Mise à niveau Défense contre les menaces

- Liste de contrôle des mises à niveau pour Défense contre les menaces, à la page 1
- Chemins de mise à niveau pour Défense contre les menaces, à la page 5
- Paquets de mise à niveau pour Défense contre les menaces, à la page 10
- Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 10
- Mise à niveau Défense contre les menaces, à la page 12
- Surveilla des mises à niveau de Défense contre les menaces, à la page 15
- ou nouvelle Défense contre les menaces mises à niveau, à la page 15
- , à la page 16
- Dépannage des mises à niveau de Threat Defense , à la page 17

Liste de contrôle des mises à niveau pour Défense contre les menaces

Planification et faisabilité

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

✓	Action/Vérification	Détails
	Évaluez votre déploiement.	Comprendre où vous êtes détermine comment vous atteindrez votre objectif. En plus des informations sur la version et le modèle actuels, déterminez si votre déploiement est configuré pour une haute disponibilité
	Planifiez votre chemin de mise à niveau.	Cela est particulièrement important pour les déploiements à haute disponibilité, les mises à niveau multisauts et les situations où vous devez mettre à niveau des systèmes d'exploitation ou des environnements d'hébergement. Les mises à niveau peuvent être majeures (A.x), de maintenance (A.x.y) ou de correctifs (A.x.y.z). Voir : • Chemins de mise à niveau pour Défense contre les menaces, à la page 5 • Chemins de mise à niveau pour FXOS

✓	Action/Vérification	Détails
	Lisez les directives de mise à niveau et prévoyez les modifications de configuration.	Surtout avec les mises à niveau majeures, la mise à niveau peut entraîner ou nécessiter des modifications de configuration importantes avant ou après la mise à niveau. Commencez par celles-ci : • Directives relatives aux mises à niveau logicielles, pour les directives relatives aux mises à niveau critiques et spécifiques aux versions. • Nouvelles fonctionnalités de Cisco Secure Firewall Device Manager par version, pour les fonctionnalités nouvelles et obsolètes qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions entre votre version actuelle et la version cible. • Cisco Secure Firewall Threat Defense Notes de mise à jour, dans le chapitre *Bogues ouverts et résolus*, pour les bogues qui ont une incidence sur les mises à niveau. Vérifiez toutes les versions des notes de mise à jour entre votre version actuelle et la version cible. Si vous disposez d'un contrat d'assistance, vous pouvez utiliser l'outil de recherche de bogues pour obtenir des listes de bogues à jour. • Notes de version Cisco Firepower 4100/9300 FXOS, pour les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300.
	Vérifiez l'accès à l'appareil.	Les périphériques peuvent arrêter de transmettre le trafic pendant la mise à niveau ou en cas d'échec de celle-ci. 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 .
	Vérifiez la bande passante.	Assurez-vous que votre réseau de gestion dispose de la bande passante nécessaire pour effectuer des transferts de données volumineux. Chaque fois que cela est possible, chargez les paquets de mise à niveau à l'avance. Si vous transférez un ensemble de mise à niveau vers un périphérique au moment de la mise à niveau, une bande passante insuffisante peut prolonger le délai de mise à niveau. Consultez les Directives relatives au téléchargement de données du centre de gestion Cisco Firepower Management Center vers des périphériques gérés (Note technique de dépannage).

✓	Action/Vérification	Détails
	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 les mises à niveau sont susceptibles de prendre. Tenez compte des tâches que vous devez effectuer dans la fenêtre et de celles que vous pouvez effectuer à l'avance. Voir : • Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces • Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces • Flux de trafic et inspection pour les mises à niveau de châssis • Tests de temps et d'espace disque

Sauvegardes

À l'exception des correctifs rapides, la mise à niveau supprime toutes les sauvegardes stockées sur le système. Nous vous recommandons *fortement* de procéder à une sauvegarde dans un emplacement distant sécurisé et de vérifier la réussite du transfert, avant et après la mise à niveau :

- Avant la mise à niveau : si une mise à niveau échoue de manière catastrophique, vous devrez peut-être effectuer une réinitialisation et une restauration. La recréation d'image rétablit la plupart des paramètres aux valeurs par défaut, y compris le mot de passe système. Si vous avez une sauvegarde récente, vous pouvez revenir aux opérations normales plus rapidement.
- Après la mise à niveau : cela crée un instantané de votre déploiement nouvellement mis à niveau.

