

# Configurazione della funzionalità FTD High Availability nei dispositivi Firepower

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Attività 1. Verifica condizioni](#)

[Attività 2. Configura FTD HA](#)

[Condizioni](#)

[Attività 3. Verifica FTD HA e licenza](#)

[Attività 4. Cambia ruoli di failover](#)

[Attività 5. Interrompere la coppia HA](#)

[Attività 6. Eliminare una coppia HA](#)

[Attività 7. Sospendi HA](#)

[Domande frequenti \(FAQ\)](#)

[Informazioni correlate](#)

---

## Introduzione

Questo documento descrive come configurare e verificare Firepower Threat Defense (FTD) High Availability (HA) (failover attivo/standby) sui dispositivi Firepower.

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 2 Cisco Firepower 9300
- 2 Cisco Firepower 4100 (7.2.8)
- Firepower Management Center (FMC) (7.2.8)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

---

 Nota: su un accessorio FPR9300 con FTD, è possibile configurare solo HA tra chassis. Le due unità di una configurazione HA devono soddisfare le condizioni indicate qui.

---

## Attività 1. Verifica condizioni

Attività richiesta:

Verificare che entrambi gli accessori FTD soddisfino i requisiti della nota e possano essere configurati come unità HA.

Soluzione:

Passaggio 1. Connettersi all'IP di gestione FPR9300 e verificare l'hardware del modulo.

Verificare l'hardware FPR9300-1.

```
<#root>
```

```
KSEC-FPR9K-1-A#
```

```
show server inventory
```

Server	Equipped	PID	Equipped VID	Equipped Serial (SN)	Slot	Status	Ackd Memory (MB)	Ackd Cores
1/1	FPR9K-SM-36	V01		FLM19216KK6		Equipped	262144	36
1/2	FPR9K-SM-36	V01		FLM19206H71		Equipped	262144	36
1/3	FPR9K-SM-36	V01		FLM19206H7T		Equipped	262144	36

```
KSEC-FPR9K-1-A#
```

Verificare l'hardware FPR9300-2.

```
<#root>
```

```
KSEC-FPR9K-2-A#
```

```
show server inventory
```

Server	Equipped	PID	Equipped VID	Equipped Serial (SN)	Slot	Status	Ackd Memory (MB)	Ackd Cores
1/1	FPR9K-SM-36	V01		FLM19206H9T		Equipped	262144	36
1/2	FPR9K-SM-36	V01		FLM19216KAX		Equipped	262144	36
1/3	FPR9K-SM-36	V01		FLM19267A63		Equipped	262144	36

```
KSEC-FPR9K-2-A#
```

Passaggio 2. Accedere a FPR9300-1 Chassis Manager e selezionare Logical Devices.

Verificare la versione del software, il numero e il tipo di interfacce.

## Attività 2. Configura FTD HA

Attività richiesta:

Configurare il failover Attivo/Standby (HA) come nell'immagine seguente. In questo caso, viene utilizzata una coppia 41xx.

