Planifier les étapes de la procédure de mise à niveau de haute disponibilité FTD et l'impact opérationnel

Table des matières

Problème

Un administrateur de pare-feu doit comprendre la procédure de mise à niveau recommandée pour les périphériques Firewall Threat Defense (FTD) configurés dans une paire haute disponibilité (HA) et gérés par Cisco Firewall Management Center (FMC). Les questions spécifiques incluent le processus recommandé pour les mises à niveau logicielles sur ces unités, si les mises à niveau peuvent être effectuées à la volée sans temps d'arrêt, et quel impact prévoir pendant le processus de mise à niveau.

Environnement

- FTD exécutant la version 7.4. D'autres versions logicielles peuvent également être affectées.
- FTD configuré en mode paire haute disponibilité (HA).
- FMC 7.4 gestion de la haute disponibilité de la FTD. D'autres versions logicielles peuvent également être affectées.

Résolution

La procédure de mise à niveau pour FTD dans la configuration haute disponibilité utilise une séquence spécifique pour minimiser les temps d'arrêt et maintenir l'intégrité du système.

Commande de mise à niveau recommandée

Étape 1. Mise à niveau du FMC en premier

Les conseils de Cisco exigent que le FMC exécute la même version ou une version plus récente que les périphériques qu'il gère. Vous ne pouvez pas mettre à niveau un périphérique FTD passé le FMC vers une version majeure ou une version de maintenance plus récente.

Étape 2. Mise à niveau de la paire FTD HA à partir de FMC

Lors de la mise à niveau d'une paire FTD HA gérée par FMC, le FMC met à niveau un homologue à la fois (en veille d'abord, puis actif) et un basculement se produit dans le cadre du processus.

Attentes en matière de temps d'arrêt et de trafic

- Vous devez planifier une fenêtre de maintenance. Cisco note que les mises à niveau peuvent inclure des interruptions du flux et de l'inspection du trafic, et que les périphériques peuvent arrêter de transmettre le trafic pendant la mise à niveau ou en cas d'échec de la mise à niveau.
- Avec une paire haute disponibilité, l'objectif est de minimiser l'impact, mais vous devez vous attendre à au moins un événement de basculement et à une brève interruption possible (par exemple, la contiguïté de routage ou la renégociation VPN en fonction de votre environnement).
- Éviter les modifications de stratégie et de configuration pendant la mise à niveau (aucun déploiement ni aucune modification jusqu'à ce que les deux membres HA soient entièrement mis à niveau et stables).

Vérifications d'intégrité avant mise à niveau pour FTD HA

Avant de commencer la mise à niveau, vérifiez que FTD HA est stable et que les deux unités sont d'accord sur les états Actif et Prêt en veille :

<#root>

```
device#

show failover state


               State          Last Failure Reason      Date/Time
This host  -   Primary

Active

None
Other host -   Secondary

Standby Ready

  Comm Failure             16:10:34 UTC Apr 13 2026

====Configuration State===
        Sync Skipped
====Communication State===
        Mac set
```

Motif

Il s'agit d'une demande procédurale concernant les meilleures pratiques de mise à niveau des systèmes FMC et FTD en configuration HA. Cette question répond au besoin de comprendre le séquençage des mises à niveau, les attentes en matière d'indisponibilité et les stratégies d'atténuation des impacts pour les infrastructures critiques de pare-feu.

Autres informations utiles

- Planification de la mise à niveau de Secure Firewall Management Center
- Mise à niveau FTD HA gérée par FMC

- Guide de compatibilité de Management Center
- Guide de compatibilité de la défense
- 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.