Mettre à niveau le On-Prem Firewall Management Center

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

- Liste de contrôle des mises à niveau pour On-Prem Firewall Management Center, à la page 1
- Chemin de mise à niveau pour On-Prem Firewall Management Center, à la page 5
- Charger les paquets de mise à niveau pour On-Prem Firewall Management Center, à la page 7
- Exécuter la vérification de l'état de préparation pour On-Prem Firewall Management Center, à la page 8
- Mettre à niveau le On-Prem Firewall Management Center : autonome, à la page 9
- Mettre à niveau le On-Prem Firewall Management Center : Haute disponibilité, à la page 10

Liste de contrôle des mises à niveau pour On-Prem 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 On-Prem Firewall Management Center, à la page 5 • Chemins de mise à niveau pour Firewall Threat Defense • Chemins de mise à niveau pour FXOS
	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, 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. • Cisco Secure Firewall Threat Defense Notes de mise à jour, dans le chapitre *Bogues ouverts et résolus*, pour les bogues qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions des notes de mise à jour entre votre version actuelle et la version cible. Si vous disposez d'un contrat d'assistance, vous pouvez utiliser l'Outil de recherche de bogues pour obtenir des listes de bogues à jour. • Notes de version Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.
	Vérifiez 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 On-Prem Firewall Management Center après la mise à niveau de ses périphériques gérés, afin que votre nouveau fichier de sauvegarde On-Prem 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 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 On-Prem 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 On-Prem Firewall Management Center pour effectuer un téléchargement direct. Pour une haute disponibilité On-Prem Firewall Management Center, vous devez téléverser le paquet de mise à niveau On-Prem 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 On-Prem Firewall Management Center, à la page 7.

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 : • On-Prem 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.
	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 On-Prem Firewall Management Center, à la page 8.
	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 On-Prem Firewall Management Center, choisissez **Système** (⚙) > **Monitoring (Surveillance)** > **Statistics (Statistiques)** et sélectionnez le On-Prem 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 repris. 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 On-Prem Firewall Management Center

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

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

Notez que si votre version actuelle Firewall Threat Defense/On-Prem 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 1 : Mises à niveau directes de On-Prem 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 le magasin de données, vous ne pouvez pas mettre à niveau FMC 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 On-Prem Firewall Management Center

Utilisez cette procédure pour charger manuellement les paquets de mise à niveau sur le On-Prem 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 On-Prem 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 On-Prem 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 On-Prem 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 On-Prem Firewall Management Center dans une paire à haute disponibilité, suspendez la synchronisation.

Pour une haute disponibilité On-Prem Firewall Management Center, vous devez téléverser le paquet de mise à niveau On-Prem 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 On-Prem 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 On-Prem Firewall Management Center

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

Procédure

Étape 1 Dans On-Prem 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 On-Prem 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 On-Prem Firewall Management Center : autonome

Utilisez cette procédure pour mettre à niveau un périphérique autonome On-Prem 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 On-Prem 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 On-Prem 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. 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 dont la configuration n'est plus à jour.

Mettre à niveau le On-Prem Firewall Management Center : Haute disponibilité

La mise à niveau de la haute disponibilité On-Prem 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, On-Prem Firewall Management Center devient actif, ce qui vous permet de mettre à niveau l'autre On-Prem 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 On-Prem Firewall Management Center actif, suspendez la synchronisation.

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

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

Pour une haute disponibilité On-Prem Firewall Management Center, vous devez téléverser le paquet de mise à niveau On-Prem 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 On-Prem Firewall Management Center : autonome, à la page 9, 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 On-Prem 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 On-Prem 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. 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 dont la configuration n’est plus à jour.

À propos de la traduction

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

À propos de la traduction

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