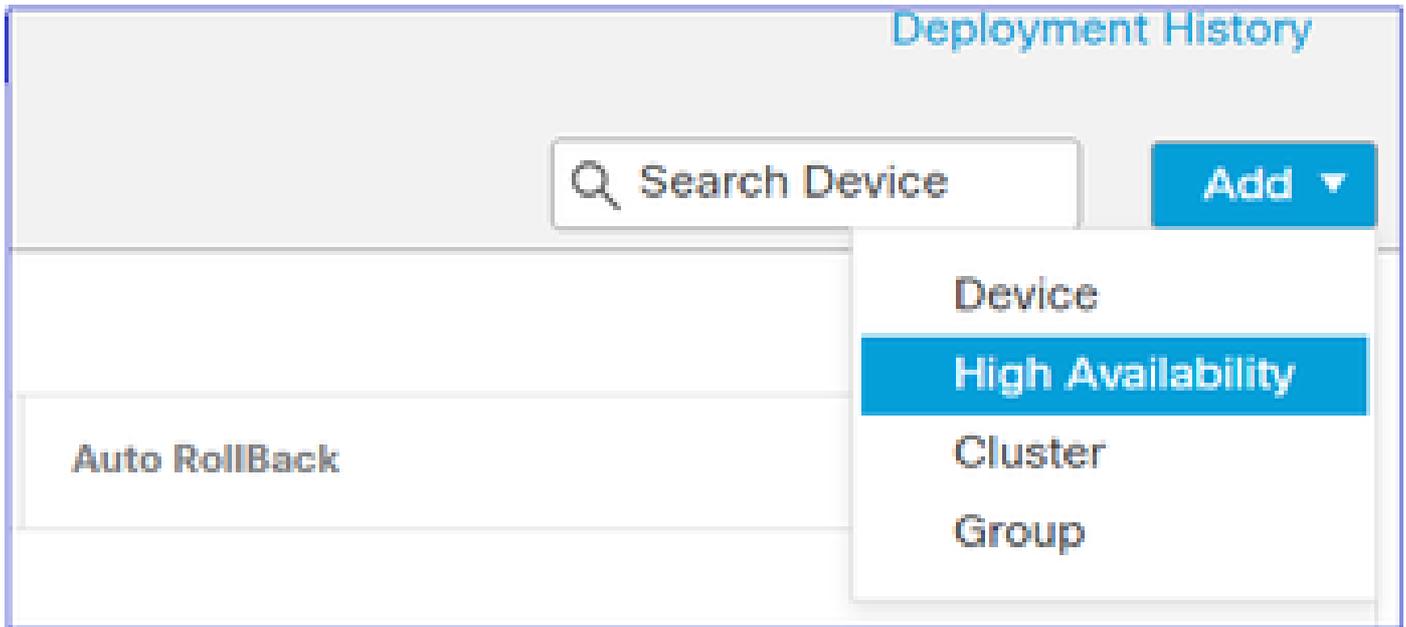


Soluzione

Entrambi i dispositivi FTD sono già registrati sull'FMC, come mostrato nell'immagine.

FTD4100-5 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5-443 Security Module - 1	Base, Threat (2 more...)	acp_simple	⊞	✎
FTD4100-6 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6-443 Security Module - 1	Base, Threat (2 more...)	acp_simple	⊞	✎

Passaggio 1. Per configurare il failover FTD, selezionare Dispositivi > Gestione dispositivi e scegliere Aggiungi alta disponibilità come mostrato nell'immagine.



Passaggio 2. Immettere il peer primario e il peer secondario, quindi scegliere Continua come mostrato nell'immagine.

## Add High Availability Pair



Name:\*

FTD4100-HA

Device Type:

Firewall Threat Defense

Primary Peer:

FTD4100-5

Secondary Peer:

