# Schritte und Auswirkungen des Hochverfügbarkeits-Upgrade-Verfahrens für FTD verstehen

## Inhalt

## Problem

Ein Firewall-Administrator muss mit dem empfohlenen Upgrade-Verfahren für FTD-Geräte (Firewall Threat Defense) vertraut sein, die in einem HA-Paar konfiguriert und vom Cisco Firewall Management Center (FMC) verwaltet werden. Zu den spezifischen Fragen gehören der empfohlene Prozess für Software-Upgrades auf diesen Geräten, die Möglichkeit, Upgrades ohne Ausfallzeiten ohne Betriebsunterbrechung durchzuführen, und die möglichen Auswirkungen während des Upgrade-Prozesses.

## Umwelt

- FTD mit Version 7.4. Andere Softwareversionen können ebenfalls betroffen sein.
- FTD im Paarmodus für hohe Verfügbarkeit (HA) konfiguriert.
- FMC 7.4 verwaltet die FTD HA. Auch andere Softwareversionen können betroffen sein.

## Auflösung

Das Upgrade-Verfahren für FTD in HA-Konfiguration verwendet eine bestimmte Sequenz, um Ausfallzeiten zu minimieren und die Systemintegrität aufrechtzuerhalten.

### Empfohlene Upgrade-Bestellung

Schritt 1: Upgrade des FMC zuerst

Für die Beratung durch Cisco ist es erforderlich, dass das FMC dieselbe oder eine neuere Version als die verwalteten Geräte ausführt. Sie können ein FTD-Gerät nicht über das FMC hinaus auf eine neuere Wartungs- oder Hauptversion aktualisieren.

Schritt 2: FTD HA-Paar von FMC aktualisieren

Beim Upgrade eines von FMC verwalteten FTD HA-Paares führt das FMC ein Upgrade von einem Peer nach dem anderen durch (zunächst Standby, dann Aktiv), und es tritt im Rahmen des Prozesses ein Failover auf.

## Erwartungen an Ausfallzeiten und Auswirkungen auf den Datenverkehr

- Sie müssen ein Wartungsfenster planen. Cisco stellt fest, dass Upgrades Unterbrechungen des Datenverkehrsflusses und der Überprüfung umfassen können und dass Geräte den Datenverkehr während des Upgrades oder bei einem Upgrade-Fehler nicht mehr weiterleiten können.
- Bei einem HA-Paar besteht das Ziel darin, die Auswirkungen zu minimieren. Sie müssen jedoch mit mindestens einem Failover-Ereignis und einer möglichen kurzen Unterbrechung rechnen (z. B. Routing-Adjacency oder VPN-Neuverhandlung je nach Ihrer Umgebung).
- Vermeiden Sie während des Upgrades Änderungen an Richtlinien und Konfigurationen (keine Bereitstellungen oder Änderungen, bis beide HA-Mitglieder vollständig aktualisiert und stabil sind).

## Health Checks vor dem Upgrade auf FTD HA

Stellen Sie vor dem Upgrade sicher, dass die FTD-HA stabil ist, und stimmen Sie beide Einheiten auf den Status "Aktiv" und "Standby Ready" zu:

<#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
```

# Ursache

Hierbei handelt es sich um eine Verfahrensanfrage bezüglich Best Practices für das Upgrade von FMC- und FTD-Systemen in HA-Konfiguration. In dieser Frage geht es um die Notwendigkeit, die richtige Reihenfolge der Upgrades, die erwarteten Ausfallzeiten und Strategien zur Risikominimierung für kritische Firewall-Infrastrukturen zu kennen.

# Verwandte Inhalte

- Upgrade-Planung für Secure Firewall Management Center
- FTD HA-Upgrade von FMC verwaltet
- Management Center-Kompatibilitätsleitfaden
- Threat Defence-Kompatibilitätsleitfaden
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.