

Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center, version 7.3.x

Dernière modification : 2026-10-24

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.

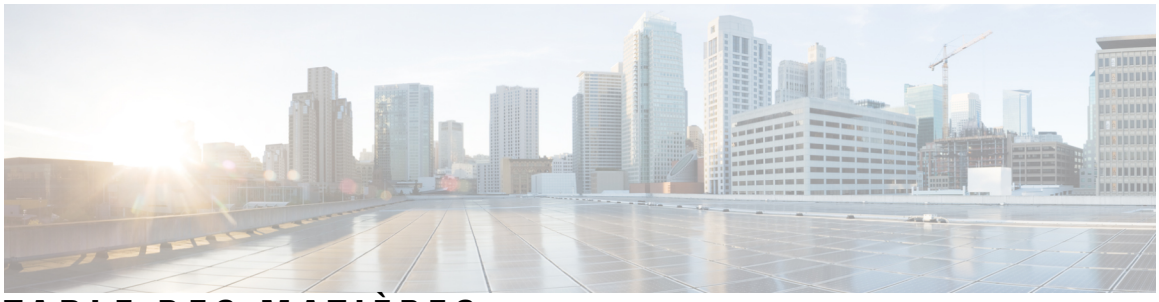


TABLE DES MATIÈRES

CHAPITRE 1 **Pour commencer** 1

Ce guide est-il pour vous? 1

Planification de votre mise à niveau 4

Historique des fonctionnalités de mise à niveau 5

Pour de l'assistance 16

CHAPITRE 2 **Configuration système requise** 19

Plateformes Firewall Management Center 19

Plateformes Firewall Threat Defense 20

Gestion du Firewall Threat Defense 22

CHAPITRE 3 **Directives relatives aux mises à niveau logicielles** 25

Version minimale pour la mise à niveau 25

Directives de mise à niveau pour Version 7.3 26

Déploiement étendu après la mise à niveau, pour les configurations de taille importante 27

Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) 28

Mises à niveau qui ne répondent pas 28

Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense 29

Flux de trafic et inspection lors du déploiement de configurations 32

Temps et espace disque 33

CHAPITRE 4 **Mettre à niveau le Firewall Management Center** 35

Liste de contrôle des mises à niveau pour Firewall Management Center 35

Chemin de mise à niveau pour Firewall Management Center 39

Charger les paquets de mise à niveau pour Firewall Management Center 41

Exécuter la vérification de l'état de préparation pour Firewall Management Center 42
Mettre à niveau le Firewall Management Center : autonome 43
Mettre à niveau le Firewall Management Center : Haute disponibilité 44

CHAPITRE 5 **Mise à niveau Firewall Threat Defense 47**

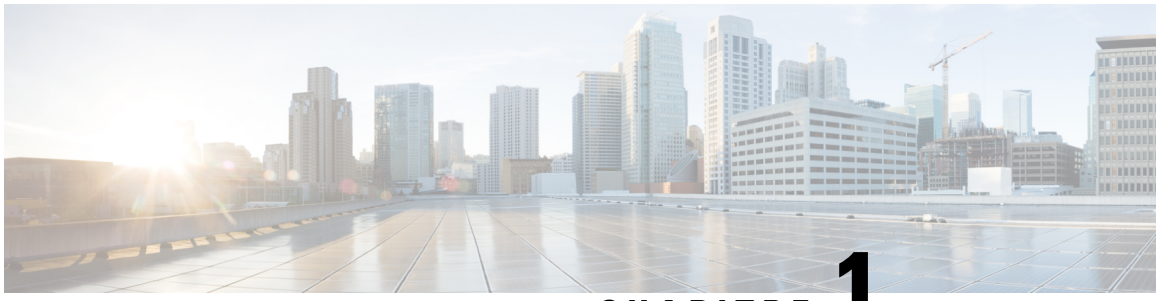
Liste de contrôle des mises à niveau pour Firewall Threat Defense 47
Chemins de mise à niveau pour Firewall Threat Defense 53
Chemin de mise à niveau pour Firewall Threat Defense sans FXOS 53
Chemin de mise à niveau pour Firewall Threat Defense avec FXOS 56
Ordre de mise à niveau pour Firewall Threat Defense haute disponibilité/évolutivité avec FXOS 58
Paquets de mise à niveau pour Firewall Management Center et Firewall Threat Defense 59
Charger les paquets de mise à niveau avec le Firewall Management Center 60
Charger les paquets de mise à niveau Firewall Threat Defense avec l'assistant 61
Charger les paquets de mise à niveau Firewall Threat Defense avec l'assistantFirewall Management Center 61
Chargez les paquets de mise à niveau Firewall Threat Defense sur un serveur interne avec le système (Système) > Mises à jour (Updates) 61
Charger les paquets de mise à niveau Firewall Threat Defense avec Système > Mises à jour 63
Chargez les paquets de mise à niveau Firewall Threat Defense vers le Firewall Management Center avec System (Système) > Updates (Mises à jour) 63
Charger les paquets de mise à niveau Firewall Threat Defense sur un serveur interne avec System (Système) > Updates (Mises à jour) 63
Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques 65
Mettre à niveau Firewall Threat Defense à l'aide de l'assistant (désactiver la restauration) 66
Mettre à niveau Firewall Threat Defense à l'aide de l'assistant en mode sans surveillance (désactiver la restauration) 70
Mettre à niveau Firewall Threat Defense via System (Système) > Updates (Mises à jour) (Enable Revert (Activer la restauration)) 74

CHAPITRE 6 **Mettre à niveau le châssis sur le Firepower 4100/9300 77**

Progiciels de mise à niveau pour FXOS 77
Directives de mise à niveau pour le châssis Firepower 4100/9300 77
Flux de trafic et inspection pour les mises à niveau de châssis 78
Chemins de mise à niveau pour FXOS 79
Chemin de mise à niveau pour FXOS avec Firewall Threat Defense 79

Chemin de mise à niveau pour FXOS avec Firewall Threat Defense et ASA 82
Ordre de mise à niveau pour FXOS avec Firewall Threat Defense haute disponibilité/évolutivité 85
Mettre à niveau FXOS avec Firewall Chassis Manager 86
Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intrachâssis FTD à l'aide de Firepower Chassis Manager 86
Mettre à niveau FXOS sur une grappe intrachâssis FTD à l'aide de Firepower Chassis Manager 88
Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de Firepower Chassis Manager 91
Mettre à niveau FXOS avec l'interface de ligne de commande 94
Mettre à niveau FXOS pour les périphériques logiques FTD autonomes ou une grappe intrachâssis FTD à l'aide de l'interface de ligne de commande de FXOS 94
Mettre à niveau FXOS sur une grappe intrachâssis FTD à l'aide de l'interface de ligne de commande de FXOS 97
Mettre à niveau FXOS sur une paire à haute accessibilité FTD à l'aide de l'interface de ligne de commande de FXOS 100

CHAPITRE 7 **Annuler ou désinstaller la mise à niveau 107**
Restauration de Threat Defense 107
À propos de la restauration de Threat Defense 107
Directives pour la restauration Firewall Threat Defense 108
Restauration de Firewall Threat Defense avec Firewall Management Center 110
Désinstaller un correctif 111
Ordre de désinstallation pour la haute disponibilité/évolutivité 112
Désinstaller les correctifs des Threat Defense 113
Désinstaller les correctifs Firewall Management Center autonomes 115
Désinstaller les correctifs de haute disponibilité Firewall Management Center 116



CHAPITRE 1

Pour commencer

- Ce guide est-il pour vous?, à la page 1
- Planification de votre mise à niveau, à la page 4
- Historique des fonctionnalités de mise à niveau, à la page 5
- Pour de l'assistance, à la page 16

Ce guide est-il pour vous?

Ce guide explique comment utiliser un **Secure Firewall Management Center** exécutant actuellement **Version 7.3** pour préparer et terminer avec succès :

- Mise à niveau des périphériques Firewall Threat Defense actuellement gérés *jusqu'à* Version 7.3.
- Mise à niveau du Firewall Management Center vers des versions *ultérieures à* Version 7.3.

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 Firewall Management Center

Version actuelle de Firewall Management Center	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 Firewall Threat Defense avec Firewall Management Center

Version actuelle de Firewall Management Center	Guide
Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)	Guides de mise à niveau de Cisco Secure Firewall Threat Defense pour le Firewall Management Center en 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 Firewall Threat Defense avec Gestionnaire de périphériques de pare-feu

Version actuelle de Firewall Threat Defense	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 Contrôle de Security Cloud	*Cisco Security Cloud Control : pare-feu de protection contre les menaces géré par FDM*

Tableau 4 : Guides de mise à niveau pour NGIPS

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

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

Tableau 5 : Mettre à niveau d'autres composants

Version	Composant	Guide
N'importe laquelle	Périphériques logiques ASA sur le Firepower 4100/9300	*Guide de mise à niveau de Cisco Secure Firewall ASA*
Nouvelle	BIOS et micrologiciel pour Firewall Management Center	Notes de mise à jour du correctif de Cisco Secure Firewall Threat Defense/Firepower
Nouvelle	Micrologiciel pour le Firepower 4100/9300	*CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS*
Nouvelle	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 6 : 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 les configurations et les événements. 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.
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 7 : Historique des fonctionnalités de mise à niveau de l'appareil

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Choisir et télécharger directement les paquets de mise à niveau sur le Firewall Management Center.	7.3.0	N'importe laquelle	Vous pouvez maintenant choisir les paquets de mise à niveau de Firewall Threat Defense que vous souhaitez télécharger directement vers le Firewall Management Center. Utilisez le nouveau sous-onglet **Télécharger les mises à niveau** sur la page > **Updates (Mises à jour)** > **Product Updates (Mises à jour de produit)**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1.
Charger les paquets de mise à niveau vers le Firewall Management Center depuis l'assistant Firewall Threat Defense.	7.3.0	N'importe laquelle	Vous utilisez maintenant l'assistant pour charger les paquets de mise à niveau de Firewall Threat Defense ou pour préciser leur emplacement. Auparavant (selon la version), vous utilisiez **System (Système)** > **Updates (Mises à jour)** ou **System (Système)** > **Product Upgrades (Mises à niveau des produits)**. Restrictions de version : cette fonctionnalité est remplacée par un système de gestion des paquets amélioré dans les versions 7.2.6 et 7.4.1.
La mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la Firewall Threat Defense n'est plus une option.	7.3.0	N'importe laquelle	**Incidence sur la mise à niveau. Tous les périphériques éligibles sont mis à niveau vers Snort 3 lors du déploiement.** Lorsque vous mettez à niveau Firewall Threat Defense vers la version 7.3 ou ultérieure, vous ne pouvez plus désactiver l'option de **mise à niveau de Snort 2 vers Snort 3**. Après la mise à niveau logicielle, tous les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Bien qu'il soit possible de rétablir des périphériques individuels, Snort 2 n'est pas pris en charge sur Firewall Threat Defense 7.7 et versions ultérieures. Vous devriez cesser de l'utiliser dès à présent. Pour les périphériques qui ne sont pas éligibles à la mise à niveau automatique, car ils utilisent des politiques de prévention des intrusions ou d'analyse de réseau personnalisées, procédez à une mise à niveau manuelle vers Snort 3 afin d'améliorer la détection et les performances. Pour obtenir de l'aide lors de la migration, consultez *Politiques de prévention des intrusions personnalisées pour Snort 3* pour votre version.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Ensemble de mise à niveau et d'installation combinées pour Cisco Secure Firewall 3100.	7.3.0	7.3.0	

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Incidence de la recréation d'image. Dans la version 7.3, nous avons combiné l'ensemble d'installation et de mise à niveau de Firewall Threat Defense pour Secure Firewall 3100, comme suit : • Paquet d'installation des versions 7.1 à 7.2 : cisco-ftd-fp3k.*version*.SPA • Paquet de mise à niveau, versions 7.1 à 7.2 : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Ensemble combiné version 7.3+ : Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Bien que vous puissiez mettre à niveau la Firewall Threat Defense sans problème, vous ne pouvez pas restaurer l'image des anciennes versions de Firewall Threat Defense et des versions ASA directement vers la version 7.3 ou versions ultérieures de Firewall Threat Defense Cela est dû à une mise à jour de ROMMON requise par le nouveau type d'image. Pour recréer l'image de ces anciennes versions, vous devez « passer par » ASA 9.19+, qui est pris en charge avec l'ancienne ROMMON, mais aussi les mises à jour de la nouvelle ROMMON. Il n'y a pas de programme de mise à jour de ROMMON distinct. Pour accéder à la version 7.3+ de Firewall Threat Defense, vos options sont les suivantes : • Mise à niveau de la version de Firewall Threat Defense 7.1 ou 7.2 : utilisez le processus de mise à niveau normal. Consultez le guide de mise à niveau approprié. • Recréation de l'image à partir de la version 7.1 ou 7.2 de Firewall Threat Defense : en effectuant une recréation d'image vers ASA 9.19 et versions ultérieures d'abord, puis vers la version de Firewall Threat Defense 7.3 et versions ultérieures. voir *Défense contre les menaces→ASA : Firepower 1000, 2100 ; Secure Firewall 3100*, puis *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans *Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense*. • Recréation d'image à partir d'ASA 9.17 ou 9.18 : mise à niveau vers ASA 9.19 et versions ultérieures d'abord, puis recréation d'image vers la version de Firewall Threat Defense 7.3 et versions ultérieures. Reportez-vous à *Guide de mise à niveau de Cisco Secure Firewall ASA*, puis à *ASA→Threat Defense : Firepower 1000, 2100 Mode l'appareil; Secure Firewall 3100* dans *Guide de réimage de Cisco Secure Firewall ASA et Secure Firewall Threat Defense*. • Recréation d'image à partir de la Firewall Threat Defense version 7.3 et versions ultérieures : utilise le processus normal de recréation d'image.

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
			Voir *Recréer l'image du système avec une nouvelle version du logiciel* dans *Guide de résolution de problèmes Cisco FXOS pour le Firewall Threat Defense*.
Sélectionner les périphériques à mettre à niveau dans l'assistant de mise à niveau de Firewall Threat Defense.	7.2.6 7.3.0 13 décembre 2022	N'importe laquelle	Utilisez l'assistant pour sélectionner les périphériques à mettre à niveau. Vous pouvez désormais utiliser l'assistant de mise à niveau de Firewall Threat Defense pour sélectionner ou affiner les périphériques à mettre à niveau. Dans l'assistant, vous pouvez basculer l'affichage entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques non admissibles (avec les motifs), les périphériques qui ont besoin du paquet de mise à niveau, etc. Auparavant, vous ne pouviez utiliser que la page de gestion des périphériques et le processus était beaucoup moins flexible.
Mises à niveau de la Firewall Threat Defensesans surveillance.	7.2.6 7.3.0 13 décembre 2022	N'importe laquelle	L'assistant de mise à niveau Firewall Threat Defense prend désormais en charge les mises à niveau sans surveillance, à l'aide d'un nouveau menu **Unattended Mode** (mode sans surveillance). Il vous suffit de sélectionner la version cible et les périphériques que vous souhaitez mettre à niveau, de spécifier quelques options de mise à niveau et de partir. Vous pouvez même vous déconnecter ou fermer le navigateur.
Flux de mise à niveau simultanée de Firewall Threat Defense par différents utilisateurs.	7.2.6 7.3.0 13 décembre 2022	N'importe laquelle	Nous autorisons désormais les flux de travail de mise à niveau simultanée par différents utilisateurs, pourvu que vous mettez à niveau différents périphériques. Le système vous empêche de mettre à niveau des périphériques déjà présents dans le flux de travail d'une autre personne. Auparavant, un seul flux de travail de mise à niveau était autorisé à la fois pour tous les utilisateurs.
Ignorer la génération de dépannage avant la mise à niveau pour les périphériques de Firewall Threat Defense.	7.2.6 7.3.0 13 décembre 2022	N'importe laquelle	Vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant les mises à niveau majeures et de maintenance en désactivant la nouvelle option **Generate troubleshooting files before upgrade begins** (Générer les fichiers de dépannage avant le début de la mise à niveau). Cela permet de gagner du temps et de l'espace disque. Pour générer manuellement des fichiers de dépannage pour un périphérique Firewall Threat Defense, choisissez **System (système)**(⚙) > **Health (intégrité)** > **Monitor (moniteur)**, cliquez sur le périphérique dans le panneau de gauche, sur **View System & Troubleshoot Details** (afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (générer les fichiers de résolution de problèmes).

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Copier les paquets de mise à niveau (« synchronisation homologue à homologue ») d'un appareil à l'autre.	7.2.0	7.2.0	Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de Firewall Management Center ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur Firewall Management Center. Chaque périphérique peut accueillir 5 transferts simultanés de paquets. Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même Firewall Management Center de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour : • Instances de conteneur. • Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe. • Périphériques gérés par des Firewall Management Centerà haute disponibilité. • Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT. • Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de Firewall Management Center. • Périphériques exécutant la version 7.6+. Commandes CLI nouvelles ou modifiées : **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Mise à niveau automatique vers Snort 3 après une mise à niveau réussie de la Firewall Threat Defense.	7.2.0	7.0.0	Lorsque vous utilisez un Firewall Management Center de la version 7.2+ pour mettre à niveau Firewall Threat Defense à la version 7.2 ou ultérieure, vous pouvez désormais choisir de **mettre à niveau Snort 2 vers Snort 3**. Après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide, consultez *Politiques de prévention des intrusions personnalisées pour Snort 3* pour votre version. Restrictions de version : non pris en charge pour les mises à niveau de Firewall Threat Defense vers la version 7.0.x ou 7.1.x..