FTD4100-6

- i** Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

Cancel

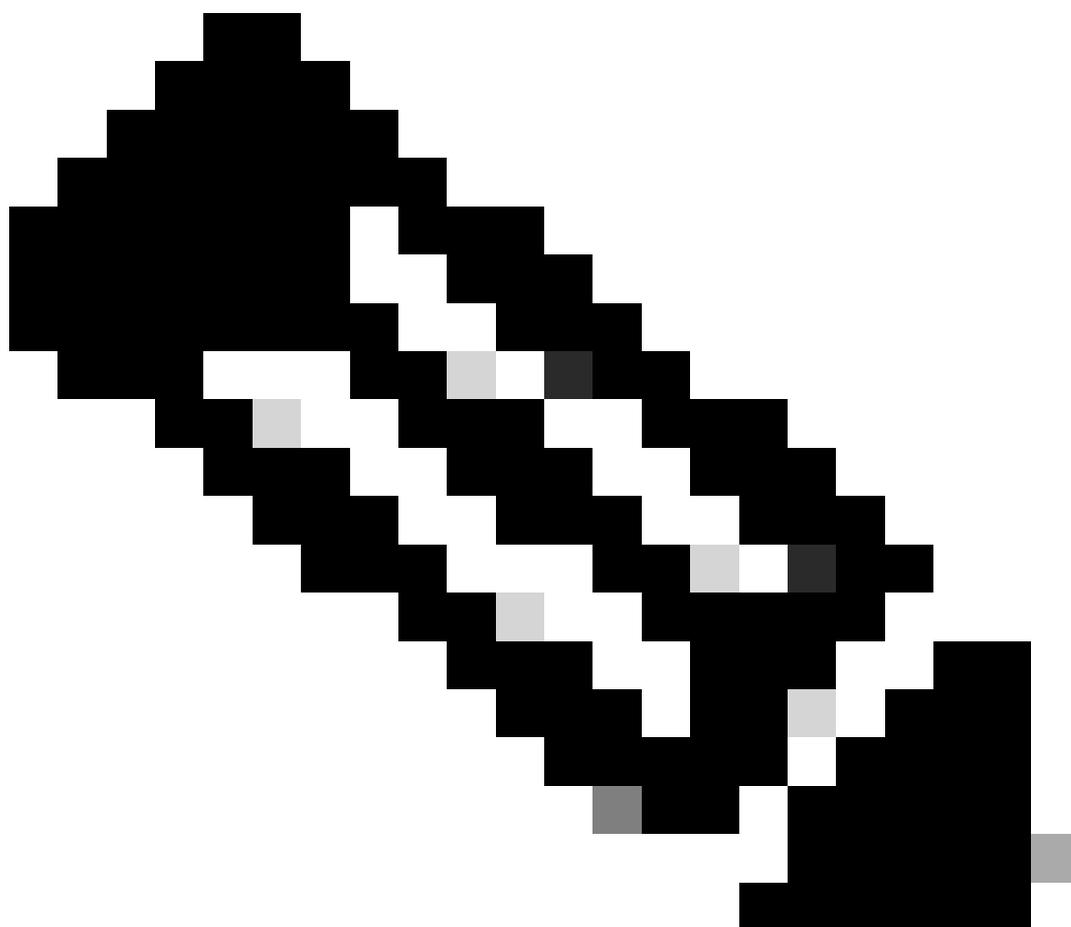
Continue

**⚠** Avvertenza: assicurarsi di selezionare l'unità corretta come unità principale. Tutte le configurazioni sull'unità primaria selezionata vengono replicate sull'unità FTD secondaria selezionata. In seguito alla replica, la configurazione corrente sull'unità secondaria può essere sostituita.

Condizioni

Per creare una coppia HA tra 2 dispositivi FTD, è necessario soddisfare le seguenti condizioni:

- Stesso modello
  - Stessa versione - vale per FXOS e per FTD - maggiore (primo numero), minore (secondo numero) e manutenzione (terzo numero) devono essere uguali.
  - Stesso numero di interfacce
  - Stesso tipo di interfacce
  - Entrambi i dispositivi fanno parte dello stesso gruppo/dominio in FMC.
  - Hanno una configurazione NTP (Network Time Protocol) identica.
  - essere pienamente implementato nel CCP senza modifiche non sottoposte a commit.
  - Modalità firewall uguale: instradato o trasparente.
- 



Nota: questa condizione deve essere verificata sia sui dispositivi FTD che sull'interfaccia grafica dell'FMC, in quanto in alcuni casi gli FTD avevano la stessa modalità, ma l'interfaccia dell'FMC non la riflette.

---

- Il protocollo DHCP/Point-to-Point over Ethernet (PPPoE) non è configurato in alcuna

interfaccia.

- Nome host [FQDN (Fully Qualified Domain Name)] diverso per entrambi gli chassis. Per controllare il nome host dello chassis, passare alla CLI FTD ed eseguire questo comando:

```
<#root>
firepower#
show chassis-management-url

https://
KSEC-FPR9K-1.cisco.com
:443//
```



Nota: nell'FTD successivo alla 6.3 usare il comando `show chassis detail`.