✓	Action/Vérification	Détails
	Sauvegardez défense contre les menaces .	Pour sauvegarder les configurations de défense contre les menaces , consultez le chapitre *Gestion du système* dans le Guide Cisco Secure Firewall Device Manager Configuration . Si vous avez un Firepower 9300 avec défense contre les menaces et des périphériques logiques ASA s'exécutant sur des modules distincts, utilisez ASDM ou l'interface de ligne de commande d'ASA pour sauvegarder les configurations et les autres fichiers critiques, en particulier s'il y a une migration de la configuration de l'ASA. Consultez le chapitre *Logiciels et configurations* du Guide de configuration des opérations générales de la gamme Cisco ASA.
	Sauvegardez FXOS sur le Firepower 4100/9300.	Utilisez le gestionnaire de châssis ou l'interface de ligne de commande de FXOS pour exporter les configurations des châssis, y compris les paramètres de configuration des périphériques logiques et de la plateforme. Consultez le chapitre *Importation et exportation de la configuration* du Guide de configuration de Cisco Firepower 4100/9300 FXOS.

Progiciels de mise à niveau

Le chargement des paquets de mise à niveau vers le système avant de commencer la mise à niveau peut réduire la durée de votre fenêtre de maintenance.

✓	Action/Vérification	Détails
	Téléchargez le paquet de mise à niveau à partir de Cisco et chargez-le sur le périphérique.	Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : Paquets de mise à niveau pour Défense contre les menaces, à la page 10. Pour la haute disponibilité de défense contre les menaces , vous devez charger le paquet de mise à niveau sur les deux unités.

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.

✓	Action/Vérification	Détails
	Mettez à niveau l'hébergement virtuel.	Si nécessaire, mettez à niveau l'environnement d'hébergement. Si cela est nécessaire, c'est généralement parce que vous utilisez une ancienne version de VMware et effectuez une mise à niveau majeure.
	Mettez à niveau le micrologiciel sur le Firepower 4100/9300.	Nous vous recommandons d'utiliser le micrologiciel le plus récent. Consultez la section CGuide de mise à niveau du micrologiciel Cisco Firepower 4100/9300 FXOS.
	Mettez à niveau FXOS sur le Firepower 4100/9300.	La mise à niveau de FXOS est généralement requise pour les mises à niveau majeures, mais très rare pour les versions de maintenance et les correctifs. Pour minimiser les perturbations, mettez à niveau FXOS dans les paires à haute accessibilité défense contre les menaces et les grappes inter-châssis, . Consultez Mettre à niveau le châssis sur le Firepower 4100/9300.

Contrôle final

Un ensemble de vérifications finales garantit que vous êtes prêt à mettre à niveau le logiciel.

✓	Action/Vérification	Détails
	Vérifiez les configurations.	Assurez-vous d'avoir apporté les modifications de configuration requises avant la mise à niveau et d'être prêt à apporter les modifications de configuration requises après la mise à niveau.
	Vérifiez la synchronisation NTP.	Assurez-vous que tous les périphériques sont synchronisés avec le serveur NTP que vous utilisez pour donner l'heure. La désynchronisation peut entraîner l'échec de la mise à niveau. Pour vérifier l'heure, utilisez la commande **show time** de l'interface de ligne de commande.

✓	Action/Vérification	Détails
	Déployez des configurations.	Si vous procédez au déploiement des configurations avant la mise à niveau, vous réduisez les risques d'échec. Le déploiement peut affecter le flux de trafic et l'inspection; voir Flux de trafic et inspection pour les mises à niveau de Défense contre les menaces.
	Exécutez la vérification de l'état de préparation.	La réussite des vérifications de l'état de préparation réduit considérablement les risques d'échec de la mise à niveau. Consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 10.
	Vérifiez l'espace disque.	Les vérifications de l'état de préparation comprennent une vérification de l'espace disque. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Pour vérifier l'espace disque disponible sur le périphérique, utilisez la commande **show disk** de l'interface de ligne de commande.
	Vérifiez les tâches en cours.	Assurez-vous que les tâches essentielles sont terminées avant de procéder à la mise à niveau. Les tâches en cours d'exécution au début de la mise à niveau sont arrêtées, deviennent des tâches ayant échoué et ne peuvent pas être repris. Nous vous recommandons également de vérifier les tâches programmées pour s'exécuter lors de la mise à niveau et de les annuler ou de les reporter.

Chemins de mise à niveau pour Défense contre les menaces

Choisissez le chemin de mise à niveau qui correspond à votre déploiement.

Chemin de mise à niveau pour Défense contre les menaces avec FXOS

Ce tableau fournit le chemin de mise à niveau pour défense contre les menaces sur le Firepower 4100/9300.

Notez que si votre version actuelle défense contre les menaces est publiée après une date postérieure à celle de votre version cible, vous ne pourrez peut-être pas mettre à niveau comme prévu. Dans ces cas, la mise à niveau échoue rapidement et affiche une erreur expliquant qu'il existe des incompatibilités de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Ce tableau répertorie nos combinaisons de versions spécialement qualifiées. Comme vous devez d'abord mettre à niveau FXOS, vous exécuterez brièvement une combinaison prise en charge, mais non recommandée, dans laquelle le système d'exploitation est « en avance » sur le logiciel du périphérique. Assurez-vous que la mise à niveau de FXOS ne vous rend pas compatible avec des périphériques logiques. Pour les configurations minimales et d'autres informations détaillées sur la compatibilité, consultez le Guide de compatibilité de Cisco Secure Firewall Threat Defense.