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Mise à niveau pour les grappes à un seul nœud.	7.2.0	N'importe lequel	Vous pouvez désormais utiliser la page de mise à niveau des périphériques (**Périphériques** > **Mise à niveau de périphériques** pour mettre à niveau les grappes avec un seul nœud actif. Tous les nœuds désactivés sont également mis à niveau. Auparavant, ce type de mise à niveau échouait. Cette fonction n'est pas prise en charge à partir de la page des mises à jour du système (**System (Système)** > **Updates (Mises à jour)**). Les mises à niveau rapides ne sont pas non plus prises en charge dans ce cas. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de la seule unité active, tout comme pour les périphériques autonomes. Plateformes prises en charge : Firepower 4100/9300, Secure Firewall 3100
Restaurer une mise à niveau de périphérique réussie.	7.1.0	7.1.0	Vous pouvez désormais effectuer une restauration des mises à niveau majeures et de maintenance à FTD. Le rétablissement ramène le logiciel à l'état où il était avant la dernière mise à niveau, également appelée « *instantané* ». Si vous annulez une mise à niveau après avoir installé un correctif, vous annulez le correctif ainsi que la mise à niveau majeure ou de maintenance. **Important** Si vous pensez devoir revenir en arrière, vous devez utiliser **System (Système)** > **Updates (Mises à jour)** pour mettre à niveau FTD. La page System Updates (Mises à jour système) est le seul endroit où vous pouvez activer l'option **Enable revert after successful upgrade** (Activer le retour en arrière après une mise à niveau réussie), qui configure le système pour enregistrer un instantané de restauration lorsque vous lancez la mise à niveau. Cela contraste avec notre recommandation usuelle d'utiliser l'assistant sur la page **Devices (Périphériques)** > **Device Upgrade (Mise à niveau du périphérique)**. Cette fonctionnalité n'est pas prise en charge pour les instances de conteneur. Version FTD minimale : 7.1

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
Améliorations du flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité.	7.1.0	N'importe laquelle	Nous avons apporté les améliorations suivantes au flux de travail de mise à niveau pour les périphériques en grappe et à haute disponibilité : • L'assistant de mise à niveau affiche désormais correctement les unités en grappe et à haute disponibilité en tant que groupes plutôt que comme périphériques individuels. Le système peut repérer, signaler et exiger à titre provisoire des correctifs pour les problèmes de groupe que vous pourriez rencontrer. Par exemple, vous ne pouvez pas mettre à niveau une grappe sur des périphériques Firepower 4100/9300 si vous avez effectué des modifications non synchronisées sur le gestionnaire de châssis Firepower. • Nous avons amélioré la vitesse et l'efficacité de la copie des paquets de mise à niveau vers les grappes et les paires à haute disponibilité. Auparavant, FMC copiait le paquet sur chaque membre du groupe dans l'ordre. Désormais, les membres du groupe peuvent se procurer le paquet dans le cadre de leur processus de synchronisation normal. • Vous pouvez désormais préciser l'ordre de mise à niveau des unités de données dans une grappe. L'unité de contrôle est toujours mise à niveau en dernier.
L'amélioration des rapports d'état et de performance de la mise à niveau FTD.	7.0.0	7.0.0	Les mises à niveau de FTD sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Un nouvel onglet **Mises à niveau** dans le centre de messages fournit d'autres améliorations à l'état des mises à niveau et aux rapports d'erreurs.

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

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

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

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

Tableau 8 : Historique des fonctionnalités de mise à niveau de Firewall Management Center

Fonctionnalités	Version minimale du centre de gestion	Défense minimale contre les menaces	Détails
La mise à niveau du Firewall Management Center ne génère pas automatiquement des fichiers de dépannage.	7.2.0	N'importe laquelle	Pour économiser du temps et de l'espace disque, le processus de mise à niveau du Firewall Management Center ne génère plus automatiquement les fichiers de dépannage avant le début de la mise à niveau. Notez que les mises à niveau de périphériques ne sont pas affectées et continuent de générer des fichiers de dépannage. Pour générer manuellement des fichiers de dépannage pour le Firewall Management Center, choisissez **System (Système)**(⚙) > **Health (Intégrité)** > **Monitor (Moniteur)**, cliquez sur **Firewall Management Center** dans le panneau de gauche, sur **View System & Troubleshoot Details** (Afficher les détails du système et du dépannage), puis sur **Generate Troubleshooting Files** (Générer les fichiers de résolution de problèmes).

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

Pour de l'assistance

Guides de mise à niveau

Dans les déploiements Firewall Management Center, le Firewall Management Center doit exécuter une version de maintenance (le troisième chiffre) identique ou plus récente que celle de ses périphériques gérés. Mettez d'abord le Firewall Management Center à niveau, puis les 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

Observations	Guide de mise à niveau	Lien
Firewall Management Center	version Firewall Management Center que vous utilisez *actuellement*.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense avec Firewall Management Center	version Firewall Management Center que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense avec gestionnaire d'appareil	version Firewall Threat Defense que vous utilisez *actuellement*.	https://cisco.com/go/ftd-fdm-upgrade
Firewall 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 Firewall 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

Observations	Guide d'installation	Lien
Firewall Management Center matériel	Guide de démarrage du modèle de Firewall Management Center matériel.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Guide de démarrage pour le Firewall Management Center Virtual	https://cisco.com/go/fmcv-quick
Firewall Threat Defense matériel	Guide de démarrage ou de recréation d'image relatif à votre modèle de périphérique.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Guide de démarrage de votre version Firewall Threat Defense Virtual.	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 résolution de problèmes Cisco FXOS pour le Firewall 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.

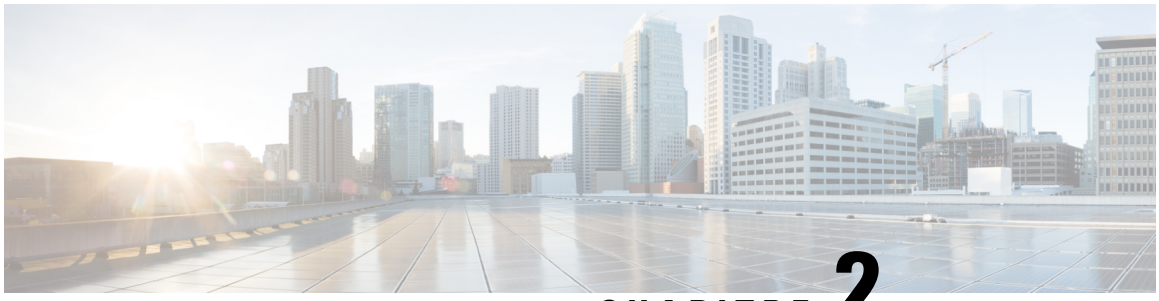
- Documentation : https://cisco.com/go/threatdefense-73-docs
- Site d'assistance et de téléchargement Cisco : https://cisco.com/c/en/us/support/index.html
- Outil de recherche de bogues de Cisco : https://tools.cisco.com/bugsearch/
- Service de notification de Cisco : https://cisco.com/cisco/support/notifications.html

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 7.3.

- Plateformes Firewall Management Center , à la page 19
- Plateformes Firewall Threat Defense , à la page 20
- Gestion du Firewall Threat Defense, à la page 22

Plateformes Firewall Management Center

Le Firewall Management Center fournit une console de gestion de pare-feu centralisée. Pour la compatibilité des périphériques avec le Firewall Management Center, consultez Gestion du Firewall Threat Defense, à la page 22. Pour des informations générales sur la compatibilité, consultez le *Guide de compatibilité de Cisco Secure Firewall Management Center*.

Matériel Firewall Management Center

Version 7.3 prend en charge le matériel Firewall Management Center suivant :

- Firepower Management Center 1600
- Firepower Management Center 2600
- Firepower Management Center 4600

Vous devez également maintenir à jour le micrologiciel du contrôleur BIOS et RAID; consultez les Notes de mise à jour du correctif de Cisco Secure Firewall Threat Defense/Firepower.

Firewall Management Center Virtual

Version 7.3 prend en charge les déploiements Firewall Management Center Virtual dans les nuages publics et privés.

Avec le Firewall Management Center Virtual, vous pouvez acheter une licence pour gérer 2, 10 ou 25 périphériques. Certaines plateformes prennent en charge 300 périphériques. Notez que les licences à deux appareils ne prennent pas en charge la haute disponibilité Firewall Management Center. Pour plus de détails sur les instances prises en charge, consultez le *Guide de démarrage de Cisco Secure Firewall Management Center Virtual*.

Tableau 11 : Plateformes Version 7.3 Firewall Management Center Virtual

Plateforme	Appareils gérés		haute accessibilité
	2, 10, 25	300	
Nuage public			
Alibaba	OUI	—	—
Amazon Web Services (AWS)	OUI	OUI	OUI
Google Cloud Platform (GCP)	OUI	—	—
Microsoft Azure	OUI	—	OUI
Oracle Cloud Infrastructure (OCI)	OUI	OUI	OUI
Nuage privé			
Cisco HyperFlex	OUI	—	OUI
Machine virtuelle basée sur le noyau (KVM)	OUI	OUI	OUI
Nutanix Enterprise Cloud	OUI	—	—
OpenStack	OUI	—	—
VMware vSphere/VMware ESXi 6.5, 6.7 ou 7.0	OUI	OUI	OUI

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) est fourni via Contrôle de Security Cloud, qui unit la gestion de plusieurs solutions de sécurité Cisco. Nous nous assurons des mises à jour des fonctionnalités. Notez qu'un Firewall Management Center déployé par le client est souvent appelé *sur site*, même pour les déploiements dans le nuage public.

Pour des informations à jour sur la compatibilité, consultez le *Guide de compatibilité de Cisco Secure Firewall Management Center*.

Plateformes Firewall Threat Defense

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 Firewall Threat Defense, à la page 22. Pour des informations générales sur la compatibilité, consultez *Guide de compatibilité de Cisco Secure Firewall Threat Defense*.

Matériel Firewall Threat Defense

Le matériel Version 7.3Firewall Threat Defense est proposé en divers débits, capacités d'évolutivité et tailles.

Tableau 12 : Matériel Version 7.3 Firewall Threat Defense

Plateforme	Compatibilité Firewall Management Center		Compatibilité Gestionnaire de périphériques de pare-feu		Notes
	Déployé par le client	Envoyé par nuage	Gestionnaire de périphériques de pare-feu uniquement	Gestionnaire de périphériques de pare-feu + CDO	
Firepower 1010, 1120, 1140, 1150	OUI	OUI	OUI	OUI	L'appareil Firepower 1010E ne peut pas exécuter Threat Defense 7.3. Le soutien sera de retour dans une version ultérieure. Vous pouvez utiliser un centre de gestion de la version 7.3.1et ultérieures pour gérer un appareil Firepower 1010E plus ancien.
Firepower 2110, 2120, 2130, 2140	OUI	OUI	OUI	OUI	—
Secure Firewall 3105, 3110, 3120, 3130, 3140	OUI	OUI	OUI	OUI	Cisco Secure Firewall 3105 nécessite la version 7.3.1 ou ultérieure.
Firepower 4112, 4115, 4125, 4145 Firepower 9300 : modules SM-40, SM-48 et SM-56	OUI	OUI	OUI	OUI	Nécessite la version FXOS 2.13.0.198 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*.

Firewall Threat Defense Virtual

Les implémentations de Version 7.3 Firewall Threat Defense Virtual 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 13 : Plateformes Version 7.3 Firewall Threat Defense Virtual

Plateforme du périphérique	Compatibilité Firewall Management Center		Compatibilité Gestionnaire de périphériques de pare-feu	
	Déployé par le client	Envoyé par nuage	Gestionnaire de périphériques de pare-feu uniquement	Gestionnaire de périphériques de pare-feu + 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
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 Firewall Threat Defense

Selon le modèle et la version du périphérique, nous prenons en charge les méthodes de gestion suivantes.

Firewall Management Center Sur place

Tous les périphériques prennent en charge la gestion à distance avec un Firewall Management Centerdéployé par le client (*sur site*).

Les versions sont majeures (a.x), maintenance (a.x.y) ou correctif (a.x.y.z). Le Firewall Management Center doit exécuter la même version ou une version plus récente que ses périphériques. Les nouvelles fonctionnalités et les correctifs exigent souvent la dernière version tant sur le Firewall Management Center que sur ses périphériques. Mettez d'abord le Firewall Management Center à niveau : vous pourrez toujours gérer les anciens périphériques, généralement quelques versions majeures.

Remarque Vous ne pouvez pas mettre à niveau un périphérique au-delà du Firewall Management Center vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un Firewall Management Centernon corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Notez que dans la plupart des cas, vous pouvez mettre à niveau un périphérique plus ancien directement à la version majeure ou de maintenance de Firewall Management Center. Cependant, il est parfois possible de gérer un périphérique plus ancien que vous ne pouvez pas mettre à niveau directement, même si la version cible est prise en charge sur le périphérique. Dans de rares cas, des problèmes surviennent avec des combinaisons Firewall Management Center-périphérique spécifiques. Pour connaître les exigences propres à la version, consultez les notes de mise à jour.

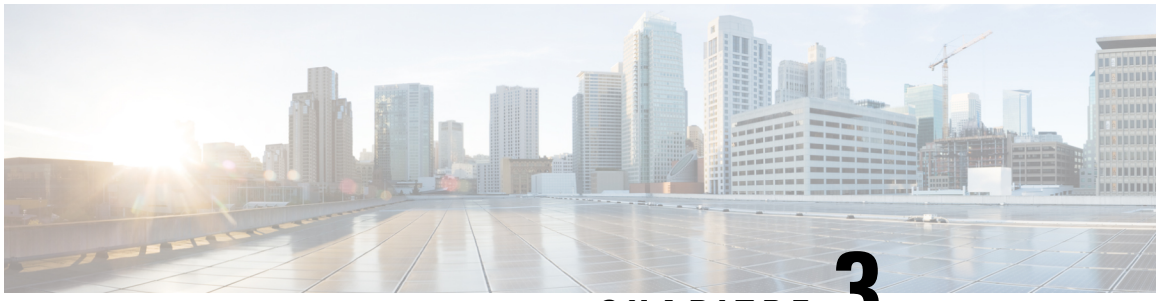
Tableau 14 : Compatibilité du périphérique Firewall Management Centersur site

Version Firewall Management Center	Plus ancienne version de périphérique que vous pouvez gérer
10.x	7.3
7.7	7.2
7.6	7.1
7.4 Dernier soutien pour la gestion des périphériques NGIPS.	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.4	6.1

Version Firewall Management Center	Plus ancienne version de périphérique que vous pouvez gérer
6.2.3	6.1

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Pour la compatibilité de Firewall Threat Defense avec Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez le *Guide de compatibilité de Cisco Secure Firewall Threat Defense*.



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 Firewall Threat Defense. 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 77.

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, à la page 25
- Directives de mise à niveau pour Version 7.3, à la page 26
- Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 28
- Mises à niveau qui ne répondent pas, à la page 28
- Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense, à la page 29
- Flux de trafic et inspection lors du déploiement de configurations, à la page 32
- Temps et espace disque, à la page 33

Version minimale pour la mise à niveau

Version minimale pour la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers Version 7.3, y compris les versions de maintenance, comme suit.

Tableau 15 : Version minimale pour la mise à niveau vers Version 7.3

Plateforme	Version minimale
Firewall Management Center	7

Plateforme	Version minimale
Firewall Threat Defense (sauf Threat Defense Virtual avec GCP)	7 FXOS 2.13.0.198 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, 2.13.
Threat Defense Virtual avec GCP	7.2 Vous ne pouvez pas mettre à niveau à la version 7.2+ à partir de la version 7.1 ou antérieure; vous devez déployer une nouvelle instance.

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 7.3

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

Tableau 16 : Directives de mise à niveau pour Firewall Threat Defense avec Firewall Management Center Version 7.3

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
TOUJOURS VÉRIFIER				
	Version minimale pour la mise à niveau, à la page 25	N'importe laquelle	N'importe laquelle	N'importe laquelle
	Nouvelles fonctionnalités de Cisco Secure Firewall Management Center 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 laquelle	N'importe lequel	N'importe lequel
	Notes de mise à jour de Cisco Secure Firewall Threat Defense, 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 laquelle	N'importe lequel	N'importe lequel

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
	Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), à la page 28	Firewall Threat Defense	N'importe lequel	N'importe lequel
	Directives de mise à niveau pour le châssis Firepower 4100/9300, à la page 77	Firepower 4100/9300	N'importe laquelle	N'importe laquelle
DIRECTIVES SUPPLÉMENTAIRES POUR LES DÉPLOIEMENTS SPÉCIFIQUES				
	Déploiement étendu après la mise à niveau, pour les configurations de taille importante, à la page 27	Firewall Management Center	6.6.0 et les versions ultérieures	7.3.x

Déploiement étendu après la mise à niveau, pour les configurations de taille importante

Déploiement : Firewall Management Center

Mise à niveau à partir de : tout déploiement pour lequel l'optimisation des objets est activée.

