Aggiorna flusso di lavoro HA FTD gestito da FMC con versione 7.4.2

Problema

Il problema principale affrontato è il flusso di lavoro e i requisiti tecnici per eseguire un aggiornamento ad alta disponibilità (HA, High Availability) sui dispositivi Cisco Firepower Threat Defense (FTD) (in particolare FPR1120) gestiti da un Firepower Management Center (FMC) 4700 in esecuzione versione 7.4.2. In questo articolo vengono illustrati in dettaglio i passaggi preparatori, le best practice e le considerazioni per garantire la riuscita dell'operazione di aggiornamento FTD HA.

Ambiente

- Tecnologia: Cisco Secure Firewall Firepower - 7.4
- Sottotecnologia: Firepower Threat Defense (FTD) - Aggiornamento software / Aggiornamento sicurezza / Nuova immagine / Migrazione / Backup e ripristino
- Famiglia di prodotti: FPRFLOW (include FPR1120)
- Firepower Threat Defense (FTD) in una coppia ad alta disponibilità (HA)
- Gestito da Firepower Management Center (FMC) 4700
- Versione software FMC: 7.4.2
- Attività di aggiornamento pianificata pianificata in una finestra di manutenzione definita

Risoluzione

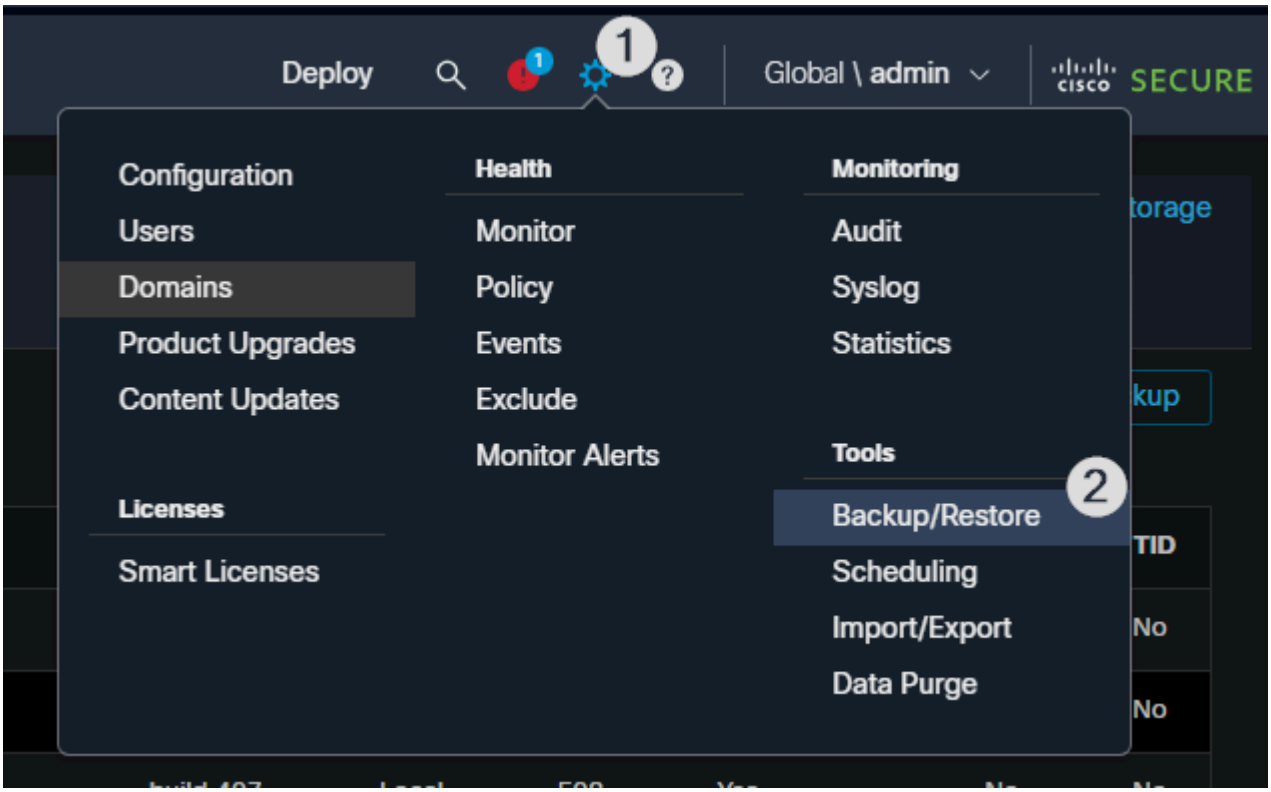
Attenersi a questo flusso di lavoro dettagliato per garantire un aggiornamento corretto delle coppie FTD HA gestite da FMC:

