Mettre à niveau des dispositifs logiques FTD

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

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

Remarque

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

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

Planification et faisabilité

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

Tableau 1 :

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

Progiciels de mise à niveau

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

Tableau 2 :

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

Sauvegardes

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

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

⚠

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

Tableau 3 :

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

Mises à niveau associées

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

Tableau 4 :

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

Contrôle final

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

Tableau 5 :

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

Procédure

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

Étape 2 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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

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

Exemple :

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

Procédure

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

Étape 3 Si nécessaire, revenez au mode micrologiciel :

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

Étape 4 Passez en mode d'installation automatique :

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

Étape 5 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

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

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

Étape 8 Pour superviser le processus de mise à niveau :

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

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

Exemple :

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

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

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

FP9300-A /system #
```

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

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

Mettre à niveau FXOS : paires FTD à haute disponibilité

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

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

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

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

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

Avant de commencer

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

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

Procédure

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

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

Étape 3 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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

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

Exemple :

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

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

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

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

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

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

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

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

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

Étape 11 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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

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

Exemple :

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

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

Procédure

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

Étape 3 Si nécessaire, revenez au mode micrologiciel :

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

Étape 4 Passez en mode d'installation automatique :

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

Étape 5 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

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

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

Étape 8 Pour superviser le processus de mise à niveau :

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

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

Exemple :

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

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

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

FP9300-A /system #
```

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

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

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

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

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

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

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

a) Entrez en mode micrologiciel :

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

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

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

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

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

c) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

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

Étape 13 Si nécessaire, revenez au mode micrologiciel :

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

Étape 14 Passez en mode d'installation automatique :

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

Étape 15 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

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

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

Étape 18 Pour superviser le processus de mise à niveau :

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

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

Exemple :

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

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

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

FP9300-A /system #
```

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

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

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

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

Mettre à niveau FXOS : grappes FTD inter-châssis.

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

Par exemple, pour une grappe à deux châssis :

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

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

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

Avant de commencer

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

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

Procédure

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

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

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

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

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

show version.

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

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

Étape 4 Chargez la nouvelle image groupée de la plateforme :

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

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

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

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

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

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

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

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

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

Exemple :

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

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

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

Procédure

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

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

a) Entrez **top**.

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

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

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

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

show version.

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

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

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

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

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

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

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

d) Pour surveiller le processus de téléchargement :

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

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

Exemple :

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

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

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

Étape 4 Si nécessaire, revenez au mode micrologiciel :

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

Étape 5 Passez en mode d'installation automatique :

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

Étape 6 Installez l'ensemble de la plateforme FXOS :

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

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

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

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

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

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

Étape 9 Pour superviser le processus de mise à niveau :

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

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

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

Exemple :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

Procédure

Sélectionnez les périphériques à mettre à niveau

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

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

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

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

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

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

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

Étape 4 Vérifiez votre sélection de périphérique.

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

Copiez les paquets de mise à niveau vers les périphériques.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Effectuez une mise à niveau.

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

Étape 12 Choisissez les options de restauration.

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

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

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

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

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

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

Étape 14 Vérifiez la réussite de la mise à niveau.

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

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

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

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

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

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

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

Prochaine étape

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

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

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

Avant de commencer

- Décidez si vous souhaitez utiliser cette procédure. Pour les mises à niveau de Cisco FTD vers la version 7.0.x, nous vous recommandons d'utiliser l' assistant de mise à niveau ; voir Mettre à niveau Firepower Threat Defense avec FMC (version 7.0.0), à la page 25.
- Remplissez la liste de contrôle avant la mise à niveau. Vérifiez que les périphériques de votre déploiement sont intègres et communiquent correctement.
- (Facultatif) Modifiez les rôles actif/de secours de vos paires de périphériques à haute disponibilité. Choisissez **Devices (Périphériques)** > **Device Management (Gestion des périphériques)**, cliquez sur l'icône **Switch Active Peer** (Commuter l'homologue actif) à côté de la paire et confirmez votre choix.

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

Procédure

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

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

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

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

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

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

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

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

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

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

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

Étape 6 Vérifiez la réussite de la mise à niveau.

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

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

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

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

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

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.