Tableau 1 : Défense contre les menaces Mises à niveau directes sur Firepower 4100/9300

Versions actuelles	Versions cibles
FXOS 2.13 avec Threat Defense 7.3	→ FXOS 2.13 avec toute version ultérieure de Threat Defense 7.3.x
FXOS 2.12 avec Threat Defense 7.2 Dernière prise en charge de Firepower 4110, 4120, 4140, 4150. Dernière prise en charge de l'appareil Firepower 9300 avec les modules SM-24, SM-36 ou SM-44.	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec toute version ultérieure de Threat Defense 7.2.x
FXOS 2.11.1 avec Threat Defense 7.1	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec toute version ultérieure de Threat Defense 7.1.x
FXOS 2.10.1 avec Threat Defense 7.0	Une des versions suivantes : → FXOS 2.13 avec Threat Defense 7.3.x → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec toute version ultérieure de Threat Defense 7.0.x **Remarque** En raison d'incompatibilités avec le magasin de données, vous ne pouvez pas mettre à niveau de la version 7.0.4+ à la version 7.1.0. Nous vous recommandons de mettre à niveau directement vers la version 7.2+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Versions actuelles	Versions cibles
FXOS 2.9.1 avec Threat Defense 6.7	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec toute version ultérieure de Threat Defense 6.7.x
FXOS 2.8.1 avec Threat Defense 6.6	Une des versions suivantes : → FXOS 2.12 avec Threat Defense 7.2.x → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec toute version ultérieure de Threat Defense 6.6.x
FXOS 2.7.1 avec Threat Defense 6.5	Une des versions suivantes : → FXOS 2.11.1 avec Threat Defense 7.1.x → FXOS 2.10.1 avec Threat Defense 7.0.x → FXOS 2.9.1 avec Threat Defense 6.7.x → FXOS 2.8.1 avec Threat Defense 6.6.x

Chemin de mise à niveau pour Défense contre les menaces sans FXOS

Ce tableau fournit le chemin de mise à niveau pour défense contre les menaces lorsque vous n'avez pas besoin de mettre à niveau le système d'exploitation. Cela comprend Cisco les séries Firepower 1000/2100, la série ASA-5500-X et l'ISA 3000.

Notez que si votre version actuelle défense contre les menaces est publiée après une date postérieure à celle de votre version cible, vous ne pourrez peut-être pas mettre à niveau comme prévu. Dans ces cas, la mise à niveau échoue rapidement et affiche une erreur expliquant qu'il existe des incompatibilités de banque de données entre les deux versions. Les notes de version de votre version actuelle et cible répertorient toutes les restrictions spécifiques.

Tableau 2 : Mises à niveau directes de Défense contre les menaces

Version actuelle	Version cible
7.4	→ Toute version ultérieure à 7.4.x
7.3	Une des versions suivantes : → 7.4.x → Toute version ultérieure à 7.3.x

Version actuelle	Version cible
7.2	Une des versions suivantes : → 7.4.x → 7.3.x → Toute version ultérieure à 7.2.x **Remarque** Le Firepower 1010E, introduit dans la version 7.2.3, n'est pas pris en charge dans la version 7.3. L'assistance revient dans la version 7.4.1.
7.1	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → Toute version ultérieure à 7.1.x
7.0 Dernière prise en charge pour ASA 5508-X et 5516-X.	Une des versions suivantes : → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Toute version ultérieure à 7.0.x **Remarque** En raison d'incompatibilités avec le magasin de données, vous ne pouvez pas mettre à niveau de la version 7.0.4+ à la version 7.1.0. Nous vous recommandons de mettre à niveau directement vers la version 7.2+. **Remarque** Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ne peut pas gérer défense contre les menaces les périphériques exécutant la version 7.1, ou les périphériques classiques exécutant n'importe quelle version. Vous ne pouvez pas mettre à niveau un périphérique géré en nuage de la version 7.0.x vers la version 7.1, à moins de vous désinscrire et de désactiver la gestion en nuage. Nous vous recommandons de mettre à niveau directement vers la dernière version.

