Mise à niveau de FMCv et migration de VMware ESXi 7.0 vers ESXi 8.0 : Approche par étapes et meilleures pratiques

Table des matières

Problème

Un administrateur exécutant Firewall Management Center virtual (FMCv) version 7.3.1 sur VMware ESXi 7.0 prévoit de mettre à niveau FMC vers une version prise en charge plus élevée et de migrer ensuite la machine virtuelle FMCv vers un nouveau cluster VMware ESXi 8.0. Ces préoccupations ont été soulevées au cours de cet effort de planification :

- S'il est sûr de mettre à niveau FMCv de 7.3.1 vers 7.4.2 d'abord, puis de migrer la VM vers le cluster ESXi 8.0, avant d'effectuer d'autres mises à niveau.
- Si des problèmes ou des contraintes de compatibilité sont connus lors de la migration d'un FMCv exécutant la version 7.3.1 ou 7.4.2 vers un environnement VMware ESXi 8.0.
- Si VMware vMotion peut être utilisé pour effectuer une migration transparente, sur le même IP, de la machine virtuelle FMCv vers le nouveau cluster sans créer de nouvelle instance de VM.
- Indique si les snapshots VMware peuvent être utilisés comme mécanisme de sauvegarde et de restauration en cas d'échec de la mise à niveau ou de la migration.
- Quelle est la version FMC la plus élevée prise en charge pour l'environnement de périphériques gérés existant, qui inclut les périphériques Firewall Threat Defense (FTD) allant de la version 7.2.8 à la version 7.4.2 ?
- Comment éviter les conflits d'adresses IP lors du passage à la nouvelle instance FMCv sur le nouveau cluster tout en conservant la même adresse IP de gestion et le même nom d'hôte.
- Quel est l'ordre d'exécution correct pour un plan de mise à niveau et de migration par étapes qui minimise les risques et les temps d'arrêt ?

Environnement

- Produit : FMCv
- Version actuelle du logiciel FMC : 7.3.1
- Plate-forme hyperviseur actuelle : VMware ESXi 7.0
- Plate-forme hyperviseur cible : VMware ESXi 8.0.3 (nouveau cluster)
- Type de déploiement FMC : Autonome (ne fait pas partie d'une paire haute disponibilité)
- Périphériques gérés : Plusieurs périphériques FTD allant de la version 7.2.8 à la version 7.4.2

Résolution

L'approche recommandée pour cet environnement est un plan de mise à niveau et de migration par étapes. Ce plan sépare la mise à niveau du logiciel FMC, la migration de la plate-forme d'hyperviseur et toute mise à niveau ultérieure de la version FMC en événements de maintenance distincts. Cette approche réduit les risques à chaque phase et fournit des points de restauration clairs. L'utilisation de VMware vMotion, de snapshots, du clonage ou de la migration directe au niveau de la VM n'est pas explicitement la méthode prise en charge pour migrer FMCv entre les clusters ou les versions.

Important : Les snapshots, vMotion et le clonage VMware ne sont pas pris en charge pour la migration FMCv

Avant de passer à l'une des phases de ce plan, il est essentiel de comprendre les contraintes suivantes concernant les méthodes de migration natives VMware :

- Les snapshots VMware ne sont pas une méthode de sauvegarde, de restauration ou de restauration prise en charge pour les mises à niveau ou les migrations FMCv. La restauration d'un FMCv vers un snapshot VMware peut entraîner une corruption de la base de données, des incohérences entre les versions et les mises à jour de contenu, ou un état système non pris en charge.
- VMware vMotion, le clonage et la migration directe des machines virtuelles entre les clusters

ne sont pas la méthode prise en charge pour migrer FMCv vers une nouvelle plate-forme d'hyperviseur. Ces méthodes contournent les mécanismes internes d'intégrité des données du FMC.

- La seule méthode prise en charge pour la migration de FMCv vers un nouveau cluster ou hôte est le workflow de sauvegarde et de restauration natif FMC, combiné au déploiement d'une nouvelle instance FMCv sur la plate-forme cible.

Si la validation échoue après le basculement, la stratégie de restauration correcte consiste à mettre hors tension la nouvelle instance FMCv et à remettre en service le FMCv d'origine. Ne comptez pas sur les restaurations de snapshots à cette fin.

Phase 1 : Vérification de la compatibilité avant la mise à niveau

Avant de lancer une mise à niveau logicielle FMC, vérifiez les versions logicielles exactes de tous les périphériques FTD gérés dans l'environnement.