Directement à : la version 7.3.x

L'optimisation des objets de contrôle d'accès améliore les performances et consomme moins de ressources de périphérique lorsque vous avez des règles de contrôle d'accès avec des réseaux qui se chevauchent. Les optimisations ont lieu sur le *périphérique géré* lors du premier déploiement, après l'activation de la fonctionnalité sur Firewall Management Center (y compris s'il est activé par une mise à niveau). Si vous avez un grand nombre de règles, le système peut prendre de quelques minutes à une heure pour évaluer vos politiques et effectuer l'optimisation des objets. Pendant ce temps, vous pourriez également constater une utilisation plus élevée du processeur sur vos périphériques. Une situation similaire se produit lors du premier déploiement après la désactivation de la fonctionnalité (y compris si elle est désactivée par la mise à niveau). Une fois cette fonctionnalité activée ou désactivée, nous vous recommandons de la déployer au moment où elle aura le moins d'incidence, comme une fenêtre de maintenance ou une période de faible trafic.

Pour planifier, utilisez le tableau suivant.

Tableau 17 : Planification des mises à niveau du Firewall Management Center avec optimisation des objets

Version	Paramètre par défaut/de recréation d'image	Mise à niveau	Pour Activer/Désactiver
7.0.5 et versions antérieures	Non pris en charge (désactivé).	—	—
7.0.6 ou version ultérieure, versions de maint.	Disabled (Désactivé)	Respecte votre paramètre actuel.	Communiquez avec le Centre d'assistance technique Cisco (TAC).

Version	Paramètre par défaut/de recréation d'image	Mise à niveau	Pour Activer/Désactiver
7.1.0 à 7.2.3	Non pris en charge (désactivé).	Désactive.	—
7.2.4 à 7.2.5	Activé.	Active.	Communiquez avec le Centre d'assistance technique Cisco (TAC).
7.3.x	Non pris en charge (désactivé).	Désactive.	—
7.4.0	Activé.	Active.	Communiquez avec le Centre d'assistance technique Cisco (TAC).

Directives de mise à niveau pour Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Vous ne mettez pas à niveau le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage). Nous nous assurons des mises à jour des fonctionnalités. Pour mettre à niveau Firewall Threat Defense avec le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez le Guides de mise à niveau de Cisco Secure Firewall Threat Defense pour le Firewall Management Center en Nuage.

Mises à niveau qui ne répondent pas

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

Mise à niveau ne répondant pas

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

Mise à niveau Firewall Threat Defense sans réponse

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

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

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

Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense

Mises à niveau logicielles pour les périphériques autonomes

Les périphériques fonctionnent en mode maintenance pendant leur mise à niveau. Le passage en mode maintenance au début de la mise à niveau entraîne une interruption de 2 à 3 secondes dans l'inspection du trafic. Les configurations des interfaces déterminent la façon dont un périphérique autonome gère le trafic à ce moment-là et pendant la mise à niveau.

Tableau 18 : Flux de trafic et inspection : mises à niveau logicielles pour les périphériques autonomes

Configuration de l'interface		Comportement du trafic
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné. Pour les interfaces de groupe de ponts sur ISA 3000 uniquement, vous pouvez utiliser une politique FlexConfig pour configurer le contournement matériel en cas de panne de courant. Cela entraîne une baisse du trafic pendant les mises à niveau logicielles, mais sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Configuration de l'interface		Comportement du trafic
Interfaces IPS uniquement	Ensemble en ligne, contournement matériel activé de force : **contournement : forcé**	Réussite sans inspection jusqu'à ce que vous désactiviez le contournement matériel ou que vous le remettiez en mode veille.
	Ensemble en ligne, contournement matériel en mode veille : **Contournement : en veille**	Abandonné lors de la mise à niveau, alors que le périphérique est en mode de maintenance. Ensuite, réussite sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.
	Ensemble en ligne, contournement matériel désactivé : **contournement : désactivé**	Abandonné.
	Ensemble en ligne, pas de module de contournement matériel.	Abandonné.
	en ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	sans interruption, sans inspection

Mises à niveau logicielles pour une disponibilité et une évolutivité élevées

Vous ne devriez pas subir d'interruptions dans le flux de trafic ou l'inspection lors de la mise à niveau des périphériques à haute disponibilité ou en grappe. Pour les paires à haute disponibilité, le périphérique de secours est mis à niveau en premier. Les périphériques changent de rôle, puis le nouvel appareil en attente effectue la mise à niveau.

Dans le cas des grappes, le ou les modules de sécurité des données sont mis à niveau en premier, puis le module de contrôle. Pendant la mise à niveau du module de contrôle de sécurité, bien que l'inspection et le traitement du trafic se poursuivent normalement, le système interrompt la journalisation des événements. Les événements du trafic traité pendant le temps d'arrêt de la journalisation s'affichent avec des horodatages non synchronisés une fois la mise à niveau terminée. Toutefois, si le temps d'arrêt pour la journalisation est important, le système peut supprimer les événements les plus anciens avant de pouvoir être journalisés.

Notez que les mises à niveau transparentes ne sont pas prises en charge pour les grappes à une seule unité. Les interruptions du flux de trafic et de l'inspection dépendent des configurations d'interface de l'unité active, tout comme pour les périphériques autonomes.

Restauration logicielle (versions majeures et de maintenance)

Vous devez vous attendre à des interruptions du flux de trafic et de l'inspection pendant la reprise, même dans un déploiement à disponibilité et à évolutivité élevée. En effet, la restauration fonctionne mieux lorsque toutes les unités sont restaurées simultanément. La restauration simultanée signifie que les interruptions du flux de trafic et de l'inspection dépendent des configurations des interfaces uniquement, comme si chaque périphérique était autonome.

Désinstallation logicielle (correctifs)

Pour les périphériques autonomes, les interruptions du flux de trafic et de l'inspection pendant la désinstallation du correctif sont les mêmes que pour la mise à niveau. Dans les déploiements à haute disponibilité et évolutivité,

vous devez explicitement planifier un ordre de désinstallation qui réduit les perturbations au minimum. En effet, vous désinstallez les correctifs des périphériques individuellement, même ceux que vous avez mis à niveau sous forme d'unité.

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 et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. 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.

Tableau 19 : Flux de trafic et inspection : déploiement des modifications de configuration

Configuration de l'interface		Comportement du trafic
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné.
Interfaces IPS uniquement	Ensemble en ligne : **Failsafe** (sécurité intégrée) activée ou désactivée	Réussi sans inspection Quelques paquets peuvent être perdus si l'option **Failsafe** est désactivé et si le processus Snort est occupé mais pas arrêté.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	Abandonné.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	Réussi sans inspection
	en ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	sans interruption, sans inspection

Flux de trafic et inspection lors du déploiement de configurations

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Cela signifie que pour les mises à niveau Firewall Management Center, Snort peut redémarrer sur tous les périphériques gérés. Snort ne redémarre pas après les déploiements suivants, sauf si, préalablement au déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

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 et l'évolutivité. Les configurations de l'interface déterminent si le trafic chute ou s'il passe sans inspection pendant l'interruption. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Tableau 20 : Flux de trafic et inspection : déploiement des modifications de configuration

Configuration de l'interface		**Comportement du trafic**
Interfaces de pare-feu	Routées ou commutées, y compris EtherChannel, redondant, sous-interfaces. Les interfaces commutées sont également appelées interfaces de groupe de ponts ou interfaces transparentes.	Abandonné.
Interfaces IPS uniquement	Ensemble en ligne : **Failsafe** (sécurité intégrée) activée ou désactivée	Réussi sans inspection Quelques paquets peuvent être perdus si l'option **Failsafe** est désactivé et si le processus Snort est occupé mais pas arrêté.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : désactivée	Abandonné.
	Ensemble en ligne : **Snort Fail Open: Down** (admission même en cas de non-conformité de Snort : inactif) : activés	Réussi sans inspection
	En ligne : tap mode (mode Tap)	Sortie de paquet immédiate, copie non inspectée.
	Passif, ERSPAN passif.	Sans interruption, sans inspection

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.

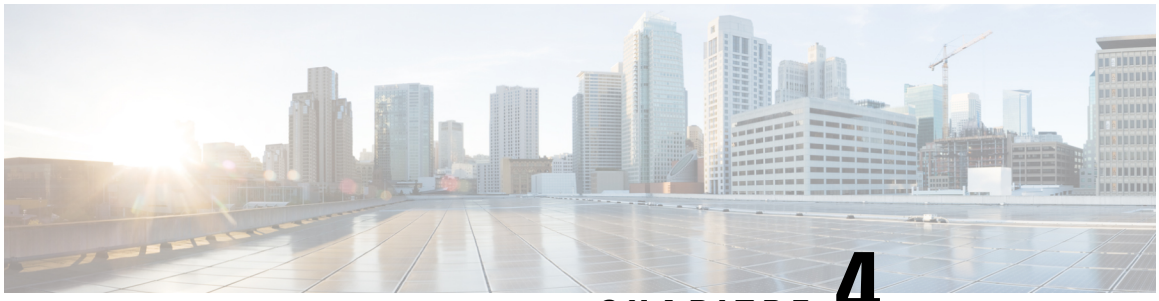
Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système 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 Mises à niveau qui ne répondent pas, à la page 28.

Tableau 21 : 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 et mise en grappe	Dans une configuration à haute disponibilité ou en grappe, les périphériques sont mis à niveau un par un afin de préserver la continuité des opérations, chaque périphérique fonctionnant en mode maintenance pendant sa mise à niveau. Par conséquent, la mise à niveau d'une paire de périphériques ou d'une grappe complète prend plus de temps que la mise à niveau d'un périphérique autonome.
Configurations	Le délai de mise à niveau peut augmenter en fonction de la complexité de vos configurations, de la taille de vos bases de données d'événements 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 l'appliance. Pour les mises à niveau de périphérique, vous devez également disposer d'un espace suffisant sur le Firewall Management Center (dans / Volume ou /var) pour le paquet de mise à niveau du périphérique. Sinon, vous pouvez utiliser un serveur interne pour les stocker. 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.



CHAPITRE 4

Mettre à niveau le Firewall Management Center

Ce chapitre explique comment mettre à niveau un Firewall Management Center local qui *exécute actuellement la* Version 7.3.

- Liste de contrôle des mises à niveau pour Firewall Management Center, à la page 35
- Chemin de mise à niveau pour Firewall Management Center, à la page 39
- Charger les paquets de mise à niveau pour Firewall Management Center, à la page 41
- Exécuter la vérification de l'état de préparation pour Firewall Management Center, à la page 42
- Mettre à niveau le Firewall Management Center : autonome, à la page 43
- Mettre à niveau le Firewall Management Center : Haute disponibilité, à la page 44

Liste de contrôle des mises à niveau pour Firewall Management Center

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/évolutivité, si vos appareils sont déployés en tant qu'IPS ou pare-feu, etc.

✓	Action/Vérification	Détails
	Planifiez votre chemin de mise à niveau.	Cela est particulièrement important pour les déploiements importants, 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 : • Chemin de mise à niveau pour Firewall Management Center, à la page 39 • Chemins de mise à niveau pour Firewall Threat Defense, à la page 53 • Chemins de mise à niveau pour FXOS, à la page 79
	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 25, pour les directives relatives aux mises à niveau critiques et spécifiques aux versions. • *Nouvelles fonctionnalités de Cisco Secure Firewall Management Center 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. • Notes de mise à jour de Cisco Secure Firewall Threat Defense, 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 mise à jour de Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.
	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.
	Planifiez des périodes de maintenance.	Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant particulièrement compte du temps que la mise à niveau est susceptible de prendre. Tenez compte des tâches que vous devez effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Voir 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. Sauvegardez Firewall Management Center après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde Firewall Management Center « sache » que ses périphériques ont été mis à niveau.

✓	Action/Vérification	Détails
	Sauvegardez les configurations et les événements.	Consultez le chapitre *Sauvegarde/restauration* dans le *Guide d'administration de Cisco Secure Firewall Management Center*.

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 Firewall Management Center.	Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco. Vous pouvez également utiliser le Firewall Management Center pour effectuer un téléchargement direct. Pour une haute disponibilité Firewall Management Center, vous devez téléverser le paquet de mise à niveau Firewall Management Center sur les deux homologues, en suspendant la synchronisation avant de transférer le paquet sur le paquet de secours. Pour limiter les interruptions de la synchronisation, vous pouvez transférer le paquet vers l'homologue actif pendant l'étape de préparation de la mise à niveau, et vers l'homologue de secours dans le cadre du processus de mise à niveau lui-même, après avoir suspendu la synchronisation. Consultez Charger les paquets de mise à niveau pour Firewall Management Center, à la page 41.

Mises à niveau associées

Nous vous recommandons d'effectuer les mises à niveau de l'environnement d'hébergement pendant une fenêtre 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.

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. Bien que le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, il convient de toujours vérifier manuellement. La désynchronisation peut entraîner l'échec de la mise à niveau. Pour vérifier l'heure : • Firewall Management Center : Choisissez **Système** (⚙) > **Configuration** > **Time (Heure)**. • Firewall Threat Defense : Utilisez la commande **show time** de l'interface de ligne de commande.
	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 Firewall Threat Defense, à la page 29.
	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 Exécuter la vérification de l'état de préparation pour Firewall Management Center, à la page 42.
	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 Firewall Management Center, choisissez **Système** (⚙) > **Monitoring (Supervision)** > **Statistics (Statistiques)** et sélectionnez le Firewall Management Center. Sous Disk Usage (Utilisation du disque), développez les informations de By partition (Par partition).

✓	Action/Vérification	Détails
	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 reprises. Les mises à niveau reportent automatiquement les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. Si vous ne souhaitez pas que cela se produise, vérifiez les tâches programmées pour s'exécuter lors de la mise à niveau et annulez ou reportez-les.

Chemin de mise à niveau pour Firewall Management Center

Ce tableau fournit le chemin de mise à niveau pour les Firewall Management Center déployés par le client.

Mettez d'abord le Firewall Management Center à niveau. Vous ne pouvez pas mettre à niveau un périphérique au-delà du Firewall Management Center vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un Firewall Management Centernon corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Notez que si votre version actuelle Firewall Threat Defense/Firewall Management Center 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 Firewall Management Center

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
7.2	Une des versions suivantes : → 7.4.x → 7.3.x → Toute version ultérieure à 7.2.x

Version actuelle	Version cible
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 de FMC 1000, 2500 et 4500	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+.
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 de FMC 2000 et 4000.	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Toute version ultérieure à 6.6.x **Remarque** En raison d'incompatibilités avec la banque de données, vous ne pouvez pas mettre à niveau Firewall Management Center de la version 6.6.5+ à la version 6.7.0. Nous vous recommandons de procéder à une mise à niveau directe vers la version 7.0+.

Version actuelle	Version cible
6.5	Une des versions suivantes : → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Dernière prise en charge de FMC 750, 1500 et 3500.	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	Une des versions suivantes : → 6.6.x → 6.5 → 6.4 → 6.3

Charger les paquets de mise à niveau pour Firewall Management Center

Utilisez cette procédure pour charger manuellement les paquets de mise à niveau sur le Firewall Management Center.



Astuces Sélectionnez les paquets de mise à niveau disponibles pour le téléchargement direct quelque temps après que la version puisse être téléchargée manuellement. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. SI le Firewall Management Center dispose d'un accès Internet, cliquez sur le bouton **Download Updates** (Télécharger les mises à jour) pour télécharger immédiatement la dernière VDB, la dernière version de maintenance et les derniers correctifs critiques pour le Firewall Management Center et tous les périphériques gérés.

Les paquets de mise à niveau Sont des archives TAR signées (.tar). Après avoir chargé un paquet signé, la page System Updates (Mises à jour du système) sur le Firewall Management Center peut prendre plus de temps à se charger pendant la vérification du paquet. Pour accélérer l'affichage, supprimez les paquets de mises à niveau inutiles. Ne pas décompresser les paquets signés.

Avant de commencer

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

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

Procédure

Étape 1 Téléchargez le paquet de mise à niveau à partir du Site d'assistance et de téléchargement Cisco : https://www.cisco.com/go/firepower-software.

Vous utilisez le même paquet de mises à niveau logicielles pour tous les modèles d'une famille ou d'une série. Pour trouver le bon modèle, sélectionnez ou recherchez votre modèle, 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 rapide), la version du logiciel et la version, comme suit :

```
Cisco_Secure_FW_Mgmt_Center_Upgrade-7.3-999.sh.REL.tar
```

Étape 2 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 3 Cliquez sur **Charger la mise à jour**.

Étape 4 Pour l'**Action**, cliquez sur le bouton radio **Upload local software update package** (Charger le paquet de mise à jour du logiciel local).

Étape 5 Cliquez sur **Choisir le fichier**.

Étape 6 Accédez au paquet et cliquez sur **Charger**.

Exécuter la vérification de l'état de préparation pour Firewall Management Center

Utilisez cette procédure pour exécuter les vérifications de l'état de préparation de Firewall Management Center.