Version actuelle	Version cible
6.7	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → Toute version ultérieure à 6.7.x
6.6 Dernière prise en charge pour ASA 5525-X, 5545-X et 5555-X.	Une des versions suivantes : → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Toute version ultérieure à 6.6.x
6.5	Une des versions suivantes : → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Dernière prise en charge pour ASA 5515-X.	Une des versions suivantes : → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Une des versions suivantes : → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Dernière prise en charge pour la série ASA 5506-X.	Une des versions suivantes : → 6.6.x → 6.5 → 6.4 → 6.3

Paquets de mise à niveau pour Défense contre les menaces

Les paquets de mise à niveau sont disponibles sur le Site d'assistance et de téléchargement Cisco : https://www.cisco.com/go/ftd-software.

Vous utilisez le même ensemble de mises à niveau pour tous les modèles d'une famille ou d'une série. Pour trouver le bon modèle, sélectionnez ou recherchez votre modèle sur le Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Notez que les paquets de mise à niveau à sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Tableau 3 : Paquets de mise à niveau logicielle

Plateforme	Paquet de mise à niveau
Série Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Série Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Cisco Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Défense contre les menaces virtuelles	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar
ISA 3000 avec FTD	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar

Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces

Avant d'installer une mise à niveau, le système exécute une vérification de préparation pour s'assurer que la mise à niveau est valide pour le système et pour examiner les autres facteurs qui peuvent empêcher la réussite de la mise à niveau. Si la vérification de préparation échoue, vous devez résoudre les problèmes avant de relancer l'installation. Si la vérification a échoué, vous serez informé de l'échec la prochaine fois que vous tenterez l'installation, et vous aurez la possibilité de forcer l'installation si vous le souhaitez.

Vous pouvez également exécuter manuellement le test de préparation avant de lancer la mise à niveau, comme le décrit cette procédure.

Avant de commencer

Chargez l'ensemble de mises à niveau que vous souhaitez vérifier.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour (Updates).

La section **System Upgrade** (mise à niveau du système) affiche la version du logiciel en cours d'exécution et toute mise à jour que vous avez déjà téléchargée.

Étape 2 Consultez la section **Readiness Check** (vérification de l'état de préparation).

- Si la vérification de mise à niveau n'a pas encore été effectuée, cliquez sur le lien **Run Upgrade Readiness Check** (exécuter la vérification de l'état préparation aux mises à niveau). La progression de la vérification s'affiche dans cette zone. Le processus devrait prendre environ 20 secondes.
- Si la vérification de mise à niveau a déjà été exécutée, cette section indique si la vérification s'est soldée par une réussite ou un échec. En cas d'échec, cliquez sur **See Details** (Consulter les détails) pour consulter plus d'information au sujet de la vérification de l'état de préparation. Après avoir résolu les problèmes, relancez la vérification.

Étape 3 Si la vérification de l'état de préparation conduit à un échec, vous devez résoudre les problèmes avant d'installer la mise à niveau. Les informations détaillées comprennent de l'aide pour résoudre les problèmes signalés. À la suite d'un script d'échec, cliquez sur le lien **Show Recovery Message** (Afficher le message de récupération) pour afficher les informations.

Voici quelques problème courants :

- Incompatibilité de la version de FXOS - Sur les systèmes où vous installez les mises à niveau de FXOS séparément, comme le Firepower 4100/9300, un paquet de mise à niveau peut nécessiter une version minimale de FXOS différente de la version du logiciel défense contre les menaces que vous exécutez actuellement. Dans ce cas, vous devez d'abord mettre à niveau FXOS avant de pouvoir mettre à niveau le logiciel défense contre les menaces .
- Modèle de périphérique non pris en charge : l'ensemble de mise à niveau ne peut pas être installé sur ce périphérique. Vous avez peut-être téléchargé le mauvais paquet, ou l'appareil est un ancien modèle qui n'est tout simplement plus pris en charge par la nouvelle version du logiciel défense contre les menaces . Veuillez vérifier la compatibilité de l'appareil et télécharger un ensemble pris en charge, s'il en existe un.
- Espace disque insuffisant : Si l'espace disponible est insuffisant, essayez de supprimer les fichiers inutiles, comme les sauvegardes du système. Supprimez uniquement les fichiers que vous avez créés.

Mise à niveau Défense contre les menaces

Mise à niveau du système autonome Défense contre les menaces

Utilisez cette procédure pour mettre à niveau un périphérique autonome défense contre les menaces . Si vous devez mettre à jour FXOS, faites-le en premier. Pour mettre à niveau la défense contre les menaces haute disponibilité, voir Mise à de la haute disponibilité Défense contre les menaces, à la page 13.

Mise en garde Le trafic est abandonné pendant la mise à niveau. Même si le système semble inactif ou ne répond pas, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense , à la page 17.

Avant de commencer

Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 2 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Browse** (Parcourir) ou sur ,**Replace File** (Remplacer le fichier) pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Run Upgrade Immediately** (Exécuter la mise à niveau immédiatement) pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 3 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour plus de renseignements, consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 10

Étape 4 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continue** (Continuer) pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 5 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (sommaire du périphérique) affiche la version du logiciel actuellement exécutée.

