# 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 On-Prem 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.


- Revenir Firewall Threat Defense, à la page 1
- Désinstaller un correctif, à la page 5


# Revenir Firewall Threat Defense

## À propos de la restauration Firewall Threat Defense

La restauration 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 Cisco Secure Firewall chassis manager ou FXOS CLI.

  Synchroniser 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 2.

# 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 On-Prem 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 On-Prem 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 1 : Scénarios de prévention de la restauration***

| Scénario | Solution |
|---|---|
| L'instantané de rétablissement n'est pas disponible pour les raisons suivantes :<br>• Vous n'avez pas activé l'option de rétablissement lorsque vous avez mis à niveau le périphérique.<br>• Vous avez supprimé l'instantané de On-Prem Firewall Management Center ou du périphérique, ou il a expiré.<br>• Vous avez mis à niveau le périphérique avec un autre On-Prem Firewall Management Center. | Aucun.<br>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 après réussite de la mise à niveau), ce qui va à l'encontre de notre recommandation habituelle d'utiliser l'assistant de mise à niveau de Firewall Threat Defense.<br>L'instantané de restauration est enregistré sur le On-Prem 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.<br><br>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-le 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 On-Prem 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. |

# Revenir sur Firewall Threat Defense avec On-Prem Firewall Management Center

Vous devez utiliser On-Prem Firewall Management Center pour rétablir le périphérique, sauf si les communications entre le On-Prem 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 On-Prem 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 (appareils)** > **Device Management (gestion des appareils)**.

**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 (appareils)** > **Device Management (gestion des appareils)** 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 On-Prem Firewall Management Center, choisissez **Devices (appareils)** > **Device Management (gestion des appareils)**, 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 On-Prem 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 On-Prem 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 2 : Ordre de désinstallation pour la haute disponibilité On-Prem Firewall Management Center***

| Configuration | Ordre de désinstallation |
|---|---|
| On-Prem 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)<br>**1.** Suspendez la synchronisation (entrez dans l'état split-brain).<br>**2.** Désinstallez du périphérique en veille.<br>**3.** Désinstallez du périphérique actif.<br>**4.** Redémarrez la synchronisation (sortez de l'état split-brain). |

***Tableau 3 : 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.<br>**1.** Rompre la haute accessibilité<br>**2.** Désinstallez de l'ancien périphérique en veille.<br>**3.** Désinstallez de l'ancien périphérique actif.<br>**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.<br>**1.** Désinstallez des modules de données un à la fois.<br>**2.** Faites de l'un des modules de données le nouveau module de contrôle.<br>**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 On-Prem 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 les Firewall Threat Defense les paires à haute accessibilité ; voir Ordre de désinstallation pour la haute disponibilité/évolutivité, à la page 6.
- Vérifiez que votre déploiement est intègre et communique correctement.

### Procédure

**Étape 1** Si les configurations du périphérique sont obsolètes, déployez maintenant à partir du On-Prem 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 On-Prem 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 On-Prem Firewall Management Center autonomes

Nous vous recommandons d'utiliser l'interface Web pour désinstaller les correctifs On-Prem 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 On-Prem 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 On-Prem 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 On-Prem 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 dont la configuration n'est plus à jour.

# Désinstaller les correctifs de haute disponibilité On-Prem Firewall Management Center

Nous vous recommandons d'utiliser l'interface Web pour désinstaller les correctifs On-Prem 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 de pourrait placer le système dans un état inutilisable et nécessiter une recréation d'image. Évitez d'apporter ou de déployer des modifications à la configuration durant la désinstallation. Même si le système semble inactif, ne redémarrez pas, n'éteignez pas ou ne redémarrez pas manuellement une désinstallation en cours. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes avec la désinstallation, comme son échec, ou si un appareil ne répond pas, communiquez avec Centre d'assistance technique Cisco (TAC).

### Avant de commencer

- Si la désinstallation place les On-Prem 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 On-Prem 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 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 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 On-Prem Firewall Management Center autonomes , à la page 9, 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 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** Déployez de nouveau les configurations sur 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.