Les vérifications de l'état de préparation évaluent l'état de préparation pour les mises à niveau majeures et de maintenance. Si vous échouez aux vérifications de l'état de préparation, vous ne pouvez pas procéder à la mise à niveau tant que vous n'avez pas corrigé les problèmes. Le temps nécessaire pour exécuter une vérification

de l'état de préparation varie en fonction du modèle et de la taille de la base de données. Ne redémarrez pas ou n'arrêtez pas les vérifications de l'état de préparation manuellement.

Avant de commencer

Chargez le paquet de mise à niveau vers le Firewall Management Center.

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Sous Mises à jour disponibles, cliquez sur l'icône **Install** (installer) à côté du paquet de mise à niveau, puis choisissez Firewall Management Center.

Étape 3 Cliquez sur **Check Readiness** (Vérifier l'état de préparation).

Vous pouvez surveiller l'état de préparation de la mise à jour dans le centre de messages.

Prochaine étape

Sur **Système** (⚙) > **Mises à jour**, cliquez sur **Readiness Checks** (Vérifications de l'état de préparation) pour afficher l'état de vérification de la préparation pour l'ensemble de votre déploiement, y compris les vérifications en cours et les vérifications ayant échoué. Vous pouvez également utiliser cette page pour réexécuter facilement les vérifications après un échec.

Mettre à niveau le Firewall Management Center : autonome

Utilisez cette procédure pour mettre à niveau un périphérique autonome Firewall Management Center.

⚠

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 redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement 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 avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC)

Avant de commencer

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

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Sous Mises à jour disponibles, cliquez sur l'icône **Install** (installer) à côté du paquet de mise à niveau, puis choisissez Firewall Management Center.

Étape 3 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer.

Vous pouvez surveiller la progression de la vérification préalable dans le centre de messages jusqu'à ce que vous soyez déconnecté.

Étape 4 Reconnectez-vous à quand cela est possible.

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

Étape 5 Vérifiez la réussite de la mise à niveau.

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

Étape 6 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Si le site d'assistance et de téléchargement Cisco dispose d'une version plus récente, installez-la. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 7 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 8 Déployez de nouveau les configurations sur tous les périphériques gérés.

Mettre à niveau le Firewall Management Center : Haute disponibilité

La mise à niveau de la haute disponibilité Firewall Management Centers'effectue une à la fois. Une fois la synchronisation suspendue, mettez à niveau le serveur de secours. Lorsque la mise à niveau en veille est terminée, Firewall Management Center devient actif, ce qui vous permet de mettre à niveau l'autre Firewall Management Center. Cet état temporaire s'appelle *split-brain* (déconnexion cérébrale) et n'est pris en charge que pendant une mise à niveau ou la désinstallation d'un correctif.. Ne pas effectuer ou déployer de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale). Vos modifications seront perdues après le redémarrage de la synchronisation. Le déploiement pourrait placer le système dans un état inutilisable et nécessiter une recréation d'image.

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 redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement 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 avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC)

Avant de commencer

Remplissez la liste de contrôle avant la mise à niveau pour les deux homologues. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Sur le Firewall Management Center actif, suspendez la synchronisation.

a) Choisissez **Integration (Intégration)** > **Other Integrations (Autres intégrations)**.
b) Sous l'onglet **High Availability**, cliquez sur **Suspendre la synchronisation**.

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

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

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

Suivez les instructions dans Mettre à niveau le Firewall Management Center : autonome, à la page 43, en vous arrêtant après avoir vérifié la réussite de la mise à jour sur chaque homologue. En résumé, pour chaque homologue :

a) Sur **Système** (⚙) > **Mises à jour**, installez le fichier de mise à niveau.
b) Surveillez la progression jusqu'à ce que vous soyez déconnecté, puis reconnectez-vous lorsque possible (cela peut se produire deux fois).
c) Vérifiez la réussite de la mise à niveau.

Étape 4 Sur le Firewall Management Center que vous souhaitez définir comme homologue actif, redémarrez la synchronisation.

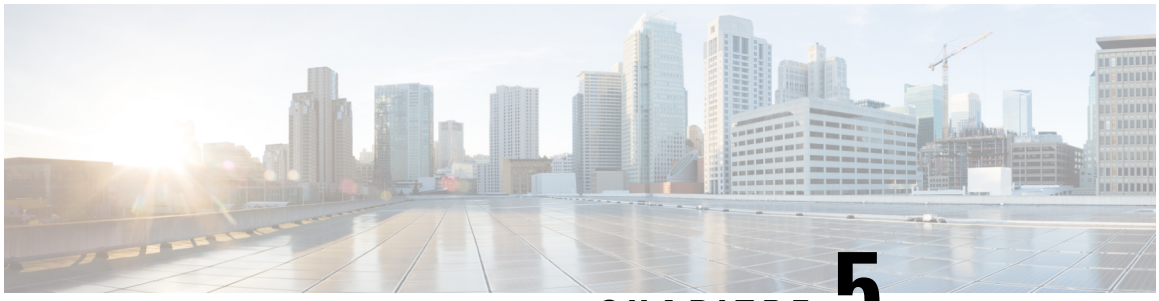
a) Choisissez **Integration (Intégration)** > **Other Integrations (Autres intégrations)**.
b) Sous l'onglet **High Availability (haute disponibilité**), cliquez sur **Make-Me-Active** (Rendez-moi actif).
c) Attendez que la synchronisation redémarre et que l'autre Firewall Management Center passe en mode veille.

Étape 5 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Si le site d'assistance et de téléchargement Cisco dispose d'une version plus récente, installez-la. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 6 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 7 Déployez de nouveau les configurations sur tous les périphériques gérés.



CHAPITRE 5

Mise à niveau Firewall Threat Defense

Ce chapitre explique comment utiliser un Version 7.3 Firewall Management Center pour mettre à niveau Firewall Threat Defense. Si votre Firewall Management Center exécute une version différente ou si vous utilisez Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), consultez Ce guide est-il pour vous?, à la page 1.

- Liste de contrôle des mises à niveau pour Firewall Threat Defense, à la page 47
- Chemins de mise à niveau pour Firewall Threat Defense, à la page 53
- Paquets de mise à niveau pour Firewall Management Center et Firewall Threat Defense, à la page 59
- Mettre à niveau Firewall Threat Defense à l'aide de l'assistant (désactiver la restauration), à la page 66
- Mettre à niveau Firewall Threat Defense à l'aide de l'assistant en mode sans surveillance (désactiver la restauration), à la page 70
- Mettre à niveau Firewall Threat Defense via System (Système) > Updates (Mises à jour) (Enable Revert (Activer la restauration)), à la page 74

Liste de contrôle des mises à niveau pour Firewall Threat Defense

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/évolutivité, si vos appareils sont déployés en tant qu'IPS ou pare-feu, etc.

✓	Action/Vérification	Détails
	Planifiez votre chemin de mise à niveau.	Cela est particulièrement important pour les déploiements importants, 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 : • Chemin de mise à niveau pour Firewall Management Center, à la page 39 • Chemins de mise à niveau pour Firewall Threat Defense, à la page 53 • Chemins de mise à niveau pour FXOS, à la page 79
	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 25, pour les directives relatives aux mises à niveau critiques et spécifiques aux versions. • *Nouvelles fonctionnalités de Cisco Secure Firewall Management Center 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. • Notes de mise à jour de Cisco Secure Firewall Threat Defense, 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 mise à jour de Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.

✓	Action/Vérification	Détails
	Décidez s'il faut utiliser l'assistant ou la page System Updates (Mises à jour du système).	Certains des éléments de la liste de contrôle font référence à l'utilisation de l'assistant de mise à niveau de Firewall Threat Defense sur la page System Updates (Mises à jour du système). L'assistant vous guide à travers les étapes de mise à niveau importantes, y compris la sélection des périphériques à mettre à niveau, la copie de l'ensemble de mises à niveau sur les périphériques, ainsi que les vérifications de la compatibilité et de l'état de préparation. Les mises à niveau effectuées avec cet assistant sont maintenant plus faciles, plus rapides, plus fiables et elles prennent moins d'espace disque. Nous vous recommandons généralement d'utiliser l'assistant pour mettre à niveau Firewall Threat Defense. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0 cependant, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour**. Vous devez également utiliser la page System Updates (mises à jour du système) pour la suppression des paquets de mise à niveau et pour mettre à niveau les périphériques Firewall Management Center et les périphériques plus anciens.
	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 . Vous devriez également pouvoir accéder à l'interface de gestion du Firewall Management Center sans traverser le périphérique.
	Vérifiez la bande passante.	Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. 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 ou même entraîner son expiration. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).
	Planifiez des périodes de maintenance.	Planifiez les périodes de maintenance lorsqu'elles auront le moins d'impact, en tenant compte de tout effet sur le flux de trafic et l'inspection, et le temps que 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 châssis, à la page 78 • 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. Sauvegardez Firewall Management Center après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde Firewall Management Center « sache » que ses périphériques ont été mis à niveau.

✓	Action/Vérification	Détails
	Sauvegardez Firewall Threat Defense.	Utilisez le Firewall Management Center pour sauvegarder les configurations Firewall Threat Defense, lorsqu'elles sont prises en charge. Consultez le chapitre *Sauvegarde/restauration* dans le *Guide d'administration de Cisco Secure Firewall Management Center*. Si vous avez un Firepower 9300 avec Firewall Threat Defense 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 Firewall Chassis Manager 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 les paquets de mise à niveau à partir de Cisco et chargez-les sur le Firewall Management Center ou le serveur web interne.	Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : Paquets de mise à niveau pour Firewall Management Center et Firewall Threat Defense, à la page 59. Vous pouvez également utiliser le Firewall Management Center pour effectuer un téléchargement direct : Charger les paquets de mise à niveau avec le Firewall Management Center, à la page 60. Chargez les paquets de mise à niveau des périphériques sur le Firewall Management Center ou configurez les périphériques pour les obtenir à partir d'un serveur interne : • Charger les paquets de mise à niveau Firewall Threat Defense avec l'assistant, à la page 61 • Charger les paquets de mise à niveau Firewall Threat Defense avec Système > Mises à jour, à la page 63 Pour les périphériques Firepower 4100/9300, les instructions de chargement FXOS sont incluses dans les procédures de mise à niveau FXOS.
	Copiez les paquets de mise à niveau vers les périphériques.	Pour mettre à niveau Firewall Threat Defense, le paquet de mise à niveau doit se trouver sur le périphérique. L'assistant de mise à niveau de Threat Defense vous invite à copier les paquets de mise à niveau sur les périphériques qui en ont besoin. Sinon, vous pouvez utiliser la page System Updates (Mises à jour du système).

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 Firewall Threat Defense et les grappes interchâssis un châssis à la fois. Consultez Mettre à niveau le châssis sur le Firepower 4100/9300, à la page 77.

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. Bien que le moniteur d'intégrité signale si les horloges ne sont pas synchronisées de plus de 10 secondes, il convient de toujours vérifier manuellement. La désynchronisation peut entraîner l'échec de la mise à niveau. Pour vérifier l'heure : • Firewall Management Center : Choisissez **Système** (⚙) > **Configuration** > **Time (Heure)**. • Firewall Threat Defense : Utilisez la commande **show time** de l'interface de ligne de commande.
	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 Firewall Threat Defense, à la page 29.
	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. L'assistant de mise à niveau de Firewall Threat Defense vous invite à effectuer des vérifications de l'état de préparation. Sinon, vous pouvez utiliser la page System Updates (Mises à jour du système).
	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 un périphérique, choisissez **Système** (⚙) > **Monitoring (Supervision)** > **Statistics (Statistiques)** et sélectionnez le périphérique que vous souhaitez vérifier. Sous Disk Usage (Utilisation du disque), développez les informations de By partition (Par partition).

✓	Action/Vérification	Détails
	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 reprises. Les mises à niveau reportent automatiquement les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. Si vous ne souhaitez pas que cela se produise, vérifiez les tâches programmées pour s'exécuter lors de la mise à niveau et annulez ou reportez-les.

Chemins de mise à niveau pour Firewall Threat Defense

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

Mettez d'abord le Firewall Management Center à niveau. Vous ne pouvez pas mettre à niveau un périphérique au-delà du Firewall Management Center vers une version majeure ou de maintenance plus récente. Bien qu'un périphérique corrigé (quatre chiffres) puisse être géré avec un Firewall Management Centernon corrigé, les déploiements entièrement corrigés sont soumis à des tests avancés.

Chemin de mise à niveau pour Firewall Threat Defense sans FXOS

Ce tableau fournit le chemin de mise à niveau pour Firewall Threat Defense lorsque vous n'avez pas besoin de mettre à niveau le système d'exploitation. Cela comprend Cisco Secure Firewall 3100 en mode périphérique, les séries Firepower 1000/2100, la série ASA-5500-X et l'ISA 3000.

Notez que si votre version actuelle Firewall Threat Defense/Firewall Management Center 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.

Remarque En raison des modifications de l'interface requises pour prendre en charge l'évolutivité automatique, les mises à niveau de Threat Defense Virtual pour GCP ne peuvent pas dépasser la version 7.2.0. C'est-à-dire que vous ne pouvez pas mettre à niveau vers la version 7.2.0+ à partir de la version 7.1.x ou des versions antérieures. Vous devez déployer une nouvelle instance et refaire toutes les configurations propres au périphérique.

Tableau 23 : Mises à niveau directes de Firewall Threat Defense

Version actuelle	Version cible
7.4	→ Toute version ultérieure à 7.4.x

Version actuelle	Version cible
7.3	Une des versions suivantes : → 7.4.x → Toute version ultérieure à 7.3.x
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 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** Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer les périphériques Firewall Threat Defense 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

Chemin de mise à niveau pour Firewall Threat Defense avec FXOS

Ce tableau fournit le chemin de mise à niveau pour Firewall Threat Defense sur le Firepower 4100/9300.

Notez que si votre version actuelle Firewall Threat Defense/Firewall Management Center 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 ou des instances d'applications. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le *Guide de compatibilité de Cisco Secure Firewall Threat Defense*.

Tableau 24 : Firewall Threat Defense Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Firewall Threat Defense7.3	→ FXOS 2.13 avec toute version ultérieure de Firewall Threat Defense 7.3.x
FXOS 2.12 avec Firewall 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 Firewall Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Firewall Threat Defense 7.2.x
FXOS 2.11.1 avec Firewall Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Firewall Threat Defense 7.1.x

Versions actuelles	Versions cibles
FXOS 2.10.1 avec Firewall Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Firewall 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** Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer les périphériques Firewall Threat Defense 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 Firewall Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Firewall Threat Defense 6.7.x
FXOS 2.8.1 avec Firewall Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Firewall Threat Defense 6.6.x

Versions actuelles	Versions cibles
FXOS 2.7.1 avec Firewall Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x
FXOS 2.6.1 avec Firewall Threat Defense 6.4	Une des versions suivantes : → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5
FXOS 2.4.1 avec Firewall Threat Defense 6.3	Une des versions suivantes : → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4
FXOS 2.3.1 avec Firewall Threat Defense 6.2.3	Une des versions suivantes : → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4 → FXOS 2.4.1 avec Firewall Threat Defense 6.3

Ordre de mise à niveau pour Firewall Threat Defense haute disponibilité/évolutivité avec FXOS

Même dans les déploiements à disponibilité et à évolutivité élevées, 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. Pour les mises à niveau Firewall Threat Defense, le système met automatiquement à niveau un périphérique groupé à la fois.

Tableau 25 : Ordre de mise à niveau FXOS-Threat Defense pour Firepower 4100/9300

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Autonomes	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Haute disponibilité	Mettez à niveau FXOS sur les deux châssis avant de mettre à niveau Firewall Threat Defense. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. **1.** Mettez à niveau FXOS sur le châssis avec le serveur de secours. **2.** Changez de rôle. **3.** Mettez à niveau FXOS sur le châssis avec le nouveau serveur de secours. **4.** Mettez à niveau Firewall Threat Defense.
Grappe intrachâssis (unités sur le même châssis)	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.
Grappe inter-châssis (unités sur des châssis différents)	Mettez à niveau FXOS sur tous les châssis avant de mettre à niveau Firewall Threat Defense. Pour réduire au minimum les perturbations, mettez toujours à niveau un châssis d'unités de données. **1.** Mettez à niveau FXOS sur un châssis de l'unité de données. **2.** Basculez le module de contrôle sur le châssis que vous venez de mettre à niveau. **3.** Mettez à niveau FXOS sur les châssis restants. **4.** Mettez à niveau Firewall Threat Defense.

Paquets de mise à niveau pour Firewall Management Center et Firewall Threat Defense

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 26 : Paquets de mise à niveau logicielle

Plateforme	Paquet de mise à niveau
Série Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-7.3-999.sh.REL.tar
Série Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-7.3-999.sh.REL.tar
Cisco Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.3-999.sh.REL.tar
Cisco Secure Firewall 4200 series	Cisco_Secure_FW_TD_4200_Upgrade-7.3-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP-FP3K_Upgrade-7.3-999.sh.REL.tar
Firewall Threat Defense Virtual	Cisco_FTD_Upgrade-7.3-999.sh.REL.tar
ISA 3000 avec FTD	Cisco_FTD_Upgrade-7.3-999.sh.REL.tar

Astuces De nombreux paquets de mise à niveau deviennent disponibles pour le téléchargement direct quelque temps après que la version puisse être téléchargée manuellement. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs. Pour en savoir plus, consultez Charger les paquets de mise à niveau avec le Firewall Management Center, à la page 60.