Passaggio 1: Prepararsi all'aggiornamento

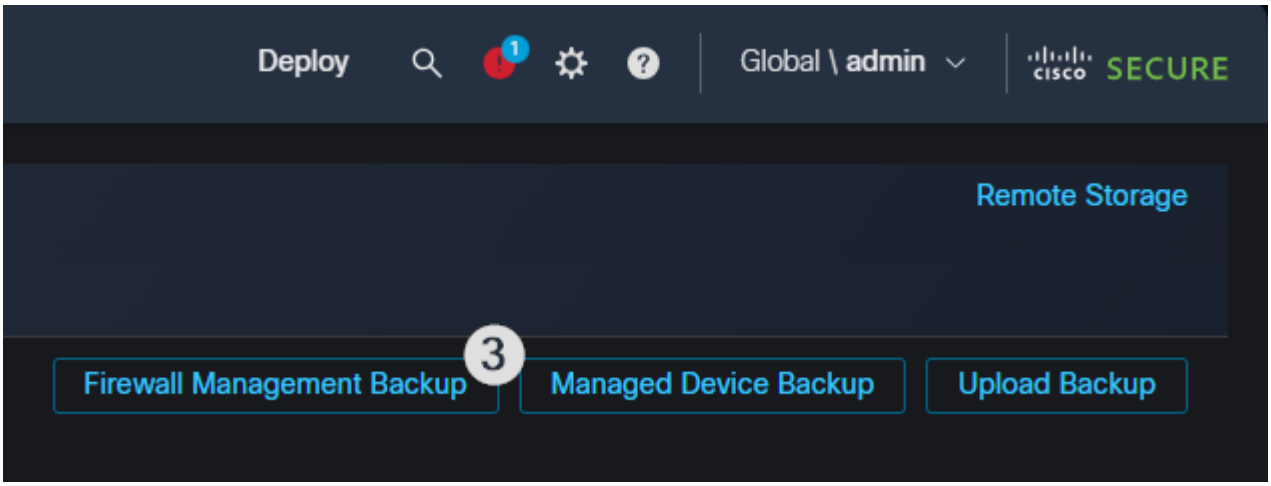
Prima di avviare il processo di aggiornamento, è essenziale generare e memorizzare i backup

della configurazione dei dispositivi FTD HA e FMC. Ciò garantisce che le configurazioni possano essere ripristinate in caso di errore dell'aggiornamento o di problema imprevisto.

Per eseguire il backup della configurazione di FMC: Passare a Sistema > Strumenti: Backup/Ripristino nell'interfaccia utente di FMC e fare clic sul pulsante Backup gestione firewall:



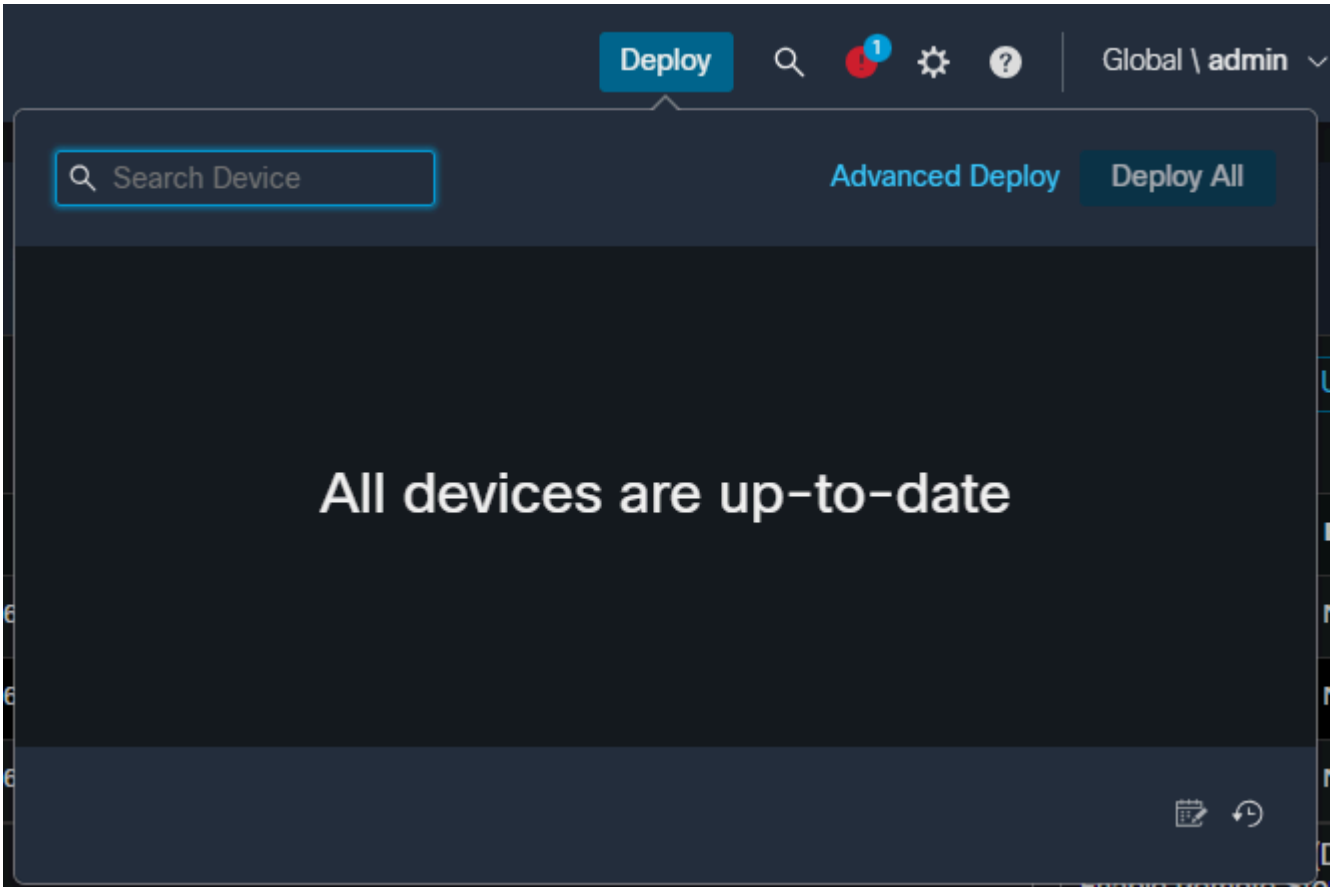
inline_image_0.png



inline_image_1.png

Fare clic sul pulsante Managed Device Backup per eseguire il backup della coppia FTD HA.

Per garantire il mantenimento dello stato di configurazione del dispositivo FTD, verificare che la distribuzione della configurazione più recente sia stata completata dal CCP a entrambi i peer HA:



inline_image_2.png

Passaggio 2: Verificare lo stato corrente della coppia HA FTD

Prima di procedere con l'aggiornamento, controllare lo stato HA per verificare che entrambi i peer siano integri e sincronizzati. Nella CLI FTD, utilizzare questo comando per controllare lo stato del dispositivo:

```
> mostra stato failover
```