- FMC 7.4.2 prend en charge la gestion des périphériques FTD exécutant la version 7.0 et les versions ultérieures.
- FMC 7.6.6 prend en charge la gestion des périphériques FTD exécutant les versions 7.1 et ultérieures.
- Si un périphérique FTD dans l'environnement exécute une version < 7.0, ce périphérique doit être mis à niveau vers au moins la version 7.0 tant que le FMC reste sur la version 7.3.1, avant que le FMC lui-même ne soit mis à niveau.
- Pour l'environnement documenté (plage FTD : 7.2.8 à 7.4.2), tous les périphériques gérés sont dans la plage de compatibilité pour FMC 7.4.2 et FMC 7.6.6. Aucune mise à niveau préalable FTD n’est requise dans ce cas.

Confirmez également ces informations avant de continuer :

- Le FMC est autonome et ne fait pas partie d'une paire haute disponibilité (HA).
- La version exacte de VMware ESXi 8.0 repose sur le nouveau cluster (confirmé comme ESXi 8.0.3 dans cet environnement).
- Le profil de ressources FMCv (vCPU, mémoire, disque) répond aux exigences de la version FMC cible. Les spécifications actuelles de 4 processeurs virtuels, 32 Go de RAM et 250 Go de disque doivent être revues par rapport aux directives de déploiement actuelles, en

particulier avant la mise à niveau vers FMC 7.6.6.

- Indique si l'adresse IP et le nom d'hôte de gestion FMC restent identiques après la migration (fortement recommandé pour éviter d'exiger des mises à jour d'adresse de gestionnaire sur tous les périphériques FTD gérés).

Phase 2 : Mise à niveau de FMCv existant de 7.3.1 vers 7.4.2 sur le cluster ESXi 7.0 actuel

Cette phase permet de mettre à niveau le logiciel FMCv vers la version 7.4.2 tout en conservant l'infrastructure ESXi 7.0 existante. FMCv 7.4.2 ajoute la prise en charge explicite de VMware ESXi 8.0, qui est requise avant la migration de la plate-forme au cours de la Phase 3.

Étape 1: Vérifiez qu'aucun déploiement de stratégie en attente, aucune tâche de sauvegarde active ou aucune tâche en arrière-plan n'est en cours d'exécution sur le FMC avant de commencer la mise à niveau.

Étape 2: Effectuez une sauvegarde FMC native complète à l'aide de l'utilitaire de sauvegarde FMC intégré. Stockez la sauvegarde dans un emplacement distant sécurisé en dehors de la machine virtuelle FMCv. Vérifiez que la sauvegarde s'est terminée correctement avant de continuer.

Étape 3: Effectuez toutes les vérifications du niveau de préparation à la mise à niveau comme indiqué dans le guide de planification de la mise à niveau FMC 7.4. Résolvez les problèmes signalés avant de lancer la mise à niveau.

Étape 4: Mettez à niveau le FMCv existant de la version 7.3.1 vers la version 7.4.2. Ceci utilise le chemin de transition de mise à niveau pris en charge : 7,3 → 7,4.

Étape 5: Une fois la mise à niveau terminée, effectuez la validation post-mise à niveau :

- Vérifiez que tous les périphériques FTD gérés sont reconnectés au FMC.
- Vérifiez que l'ingestion d'événements est active et que des événements apparaissent dans le FMC.
- Vérifiez que l'état de la licence est correct.
- Exécutez un déploiement de stratégie de test sur un périphérique géré et vérifiez qu'il a réussi.

Ne passez pas à la Phase 3 tant que toutes les étapes de validation post-mise à niveau n’ont pas réussi sur le FMCv 7.4.2 mis à niveau.

Phase 3 : Migration de FMCv vers le cluster VMware ESXi 8.0.3 à l'aide de la sauvegarde et de la restauration natives

Cette phase migre le FMCv du cluster ESXi 7.0 existant vers le nouveau cluster ESXi 8.0.3. Pour ce faire, une nouvelle instance FMCv est déployée sur le cluster cible et une sauvegarde FMC native est restaurée. Les mêmes adresse IP et nom d'hôte de gestion sont conservés pour éviter d'avoir à modifier l'adresse du gestionnaire sur tous les périphériques FTD gérés.

Étape 1: Une fois que la stabilité du FMCv est confirmée sur la version 7.4.2, générez une nouvelle sauvegarde native du FMC. Stockez-le dans un emplacement distant sécurisé. Vérifiez que la sauvegarde est terminée et valide avant de continuer.

