

Mises à Niveau Cisco Firepower Management Center

- Liste de contrôle de mise à niveau : Firepower Management Center.contrôle, à la page 1
- Mettre à niveau un élément autonome Cisco Firepower Management Center, à la page 5
- Mettre à niveau les Firepower Management Center à haute disponibilité, à la page 7

Liste de contrôle de mise à niveau : Firepower Management Center.contrôle

Terminez cette liste de contrôle avant de mettre à niveau un FMC, y compris FMCv. Si vous mettez à niveau une paire à haute disponibilité, remplissez la liste de contrôle pour chaque homologue.

Remarque En tout temps pendant le processus, assurez-vous de maintenir la communication et l'intégrité de déploiement. *Ne redémarrez pas* une mise à niveau FMC en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez 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 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
	Téléverser le paquet de mise à niveau Pour des déploiements FMC à haute disponibilité, vous devez charger le paquet de mise à niveau FMC sur les deux homologues, en suspendant la synchronisation avant de transférer le paquet sur le paquet de secours. Pour limiter les interruptions de la synchronisation à haute disponibilité, vous pouvez transférer le paquet vers l'homologue actif pendant l'étape de préparation de la mise à niveau, et vers l'homologue de secours dans le cadre du processus de mise à niveau lui-même, après avoir suspendu la synchronisation. Consultez Charger vers Cisco Firepower Management Center.

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. 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.

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. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau de FMC majeure.

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.

✓	Action/Vérification
	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. Consultez Vérification de l'état de préparation du logiciel Firepower.
	Vérifiez les tâches en cours. Assurez-vous que les tâches essentielles, 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. **Remarque** Dans certains déploiements, les mises à niveau reportent automatiquement les tâches planifiées. Toute tâche planifiée pour commencer pendant la mise à niveau commencera cinq minutes après le redémarrage suivant la mise à niveau. Cette fonctionnalité est actuellement prise en charge pour les FMC exécutant la version 6.4.0.10 et les versions ultérieures, la version 6.6.3 et les versions de maintenance ultérieures ainsi que la version 6.7.0 et les versions ultérieures. Notez que cette fonctionnalité est prise en charge pour toutes les mises à niveau *à partir d'* une version prise en charge. Cette fonctionnalité n'est pas prise en charge pour les mises à niveau *vers* une version prise en charge à partir d'une version non prise en charge.

Mettre à niveau un élément autonome Cisco Firepower Management Center

Utilisez cette procédure pour mettre à niveau un Cisco Firepower Management Center autonome, y compris Cisco Firepower Management Center Virtual.

⚠

Mise en garde N'apportez *pas* et ne déployez pas de modifications de configuration, ne redémarrez pas le système manuellement ou ne l'éteignez pas pendant la mise à niveau du FMC. Ne redémarrez *pas* une mise à niveau en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez 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

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

Étape 2 Cliquez sur l'icône Installer à côté du paquet de mise à niveau que vous souhaitez utiliser, puis choisissez FMC.

Étape 3 Cliquez sur **Installer** pour commencer la mise à niveau.

Confirmez que vous souhaitez procéder à la mise à niveau et redémarrez le système.

Étape 4 Surveillez la progression de la vérification préalable jusqu'à ce que vous soyez déconnecté. Évitez d'apporter des modifications à la configuration pendant ce temps.

Étape 5 Reconnectez-vous quand vous le pouvez.

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

Étape 6 Si vous y êtes invité, passez en revue le contrat de licence de l'utilisateur final (CLUF) et acceptez-le.

Étape 7 Vérifiez la réussite de la mise à niveau.

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

Étape 8 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 9 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 10 Redéployez les configurations.

Redéployez les configurations sur *tous* les périphériques gérés. Si vous ne les déployez pas sur un périphérique, la mise à niveau ultérieure de ce dernier risque d'échouer et vous devrez peut-être le réinitialiser.

Mettre à niveau les Firepower Management Center à haute disponibilité

Utilisez cette procédure pour mettre à niveau le logiciel Firepower sur les FMC dans une paire à haute disponibilité.

Vous mettez à niveau les homologues un à la fois. Une fois que la synchronisation est interrompue, mettez d'abord à niveau l'unité de secours, puis l'unité active. Lorsque le périphérique de secours commence les vérifications préalables, 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 lors de la mise à niveau. N'effectuez ni ne déployez *pas* de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale) Vos modifications seront perdues après le redémarrage de la synchronisation.

⚠

Mise en garde N'apportez *pas* et ne déployez pas de modifications de configuration, ne redémarrez pas le système manuellement ou ne l'éteignez pas pendant la mise à niveau du FMC. Ne redémarrez *pas* une mise à niveau en cours. Le processus de mise à niveau peut sembler inactif pendant les vérifications préalables, ce qui est normal. Si vous rencontrez des problèmes avec la mise à niveau, comme son échec, ou si un appareil ne répond pas, communiquez le Centre d'assistance technique Cisco (TAC)

Avant de commencer

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

Procédure

Étape 1 Suspendez la synchronisation.

a) Choisissez **Intégration** > **système**.
b) Sous l'onglet **High Availability**, cliquez sur **Suspendre la synchronisation**.

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

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

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

Suivez les instructions dans Mettre à niveau un élément autonome Cisco Firepower Management Center, à la page 5, en vous arrêtant après avoir vérifié la réussite de la mise à jour sur chaque homologue. En résumé, pour chaque homologue :

a) Sur la page **Système** > **Mises à jour**, installez la mise à niveau.
b) Surveillez la progression jusqu'à ce que vous soyez déconnecté, puis reconnectez-vous lorsque vous le pouvez (cela se produit deux fois pour les mises à niveau majeures).
c) Vérifiez la réussite de la mise à niveau.

N'effectuez ni ne déployez *pas* de changements de configuration lorsque la paire est en état split-brain (déconnexion cérébrale)

Étape 4 Redémarrez la synchronisation.

a) Connectez-vous au FMC que vous souhaitez utiliser comme homologue actif.
b) Choisissez **Système** > **Intégration**.
c) Sous l'onglet **Haute disponibilité**, cliquez sur **Rendez-moi actif**.
d) Attendez que la synchronisation redémarre et que l'autre FMC passe en mode de secours.

Étape 5 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 6 Apportez toutes les modifications de configuration après la mise à niveau décrites dans les notes de mise à jour.

Étape 7 Redéployez les configurations.

Redéployez les configurations sur *tous* les périphériques gérés. Si vous ne les déployez pas sur un périphérique, la mise à niveau ultérieure de ce dernier risque d'échouer et vous devrez peut-être le réinitialiser.

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.