Charger les paquets de mise à niveau avec le Firewall Management Center

De nombreux paquets de mise à niveau deviennent disponibles pour le téléchargement direct quelque temps après que la version puisse être téléchargée manuellement. La durée du délai dépend du type de version, de l'adoption de la version et d'autres facteurs.

Avant de commencer

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

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

Étape 2 Choisissez à partir de ces options de téléchargement direct :

- Cliquez sur le bouton **Download Updates** (Télécharger les mises à jour) pour télécharger immédiatement la dernière VDB, la dernière version de maintenance et les derniers correctifs critiques pour votre déploiement.
- Sous l'onglet **Product Updates** (Mises à jour de produits), cliquez sur le sous-onglet **Download Updates** (Télécharger les mises à jour) pour choisir les paquets de mise à niveau Firewall Threat Defense à télécharger. Passez à l'étape suivante.

Étape 3 Cliquez sur **Actualisation** ( ).
Le système interroge Cisco et affiche les mises à niveau disponibles pour vos appareils Firewall Threat Defense.

Étape 4 Sélectionnez les paquets de mise à niveau que vous souhaitez télécharger et cliquez sur **Download Major Updates** (Télécharger les mises à jour majeures).

Charger les paquets de mise à niveau Firewall Threat Defense avec l'assistant

Charger les paquets de mise à niveau Firewall Threat Defense avec l'assistant Firewall Management Center

Vous pouvez utiliser l'assistant pour charger des paquets de mise à niveau vers l Firewall Management Center.

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

Étape 2 Cliquez sur **Add Upgrade Package** (Ajouter un paquet de mise à niveau).

Étape 3 Cliquez sur le bouton radio **Upload upgrade package** (Charger un paquet de mise à niveau).

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

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

Prochaine étape

(Facultatif) Pour voir et gérer tous les paquets de mise à niveau téléversés, choisissez **Système** ( ) > **Mises à jour**. Les paquets de mise à niveau chargés et les URL des paquets de mise à niveau sont listés ensemble, mais étiquetés distinctement. sont des archives TAR signées (.tar). Après avoir téléchargé un paquet signé, la page System Updates peut prendre plus de temps à se téléverser pendant la vérification du paquet. Pour accélérer l'affichage, supprimez les ensembles de mises à niveau inutiles. Ne pas décompresser les paquets signés.

Chargez les paquets de mise à niveau Firewall Threat Defense sur un serveur interne avec le système (Système) > Mises à jour (Updates)

Utilisez cette procédure pour configurer les périphériques Firewall Threat Defense afin d'obtenir les paquets de mise à niveau à partir d'un serveur web interne, plutôt qu'à partir du Firewall Management Center. Cela est particulièrement utile si la bande passante entre le Firewall Management Center et ses périphériques est limitée. Cela permet également de gagner de la place sur le Firewall Management Center.

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

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

Avant de commencer

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

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

Étape 2 Cliquez sur **Add Upgrade Package** (Ajouter un paquet de mise à niveau).

Étape 3 Cliquez sur le bouton radio **Specify remote location** (Spécifier l'emplacement distant).

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

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

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

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

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

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

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

Prochaine étape

(Facultatif) Pour voir et gérer tous les paquets de mise à niveau associés, choisissez **Système** (⚙) > **Mises à jour**. Les paquets de mise à niveau chargés et les URL des paquets de mise à niveau sont listés ensemble, mais étiquetés distinctement. sont des archives TAR signées (.tar). Après avoir téléchargé un paquet signé, la page System Updates peut prendre plus de temps à se téléverser pendant la vérification du paquet. Pour accélérer l'affichage, supprimez les ensembles de mises à niveau inutiles. Ne pas décompresser les paquets signés.

Charger les paquets de mise à niveau Firewall Threat Defense avec Système > Mises à jour

Chargez les paquets de mise à niveau Firewall Threat Defense vers le Firewall Management Center avec System (Système) > Updates (Mises à jour)

sont des archives TAR signées (.tar). Après avoir téléchargé un paquet signé, la page System Updates peut prendre plus de temps à se téléverser pendant la vérification du paquet. Pour accélérer l'affichage, supprimez les ensembles de mises à niveau inutiles. Ne pas décompresser les paquets signés.

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

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

Étape 3 Pour l'**Action**, cliquez sur le bouton radio **Upload local software update package** (Charger le paquet de mise à jour du logiciel local).

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

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

Étape 6 (Facultatif) Copiez les paquets de mise à niveau vers les périphériques gérés.

Si vous n'avez pas besoin d'activer la restauration et que vous prévoyez donc d'utiliser l'assistant de mise à niveau Firewall Threat Defense, l'assistant vous demandera de copier le paquet. Si vous utilisez la page System Updates (Mises à jour de système) pour effectuer la mise à niveau parce que vous souhaitez activer le rétablissement, nous vous recommandons de copier les paquets de mise à niveau sur les périphériques maintenant, comme suit :

a) Cliquez sur l'icône **Push or Stage Update** (Pousser la mise à jour ou lui affecter une étape) à côté du paquet de mise à niveau que vous souhaitez copier.

b) Choisissez les périphériques de destination.

Vous pouvez copier le paquet sur tous les périphériques admissibles maintenant, ou vous pouvez le copier dans un sous-ensemble, puis utiliser l'interface de ligne de commande Firewall Threat Defense pour copier le paquet de mise à niveau entre les périphériques; voir Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 65.

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

c) Cliquez sur **Push** (Pousser).

Charger les paquets de mise à niveau Firewall Threat Defense sur un serveur interne avec System (Système) > Updates (Mises à jour)

Utilisez cette procédure pour configurer les périphériques Firewall Threat Defense afin d'obtenir les paquets de mise à niveau à partir d'un serveur web interne, plutôt qu'à partir du Firewall Management Center. Cela est particulièrement utile si la bande passante entre le Firewall Management Center et ses périphériques est limitée. Cela permet également de gagner de la place sur le Firewall Management Center.

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

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

Avant de commencer

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

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

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

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

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

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

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

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

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

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

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

Étape 6 Cliquez sur **Save** (enregistrer).
L'emplacement est enregistré. Les paquets de mise à niveau chargés et les URL des paquets de mise à niveau sont listés ensemble, mais étiquetés distinctement.

Étape 7 (Facultatif) Copiez les paquets de mise à niveau vers les périphériques gérés.

Si vous n'avez pas besoin d'activer la restauration et que vous prévoyez donc d'utiliser l'assistant de mise à niveau Firewall Threat Defense, l'assistant vous demandera de copier le paquet. Si vous utilisez la page System Updates (Mises à jour de système) pour effectuer la mise à niveau parce que vous souhaitez activer le rétablissement, nous vous recommandons de copier les paquets de mise à niveau sur les périphériques maintenant, comme suit :

a) Cliquez sur l'icône **Push or Stage Update** (Pousser la mise à jour ou lui affecter une étape) à côté du paquet de mise à niveau que vous souhaitez copier.
b) Choisissez les périphériques de destination.

Vous pouvez copier le paquet sur tous les périphériques admissibles maintenant, ou vous pouvez le copier dans un sous-ensemble, puis utiliser l'interface de ligne de commande Firewall Threat Defense pour copier le paquet de

mise à niveau entre les périphériques; voir Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 65.

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

c) Cliquez sur **Push** (Pousser).

Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques

Au lieu de copier les paquets de mise à niveau sur chaque périphérique à partir de Firewall Management Center ou du serveur Web interne, vous pouvez utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau entre les périphériques (« synchronisation homologue à homologue »). Ce partage de ressources sécurisé et fiable passe par le réseau de gestion, mais ne repose pas sur Firewall Management Center. Chaque périphérique peut accueillir 5 transferts simultanés de paquets.

Cette fonctionnalité est prise en charge pour les périphériques autonomes de la version 7.2.x–7.4.x gérés par le même Firewall Management Center de la version autonome 7.2.x–7.4.x. Elle n'est pas prise en charge pour :

- Instances de conteneur.
- Paires et grappes de périphériques à haute disponibilité. Ces périphériques reçoivent le paquet les uns des autres dans le cadre de leur processus de synchronisation normal. La copie de l'ensemble de mises à niveau sur un membre du groupe la synchronise automatiquement avec tous les membres du groupe.
- Périphériques gérés par des Firewall Management Centerà haute disponibilité.
- Périphériques dans différents domaines, ou périphériques séparés par une passerelle NAT.
- Périphériques mis à niveau à partir de la version 7.1 ou d'une version antérieure, quelle que soit la version de Firewall Management Center.
- Périphériques exécutant la version 7.6+.

Répétez la procédure suivante pour tous les périphériques qui ont besoin de l'ensemble de mise à niveau.

Avant de commencer

- Chargez le paquet de mise à niveau de Firewall Threat Defense sur le Firewall Management Center ou sur un serveur interne.
- Copiez le paquet de mise à niveau sur le périphérique.

Procédure

Étape 1 En tant `qu'administrateur`, accédez à SSH sur tout périphérique qui a besoin du paquet.

Étape 2 Activez la fonction .

configure p2psync enable

Étape 3 Si vous ne le savez pas déjà, déterminez où vous pouvez obtenir le paquet de mise à niveau dont vous avez besoin.

show peers : répertorie les autres périphériques admissibles sur lesquels cette fonctionnalité est également activée.

show peer details *ip_address* : pour le périphérique à l'adresse IP que vous spécifiez, répertoriez les paquets de mise à niveau disponibles et leurs chemins.

Étape 4 Copiez le paquet à partir de n'importe quel périphérique disposant du paquet dont vous avez besoin, en spécifiant l'adresse IP et le chemin que vous venez de découvrir.

sync-from-peer *ip_address package_path*

Après avoir confirmé que vous souhaitez copier le lot, le système affiche un UUID de l'état de synchronisation que vous pouvez utiliser pour surveiller ce transfert.

Étape 5 Surveillez l'état de transfert à partir de l'interface de ligne de commande.

show p2p-sync-status : affiche l'état de la synchronisation des cinq derniers transferts vers cet appareil, y compris les transferts terminés et ayant échoué.

show p2p-sync-status *sync_status_UUID* : affiche l'état de la synchronisation d'un transfert en particulier vers ce périphérique.

Mettre à niveau Firewall Threat Defense à l'aide de l'assistant (désactiver la restauration)

Utilisez cette procédure pour mettre à niveau Firewall Threat Defense à l'aide d'un assistant.

Au fur et à mesure que vous continuez, l'assistant affiche des informations de base sur les périphériques sélectionnés, ainsi que l'état actuel de la mise à niveau. Cela inclut toutes les raisons pour lesquelles vous ne pouvez pas mettre à niveau. Si un périphérique ne « réussit » pas une étape dans l'assistant, il ne s'affiche pas à l'étape suivante.

Si vous quittez l'assistant, votre progression est conservée et les autres utilisateurs ne peuvent pas démarrer de nouveau flux de travail de mise à niveau pour les périphériques que vous avez déjà sélectionnés. (Exception : si vous êtes connecté avec un CAC, votre progression est effacée 24 heures après votre déconnexion.) Si vous devez réinitialiser le flux de travail de quelqu'un d'autre, vous devez avoir un accès administrateur. Vous pouvez supprimer ou désactiver l'utilisateur, ou mettre à jour son rôle d'utilisateur afin qu'il n'ait plus l'autorisation d'utiliser **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

Notez que ni votre flux de travail ni vos mises à niveau de défense contre les menaces ne sont synchronisés entre les Firewall Management Center haute disponibilité. En cas de basculement, vous devez recréer votre flux de travail sur le nouveau Firewall Management Center, ce qui comprend le chargement des paquets de mise à niveau sur Firewall Management Center et l'exécution de vérifications de l'état de préparation. (Les paquets de mise à niveau déjà copiés sur les périphériques ne sont pas supprimés, mais le Firewall Management Center doit toujours avoir le paquet ou un pointeur vers son emplacement.)

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas, à la page 28.

Historique de Threat Defense :

- 7.2 : Copiez les paquets de mise à niveau entre les périphériques

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure.

  Nous vous recommandons généralement d'utiliser l'assistant pour mettre à niveau Firewall Threat Defense. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0 cependant, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour**. Vous devez également utiliser la page System Updates (mises à jour du système) pour la suppression des paquets de mise à niveau et pour mettre à niveau les périphériques Firewall Management Center et les périphériques plus anciens.

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

Procédure

Commencez le flux de travail.

Étape 1 Choisissez **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

L'assistant comporte deux volets : la sélection du périphérique à gauche et les détails du périphérique à droite. Cliquez sur le lien d'un périphérique dans le volet de sélection de périphériques (par exemple, « `4 périphériques` ») pour afficher les détails du périphérique correspondant.

Remarque Cette procédure explique comment utiliser l'assistant pour sélectionner des périphériques. Mais vous pouvez également utiliser **Devices (périphériques)** > **Device Management (gestion des périphériques)** pour sélectionner simplement les périphériques que vous souhaitez mettre à niveau, puis sélectionnez dans le menu **Select Action** (Sélectionner une action) ou **Select Bulk Action** (sélectionner une action en bloc). L'assistant apparaît, indiquant le nombre de périphériques que vous avez sélectionnés et vous invitant à sélectionner une version cible. Vous pouvez maintenant passer à l'étape 4.

Sélectionnez les périphériques à mettre à niveau et copiez les paquets de mise à niveau.

Étape 2 Dans le menu **Upgrade to** (mettre à niveau vers), sélectionnez votre version cible.

Le système détermine quels périphériques peuvent être mis à niveau vers cette version et les affiche dans le volet Device Details (détails sur le périphérique).

Notez que les choix dans le menu **Upgrade to** correspondent aux ensembles de mise à niveau de périphériques disponibles pour le système. Si votre version cible ne figure pas dans la liste, cliquez sur **Add Upgrade Package** (ajouter un paquet de mise à niveau) et téléversez ou spécifiez l'emplacement du progiciel adéquat de mise à niveau. Si vous mettez à niveau différents modèles de périphériques et que, par conséquent, vous avez besoin de plusieurs paquets de mise à niveau, assurez-vous que tous les paquets de mises à niveau nécessaires sont disponibles pour le système avant de continuer.

Étape 3 Dans le volet Device Details (détails du périphérique), sélectionnez les périphériques que vous souhaitez mettre à niveau et cliquez sur **Add to Selection** (ajouter à la sélection).

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

Étape 4 Vérifiez votre sélection de périphérique.

Utilisez les liens vers les périphériques dans le volet Sélection des périphériques pour faire basculer le volet Détails des périphériques entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques inéligibles (avec les raisons), les périphériques qui ont besoin du paquet de mise à niveau, et ainsi de suite. Vous pouvez ajouter et supprimer des périphériques à votre sélection, ou cliquer sur **Reset** (Réinitialiser) pour effacer votre sélection de périphériques et recommencer. Notez que vous n'êtes pas tenu de supprimer les périphériques non admissibles; ils sont automatiquement exclus de la mise à niveau.

Étape 5 Pour tous les périphériques qui ont encore besoin d'un ensemble de mise à niveau, cliquez sur **Copier le paquet de mise à niveau**, puis confirmez votre choix.

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



Astuces Vous pouvez également utiliser l'interface de ligne de commande Firewall Threat Defense pour copier les paquets de mise à niveau d'un appareil à l'autre. Pour en savoir plus, y compris les conditions d'admissibilité, consultez Copier les paquets de mise à niveau Firewall Threat Defense entre les périphériques, à la page 65.

Étape 6 Cliquez sur **Next** (suivant).

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

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

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

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

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

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

Étape 9 Si nécessaire, retournez à **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

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

Mettre à niveau les périphériques.

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

Étape 12 (Facultatif) Modifiez l'ordre de mise à niveau des périphériques en grappe.

Affichez les détails du périphérique pour la grappe et cliquez sur **Modifier l'ordre de mise à niveau**. L'unité de contrôle est toujours mise à niveau en dernier; vous ne pouvez pas changer cela.

Étape 13 Choisissez les options de mise à niveau.

Pour les mises à niveau majeures et de maintenance , vous pouvez :

- **Annuler automatiquement la mise à niveau en cas d'échec et restaurer la version précédente** : le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.
- **Générer les fichiers de dépannage avant que la mise à niveau ne commence** : grâce aux mises à niveau à la version 7.3+, pour économiser du temps et de l'espace disque, vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant la mise à niveau.

  Pour générer manuellement des fichiers de dépannage pour Firewall Threat Defense, choisissez **Système** (⚙) > **Health (Intégrité)** > **Monitor (Superviser)**, cliquez sur le périphérique dans le panneau de gauche, puis sur **View System & Troubleshoot Details** (Afficher les détails du système et du dépannage) et **Generate Troubleshooting Files** (Générer les fichiers de résolution de problèmes).
- **Mettre à niveau de Snort 2 vers Snort 3** : après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Du fait des mises à niveau vers la version 7.3 et ultérieures, vous ne pouvez plus désactiver cette option. Bien que vous puissiez rétablir les périphériques individuels, Snort 2 sera obsolète dans une version ultérieure et nous vous recommandons fortement de cesser de l'utiliser dès maintenant.

  Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide lors de la migration, consultez *Politiques de prévention des intrusions personnalisées pour Snort 3* pour votre version.

Ces options ne sont pas prises en charge pour les correctifs.

Étape 14 Cliquez sur **Start Upgrade** (commencer la mise à niveau), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Vous pouvez surveiller la progression globale de la mise à niveau dans le centre de messages. Pour une progression détaillée, utilisez la fenêtre contextuelle Upgrade Status (état de la mise à niveau), accessible à partir de l'onglet Upgrade (Mise à niveau) sur la page Device Management (gestion des périphériques) et à partir du centre de messages. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense, à la page 29.

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

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

Étape 15 Vérifiez la réussite.

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

Étape 16 (Facultatif) Dans les déploiements à haute disponibilité ou en grappe, examinez les rôles des périphériques.

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

Étape 17 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Si le site d'assistance et de téléchargement Cisco dispose d'une version plus récente, installez-la. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 18 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 19 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Snort redémarre généralement lors du premier déploiement après la mise à niveau. 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 ou la mise en grappe. Pour obtenir plus de renseignements, consultez Flux de trafic et inspection lors du déploiement de configurations, à la page 32.

Avant de déployer, vous souhaiterez peut-être passer en revue les modifications apportées par la mise à niveau (ainsi que toutes les modifications que vous avez apportées depuis la mise à niveau) : Choisissez **Deploy (Déploiement)** > **Advanced Deploy (Déploiement avancé)** , sélectionnez les périphériques que vous venez de mettre à niveau, puis cliquez sur **Pending Changes Reports** (Rapports de modifications en attente). Une fois les rapports générés, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages.

Prochaine étape

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

Mettre à niveau Firewall Threat Defense à l'aide de l'assistant en mode sans surveillance (désactiver la restauration)

Utilisez cette procédure pour mettre à niveau Firewall Threat Defense à l'aide d'un assistant. Il vous suffit de sélectionner la version cible et les périphériques que vous souhaitez mettre à niveau, de spécifier quelques options de mise à niveau et de partir. Vous pouvez même vous déconnecter ou fermer le navigateur.

Lorsque vous démarrez une mise à niveau sans surveillance, le système copie automatiquement les paquets de mise à niveau sur les périphériques, effectue des vérifications de compatibilité et de préparation, puis commence la mise à niveau. Tout comme cela se produit lorsque vous exécutez manuellement l'assistant, tous les périphériques qui ne « franchissent » pas une étape de la mise à niveau (par exemple, l'échec des

vérifications) ne sont pas inclus dans l'étape suivante. Une fois la mise à niveau terminée, vous reprenez les tâches de vérification et après la mise à niveau.

Vous pouvez suspendre et redémarrer le processus pendant les étapes de copie et de vérification. Cependant, la suspension du mode sans surveillance *n'arrête* pas les tâches en cours. Les copies et les vérifications qui ont commencé s'exécuteront jusqu'à la fin. De même, vous ne pouvez pas annuler une mise à niveau en cours en arrêtant le mode sans surveillance ; pour l'annuler, utilisez la fenêtre contextuelle Upgrade Status (État de la mise à niveau), accessible depuis l'onglet Upgrade (Mise à niveau) de la page Device Management (Gestion des périphériques), ainsi que depuis le Message Center (Centre de messages).



Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas, à la page 28.

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure.

  Nous vous recommandons généralement d'utiliser l'assistant pour mettre à niveau Firewall Threat Defense. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0 cependant, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour**. Vous devez également utiliser la page System Updates (mises à jour du système) pour la suppression des paquets de mise à niveau et pour mettre à niveau les périphériques Firewall Management Center et les périphériques plus anciens.

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

Procédure

Commencez le flux de travail.

Étape 1 Choisissez **Devices (Périphériques)** > **Device Upgrade (Mise à niveau des périphériques)** > **Upgrade Threat Defense (Mise à niveau de Threat Defense)**.

L'assistant comporte deux volets : la sélection du périphérique à gauche et les détails du périphérique à droite. Cliquez sur le lien d'un périphérique dans le volet de sélection de périphériques (par exemple, « `4 périphériques` ») pour afficher les détails du périphérique correspondant.



Remarque Cette procédure explique comment utiliser l'assistant pour sélectionner des périphériques. Mais vous pouvez également utiliser **Devices (périphériques)** > **Device Management (gestion des périphériques)** pour sélectionner simplement les périphériques que vous souhaitez mettre à niveau, puis sélectionnez dans le menu **Select Action** (Sélectionner une action) ou **Select Bulk Action** (sélectionner une action en bloc). L'assistant apparaît, indiquant le nombre de périphériques que vous avez sélectionnés et vous invitant à sélectionner une version cible. Vous pouvez maintenant passer à l'étape 4.

Sélectionnez les périphériques à mettre à niveau

Étape 2 Dans le menu **Upgrade to** (mettre à niveau vers), sélectionnez votre version cible.

Le système détermine quels périphériques peuvent être mis à niveau vers cette version et les affiche dans le volet Device Details (détails sur le périphérique).

Notez que les choix dans le menu **Upgrade to** correspondent aux ensembles de mise à niveau de périphériques disponibles pour le système. Si votre version cible ne figure pas dans la liste, cliquez sur **Add Upgrade Package** (ajouter un paquet de mise à niveau) et téléversez ou spécifiez l'emplacement du progiciel adéquat de mise à niveau. Si vous mettez à niveau différents modèles de périphériques et que, par conséquent, vous avez besoin de plusieurs paquets de mise à niveau, assurez-vous que tous les paquets de mises à niveau nécessaires sont disponibles pour le système avant de continuer.

Étape 3 Dans le volet Device Details (détails du périphérique), sélectionnez les périphériques que vous souhaitez mettre à niveau et cliquez sur **Add to Selection** (ajouter à la sélection).

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

Étape 4 Vérifiez votre sélection de périphérique.

Utilisez les liens vers les périphériques dans le volet Sélection des périphériques pour faire basculer le volet Détails des périphériques entre les périphériques sélectionnés, les candidats à la mise à niveau restants, les périphériques inéligibles (avec les raisons), les périphériques qui ont besoin du paquet de mise à niveau, et ainsi de suite. Vous pouvez ajouter et supprimer des périphériques à votre sélection, ou cliquer sur **Reset** (Réinitialiser) pour effacer votre sélection de périphériques et recommencer. Notez que vous n'êtes pas tenu de supprimer les périphériques non admissibles; ils sont automatiquement exclus de la mise à niveau.

Effectuer les dernières vérifications préalables à la mise à niveau.

Étape 5 Effectuez les dernières vérifications préalables à la mise à niveau.

Bien que vous n'ayez pas à copier les paquets de mise à niveau vers les périphériques ni à exécuter à l'avance des vérifications de préparation, vous devez revoir la liste de contrôle préalable à la mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales.

Mettre à niveau les périphériques en mode sans surveillance.

Étape 6 Dans le menu **Unattended Mode** (Mode sans surveillance), sélectionnez **Start** (Démarrer).

Étape 7 Choisissez les options de mise à niveau sans surveillance.

Pour les mises à niveau majeures et de maintenance , vous pouvez :

- **Exiger la réussite des vérifications de compatibilité et de préparation** : bien que vous puissiez ignorer les vérifications en désactivant cette option, nous vous déconseillons de le faire. La réussite de tous les contrôles réduit considérablement les risques d'échec de la mise à niveau.
- **Annuler automatiquement la mise à niveau en cas d'échec et restaurer la version précédente** : le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.
- **Générer les fichiers de dépannage avant que la mise à niveau ne commence** : grâce aux mises à niveau à la version 7.3+, pour économiser du temps et de l'espace disque, vous pouvez désormais ignorer la génération automatique des fichiers de dépannage avant la mise à niveau.

Pour générer manuellement des fichiers de dépannage pour Firewall Threat Defense, choisissez **Système** (⚙) > **Health (Intégrité)** > **Monitor (Superviser)**, cliquez sur le périphérique dans le panneau de gauche, puis sur **View System & Troubleshoot Details** (Afficher les détails du système et du dépannage) et **Generate Troubleshooting Files** (Générer les fichiers de résolution de problèmes).

- **Mettre à niveau de Snort 2 vers Snort 3** : après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Grâce aux mises à niveau vers la version 7.3 et ultérieures, vous ne pouvez plus désactiver cette option. Bien que vous puissiez rétablir individuellement certains périphériques, Snort 2 est obsolète dans la version 7.7 et les versions ultérieures, et nous vous recommandons fortement de cesser de l'utiliser dès maintenant.

  Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide lors de la migration, consultez *Politiques de prévention des intrusions personnalisées pour Snort 3* pour votre version.

Ces options ne sont pas prises en charge pour les correctifs.

Étape 8 Cliquez à nouveau sur **Start** (Démarrer) pour lancer le mode sans surveillance et redémarrer les périphériques.

Le processus de mise à niveau se déroule comme si vous suiviez manuellement les étapes de l'assistant.

Vous pouvez suspendre et redémarrer le mode sans surveillance (mais pas les tâches en cours) pendant les phases de copie et de vérification en sélectionnant **Stop** (Arrêter) ou **Start** (Démarrer) dans le menu **Unattended Mode** (Mode sans surveillance) ; pour afficher l'état général de copie et de vérification, sélectionnez **View Status** (Afficher l'état). Notez que vous devez suspendre le mode sans surveillance pour effectuer toute action manuelle de mise à niveau.

Après le début de la mise à niveau réelle, vous pouvez surveiller la progression globale de la mise à niveau dans le centre de messages. Pour une progression détaillée, utilisez la fenêtre contextuelle Upgrade Status (état de la mise à niveau), accessible à partir de l'onglet Upgrade (Mise à niveau) sur la page Device Management (gestion des périphériques) et à partir du centre de messages. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense, à la page 29.

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

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

Étape 9 Vérifiez la réussite.

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

Étape 10 (Facultatif) Dans les déploiements à haute disponibilité ou en grappe, examinez les rôles des périphériques.

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

Étape 11 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Si le site d'assistance et de téléchargement Cisco dispose d'une version plus récente, installez-la. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 12 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 13 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Snort redémarre généralement lors du premier déploiement après la mise à niveau. 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 ou la mise en grappe. Pour obtenir plus de renseignements, consultez Flux de trafic et inspection lors du déploiement de configurations, à la page 32.

Avant de déployer, vous souhaiterez peut-être passer en revue les modifications apportées par la mise à niveau (ainsi que toutes les modifications que vous avez apportées depuis la mise à niveau) : Choisissez **Deploy (Déploiement)** > **Advanced Deploy (Déploiement avancé)** , sélectionnez les périphériques que vous venez de mettre à niveau, puis cliquez sur **Pending Changes Reports** (Rapports de modifications en attente). Une fois les rapports générés, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages.

Prochaine étape

(Facultatif) Effacez l'assistant en cliquant sur **Effacer les informations de mise à niveau**. Jusqu'à ce que vous fassiez cela, la page continue d'afficher les détails de la mise à niveau que vous venez d'effectuer. Après avoir effacé l'assistant, utilisez l'onglet Upgrade (Mise à niveau) sur la page Device Management (Gestion des périphériques) pour afficher les informations de dernière mise à niveau pour les périphériques gérés.

Mettre à niveau Firewall Threat Defense via System (Système) > Updates (Mises à jour) (Enable Revert (Activer la restauration))

Utilisez cette procédure pour mettre à niveau Firewall Threat Defense en utilisant la page de mises à jour du système.

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la mise à niveau. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement. Dans la plupart des cas, ne redémarrez pas une mise à niveau en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, consultez Mises à niveau qui ne répondent pas, à la page 28.

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure.

  Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour** pour mettre à niveau Firewall Threat Defense. C'est la seule façon de définir l'option **Enable revert after successful upgrade** (Activer le retour arrière après une mise à niveau réussie), et est en contradiction avec notre recommandation habituelle d'utiliser l'assistant de mise à niveau de Firewall Threat Defense.

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

Procédure

Étape 1 Dans Firewall Management Center, choisissez **Système** (⚙) > **Mises à jour**.

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

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

Le système affiche une liste des périphériques admissibles, ainsi que leurs résultats de vérification de compatibilité préalables à la mise à niveau. Cette vérification préalable vous empêche d'effectuer la mise à niveau s'il existe des problèmes manifestes qui entraîneront l'échec de votre mise à niveau.

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

Les vérifications de l'état de préparation évaluent l'état de préparation pour les mises à niveau majeures et de maintenance. Le temps nécessaire pour exécuter une vérification de l'état de préparation varie en fonction du modèle. Ne redémarrez pas ou n'arrêtez pas les vérifications de l'état de préparation manuellement.

Sous Readiness Checks (Vérifications de l'état de préparation) sur cette page, vous pouvez voir l'état de vérification pour l'ensemble de votre déploiement, y compris les vérifications en cours et les vérifications ayant échoué. Vous pouvez également utiliser cette page pour réexécuter facilement les vérifications après un échec. Ou, surveillez la progression des vérifications de l'état de préparation dans le centre de messages.

Si vous ne pouvez pas sélectionner un périphérique autrement admissible, assurez-vous qu'il a réussi ses vérifications de compatibilité. Si un périphérique échoue aux vérifications de l'état de préparation, corrigez les problèmes avant d'effectuer la mise à niveau.

Étape 4 Choisissez les périphériques à mettre à niveau.

Vous pouvez mettre à niveau plusieurs périphériques à la fois s'ils utilisent le même paquet de mise à niveau. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.



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

Étape 5 Choisissez les options de mise à niveau.

Pour les mises à niveau majeures et de maintenance , vous pouvez :

- **Annuler automatiquement la mise à niveau en cas d'échec et restaurer la version précédente** : le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué. Dans un déploiement à haute disponibilité ou en grappe, l'annulation automatique s'applique à chaque périphérique individuellement. Autrement dit, si la mise à niveau échoue sur un périphérique, seul ce périphérique est rétabli.
- **Activer la restauration après une mise à niveau réussie** : pendant les 30 jours suivant une mise à niveau réussie, vous pouvez rétablir l'état d'avant la mise à niveau du périphérique .

- **Mettre à niveau de Snort 2 vers Snort 3** : après la mise à niveau logicielle, les périphériques admissibles seront mis à niveau de Snort 2 vers Snort 3 lorsque vous déployez des configurations. Du fait des mises à niveau vers la version 7.3 et ultérieures, vous ne pouvez plus désactiver cette option. Bien que vous puissiez rétablir les périphériques individuels, Snort 2 sera obsolète dans une version ultérieure et nous vous recommandons fortement de cesser de l'utiliser dès maintenant.

  Pour les périphériques qui ne sont pas admissibles, car ils utilisent des stratégies d'intrusion ou d'analyse de réseau personnalisées, nous vous recommandons fortement de mettre à niveau manuellement Snort 3 pour une détection et une amélioration améliorées. Pour obtenir de l'aide lors de la migration, consultez *Politiques de prévention des intrusions personnalisées pour Snort 3* pour votre version.

Ces options ne sont pas prises en charge pour les correctifs.

Étape 6 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

Vous pouvez surveiller la progression de la mise à niveau dans le centre de messagerie. Pour en savoir plus sur le traitement du trafic pendant la mise à niveau, consultez Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense, à la page 29.

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

Étape 7 Vérifiez la réussite.

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

Étape 8 (Facultatif) Dans les déploiements à haute disponibilité ou en grappe, examinez les rôles des périphériques.

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

Étape 9 Mettez à jour les règles de prévention des intrusions et la base de données des vulnérabilités.

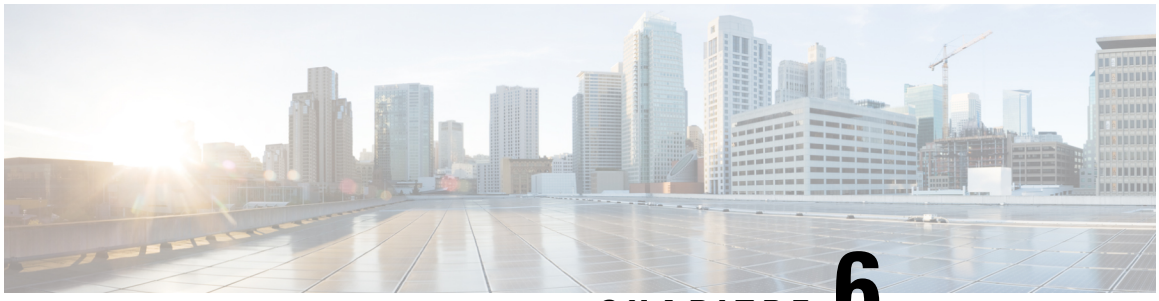
Bien que la mise à niveau mette souvent à jour ces composants, des nouveaux peuvent être disponibles. Si le site d'assistance et de téléchargement Cisco dispose d'une version plus récente, installez-la. Notez que lorsque vous mettez à jour les règles de prévention des intrusions, vous n'avez pas besoin de réappliquer automatiquement les politiques. Vous le ferez ultérieurement.

Étape 10 Apportez toutes les modifications de configuration requises après la mise à niveau.

Étape 11 Redéployez les configurations sur les périphériques que vous venez de mettre à niveau.