Étape 6 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.
b) Apportez toutes les modifications de configuration requises après la mise à niveau.
c) Déployez.

Mise à de la haute disponibilité Défense contre les menaces

Utilisez cette procédure pour mettre à niveau des périphériques à haute disponibilité. Mettez-les à niveau un à la fois. Pour minimiser les perturbations, mettez toujours à niveau le serveur de secours. C'est-à-dire que vous mettez à niveau le serveur de secours actuel, changez de rôle, puis mettez à niveau le nouveau serveur de secours. Si vous devez mettre à jour FXOS, faites-le sur les deux châssis avant de mettre à niveau défense contre les menaces sur l'un ou l'autre. Encore une fois, mettez toujours à niveau le serveur de secours.

⚠

Mise en garde N'apportez pas et n'utilisez pas de modifications de configuration sur une unité pendant que l'autre est en cours de mise à niveau, ou vers une paire de versions mixte. Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez pas manuellement pendant la mise à niveau. vous pourriez rendre le système inutilisé et nécessiter une réinitialisation. Vous pouvez annuler manuellement les mises à niveau majeures ou de maintenance en cours ou qui ont échoué, et réessayer les mises à niveau qui ont échoué. Si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Pour en savoir plus sur ces problèmes et d'autres que vous pouvez rencontrer pendant la mise à niveau, consultez Dépannage des mises à niveau de Threat Defense , à la page 17.

Avant de commencer

Terminez la planification de la mise à niveau. Vérifiez que votre déploiement est intègre et communique correctement.

Procédure

Étape 1 Connectez-vous à l'unité en veille.

Étape 2 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le volet des mises à jour (Updates).
Le volet de mise à niveau du système indique la version du logiciel en cours d'exécution et tout paquet de mise à niveau que vous avez déjà téléversé.

Étape 3 Téléverser le paquet de mise à niveau

Vous ne pouvez téléverser qu'un seul paquet. Si vous téléversez un nouveau fichier, il remplace l'ancien fichier. Assurez-vous que le paquet convient à votre version cible et au modèle de périphérique. Cliquez sur **Browse** (Parcourir) ou sur ,**Replace File** (Remplacer le fichier) pour commencer le téléversement.

Une fois le téléversement terminé, le système affiche une boîte de dialogue de confirmation. Avant de cliquer sur **OK**, sélectionnez éventuellement **Run Upgrade Immediately** (Exécuter la mise à niveau immédiatement) pour et choisissez les options de restauration et la mise à niveau maintenant. Si vous effectuez une mise à niveau maintenant, il est particulièrement important d'avoir complété autant que possible la liste de contrôles avant mise à niveau (voir l'étape suivante).

Étape 4 Effectuer les vérifications finales préalables à la mise à niveau, y compris la vérification de l'état de préparation.

Consultez la liste de contrôles avant mise à niveau. Assurez-vous d'avoir effectué toutes les tâches pertinentes, en particulier les vérifications finales. Si vous n'exécutez pas la vérification de la préparation manuellement, elle s'exécute lorsque vous lancez la mise à niveau. Si la vérification échoue, la mise à niveau est annulée. Pour plus de renseignements, consultez Vérification de l'état de préparation aux mises à niveau pour Défense contre les menaces, à la page 10

Étape 5 Cliquez sur **Upgrade Now** (Installer > Mettre à niveau maintenant) pour lancer le processus d'installation de la mise à niveau.

a) Choisissez les options de restauration.

Vous pouvez **Annuler automatiquement en cas d'échec de la mise à niveau et revenir à la version précédente**. Lorsque cette option est activée, le périphérique revient automatiquement à son état d'avant la mise à niveau en cas d'échec de celle-ci qu'elle soit majeure ou de maintenance. Désactivez cette option si vous souhaitez pouvoir annuler ou réessayer manuellement une mise à niveau qui a échoué.

b) Cliquez sur **Continue** (Continuer) pour mettre à niveau et redémarrer le périphérique.

Vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la mise à niveau jusqu'à ce que le périphérique redémarre. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, vous pouvez annuler manuellement ou tenter de nouveau la mise à niveau.

Le trafic est abandonné pendant la mise à niveau. Pour ISA 3000 uniquement, si vous avez configuré le contournement matériel pour une panne de courant, le trafic est abandonné pendant la mise à niveau, mais transmis sans inspection pendant que le périphérique termine son redémarrage après la mise à niveau.

Étape 6 Reconnectez-vous quand vous le pouvez et vérifiez la réussite de la mise à niveau.

