Directives relatives aux mises à niveau logicielles

Pour plus de commodité, ce document duplique les directives relatives aux mises à niveau logicielles critiques et spécifiques aux versions publiées dans les notes de mise à jour Firewall Threat Defense. Pour connaître les directives de mise à niveau de FXOS pour les périphériques Firepower 4100/9300, consultez Directives de mise à niveau pour le châssis Firepower 4100/9300.

Important Vous devez quand même lire les notes de mise à jour, qui peuvent contenir des informations supplémentaires essentielles et spécifiques à la version. Par exemple, les fonctionnalités nouvelles et obsolètes peuvent nécessiter des modifications de configuration avant ou après la mise à niveau, ou même empêcher la mise à niveau. Des problèmes connus (bogues ouverts) peuvent influer sur la mise à niveau.

Version minimale pour la mise à niveau

Version minimale pour la mise à niveau

Vous pouvez effectuer une mise à niveau directement vers Version 7.3, y compris les versions de maintenance, comme suit.

Tableau 1 : Version minimale pour la mise à niveau vers Version 7.3

Plateforme	Version minimale
Firewall Threat Defense	7.0 FXOS 2.13.0.198 est requis pour les périphériques Firepower 4100/9300. Dans la plupart des cas, nous vous recommandons d'utiliser la dernière version de FXOS dans chaque version principale. Pour vous aider à prendre une décision, consultez Notes de mise à jour de Cisco Firepower 4100/9300 FXOS, 2.13.

Version minimale pour les correctifs.

Les correctifs modifient *uniquement* le quatrième chiffre . Vous ne pouvez pas effectuer de mise à niveau directement vers un correctif à partir d'une version majeure ou d'une version de maintenance précédente.

Directives de mise à niveau pour Version 7.3

Ces listes de contrôle fournissent des directives de mise à niveau nouvelles et/ou déjà publiées qui peuvent vous concerner.

Tableau 2 : Directives de mise à niveau pour Firewall Threat Defense avec Firewall Device Manager Version 7.3

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
TOUJOURS VÉRIFIER				
	Version minimale pour la mise à niveau, à la page 1	N'importe lequel	N'importe lequel	N'importe lequel
	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.	N'importe lequel	N'importe lequel	N'importe lequel
	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.	N'importe lequel	N'importe lequel	N'importe lequel
	Directives de mise à niveau pour le châssis Firepower 4100/9300	Firepower 4100/9300	N'importe lequel	N'importe lequel

✓	Directives	Plateformes	Mise à niveau à partir de	Directement vers
DIRECTIVES SUPPLÉMENTAIRES POUR LES DÉPLOIEMENTS SPÉCIFIQUES				
Il n'y a aucune directive de mise à niveau supplémentaire pour le gestionnaire d'appareil spécifique à cette version.				

Mises à niveau qui ne répondent pas

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 pendant la mise à niveau. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image..

Pour les mises à niveau majeures et de maintenance, vous pouvez annuler manuellement les mises à niveau en cours ou ayant échoué, et réessayer les mises à niveau qui ont échoué. Utilisez le panneau de mise à niveau du système ou l'interface de ligne de commande Firewall Threat Defense. Notez que cette fonctionnalité est uniquement prise en charge pour les mises à niveau *à partir de* (et non vers) la version 6.7.0 ou ultérieure.

Remarque Par défaut, Firewall Threat Defense 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 qui a échoué, désactivez l'option d'annulation automatique lorsque vous lancez la mise à niveau. L'annulation automatique n'est pas prise en charge pour les correctifs. 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.

Cette fonctionnalité n'est pas prise en charge pour les correctifs ou pour les mises à niveau à partir de la version 6.6 et des versions antérieures.

Flux de trafic et inspection pour les mises à niveau de Firewall Threat Defense

Mises à niveau logicielles

Le trafic est abandonné pendant la mise à niveau. Dans un déploiement à haute disponibilité, vous pouvez minimiser les perturbations en mettant à niveau les périphériques un à la fois.

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 achève son redémarrage après la mise à niveau.

Restauration logicielle (versions majeures et de maintenance)

Le trafic est abandonné pendant la restauration. Dans le cadre d'un déploiement à haute disponibilité, la restauration est plus efficace lorsque les deux unités sont restaurées simultanément. Le flux de trafic et l'inspection reprennent lorsque la première unité est remise en ligne.

Déploiement des modifications de configuration

Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Il ne redémarre pas pendant d'autres déploiements, sauf si, avant le déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

Flux de trafic et inspection lors du déploiement de configurations

Le redémarrage du processus Snort interrompt brièvement le flux de trafic et l'inspection sur tous les périphériques, y compris ceux qui sont configurés pour la haute disponibilité. Lorsque vous déployez sans redémarrer Snort, les demandes de ressources peuvent entraîner l'abandon d'un petit nombre de paquets sans inspection.

Snort redémarre généralement lors du premier déploiement, immédiatement après la mise à niveau. Il ne redémarre pas pendant d'autres déploiements, sauf si, avant le déploiement, vous modifiez des politiques ou des configurations de périphériques spécifiques.

Temps et espace disque

Délai de mise à niveau

Nous vous recommandons de suivre et d'enregistrer vos propres délais de mise à niveau afin de pouvoir les utiliser comme références futures. Le tableau suivant répertorie certaines éléments qui peuvent influer sur le délai de mise à niveau.

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. Vous risquez de mettre le système dans un état inutilisable et de nécessiter une nouvelle image. Si vous rencontrez des problèmes lors de la désinstallation, y compris une désinstallation échouée ou un appareil ne répondant plus, voir Dépannage des mises à niveau de Threat Defense.

Tableau 3 : Remarques concernant le délai de mise à niveau

Éléments à prendre en compte	Détails
Versions	Le délai de mise à niveau augmente généralement si votre mise à niveau ignore des versions.

Éléments à prendre en compte	Détails
Modèles	Le délai de mise à niveau augmente généralement avec les modèles inférieurs.
Appliances virtuelles	Le délai de mise à niveau dans les déploiements virtuels dépend fortement du matériel.
Haute disponibilité	Dans une configuration à haute disponibilité, les périphériques sont mis à niveau un par un afin de préserver la continuité des opérations, chaque périphérique fonctionnant en mode maintenance pendant sa mise à niveau. Par conséquent, la mise à niveau d'une paire de périphériques prend plus de temps que la mise à niveau d'un périphérique autonome.
Configurations	Le délai de mise à niveau peut augmenter en fonction de la complexité de vos configurations et de l'incidence de la mise à niveau. Par exemple, si vous utilisez de nombreuses règles de contrôle d'accès et que la mise à niveau doit apporter des modifications générales à la façon dont ces règles sont stockées, la mise à niveau peut prendre plus de temps.
Composants	Vous pourriez avoir besoin de plus de temps pour effectuer des mises à niveau de systèmes d'exploitation ou d'hébergement virtuel, des transferts de paquets de mise à niveau, des vérifications de l'état de préparation, des mises à jour de la VDB et des règles de prévention des intrusions (SRU/LSP), du déploiement de la configuration et d'autres tâches connexes.

Espace disque à mettre à niveau

Pour mettre à niveau, le paquet de mise à niveau doit se trouver sur le périphérique. Les vérifications de l'état de préparation doivent indiquer si vous disposez d'un espace disque suffisant pour effectuer la mise à niveau. Sans suffisamment d'espace disque libre, la mise à niveau échoue. Pour vérifier l'espace disque, utilisez la commande **show disk** de l'interface de ligne de commande.

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.