Snort redémarre généralement lors du premier déploiement après la mise à niveau. 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 ou la mise en grappe. Pour obtenir plus de renseignements, consultez Flux de trafic et inspection lors du déploiement de configurations, à la page 32.

Avant de déployer, vous souhaiterez peut-être passer en revue les modifications apportées par la mise à niveau (ainsi que toutes les modifications que vous avez apportées depuis la mise à niveau) : Choisissez **Deploy (Déploiement)** > **Advanced Deploy (Déploiement avancé)** , sélectionnez les périphériques que vous venez de mettre à niveau, puis cliquez sur **Pending Changes Reports** (Rapports de modifications en attente). Une fois les rapports générés, vous pouvez les télécharger à partir de l'onglet Tâches dans le centre de messages.



CHAPITRE 6

Mettre à niveau le châssis sur le Firepower 4100/9300

Notes de mise à jour de Cisco Firepower 4100/9300 FXOS, 2.13

- Progiciels de mise à niveau pour FXOS, à la page 77
- Directives de mise à niveau pour le châssis Firepower 4100/9300, à la page 77
- Chemins de mise à niveau pour FXOS, à la page 79
- Mettre à niveau FXOS avec Firewall Chassis Manager, à la page 86
- Mettre à niveau FXOS avec l'interface de ligne de commande, à la page 94

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 Firewall Threat Defense 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 27 : Directives de mise à niveau pour le châssis Firepower 4100/9300

Directives	Détails
Mises à niveau de FXOS.	FXOS 2.13.0.198+ est requis pour exécuter la défense contre les menaces Version 7.3 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 les Notes de mise à jour de 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 78.
Ordre de mise à niveau du châssis avec Firewall Threat Defense haute disponibilité/évolutivité.	Même dans les déploiements à disponibilité et à évolutivité élevées, 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. Pour les mises à niveau Firewall Threat Defense, le système met automatiquement à niveau un périphérique groupé à la fois. Pour en savoir plus, consultez Ordre de mise à niveau pour FXOS avec Firewall Threat Defense haute disponibilité/évolutivité, à la page 85.
Ordre de mise à niveau du châssis avec les périphériques logiques Firewall Threat Defense et ASA.	Si vous avez des périphériques logiques Firewall Threat Defense *et* ASA configurés sur Firepower 9300, utilisez les procédures de ce chapitre pour mettre à niveau FXOS et Firewall Threat Defense. 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 Firewall Threat Defense et ASA, à la page 82. 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 Firewall Threat Defense 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/en cluster, 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 Firewall Threat Defense haute disponibilité/évolutivité, à la page 85.

Tableau 28 : Flux de trafic et inspection : mises à niveau de FXOS

Firewall Threat DefenseDéploiement	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.
Grappe inter-châssis	Non affecté.	**Bonnes pratiques :** mettez à niveau un châssis à la fois de sorte qu'au moins un module soit toujours en ligne.
	Abandonné jusqu'à ce qu'au moins un module soit en ligne.	Mettez à niveau le châssis en même temps, de sorte que tous les modules soient inactifs à un moment ou à un autre.
Grappe intrachâssis (Firepower 9300 uniquement)	Réussi sans inspection	Contournement matériel activé : **Contournement : veille** ou **Veille-Forcé**.
	Abandonné jusqu'à ce qu'au moins un module soit en ligne.	Contournement matériel désactivé : **Contournement : désactivé**
	Abandonné jusqu'à ce qu'au moins un module soit en ligne.	Pas de module de contournement matériel.

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 Firewall Threat Defense

Ce tableau fournit le chemin de mise à niveau pour Firewall Threat Defense sur le Firepower 4100/9300.

Notez que si votre version actuelle Firewall Threat Defense/Firewall Management Center 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 ou des instances d'applications. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le *Guide de compatibilité de Cisco Secure Firewall Threat Defense*.

Tableau 29 : Firewall Threat Defense Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Firewall Threat Defense7.3	→ FXOS 2.13 avec toute version ultérieure de Firewall Threat Defense 7.3.x
FXOS 2.12 avec Firewall 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 Firewall Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Firewall Threat Defense 7.2.x
FXOS 2.11.1 avec Firewall Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Firewall Threat Defense 7.1.x

Versions actuelles	Versions cibles
FXOS 2.10.1 avec Firewall Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Firewall Threat Defense 7.3.x → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Firewall 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** Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer les périphériques Firewall Threat Defense 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 Firewall Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Firewall Threat Defense 6.7.x
FXOS 2.8.1 avec Firewall Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Firewall Threat Defense 7.2.x → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Firewall Threat Defense 6.6.x

Versions actuelles	Versions cibles
FXOS 2.7.1 avec Firewall Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Firewall Threat Defense 7.1.x → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x
FXOS 2.6.1 avec Firewall Threat Defense 6.4	Une des versions suivantes : → FXOS 2.10.1 avec Firewall Threat Defense 7.0.x → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5
FXOS 2.4.1 avec Firewall Threat Defense 6.3	Une des versions suivantes : → FXOS 2.9.1 avec Firewall Threat Defense 6.7.x → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4
FXOS 2.3.1 avec Firewall Threat Defense 6.2.3	Une des versions suivantes : → FXOS 2.8.1 avec Firewall Threat Defense 6.6.x → FXOS 2.7.1 avec Firewall Threat Defense 6.5 → FXOS 2.6.1 avec Firewall Threat Defense 6.4 → FXOS 2.4.1 avec Firewall Threat Defense 6.3

Chemin de mise à niveau pour FXOS avec Firewall Threat Defense et ASA

Ce tableau indique les chemins de mise à niveau pour le Firepower 9300 avec des périphériques logiques Firewall Threat Defense 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 Firewall Threat Defense/Firewall Management Center 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) ou des instances d'applications Firewall Threat Defense. Si vous devez sauter plusieurs versions, c'est généralement Firewall Threat Defense 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 30 : Mises à niveau directes de Firewall Threat Defense 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

Versions actuelles	Versions cibles
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** Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer les périphériques Firewall Threat Defense 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 • 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

Versions actuelles	Versions cibles
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
FXOS 2.6.1 avec : • Threat Defense 6.4 • ASA 9.12(x)	Une des versions suivantes : → 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 → FXOS 2.7.1 avec ASA 9.13(x) et Threat Defense 6.5

Ordre de mise à niveau pour FXOS avec Firewall Threat Defense haute disponibilité/évolutivité

Même dans les déploiements à disponibilité et à évolutivité élevées, 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. Pour les mises à niveau Firewall Threat Defense, le système met automatiquement à niveau un périphérique groupé à la fois.

Tableau 31 : Ordre de mise à niveau FXOS-Threat Defense pour Firepower 4100/9300

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Autonomes	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.
Haute disponibilité	Mettez à niveau FXOS sur les deux châssis avant de mettre à niveau Firewall Threat Defense. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. **1.** Mettez à niveau FXOS sur le châssis avec le serveur de secours. **2.** Changez de rôle. **3.** Mettez à niveau FXOS sur le châssis avec le nouveau serveur de secours. **4.** Mettez à niveau Firewall Threat Defense.
Grappe intrachâssis (unités sur le même châssis)	**1.** Mettez à niveau FXOS. **2.** Mettez à niveau Firewall Threat Defense.

Firewall Threat DefenseDéploiement	Commande de mise à niveau
Grappe inter-châssis (unités sur des châssis différents)	Mettez à niveau FXOS sur tous les châssis avant de mettre à niveau Firewall Threat Defense. Pour réduire au minimum les perturbations, mettez toujours à niveau un châssis d'unités de données. **1.** Mettez à niveau FXOS sur un châssis de l'unité de données. **2.** Basculez le module de contrôle sur le châssis que vous venez de mettre à niveau. **3.** Mettez à niveau FXOS sur les châssis restants. **4.** Mettez à niveau Firewall Threat Defense.

Mettre à niveau FXOS avec Firewall Chassis Manager

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

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

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

Avant de commencer

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

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

Procédure

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

Étape 2 Chargez la nouvelle image groupée de la plateforme :

a) Cliquez sur **Upload Image**(télécharger une image) pour ouvrir la boîte de dialogue pour télécharger une image (Upload Image).

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

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

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

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

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

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

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

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

Exemple :

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

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

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

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

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

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

Mettre à niveau FXOS sur une grappe intrachâssis FTD à l'aide de Firepower Chassis Manager

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

Avant de commencer

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

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

Procédure

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

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



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

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

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

show version.

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

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

Étape 4 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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



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

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

Exemple :

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

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

Procédure

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

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

Étape 3 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

a) Entrez **scope system**.
b) Entrez **show firmware monitor**.

c) Attendez que tous les composants (FPRM, interconnexion de la trame et châssis) affichent `Upgrade-Status: Ready`.



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

Exemple :

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

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

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

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

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

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

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

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

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

Étape 11 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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



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

Exemple :

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

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

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

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

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

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

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

Mettre à niveau FXOS avec l'interface de ligne de commande

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

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

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

Avant de commencer

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

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

- Nom complet du fichier image.

Procédure

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

Étape 3 Si nécessaire, revenez au mode micrologiciel :

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

Étape 4 Passez en mode d'installation automatique :

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

Étape 5 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

Mettre à niveau FXOS sur une grappe intrachâssis FTD à l'aide de l'interface de ligne de commande de FXOS

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

Avant de commencer

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

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

Procédure

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

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

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

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

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

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

show version.

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

a) Entrez **top**.

b) Entrez en mode micrologiciel :

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

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

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

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

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

d) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

Étape 4 Si nécessaire, revenez au mode micrologiciel :

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

Étape 5 Passez en mode d'installation automatique :

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

Étape 6 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

Étape 8 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 9 Pour superviser le processus de mise à niveau :

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



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

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

Exemple :

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

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

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

- Collectez les informations suivantes dont vous aurez besoin pour télécharger l'image logicielle sur le Châssis Firepower 4100/9300 :
  - L'adresse IP et les informations d'authentification du serveur à partir duquel vous copiez l'image.
  - Nom complet du fichier image.

Procédure

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

Étape 3 Si nécessaire, revenez au mode micrologiciel :

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

Étape 4 Passez en mode d'installation automatique :

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

Étape 5 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

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

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

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

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

Étape 13 Si nécessaire, revenez au mode micrologiciel :

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

Étape 14 Passez en mode d'installation automatique :

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

Étape 15 Installez l'ensemble de la plateforme FXOS :