---

```
<#root>
Firepower-module1#
show chassis detail

Chassis URL : https://FP4100-5:443//

Chassis IP : 10.62.148.187
Chassis IPv6 : ::
Chassis Serial Number : JAD19500BAB
Security Module : 1
```

Se entrambi gli chassis hanno lo stesso nome, modificarne uno con questi comandi:

```
<#root>
KSEC-FPR9K-1-A#
scope system
KSEC-FPR9K-1-A /system #
set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #
commit-buffer
FPR9K-1-A /system #
exit
```

#

Dopo aver modificato il nome dello chassis, annullare la registrazione dell'FTD dall'FMC e registrarlo di nuovo. Quindi, procedere con la creazione della coppia HA.

Passaggio 3. Configurare HA e lo stato delle impostazioni dei collegamenti.

In questo caso, le impostazioni del collegamento dello stato sono le stesse del collegamento High Availability.

Scegliere Aggiungi e attendere alcuni minuti prima che la coppia HA venga distribuita come mostrato nell'immagine.

**Add High Availability Pair**

High Availability Link	State Link
Interface:* Port-channel3	Interface:* Same as LAN Failover Link
Logical Name:* FOVER	Logical Name:* FOVER
Primary IP:* 172.16.51.1	Primary IP:* 172.16.51.1
<input type="checkbox"/> Use IPv6 Address	<input type="checkbox"/> Use IPv6 Address
Secondary IP:* 172.16.51.2	Secondary IP:* 172.16.51.2
Subnet Mask:* 255.255.255.0	Subnet Mask:* 255.255.255.0

**IPsec Encryption**

Enabled

Key Generation: Auto

**i** LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Cancel Add

Passaggio 4. Configurare le interfacce dati (indirizzi IP primario e in standby)

Dall'interfaccia utente di FMC, scegliere HA Edit, come mostrato nell'immagine.

FTD4120-HA High Availability							
FTD4100-5(Primary, Active) <b>Snort 3</b> 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5.443 Security Module - 1	Base, Threat (2 more...)	acp_simple		
FTD4100-6(Secondary, Standby) <b>Snort 3</b> 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6.443 Security Module - 1	Base, Threat (2 more...)	acp_simple		

Passaggio 5. Configurare le impostazioni dell'interfaccia:

### Edit Physical Interface

General IPv4 IPv6 Path Monitoring Advanced

Name:

Enabled

Management Only

Description:

Mode:

Security Zone:

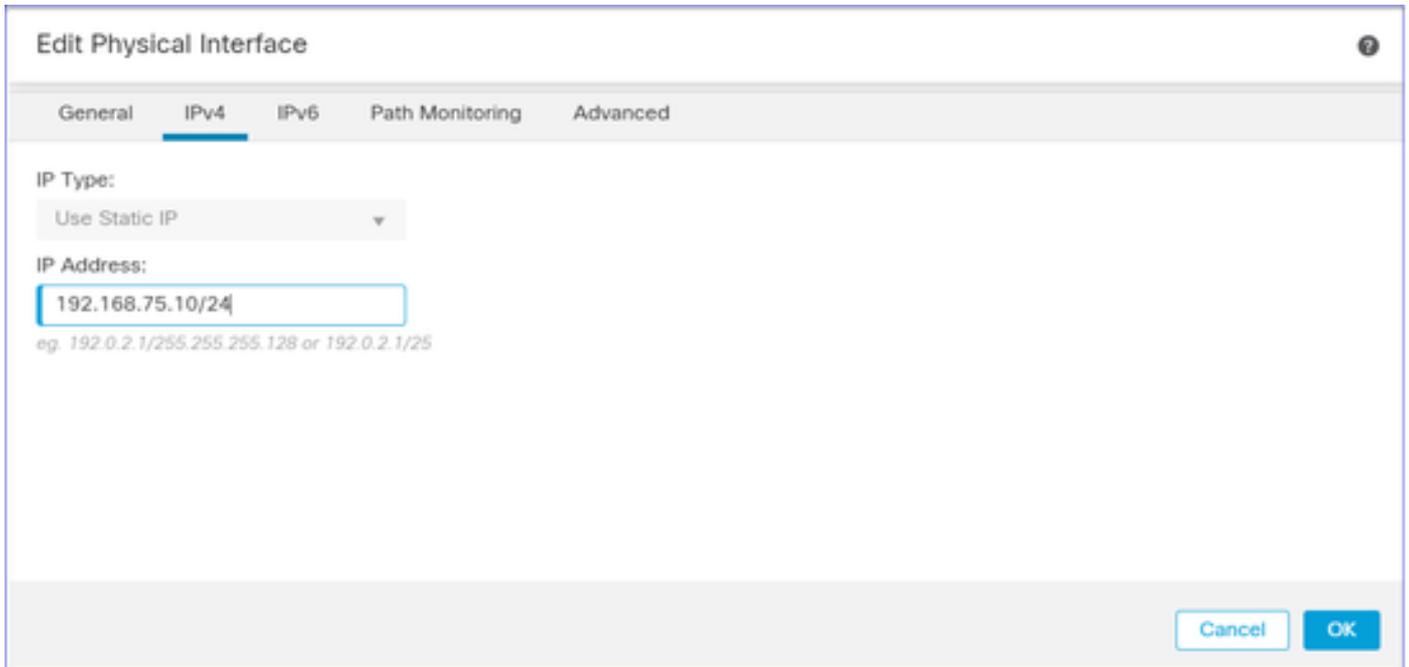
Interface ID:

MTU:   
(64 - 9184)

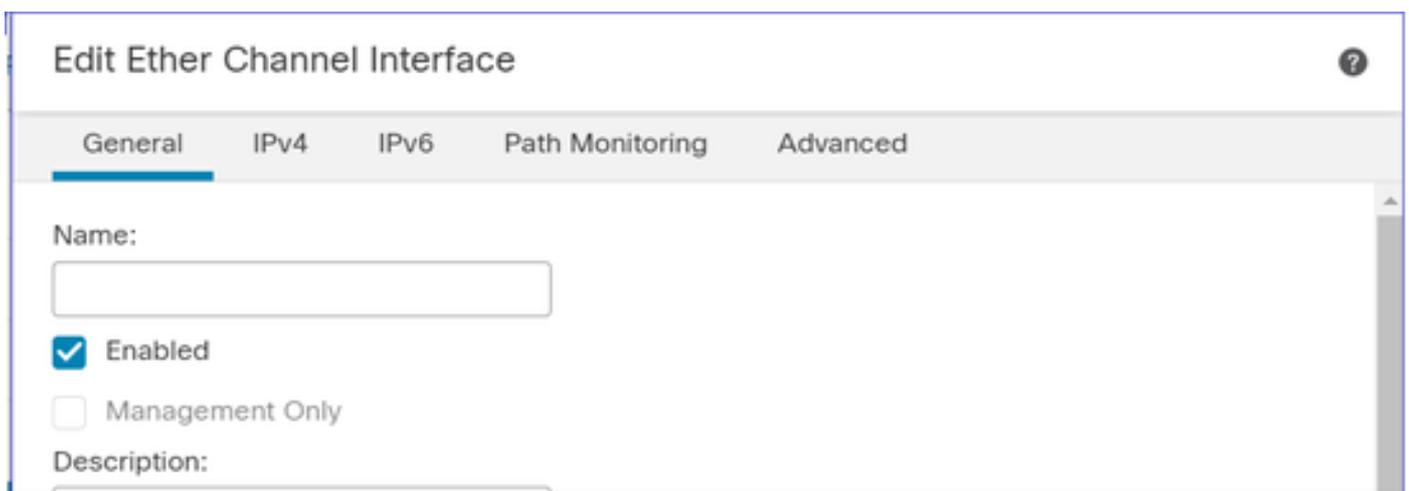
Priority:  (0 - 65535)