Output di esempio:

```
Data/ora motivo ultimo errore stato

Host corrente - Primario

 Nessuno attivo

Altro host - Secondario

 Pronto per standby Nessuno
```

```
====Stato configurazione===

 Sincronizzazione ignorata

====Stato comunicazione==
```

Mac setStep 3: Programmazione e comunicazione della finestra di manutenzione

Assicurarsi che la finestra di manutenzione sia chiaramente definita e che tutti i cointeressati siano informati. Per questo flusso di lavoro, la manutenzione è stata programmata di conseguenza:

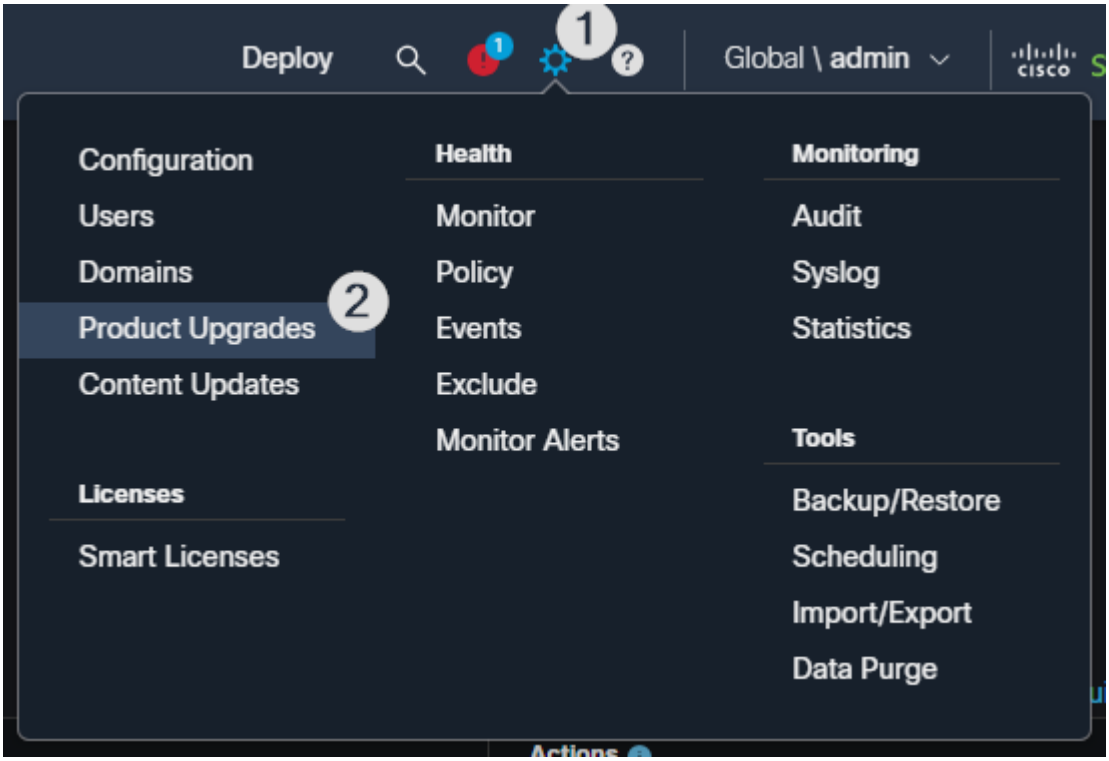
- Ora di inizio: 18/11/2025 12:00:00 (UTC -3 Argentina/Buenos_Aires)
- Ora di fine: 18/11/2025 14:00:00 (UTC -3 Argentina/Buenos_Aires)

Passo 4: avviare l'aggiornamento FTD HA

Avviare l'aggiornamento dal FMC, assicurandosi di seguire la procedura consigliata da Cisco per l'aggiornamento di coppie FTD HA. Durante il processo di aggiornamento, l'aggiornamento viene in genere eseguito in sequenza automaticamente:

1. Aggiornare l'FTD in standby.
2. Eseguire il failover sull'FTD appena aggiornato e renderlo attivo.
3. Aggiornare l'altro FTD in standby.