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

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

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

Saisissez **yes** 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

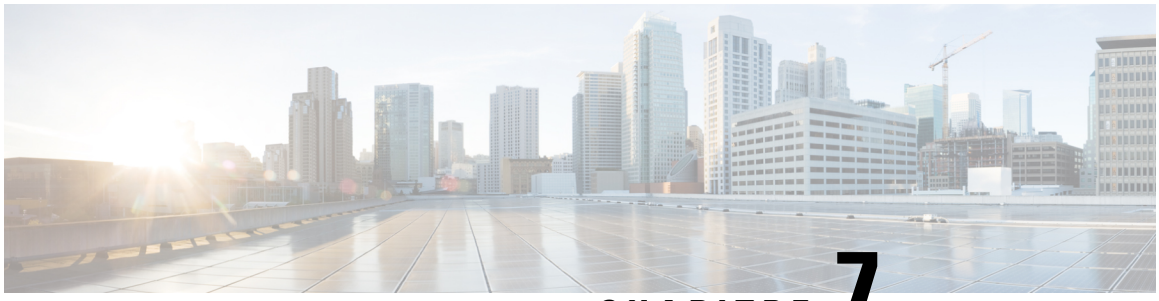
FP9300-A /system #
```

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

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

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



CHAPITRE 7

Annuler ou désinstaller la mise à niveau

Si une mise à niveau réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez annuler ou désinstaller :

- La restauration est prise en charge pour les mises à niveau majeures et de maintenance de Firewall Threat Defense version 7.1 et ultérieures.
- La désinstallation est prise en charge pour les correctifs de Firewall Threat Defense et du Firewall Management Center.

Si cela ne fonctionne pas pour vous et que vous devez toujours revenir à une version antérieure, vous devez effectuer une réinitialisation.

- Restauration de Threat Defense, à la page 107
- Désinstaller un correctif , à la page 111

Restauration de Threat Defense

À propos de la restauration de Threat Defense

La restauration de Firewall Threat Defense ramène le logiciel à l'état qu'il avait avant la dernière mise à niveau majeure ou de maintenance. Le rétablissement après l'application d'un correctif supprime également les correctifs. Vous devez activer la restauration lorsque vous mettez à niveau le périphérique, afin que le système puisse enregistrer un instantané de restauration.

Configurations restaurées

Les configurations restaurées comprennent :

- Version Snort.
- Configurations spécifiques au périphérique.

  Paramètres généraux du périphérique, routage, interfaces, ensembles en ligne, DHCP, SNMP — tout ce que vous configurez sur la page **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.
- Objets utilisés par les configurations spécifiques à votre périphérique.

Il s'agit notamment de la liste d'accès, du chemin de système autonome, de la chaîne de clés, de l'interface, du réseau, du port, de la carte de routage et des objets de moniteur SLA. Si vous avez modifié ces objets après la mise à niveau du périphérique, le système crée de nouveaux objets ou configure les remplacements d'objets pour le périphérique rétabli à utiliser. Ainsi, vos autres périphériques peuvent continuer à gérer le trafic en fonction de leur configuration actuelle.

Après une restauration réussie, nous vous recommandons d'examiner les objets utilisés par le périphérique restauré et d'effectuer les ajustements nécessaires.

Configurations non restaurées

Les configurations non restaurées comprennent :

- Politiques partagées qui peuvent être utilisées par plusieurs périphériques; par exemple, les paramètres de la plateforme ou les politiques de contrôle d'accès.

  Un périphérique restauré avec succès est marqué comme obsolète et vous devez redéployer les configurations.

- Pour le Firepower 4100/9300, modifications d'interface effectuées à l'aide de Secure Firewall Chassis Manager ou FXOS CLI.

  Synchronisez les modifications d'interface après une restauration réussie.

- Micrologiciel pour le Firepower 4100/9300.

  Si vous devez exécuter la combinaison conseillée de FXOS et Firewall Threat Defense, vous aurez peut-être besoin d'une recréation d'image complète; voir Directives pour la restauration Firewall Threat Defense, à la page 108.

Directives pour la restauration Firewall Threat Defense

Configuration système requise

La restauration est prise en charge pour les mises à niveau majeures et de maintenance de Firewall Threat Defense version 7.1 et ultérieures.

La restauration n'est pas prise en charge pour :

- Mise à niveau de versions antérieures.
- Correctifs et correctifs rapides.
- Instances de conteneur.
- Mises à niveau du Firewall Management Center

Rétablissement de la haute disponibilité ou des périphériques en grappe

Lorsque vous utilisez l'interface Web Firewall Management Center pour rétablir Firewall Threat Defense, vous ne pouvez pas sélectionner d'unités à haute disponibilité individuelles ou de nœuds en grappe.

En effet, la restauration fonctionne mieux lorsque toutes les unités sont restaurées simultanément. Lorsque vous lancez la restauration à partir de Firewall Management Center, le système le fait automatiquement. Lors de l'utilisation de l'interface de ligne de commande de l'appareil, ouvrez des sessions avec toutes les

unités/nœuds, vérifiez que le rétablissement est possible sur chacun, puis démarrez les processus en même temps. La restauration simultanée signifie que les interruptions du flux de trafic et de l'inspection dépendent des configurations des interfaces uniquement, comme si chaque périphérique était autonome.

Notez que la restauration est prise en charge pour les groupes entièrement et partiellement mis à niveau. Dans le cas d'un groupe partiellement mis à niveau, le système supprime la mise à niveau des unités ou des nœuds mis à niveau uniquement. La restauration ne rompra pas la haute disponibilité ni les grappes, mais vous pouvez rompre un groupe et restaurer ses périphériques nouvellement autonomes.

La restauration ne rétrograde pas FXOS

Les versions principales Firewall Threat Defense sont accompagnées d'une version FXOS spécialement qualifiée et recommandée. Après être revenu à la version précédente de Firewall Threat Defense, vous utilisez peut-être une version non recommandée de FXOS (trop nouvelle).

Bien que les nouvelles versions de FXOS soient compatibles avec les anciennes versions de Firewall Threat Defense FXOS , nous effectuons des tests améliorés pour les combinaisons recommandées. Vous ne pouvez pas passer à une version antérieure manuellement de FXOS. Par conséquent, si vous vous trouvez dans cette situation et que vous souhaitez exécuter une combinaison recommandée, vous aurez besoin d'une recréation d'image complète.

Scénarios de prévention de la restauration

Si vous tentez de revenir en arrière dans l'une de ces situations, le système affiche une erreur.

Tableau 32 : Scénarios de prévention de la restauration

Scénario	Solution
L'instantané de rétablissement n'est pas disponible pour les raisons suivantes : • Vous n'avez pas activé l'option de rétablissement lorsque vous avez mis à niveau le périphérique. • Vous avez supprimé l'instantané de Firewall Management Center ou du périphérique, ou il a expiré. • Vous avez mis à niveau le périphérique avec un autre Firewall Management Center.	Aucun. Dans les versions 7.1.0–7.2.5, 7.3.x et 7.4.0, si vous pensez devoir revenir en arrière après une mise à niveau réussie, utilisez **Système** (⚙) > **Mises à jour** pour mettre à niveau Firewall Threat Defense. C'est la seule façon de définir l'option **Enable revert after successful upgrade** (Activer le retour arrière après une mise à niveau réussie), et est en contradiction avec notre recommandation habituelle d'utiliser l'assistant de mise à niveau de Firewall Threat Defense. L'instantané de restauration est enregistré sur le Firewall Management Center *et* le périphérique pendant trente jours, après quoi il est automatiquement supprimé et vous ne pouvez plus revenir en arrière. Vous pouvez supprimer manuellement l'instantané de l'un ou l'autre des périphériques pour économiser de l'espace disque, mais cela supprime votre possibilité de revenir en arrière.

Scénario	Solution
Échec de la mise à niveau.	L'annulation d'une mise à niveau ramène le périphérique à l'état qu'il avait avant la mise à niveau. Ou corrigez les problèmes et réessayez. L'option de rétablissement s'applique aux situations où la mise à niveau a réussi, mais où le système mis à niveau ne fonctionne pas selon vos attentes. La restauration n'est pas la même chose que l'annulation d'une mise à niveau en cours ou ayant échoué. Si vous ne pouvez pas revenir en arrière ou annuler, vous devrez effectuer une réinitialisation.
Interface d'accès de gestion modifiée depuis la mise à niveau.	Rétablissez-la et réessayez.
Grappes dans lesquelles les unités ont été mises à niveau à partir de versions différentes.	Supprimez les unités jusqu'à ce que toutes les unités correspondent, rapprochez les membres de la grappe, puis rétablissez la grappe plus petite. Vous pouvez également être en mesure de rétablir les unités nouvellement autonomes.
Grappes dans lesquelles une ou plusieurs unités ont été ajoutées à la grappe après la mise à niveau.	Supprimez les nouvelles unités, rapprochez les membres de la grappe, puis rétablissez la grappe plus petite. Vous pouvez également être en mesure de rétablir les unités nouvellement autonomes.
Les grappes dans lesquelles le Firewall Management Center et FXOS identifient un nombre différent d'unités de grappe.	Rapprochez les membres de la grappe et réessayez, bien que vous ne puissiez pas rétablir toutes les unités.

Restauration de Firewall Threat Defense avec Firewall Management Center

Vous devez utiliser Firewall Management Center pour rétablir le périphérique, sauf si les communications entre le Firewall Management Center et le périphérique sont interrompues. Dans ces cas, vous pouvez utiliser la commande CLI **upgrade revert** sur le périphérique. Pour voir à quelle version le système retournera, utilisez **show upgrade revert-info**.

Mise en garde Le fait de revenir de l'interface de ligne de commande peut entraîner la désynchronisation des configurations entre le périphérique et le Firewall Management Center, en fonction de ce que vous avez modifié après la mise à niveau. Cela peut entraîner d'autres problèmes de communication et de déploiement.

Avant de commencer

- Assurez-vous que la restauration est prise en charge. Lisez et comprenez les lignes directrices.
- Sauvegardez vers un emplacement externe sécurisé. Un échec de restauration peut nécessiter une recréation d'image, qui rétablit la plupart des paramètres aux valeurs d'usine par défaut.

Procédure

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

Étape 2 À côté du périphérique que vous souhaitez revenir en arrière, cliquez sur **Plus** (⋮) et sélectionnez **Revenir sur la mise à niveau**.

À l'exception des paires et des grappes à haute disponibilité, vous ne pouvez pas sélectionner plusieurs périphériques à rétablir.

Étape 3 Confirmez que vous souhaitez revenir en arrière et redémarrez.

Les interruptions du flux de trafic et de l'inspection pendant la restauration dépendent uniquement des configurations des interfaces, comme si chaque périphérique était autonome. En effet, même dans les déploiements à haute disponibilité et évolutivité, le système rétablit toutes les unités simultanément.

Étape 4 Surveillez l'avancement de la restauration.

Dans les déploiements à haute disponibilité et évolutivité, le flux de trafic et l'inspection reprennent lorsque la première unité est remise en ligne. Si le système n'affiche aucune progression pendant plusieurs minutes ou indique que la restauration a échoué, communiquez avec Centre d'assistance technique Cisco (TAC).

Étape 5 Vérifiez la réussite de la restauration.

Une fois la restauration terminée, choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)** et confirmez que les périphériques que vous avez rétablis disposent de la bonne version de logiciel.

Étape 6 (Firepower 4100/9300) Synchronisez toutes les modifications d'interface que vous avez apportées aux périphériques logiques Firewall Threat Defense à l'aide de Firewall Chassis Manager ou de l'interface de ligne de commande FXOS.

Dans Firewall Management Center, choisissez **Devices (périphériques)** > **Device Management (gestion des périphériques)**, modifiez le périphérique et cliquez sur **Sync** (Synchroniser).

Étape 7 Apportez toutes les autres modifications de configuration nécessaires après la restauration.

Par exemple, si vous avez modifié des objets utilisés par des configurations spécifiques au périphérique après la mise à niveau de ce dernier, le système crée de nouveaux objets ou configure les remplacements d'objets pour le périphérique rétabli. Nous vous recommandons d'examiner les objets utilisés par le périphérique rétabli et d'effectuer les ajustements nécessaires.

Étape 8 Redéployez les configurations sur les périphériques que vous venez de rétablir.

Un périphérique rétabli avec succès est marqué comme obsolète. . Comme le périphérique exécutera une version plus ancienne, les configurations plus récentes peuvent ne pas être prises en charge, même après un déploiement réussi.

Désinstaller un correctif

La désinstallation d'un correctif vous renvoie à la version à partir de laquelle vous avez mis à niveau et ne modifie pas les configurations. Étant donné que le Firewall Management Center doit exécuter la même version ou une version plus récente que ses périphériques gérés, désinstallez d'abord les correctifs sur les périphériques. La désinstallation n'est pas prise en charge pour les correctifs rapides .

Remarque Ce guide décrit comment désinstaller les correctifs Firewall Management Center et Firewall Threat Defense. Pour désinstaller les correctifs d'anciens périphériques ASA FirePOWER ou NGIPSv, consultez le *Guide de mise à niveau de Cisco Firepower Management Center, Version 6.0–7.0*.

Ordre de désinstallation pour la haute disponibilité/évolutivité

Dans les déploiements à haute disponibilité/évolutivité, limitez les perturbations liées à la désinstallation d'un périphérique à la fois. Contrairement à la mise à niveau, le système ne le fait pas pour vous. Attendez que le correctif soit entièrement désinstallé d'une unité avant de passer à l'autre.

Tableau 33 : Ordre de désinstallation pour la haute disponibilité Firewall Management Center

Configuration	Ordre de désinstallation
Firewall Management Center Haute disponibilité	La synchronisation étant en pause, qui est un état appelé *split-brain* (déconnexion cérébrale), désinstallez des pairs à la fois. Ne pas effectuer ou déployer de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale). **1.** Suspendez la synchronisation (entrez dans l'état split-brain). **2.** Désinstallez du périphérique en veille. **3.** Désinstallez du périphérique actif. **4.** Redémarrez la synchronisation (sortez de l'état split-brain).

Tableau 34 : Ordre de désinstallation pour la haute disponibilité et les grappes Firewall Threat Defense

Configuration	Ordre de désinstallation
Firewall Threat Defense Haute disponibilité	Vous ne pouvez pas désinstaller un correctif des périphériques configurés pour la haute disponibilité. Vous devez d'abord interrompre la haute disponibilité. **1.** Rompez la haute accessibilité **2.** Désinstallez de l'ancien périphérique en veille. **3.** Désinstallez de l'ancien périphérique actif. **4.** Rétablissez la haute disponibilité.
grappe Firewall Threat Defense	Désinstallez d'une unité à la fois, en laissant l'unité de contrôle pour la fin. Les unités en grappe fonctionnent en mode maintenance pendant que le correctif est désinstallé. **1.** Désinstallez des modules de données un à la fois. **2.** Faites de l'un des modules de données le nouveau module de contrôle. **3.** Désinstallez de l'ancien module de contrôle.

Désinstaller les correctifs des Threat Defense

Utilisez l'interface Shell Linux (*mode expert*) pour désinstaller les correctifs. Vous devez avoir accès à l'interface Shell du périphérique en tant qu'utilisateur `administrateur` du périphérique ou en tant qu'autre utilisateur local avec accès à la configuration de l'interface de ligne de commande. Vous ne pouvez pas utiliser u compte d'utilisateur Firewall Management Center. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.

Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Rompre voir Ordre de désinstallation pour la haute disponibilité/évolutivité, à la page 112.
- Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Si les configurations du périphérique sont obsolètes, déployez maintenant à partir du Firewall Management Center.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec. Assurez-vous que le déploiement et les autres tâches essentielles sont terminés. Les tâches en cours d'exécution au début de la désinstallation sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être reprises. Vous pouvez supprimer les messages d'état d'échec manuellement ultérieurement.

Étape 2 Accédez à l'interface de ligne de commande Firewall Threat Defense sur le périphérique Connectez-vous en tant qu'`administrateur` ou en tant qu'autre utilisateur de l'interface de ligne de commande avec accès à la configuration.

Vous pouvez vous connecter en SSH à l'interface de gestion du périphérique (nom de domaine ou adresse IP) ou utiliser la console. Si vous utilisez la console, certains périphériques utilisent l'interface de ligne de commande du système d'exploitation et nécessitent une étape supplémentaire pour accéder à l'interface de ligne de commande Firewall Threat Defense, comme indiqué dans le tableau ci-après.

Série Firepower 1000	`connect ftd`
Série Firepower 2100	`connect ftd`
Cisco Secure Firewall 3100 series	`connect ftd`
Firepower 4100/9300	`connect module` *`slot_number`* `console`, puis `connect ftd` (première connexion uniquement)

Étape 3 Utilisez la commande `expert` pour accéder à l'interface Shell Linux.

Étape 4 Vérifiez que le paquet de désinstallation se trouve dans le répertoire de mise à niveau.

```
ls /var/sf/updates
```

Les désinstallations de correctifs sont nommées comme les paquets de mise à niveau, mais ont `Patch_Uninstaller` au lieu de `Patch` dans le nom de fichier. Lorsque vous utilisez le correctif pour un périphérique, la désinstallation de ce correctif est automatiquement créée dans le répertoire de mise à niveau. Si le programme de désinstallation n'est pas présent, communiquez avec Centre d'assistance technique Cisco (TAC).

Étape 5 Exécutez la commande de désinstallation et saisissez votre mot de passe lorsque vous y êtes invité.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

Mise en garde Le système ne vous demande *pas* de confirmer. La saisie de cette commande démarre la désinstallation, qui comprend un redémarrage du périphérique. Les interruptions du flux de trafic et de l'inspection au cours d'une désinstallation sont identiques aux interruptions qui se produisent lors d'une mise à niveau. Assurez-vous d'être prêt. Remarque : l'utilisation de l'option `--detach` garantit que le processus de désinstallation n'est pas interrompu si votre session SSH expire, ce qui peut laisser le périphérique dans un état instable.

Étape 6 Surveillez la désinstallation jusqu'à ce que vous soyez déconnecté.

Pour une désinstallation dissociée, utilisez `tail` ou `tailf` pour afficher les journaux :

```
tail /ngfw/var/log/sf/update.status
```

Sinon, surveillez la progression dans la console ou le terminal.

Étape 7 Vérifiez la réussite de la désinstallation.

Une fois la désinstallation terminée, vérifiez que les périphériques disposent de la bonne version du logiciel. Dans le Firewall Management Center, sélectionnez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**.

Étape 8 Dans les déploiements à haute disponibilité/évolutivité, répétez les étapes 2 à 6 pour chaque unité.

Pour les grappes, ne désinstallez jamais de l'unité de contrôle. Après avoir désinstallé de toutes les unités de données, faites de l'une d'elles le nouveau contrôle, puis désinstallez de l'ancien contrôle.

Étape 9 Redéployez les configurations.

Exception : Ne déployez pas sur des paires à haute accessibilité de version mixte ou des grappes de périphériques. Déployez avant de désinstaller le correctif du premier périphérique, mais pas à nouveau avant d'avoir désinstallé le correctif de tous les membres du groupe.

Prochaine étape

- Pour la haute disponibilité, rétablissez la haute disponibilité.
- Pour les grappes, si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Désinstaller les correctifs Firewall Management Center autonomes

Nous vous recommandons d'utiliser l'interface Web pour désinstaller les correctifs Firewall Management Center. Si vous ne pouvez pas utiliser l'interface Web , vous pouvez utiliser l'interface Shell Linux comme utilisateur `administrateur` de l'interface Shell ou en tant qu'utilisateur externe avec accès à l'interface Shell. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.



Mise en garde Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Si la désinstallation place le Firewall Management Center à un niveau de correctif inférieur à celui de ses périphériques gérés, désinstallez d'abord les correctifs de ces périphériques.
- Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Déployez vers les périphériques gérés dont les configurations ne sont pas à jour.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec.

Étape 2 Sous Available Updates (Mises à jour disponibles), cliquez sur l'icône **Install** (installer) à côté du paquet de mise à niveau, puis choisissez le Firewall Management Center.

Les désinstallations de correctifs sont nommées comme les paquets de mise à niveau, mais ont `Patch_Uninstaller` au lieu de `Patch` dans le nom de fichier. Lorsque vous appliquez un correctif au Firewall Management Center, la désinstallation de ce correctif est automatiquement créée dans le répertoire de mise à niveau. Si le programme de désinstallation n'est pas présent, communiquez avec Centre d'assistance technique Cisco (TAC).

Étape 3 Cliquez sur **Install (installer)**, puis confirmez que vous souhaitez désinstaller et redémarrer.

Vous pouvez surveiller la progression de la désinstallation dans le centre de messages jusqu'à ce que vous soyez déconnecté.

Étape 4 Reconnectez-vous quand vous le pouvez et vérifiez que la désinstallation a réussi.

Si le système ne vous informe pas de la réussite de la désinstallation lorsque vous vous connectez, choisissez **Help (Aide)** > **About (À propos)** pour afficher les informations sur la version actuelle du logiciel.

Étape 5 Déployez de nouveau les configurations sur tous les périphériques gérés.

Désinstaller les correctifs de haute disponibilité Firewall Management Center

Nous vous recommandons d'utiliser l'interface Web pour désinstaller les correctifs Firewall Management Center. Si vous ne pouvez pas utiliser l'interface Web , vous pouvez utiliser l'interface Shell Linux comme utilisateur `administrateur` de l'interface Shell ou en tant qu'utilisateur externe avec accès à l'interface Shell. Si vous avez désactivé l'accès à l'interface Shell, communiquez avec Centre d'assistance technique Cisco (TAC) pour annuler le verrouillage.

Désinstallez des pairs de haute disponibilité un à la fois. Une fois que la synchronisation est interrompue, désinstallez d'abord sur l'unité de secours, puis l'unité active. Lorsque le périphérique de secours commence la désinstallation, son état passe de « de secours » à « actif », de sorte que les deux homologues sont actifs. Cet état temporaire s'appelle *split-brain* (déconnexion cérébrale) et *n'est pas* pris en charge, sauf pendant une mise à niveau ou une désinstallation.



Mise en garde Ne pas effectuer ou déployer de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale). Vos modifications seront perdues après le redémarrage de la synchronisation. Le déploiement pourrait placer le système dans un état inutilisable et nécessiter une recréation d'image. Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

Avant de commencer

- Si la désinstallation place les Firewall Management Center à un niveau de correctif inférieur à celui de leurs périphériques gérés, désinstallez d'abord les correctifs sur les périphériques.
- Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Sur le Firewall Management Center actif, déployez vers les périphériques gérés dont la configuration n'est pas à jour.

Si vous procédez au déploiement avant la désinstallation, vous réduisez les risques d'échec.

Étape 2 Sur le Firewall Management Center actif, suspendez la synchronisation.

a) Choisissez **Integration (Intégration)** > **Other Integrations (Autres intégrations)**.
b) Sous l'onglet **High Availability**, cliquez sur **Suspendre la synchronisation**.

Étape 3 Désinstallez le correctif sur les homologues un à la fois : d'abord l'homologue de secours, puis l'homologue actif.

Suivez les instructions dans Désinstaller les correctifs Firewall Management Center autonomes , à la page 115, mais omettez le déploiement initial et arrêtez-vous après avoir vérifié, pour chaque homologue, la réussite de la désinstallation. En résumé, pour chaque homologue :

a) Dans la page **System (Système)** > **Updates (Mises à jour)**, désinstallez le correctif.
b) Surveillez la progression jusqu'à ce que vous soyez déconnecté, puis reconnectez-vous lorsque vous le pouvez.
c) Vérifiez la réussite de la désinstallation.

Étape 4 Sur le Firewall Management Center que vous souhaitez définir comme homologue actif, redémarrez la synchronisation.

a) Choisissez **Integration (Intégration)** > **Other Integrations (Autres intégrations)**.
b) Sous l'onglet **High Availability (haute disponibilité**), cliquez sur **Make-Me-Active** (Rendez-moi actif).
c) Attendez que la synchronisation redémarre et que l'autre Firewall Management Center passe en mode veille.

Étape 5 Déployez de nouveau les configurations sur tous les périphériques gérés.

À propos de la traduction

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