Étape 2: Déployez une nouvelle instance FMCv sur le cluster ESXi 8.0.3. La version du logiciel et la build de cette nouvelle instance doivent correspondre exactement à la version du FMCv (y compris les correctifs et les correctifs) à partir de laquelle la sauvegarde a été effectuée (FMCv 7.4.2). Assurez-vous que la nouvelle instance est configurée avec des ressources équivalentes ou supérieures (vCPU, mémoire, disque) et que la configuration réseau est préparée mais que l'adresse IP de gestion de production n'est pas encore attribuée à la nouvelle instance à ce stade.

Étape 3: Restaurez la sauvegarde FMC native sur la nouvelle instance FMCv sur ESXi 8.0.3.

Étape 4: Avant de mettre le nouveau FMCv en ligne avec l'adresse IP et le nom d'hôte de gestion de la production, mettez entièrement hors tension ou déconnectez le FMCv d'origine du réseau. Il s'agit d'une étape obligatoire pour éviter une condition IP dupliquée et pour éviter que deux instances FMC tentent de communiquer simultanément avec les mêmes périphériques FTD gérés.

Pendant la période où le FMCv d'origine est mis hors tension et avant que le nouveau FMCv ne soit en ligne, ce comportement est attendu pour les périphériques FTD gérés :

- Transfert du trafic : Les périphériques FTD exploitent les plans de données indépendamment du FMC et continuent à transférer le trafic de manière transparente et à appliquer la dernière stratégie de contrôle d'accès déployée avec succès, à l'exception des cas mentionnés ici.

- Changements de gestion et de visibilité : Les déploiements de politiques, les ajustements de configuration, les alertes d'intégrité FMC et la visibilité de la gestion des périphériques sont totalement indisponibles.

- Mise en mémoire tampon des événements et perte potentielle : La visibilité des événements en temps réel au niveau du FMC est suspendue. Alors que le FTD tente de consigner localement les événements de sécurité et de connexion dans ses fichiers unifiés temporaires, ces fichiers ont des limites de stockage strictes et fonctionnent sur une base d'écrasement circulaire. Les journaux de connexion volumineux peuvent être écrasés ou perdus au cours d'une fenêtre de migration étendue. Les événements qui restent dans la mémoire tampon locale sont diffusés au nouveau FMC une fois qu'il est en ligne.

- Règles de programme malveillant (AMP) : Les demandes de recherche en temps réel sur le cloud pour les fichiers non mis en cache sont temporairement indisponibles, car le FMC transmet ces requêtes de réputation au cloud AMP. Le FTD continue d'appliquer des règles de blocage ou d'autorisation uniquement pour les fichiers déjà stockés dans son cache local de disposition à l'installation. Les fichiers non mis en cache contournent l'analyse du cloud et utilisent les paramètres de sécurité intégrée de votre stratégie (généralement, l'ouverture échoue pour empêcher l'interruption du trafic). Les envois en sandboxing vers Threat Grid et les alertes rétrospectives sont suspendues jusqu'à ce que le nouveau FMC soit opérationnel.

- Règles basées sur l'identité : Les utilisateurs déjà connectés et mappés à une adresse IP ne subissent aucune interruption, car le FTD conserve les mappages actifs dans sa mémoire locale. Cependant, comme le FMC agit comme courtier pour les sources d'identité (par exemple, Cisco ISE ou les agents Active Directory), les nouvelles connexions d'utilisateur ou les modifications d'IP au cours de cette fenêtre ne peuvent pas être apprises par le FTD. Ces sessions inconnues reviennent aux règles par défaut ou aux règles d'invité de votre stratégie.

- Filtrage des URL : Les recherches en ligne de sites Web totalement inconnus sont temporairement indisponibles, car le FMC proxie les requêtes d'URL inconnues vers le cloud Cisco Talos. Le FTD continue de filtrer et d'appliquer entièrement la stratégie uniquement pour les sites Web déjà trouvés dans son jeu de données local poussé ou son cache de mémoire locale active. Le trafic Web atteignant une URL inconnue non mise en cache contourne la classification du cloud et correspond aux paramètres de secours de votre stratégie pour le trafic non classé (généralement autorisé). Les mises à jour du package de base de données URL sont suspendues jusqu'à ce que le nouveau FMC soit en ligne.

Étape 5: Attribuez l'adresse IP et le nom d'hôte de gestion de la production au FMCv restauré sur ESXi 8.0.3 et mettez-le en ligne. Comme la même adresse IP et le même nom d'hôte sont utilisés, les périphériques FTD gérés peuvent se reconnecter automatiquement au FMC sans nécessiter de modification de l'adresse du gestionnaire sur les périphériques FTD individuels.

