Mise à niveau de la série Firepower 7000/8000 et NGIPSv

Liste de contrôle de mise à niveau : série Firepower 7000/8000 et NGIPSv avec FMC

Remplissez cette liste de contrôle avant de mettre à niveau des périphériques Firepower 7000/8000 et NGIPSv.

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 de périphérique 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 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 vers le FMC. Consultez Charger vers Cisco Firepower Management Center.
	Copiez le paquet de mise à niveau sur le périphérique. Si votre instance de FMC utilise la version 6.2.3 ou une version ultérieure, nous vous recommandons de copier (*pousser*) les paquets sur les périphériques gérés avant de lancer la mise à niveau de ces derniers. 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
	Savegardez les périphériques de séries 7000/8000. Utilisez le FMC pour sauvegarder les périphériques de la série 7000/8000. Les sauvegardes ne sont pas prises en charge pour NGIPSv. 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 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.

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 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.

Mise à niveau de la série Firepower 7000/8000 et NGIPSv avec FMC

Utilisez cette procédure pour mettre à niveau les périphériques Firepower 7000/8000 Series et NGIPSv. Vous pouvez mettre à niveau plusieurs périphériques à la fois s'ils utilisent le même paquet de mise à niveau. Vous devez mettre à niveau les membres des grappes de périphériques et les paires à haute disponibilité en même temps.

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 (Facultatif) Modifiez les rôles actif/de secours de vos paires de périphériques à haute disponibilité qui effectuent la commutation/le routage.

Si vos paires à haute disponibilité sont déployées pour effectuer *uniquement* un contrôle d'accès, les périphériques actifs sont mis à niveau en premier. Une fois la mise à niveau terminée, les périphériques actifs et de secours conservent leurs anciens rôles.

Cependant, dans un déploiement routé ou commuté, c'est le périphérique de secours qui est d'abord mis à niveau. 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.

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.

Étape 2 Choisissez **Système** > **Mises à jour**.

Étape 3 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 4 Cliquez sur **Install** (Installer), puis confirmez que vous souhaitez mettre à niveau et redémarrer les périphériques.

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. Ne redémarrez *pas* une mise à niveau de périphérique 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 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.