Comprendere i passaggi e l'impatto della procedura di aggiornamento ad alta disponibilità FTD

Sommario

Problema

Un amministratore del firewall deve conoscere la procedura di aggiornamento consigliata per i dispositivi Firewall Threat Defense (FTD) configurati in una coppia ad alta disponibilità (HA) e gestiti da Cisco Firewall Management Center (FMC). Le domande specifiche includono il processo consigliato per gli aggiornamenti software su queste unità, se gli aggiornamenti possono essere eseguiti "immediatamente" senza tempi di inattività e quale impatto ci si può aspettare durante il processo di aggiornamento.

Ambiente

- FTD in esecuzione versione 7.4. Possono essere interessate anche altre versioni software.
- FTD configurato in modalità di coppia Alta disponibilità (HA).
- FMC 7.4 gestione dell'FTD HA. Il problema può riguardare anche altre versioni software.

Risoluzione

La procedura di aggiornamento per FTD in configurazione HA utilizza una sequenza specifica per ridurre al minimo i tempi di inattività e mantenere l'integrità del sistema.

Ordine di aggiornamento consigliato

Passaggio 1. Aggiornare prima il CCP

Le linee guida di Cisco richiedono che il FMC esegua la stessa versione o una versione più recente dei dispositivi che gestisce. Non è possibile aggiornare un dispositivo FTD dopo il FMC a una versione di manutenzione o principale più recente.

Passaggio 2. Aggiornare la coppia FTD HA da FMC

Quando si aggiorna una coppia FTD HA gestita da FMC, quest'ultimo aggiorna un peer alla volta (prima Standby, quindi Attivo) e si verifica un failover come parte del processo.

Previsioni di downtime e impatto sul traffico

- È necessario pianificare una finestra di manutenzione. Gli aggiornamenti delle note di Cisco possono includere interruzioni del flusso del traffico e ispezioni e i dispositivi possono interrompere il passaggio del traffico durante l'aggiornamento o se un aggiornamento non riesce.
- Con una coppia HA, l'obiettivo è quello di ridurre al minimo l'impatto, ma è necessario prevedere almeno un evento di failover e una possibile breve interruzione (ad esempio, adiacenza di routing o rinegoziazione VPN a seconda dell'ambiente).
- Evitare di apportare modifiche alle regole e alla configurazione durante l'aggiornamento (nessuna distribuzione o modifica fino a quando entrambi i membri HA non sono stati completamente aggiornati e stabili).

Controlli di integrità pre-aggiornamento per FTD HA

Prima di iniziare l'aggiornamento, verificare che FTD HA sia stabile e che le due unità siano in accordo sullo stato Attivo e Pronto per standby:

<#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
```

Causa

Si tratta di un'indagine procedurale riguardante le migliori pratiche per l'aggiornamento dei sistemi FMC e FTD nella configurazione HA. La domanda affronta la necessità di comprendere la sequenza di upgrade appropriata, le aspettative relative ai tempi di inattività e le strategie di riduzione dell'impatto per le infrastrutture firewall critiche.

Contenuto correlato

- Pianificazione dell'aggiornamento di Centro gestione firewall sicuro
- Aggiorna FTD HA gestito da FMC
- Guida alla compatibilità di Management Center
- Guida alla compatibilità di Threat Defense
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).