Étape 6: Effectuer une validation post-migration :

- Vérifiez que tous les périphériques FTD gérés se sont reconnectés à la nouvelle instance FMCv.
- Vérifiez l'état des licences et assurez-vous que toutes les licences sont correctement appliquées.
- Vérifiez que le flux d'événements et les intégrations externes fonctionnent correctement.
- Exécutez un déploiement de stratégies contrôlées sur un périphérique géré et vérifiez qu'il a réussi.

Si la validation échoue à un moment quelconque au cours de cette phase, mettez hors tension la nouvelle instance FMCv, restaurez le FMCv d'origine sur ESXi 7.0 en service et effectuez un dépannage avant de tenter à nouveau la migration. N'utilisez pas une restauration de snapshot VMware comme mécanisme de restauration.

Phase 4 : Mise à niveau de FMCv de 7.4.2 vers 7.6.6 (après confirmation de la stabilité de la migration)

Une fois la migration FMCv vers ESXi 8.0.3 entièrement validée et confirmée comme stable, une mise à niveau supplémentaire vers FMC 7.6.6 peut être envisagée. Il est fortement recommandé de ne pas combiner la migration de la plate-forme d'hyperviseur (Phase 3) et cette mise à niveau de version FMC supplémentaire en un seul événement de maintenance. L'exécution de la migration fournit d'abord un point de contrôle propre et à faible risque avant de poursuivre.

Avant de lancer la mise à niveau vers la version 7.6.6, vérifiez les conditions suivantes :

- Chaque périphérique FTD géré dans l'environnement exécute la version 7.1 ou ultérieure. FMC 7.6.6 ne prend pas en charge la gestion des périphériques FTD < version 7.1. Dans l'environnement documenté (plage FTD : 7.2.8 à 7.4.2), tous les dispositifs répondent à cette exigence.
- Le profil de ressources FMCv (4 processeurs virtuels, 32 Go de RAM, 250 Go de disque) a été validé par rapport aux directives de déploiement FMC 7.6.6 pour le nombre total de périphériques gérés et les exigences de rétention des événements dans cet environnement.
- Le chemin de transition de mise à niveau pris en charge est confirmé : 7,4 → 7,6.
- Le FMC est confirmé comme autonome (ne fait pas partie d'une paire haute disponibilité).

Étape 1: Créez et vérifiez une nouvelle sauvegarde FMC native à partir de l'instance FMCv 7.4.2

stable sur ESXi 8.0.3. Stockez-la dans un emplacement distant sécurisé.

Étape 2: Mettez à niveau FMCv de la version 7.4.2 vers la version 7.6.6.

Étape 3: Effectuer la validation finale après la mise à niveau :

- Vérifiez que tous les périphériques FTD gérés sont reconnectés au FMC.
- Vérifiez que la gestion et la réception des événements fonctionnent correctement.
- Confirmez que l'état des licences est correct.
- Exécutez un déploiement de stratégie contrôlée pour confirmer que l'application de la stratégie a réussi.

Résumé du chemin de mise à niveau et de la séquence de transition

Le tableau ci-dessous récapitule le plan intermédiaire complet, les transitions de mise à niveau prises en charge et l'action clé à chaque phase :

Phase	Action	Version FMC	Hyperviseur	Transition prise en charge
Phase 1	Vérification de la compatibilité avant la mise à niveau ; Confirmer les versions FTD, l'état HA FMC et le profil de ressources	7.3.1 (actuel)	ESXi 7.0	S/O — préparation seulement
Phase 2	Mettre à niveau le logiciel FMCv ; effectuer une sauvegarde native ; valider le déploiement des périphériques gérés et des politiques	7.3.1 → 7.4.2	ESXi 7.0	7,3 → 7,4 (pris en charge)
Phase 3	Déployer le nouveau FMCv sur ESXi 8.0.3 ; restaurer la sauvegarde native ; basculer en utilisant la même adresse	7.4.2 (pas de modification de version)	ESXi 7.0 → ESXi 8.0.3	Sauvegarde/restauration native — méthode prise en charge

	IP/nom d'hôte ; valider			
Phase 4	Une fois la migration stable : mettre à niveau FMCv ; valider la connectivité, la licence, les événements et la stratégie des périphériques	7.4.2 → 7.6.6	ESXi 8.0.3	7,4 → 7,6 (pris en charge)