La page Device Summary (Résumé du périphérique) affiche la version du logiciel actuellement exécutée et l'état de la haute disponibilité. Ne continuez pas tant que vous n'avez pas vérifié la réussite *et que* la haute disponibilité n'a pas été rétablie. Si la haute disponibilité reste suspendue après une mise à niveau réussie, consultez Dépannage des mises à niveau de Threat Defense , à la page 17.

Étape 7 Mettez à niveau la deuxième unité.

a) Changer de rôle, rendant cet appareil actif : sélectionnez **Device** > **High Availability**(haute disponibilité du périphérique), puis sélectionnez **Switch Mode** (changer de mode) dans le menu déroulant ( ). Attendez que l'état de l'unité passe à actif et confirmez que le trafic circule normalement. Déconnectez-vous.

b) Mise à niveau : répétez les étapes précédentes pour vous connecter au nouveau serveur de secours, téléverser le paquet, mettre à niveau le périphérique, surveiller la progression et vérifier la réussite.

Étape 8 Examiner les rôles des périphériques.

Si vous avez défini des rôles privilégiés pour des périphériques précis, modifiez-les maintenant.

Étape 9 Connectez-vous à l'unité active.

Étape 10 Effectuer les tâches postérieures à la mise à niveau.

a) Mettez à jour les bases de données du système. Si les mises à jour automatiques ne sont pas configurées pour les règles de prévention des intrusions, VDB et GeoDB, mettez-les à jour maintenant.

b) Apportez toutes les modifications de configuration requises après la mise à niveau.

c) Déployez.

Surveilla des mises à niveau de Défense contre les menaces

Lorsque vous lancez la mise à niveau de défense contre les menaces , vous êtes automatiquement déconnecté et dirigé vers une page d'état où vous pouvez surveiller la progression globale de la mise à niveau. La page comprend également une option pour annuler l'installation en cours. Si vous avez désactivé la restauration automatique et que la mise à niveau échoue, la page vous permet d'annuler manuellement ou de tenter de nouveau la mise à niveau.

Vous pouvez également vous connecter en SSH au périphérique et utiliser l'interface de ligne de commande : **show upgrade status**. Ajoutez le mot-clé **continuous** pour afficher les entrées de journal telles qu'elles sont créées et **detail** pour afficher des informations détaillées. Ajoutez les deux mots-clés pour obtenir des informations détaillées en continu.

Une fois la mise à niveau terminée, vous perdez l'accès à la page d'état et à l'interface de ligne de commande lorsque le périphérique redémarre.

ou nouvelle Défense contre les menaces mises à niveau

Utilisez la page d'état de la mise à niveau ou l'interface de ligne de commande pour annuler manuellement les mises à niveau majeures ou de maintenance qui ont échoué ou en cours, et pour réessayer les mises à niveau qui ont échoué :

- Page d'état de mise à niveau : cliquez sur **Cancel Upgrade** (Annuler la mise à niveau) pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez cliquer sur **Cancel Upgrade** (Annuler

la mise à niveau) pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou cliquer sur **Continue** (Continuer) pour réessayer la mise à niveau.

- CLI : Utilisez la commande **upgrade cancel** pour annuler une mise à niveau en cours. Si la mise à niveau échoue, vous pouvez utiliser **upgrade cancel** pour arrêter la tâche et revenir à l'état du périphérique avant la mise à niveau, ou utiliser **upgrade retry** pour réessayer la mise à niveau.

Remarque Par défaut, défense contre les menaces revient automatiquement à son état d'avant la mise à niveau en cas d'échec de cette dernière (« auto-cancel ») (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. Dans un déploiement à haute disponibilité, 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 et la nouvelle tentative ne sont pas prises en charge pour les correctifs. Pour en savoir plus sur la reprise d'une mise à niveau réussie, consultez , à la page 16.

Si une mise à niveau majeure ou de maintenance réussit, mais que le système ne fonctionne pas comme prévu, vous pouvez revenir en arrière. Le rétablissement de défense contre les menaces ramène le logiciel à l'état qu'il avait avant la dernière mise à niveau majeure ou de maintenance; les modifications de configuration ultérieures à la mise à niveau ne sont pas conservées. Le rétablissement après l'application d'un correctif supprime également les correctifs. Notez que vous ne pouvez pas annuler des correctifs ou des correctifs rapides individuels.

La procédure suivante explique comment restaurer à partir de gestionnaire d'appareil. Si vous ne pouvez pas accéder à gestionnaire d'appareil, vous pouvez revenir à la ligne de commande défense contre les menaces dans une session SSH en utilisant la commande **upgrade revert**. Vous pouvez utiliser la commande **show upgrade revert-info** pour voir à quelle version le système retournera.

