pour éviter ces problèmes, n'apportez pas et ne déployez pas de modifications de configuration sur une unité pendant que l'autre unité est en cours de mise à niveau, ou vers une paire de versions mixte.

Les modifications de configuration apportées depuis la mise à niveau seront perdues.

Si vous devez absolument apporter et déployer des modifications sur une paire de versions, vous devez apporter les modifications aux deux unités, sinon elles seront perdues après la mise à niveau de l'unité active de bas niveau.

La haute disponibilité est suspendue après la mise à niveau.

Après le redémarrage après la mise à niveau, la haute disponibilité est brièvement suspendue pendant que le système effectue certaines tâches automatisées finales, telles que la mise à jour des bibliothèques et le redémarrage de Snort. Vous êtes susceptible de le remarquer si vous vous connectez à la CLI *très* peu de temps après la mise à niveau. Si la haute disponibilité ne reprend pas d'elle-même après la fin de la mise à niveau et que gestionnaire d'appareil est disponible, faites-le manuellement :

1. Connectez-vous au périphérique actif et au périphérique en veille et consultez les listes des tâches. Attendez que toutes les tâches aient fini de s'exécuter sur les deux périphériques. Si vous remettez la haute disponibilité trop tôt, vous pourriez avoir un problème futur dans lequel le basculement provoque une panne.
2. Sélectionnez **Périphérique** > **Haute disponibilité**, puis **Reprendre** la haute disponibilité dans le menu engrenage ( ).

Le basculement ne se produit pas avec une paire de versions mixtes.

Bien que l'avantage de la haute disponibilité soit que vous puissiez mettre à niveau votre déploiement sans interruption de trafic ni inspection, le basculement est désactivé pendant l'ensemble du processus de mise à niveau. C'est-à-dire que non seulement le basculement est nécessairement désactivé lorsqu'un périphérique est hors ligne (car il n'y a rien vers lequel le basculement est effectué), mais le basculement est également désactivé avec les paires de versions mixtes. C'est le seul moment où les paires de versions mixtes sont autorisées (temporairement) pendant la mise à niveau. Planifiez les mises à niveau pendant les périodes de maintenance, au moment où elles auront le moins d'incidence en cas de problème, et assurez-vous d'avoir suffisamment de temps pour mettre à niveau les deux périphériques dans cette fenêtre.

Échec de la mise à niveau sur un seul périphérique, ou un périphérique a été annulé. La paire utilise maintenant des versions mixtes.

Les paires de versions ne sont pas prises en charge pour les opérations générales. Mettez à niveau le périphérique de version antérieure ou inversez le périphérique de version ultérieure. Pour les correctifs, car la restauration n'est pas prise en charge, si vous ne pouvez pas mettre à niveau le périphérique de version antérieure, vous devez interrompre la haute disponibilité, recréer l'image d'un ou des deux périphériques, puis rétablir la haute disponibilité.

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.