Nell'interfaccia utente di FMC, selezionare System **>** Product Upgrades (Sistema **>** Aggiornamenti prodotto) e selezionare la versione di destinazione per l'aggiornamento.



inline_image_3.png

Fase 5: Monitoraggio del processo di aggiornamento

Monitorare attentamente lo stato di avanzamento dell'aggiornamento per entrambe le unità. Utilizzare la sezione di monitoraggio dei processi della GUI FMC o la CLI per gli aggiornamenti dello stato. Per controllare lo stato di avanzamento dell'aggiornamento nella CLI:

```
> show upgrade status
```

Output di esempio:

```
Aggiornamento in corso sull'unità di standby...

Aggiornamento completato sull'unità di standby.

Avvio del failover in corso...

Aggiornamento in corso sull'unità attiva...

Aggiornamento completato su entrambe le unità.
```

La coppia HA è sincronizzata.Fase 6: verifica post-aggiornamento

Al termine dell'aggiornamento, verificare quanto segue:

- Su entrambi i dispositivi FTD è in esecuzione la versione software desiderata.
- Lo stato HA indica che entrambe le unità sono integre e sincronizzate.
- Tutti i servizi e i flussi di rete previsti funzionano come previsto.

```
> show version
```

Output di esempio:

```
-[ potenza di fuoco ]-

Modello: Cisco Firepower Threat Defense per VMware (75) versione 7.4.2.4 (Build 9)

UUID : bc9d31e8-0517-11f0-9c89-c358b8259f96

Versione LSP : lsp-rel-20260128-1954

Versione VDB: 404

-

> show failover
```

Output di esempio:

```
> show failover

Failover attivato

Unità di failover primaria

Interfaccia LAN di failover: Gigabit Ethernet0/7 (up) a stato di failover

Timeout riconnessione 0:00:00
```

Frequenza Unit Poll 1 secondi, tempo di attesa 15 secondi

Frequenza di polling interfaccia 5 secondi, tempo di attesa 25 secondi

Criterio interfaccia 1

Interfacce monitorate 4 di 361 massimo

Intervallo di notifica spostamento indirizzo MAC non impostato

http per la replica di failover

Versione: 9.20(2)121, Mate 9.20(2)121

Numero di serie: Oour SERIAL, Mate SERIAL

Ultimo failover alle: 14:29:08 UTC Dec 31 2025

 Host corrente: primario - attivo

 Tempo di attività: 3418340 (sec)

 slot 0: ASAv hw/sw rev (/9.20(2)121) status (Up Sys)

 Interface OUTSIDE (IPADDRESS): Normale (monitorato)

 Interfaccia INTERNA (IPADDRESS): normale (monitorata)

 DMZ interfaccia (IPADDRESS): Normale (monitorato)

 Gestione interfaccia (IPADDRESS): normale (monitorato)

 slot 1: stato snort rev (1.0) (su)

 slot 2: stato rev diskstatus (1.0) (su)

 Altro host: Secondario - Pronto per standby

```
Tempo di attività: 0 (sec)

Interface OUTSIDE (IPADDRESS): Normale (monitorato)

Interfaccia INTERNA (IPADDRESS): normale (monitorata)

DMZ interfaccia (IPADDRESS): Normale (monitorato)

Gestione interfaccia (IPADDRESS): normale (monitorato)

slot 1: stato snort rev (1.0) (su)
```

slot 2: stato rev diskstatus (1.0) (su)

Passaggio 7: Garantire L'Aggiornamento Dei Backup

Infine, generare nuovi backup di FMC e FTD dopo l'aggiornamento per acquisire lo stato di configurazione aggiornato.

Ripetere il processo di backup come descritto al passo 1.

Causa

Nessuna. Si tratta di un flusso di lavoro di aggiornamento standard per Cisco FTD HA gestito da FMC.

Contenuto correlato

- Supporto tecnico Cisco e download
- Aggiorna FTD HA gestito da FMC
- Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower
- Note sulla release

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).