Considérations clés

- Conformité du chemin de mise à niveau : La séquence de mise à niveau complète (7.3.1 → 7.4.2 → 7.6.6) utilise les chemins de transition de mise à niveau FMC pris en charge (7.3 → 7.4 et 7.4 → 7.6). Il n'est pas recommandé d'ignorer les versions intermédiaires ou de combiner des phases en un seul événement.
- Compatibilité FMC-FTD : FMC 7.6.6 maintient une compatibilité de gestion complète avec les périphériques FTD exécutant les versions 7.2.8 à 7.4.2. FMC 7.6 exige que tous les périphériques FTD gérés soient à la version 7.1 ou ultérieure.
- Mêmes adresses IP de basculement : Le FMCv d'origine doit être entièrement mis hors tension ou déconnecté du réseau avant que le FMCv de remplacement ne soit mis en ligne avec l'adresse IP de gestion de la production. Cela évite une condition de doublon d'IP et évite que deux centres de gestion tentent simultanément de communiquer avec les mêmes périphériques FTD. Lorsque le FMCv restauré revient avec la même adresse IP et le même nom d'hôte, les périphériques FTD gérés peuvent se reconnecter sans nécessiter de modification de l'adresse du gestionnaire.
- Validation des ressources avant 7.6.6 : Le profil de ressources FMCv (4 processeurs virtuels, 32 Go de RAM, 250 Go de disque) doit être comparé aux directives de déploiement actuelles avant la mise à niveau vers FMC 7.6.6, en tenant compte du nombre total de périphériques gérés et des exigences de rétention des événements pour l'environnement.
- Vérification de la sauvegarde native : À chaque phase où une sauvegarde FMC native est effectuée, la sauvegarde doit être vérifiée comme étant complète et valide avant de continuer. Les sauvegardes doivent être stockées dans un emplacement distant sécurisé en dehors de la machine virtuelle FMCv.
- Ne pas combiner migration et mise à niveau : La migration de la plate-forme (Phase 3) et la mise à niveau de la version FMC suivante vers la version 7.6.6 (Phase 4) doivent être effectuées comme des événements de maintenance distincts. Cela garantit l'existence d'un point de contrôle propre sur FMCv 7.4.2 sur ESXi 8.0.3 avant toute modification ultérieure.

Motif

Il ne s'agit pas d'un problème de dépannage résultant d'un défaut logiciel ou d'une mauvaise configuration. La cause sous-jacente nécessitant ces conseils est une combinaison d'exigences de compatibilité de version et de contraintes de migration de plate-forme spécifiques à Cisco FMCv sur VMware :

- Compatibilité de la version FMC avec FTD 7.4.2 : La présence d'un périphérique FTD géré exécutant la version 7.4.2 dans l'environnement nécessite la mise à niveau du FMC vers une version minimale de 7.4.2, car les versions FMC antérieures ne peuvent pas gérer les périphériques FTD à une version supérieure au FMC lui-même.
- Prise en charge de FMCv pour VMware ESXi 8.0 : FMCv 7.3.1 ne prend pas en charge VMware ESXi 8.0 en tant que plate-forme d'hyperviseur. Le FMCv doit être mis à niveau vers la version 7.4.2 (ou ultérieure) avant de pouvoir être déployé ou utilisé sur ESXi 8.0.x. Tenter de migrer la machine virtuelle FMCv 7.3.1 directement vers ESXi 8.0 sans mettre à niveau le logiciel FMC présente un risque de compatibilité.
- Méthodes de migration de VM non prises en charge : VMware vMotion, les snapshots, le clonage et la migration directe de VM ne sont pas des méthodes prises en charge pour migrer FMCv entre des clusters ou des versions d'hyperviseur. Ces méthodes peuvent entraîner une corruption de la base de données, des différences de version ou un état système non pris en charge. Le seul chemin de migration pris en charge est le workflow de sauvegarde et de restauration natif FMC combiné à un nouveau déploiement FMCv sur la plate-forme cible.

Autres informations utiles

- Guide de mise à niveau de Cisco Secure Firewall Management Center, version 7.4 — Planification de la mise à niveau et chemins pris en charge
- Guide de mise à niveau de Cisco Secure Firewall Management Center, version 7.6 — Planification de la mise à niveau et chemins pris en charge
- Guide de compatibilité de Cisco Secure Firewall Management Center (matrice de compatibilité FMC et FTD)
- Cisco Secure Firewall Management Center Nouvelles fonctionnalités par version — Version 7.4.2
- Guide de mise à niveau de Cisco Firepower Management Center - Planification de la mise à

niveau

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.