Avant de commencer

Si l'unité fait partie d'une paire à haute disponibilité, vous devez rétablir les deux unités. Idéalement, lancez la restauration sur les deux unités en même temps afin que la configuration puisse être restaurée sans problème de basculement. Ouvrez des sessions avec les deux unités et vérifiez que le rétablissement est possible sur chacune, puis démarrez les processus. Notez que le trafic sera interrompu pendant la restauration, donc effectuez-la si possible en dehors des heures ouvrables.

Pour les châssis Firepower 4100/9300, les versions principales défense contre les menaces ont une version FXOS associée spécialement qualifiée et recommandée. Cela signifie qu'après avoir rétabli le logiciel défense contre les menaces , vous exécutez peut-être une version non recommandée de FXOS (trop récente). Bien que les nouvelles versions de FXOS soient rétrocompatibles avec les anciennes versions de défense contre les menaces , nous effectuons des tests avancés des combinaisons recommandées. Vous ne pouvez pas passer à une version antérieure de FXOS, donc si vous vous trouvez dans cette situation et que vous souhaitez exécuter une combinaison recommandée, vous devrez recréer l'image du périphérique.

Procédure

Étape 1 Sélectionnez **Device** (périphérique), puis cliquez sur **View Configuration** (afficher la configuration) dans le résumé des mises à jour **(Updates)**.

Étape 2 Dans la section **System Upgrade** (mise à niveau du système), cliquez sur le lien **Revert Upgrade** (annuler la mise à niveau).

Une boîte de dialogue de confirmation s'affiche et affiche la version actuelle et la version à laquelle le système sera restauré. Si aucune version n'est disponible pour la restauration, il n'y a pas de lien **Annuler la mise à niveau**.

Étape 3 Si la version cible vous convient (et qu'une version est disponible), cliquez sur **Revert** (Restaurer).

Après avoir effectué le retour en arrière, vous devez réenregistrer le périphérique auprès du Smart Software Manager.

Dépannage des mises à niveau de Threat Defense

Dépannage général de la mise à niveau

Ces problèmes peuvent se produire lorsque vous mettez à niveau un périphérique, qu'il soit autonome ou au sein d'une paire à haute disponibilité.

Erreurs relatives au paquet de mise à niveau

Pour trouver le bon paquet de mise à niveau, sélectionnez ou recherchez votre modèle sur Site d'assistance et de téléchargement Cisco, puis accédez à la page de téléchargement du logiciel pour la version appropriée. Les paquets de mise à niveau disponibles sont répertoriés avec les paquets d'installation, les correctifs rapides et les autres téléchargements applicables. Les noms des fichiers de paquet de mise à niveau reflètent la plateforme, le type de paquet (mise à niveau, correctif, correctif), la version du logiciel et la version.

Les paquets de mise à niveau à partir de la version 6.2.1+ sont signés et se terminent par .sh.REL.tar. Ne décompressez pas les paquets de mise à niveau signés. Ne renommez pas les paquets de mise à niveau et ne les transférez pas par courriel.

Impossible d'atteindre le périphérique pendant la mise à niveau.

Les périphériques arrêtent de transmettre le trafic pendant la mise à niveau 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 .

Le périphérique semble inactif ou ne répond pas pendant la mise à niveau.

Vous pouvez annuler manuellement les mises à niveau majeures et de maintenance en cours; voir ou nouvelle Défense contre les menaces mises à niveau, à la page 15. Si le périphérique ne répond pas ou si vous ne pouvez pas annuler la mise à niveau, communiquez avec Centre d'assistance technique Cisco (TAC).

Mise en garde Même si le système semble inactif, ne le redémarrez pas ou ne l'éteignez *pas* manuellement pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image.

La mise à niveau a réussi, mais le système ne fonctionne pas comme vous le souhaitez.

Tout d'abord, assurez-vous que les informations en cache sont actualisées. N'actualisez pas simplement la fenêtre du navigateur pour vous reconnecter. Supprimez plutôt tout chemin « supplémentaire » de l'URL et reconnectez-vous à la page d'accueil; par exemple, http://threat-defense.exemple.com/.

Si vous continuez à rencontrer des problèmes et que vous devez revenir à une version majeure ou de maintenance antérieure, vous pourrez peut-être revenir à une version majeure ou de maintenance antérieure; voir , à la page 16. Si vous ne pouvez pas revenir en arrière, vous devez recréer l'image.

Échec de la mise à niveau.

Lorsque vous lancez une mise à niveau majeure ou de maintenance, utilisez la commande **Annuler automatiquement en cas d'échec de la mise à niveau...** Option d'annulation automatique pour choisir ce qui se passe en cas d'échec de la mise à niveau, comme suit :

- Annulation automatique activée (par défaut) : si la mise à niveau échoue, la mise à niveau est annulée et le périphérique revient automatiquement à l'état qu'il avait avant la mise à niveau. Corrigez les problèmes et réessayez.
- Annulation automatique désactivée : si la mise à niveau échoue, le périphérique reste tel qu'il est. Corrigez les problèmes et réessayez immédiatement, ou annulez manuellement la mise à niveau et réessayez ultérieurement.

