

Begrijp de stappen en impact van de FTD High Availability Upgrade Procedure

Inhoud

uitgeven

Een firewallbeheerder moet de aanbevolen upgradeprocedure begrijpen voor Firewall Threat Defense (FTD)-apparaten die zijn geconfigureerd in een High Availability (HA)-paar en worden beheerd door Cisco Firewall Management Center (FMC). De specifieke vragen omvatten wat het aanbevolen proces is voor software-upgrades op deze eenheden, of de upgrades "on the fly" kunnen worden uitgevoerd zonder downtime en welke impact te verwachten tijdens het upgradeproces.

milieu

- FTD met versie 7.4. Ook andere softwareversies kunnen worden beïnvloed.
- FTD is geconfigureerd in de paarmodus voor hoge beschikbaarheid (HA).
- VCC 7.4 Beheer van het FTD HA. Ook andere softwareversies kunnen worden beïnvloed.

resolutie

De upgradeprocedure voor FTD in HA-configuratie maakt gebruik van een specifieke volgorde om de downtime te minimaliseren en de systeemintegriteit te behouden.

Aanbevolen upgradevolgorde

Stap 1. Upgrade eerst de FMC

Cisco-richtlijnen vereisen dat de FMC dezelfde of nieuwere versie moet uitvoeren dan de apparaten die het beheert. U kunt een FTD-apparaat niet upgraden voorbij de FMC naar een nieuwere onderhouds- of hoofdversie.

Stap 2. Upgrade het FTD HA-paar van FMC

Bij het upgraden van een FTD HA-paar dat door FMC wordt beheerd, upgrades de FMC één peer per keer (eerst stand-by, dan actief) en een failover vindt plaats als onderdeel van het proces.

Verwachtingen inzake downtime en verkeerseffecten

- U moet een onderhoudsvenster plannen. Cisco merkt op dat upgrades kunnen bestaan uit onderbrekingen van de verkeersstroom en inspectie, en apparaten kunnen stoppen met het doorgeven van verkeer tijdens de upgrade of als een upgrade mislukt.
- Met een HA-paar is het doel om de impact te minimaliseren, maar u moet ten minste één failover-gebeurtenis en mogelijke korte onderbreking verwachten (bijvoorbeeld routing naast of VPN-heronderhandeling afhankelijk van uw omgeving).
- Vermijd wijzigingen in beleid en configuratie tijdens de upgrade (geen implementaties of wijzigingen totdat beide HA-leden volledig zijn geüpgraded en stabiel zijn).

Gezondheidscontroles vóór de upgrade voor FTD HA

Voordat u de upgrade start, moet u bevestigen dat FTD HA stabiel is en dat beide eenheden het eens zijn over de status Actief en Standby Ready:

```
<#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
```

Oorzaak

Dit is een procedureel onderzoek naar beste praktijken voor het upgraden van FMC- en FTD-systemen in HA-configuratie. De vraag richt zich op de noodzaak om de juiste upgradesequencing, downtime verwachtingen en impact mitigatie strategieën voor kritieke firewall infrastructuur te begrijpen.

Verwante inhoud

- [Upgradeplanning voor Secure Firewall Management Center](#)
- [Upgrade FTD HA beheerd door FMC](#)
- [Management Center-compatibiliteitshandleiding](#)
- [Compatibiliteitshandleiding voor bedreigingsbeveiliging](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.