Pour en savoir plus, consultez ou nouvelle Défense contre les menaces mises à niveau, à la page 15. Si vous ne pouvez pas réessayer ou annuler, ou si les problèmes persistent, communiquez avec Centre d'assistance technique Cisco (TAC).

Dépannage de la mise à niveau haute disponibilité

Ces problèmes sont spécifiques aux mises à niveau à haute disponibilité.

La mise à niveau ne commencera pas sans le déploiement des modifications non validées.

Si vous obtenez un message d'erreur indiquant que vous devez déployer toutes les modifications non validées, même s'il n'y en a pas, connectez-vous à l'unité active (n'oubliez pas que vous devriez mettre à niveau l'unité de secours), créez des modifications mineures et déployez. Ensuite, annulez la modification, redéployez et réessayez la mise à niveau sur le serveur de secours.

Si cela ne fonctionne pas et que les unités exécutent des versions logicielles différentes par rapport aux recommandations, changez de rôle pour rendre l'unité en veille active, puis suspendez la haute disponibilité. Vous pouvez ensuite effectuer le déploiement à partir de l'unité active/suspendue, reprendre la haute disponibilité, puis changer encore les rôles pour mettre l'unité active en veille à nouveau. La mise à niveau devrait alors fonctionner.

Le déploiement à partir de l'unité active échoue pendant la mise à niveau de secours ou provoque une erreur de synchronisation de l'application.

Cela peut se produire si vous déployez à partir de l'unité active tandis que l'unité de secours est en cours de mise à niveau, ce qui n'est pas pris en charge. Procédez à la mise à niveau malgré l'erreur. Après

avoir mis à niveau les deux unités, apportez les modifications de configuration requises et déployez à partir de l'unité active. L'erreur devrait être résolue.

Pour éviter ces problèmes, n'apportez pas et ne déployez pas de modifications de configuration sur une unité pendant que l'autre unité est en cours de mise à niveau, ou vers une paire de versions mixte.

Les modifications de configuration apportées depuis la mise à niveau seront perdues.

Si vous devez absolument apporter et déployer des modifications sur une paire de versions, vous devez apporter les modifications aux deux unités, sinon elles seront perdues après la mise à niveau de l'unité active de bas niveau.

La haute disponibilité est suspendue après la mise à niveau.

Après le redémarrage après la mise à niveau, la haute disponibilité est brièvement suspendue pendant que le système effectue certaines tâches automatisées finales, telles que la mise à jour des bibliothèques et le redémarrage de Snort. Vous êtes susceptible de le remarquer si vous vous connectez à la CLI *très* peu de temps après la mise à niveau. Si la haute disponibilité ne reprend pas d'elle-même après la fin de la mise à niveau et que gestionnaire d'appareil est disponible, faites-le manuellement :

1. Connectez-vous au périphérique actif et au périphérique en veille et consultez les listes des tâches. Attendez que toutes les tâches aient fini de s'exécuter sur les deux périphériques. Si vous remettez la haute disponibilité trop tôt, vous pourriez avoir un problème futur dans lequel le basculement provoque une panne.
2. Sélectionnez **Périphérique** > **Haute disponibilité**, puis **Reprendre** la haute disponibilité dans le menu engrenage ( ).

Le basculement ne se produit pas avec une paire de versions mixtes.

Bien que l'avantage de la haute disponibilité soit que vous puissiez mettre à niveau votre déploiement sans interruption de trafic ni inspection, le basculement est désactivé pendant l'ensemble du processus de mise à niveau. C'est-à-dire que non seulement le basculement est nécessairement désactivé lorsqu'un périphérique est hors ligne (car il n'y a rien vers lequel le basculement est effectué), mais le basculement est également désactivé avec les paires de versions mixtes. C'est le seul moment où les paires de versions mixtes sont autorisées (temporairement) pendant la mise à niveau. Planifiez les mises à niveau pendant les périodes de maintenance, au moment où elles auront le moins d'incidence en cas de problème, et assurez-vous d'avoir suffisamment de temps pour mettre à niveau les deux périphériques dans cette fenêtre.

Échec de la mise à niveau sur un seul périphérique, ou un périphérique a été annulé. La paire utilise maintenant des versions mixtes.

Les paires de versions ne sont pas prises en charge pour les opérations générales. Mettez à niveau le périphérique de version antérieure ou inversez le périphérique de version ultérieure. Pour les correctifs, car la restauration n'est pas prise en charge, si vous ne pouvez pas mettre à niveau le périphérique de version antérieure, vous devez interrompre la haute disponibilité, recréer l'image d'un ou des deux périphériques, puis rétablir la haute disponibilité.

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.