Propagate Security Group Tag:

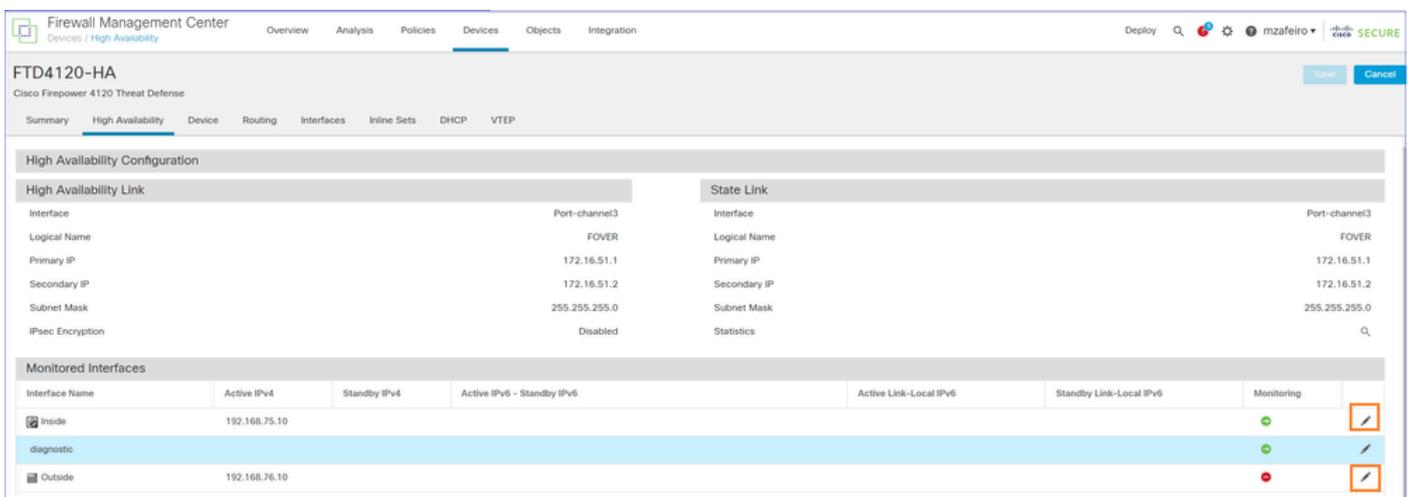
NVE Only:



Nel caso di una sottointerfaccia, è necessario prima abilitare l'interfaccia padre:



Passaggio 6. Passare a Alta disponibilità e scegliere il nome dell'interfaccia Modifica per aggiungere gli indirizzi IP in standby, come mostrato nell'immagine.



Passaggio 7. Per l'interfaccia Inside come mostrato nell'immagine.

**Edit Inside**

Monitor this interface for failures

IPv4    IPv6

Interface Name:  
Inside

Active IP Address:  
192.168.75.10

Mask:  
24

Standby IP Address:  
192.168.75.11

Cancel    OK

Passaggio 8. Ripetere l'operazione per l'interfaccia esterna.

Passaggio 9. Verificare il risultato come mostrato nell'immagine.

Monitored Interfaces						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
<input checked="" type="checkbox"/> Inside	192.168.75.10	192.168.75.11				<span style="color: green;">●</span>
diagnostic						<span style="color: green;">●</span>
<input checked="" type="checkbox"/> Outside	192.168.76.10	192.168.76.11				<span style="color: green;">●</span>

Passaggio 10. Rimanere nella scheda Alta disponibilità e configurare gli indirizzi MAC virtuali come mostrato nell'immagine.

**Interface MAC Addresses** +

Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

Passaggio 11. Per l'interfaccia interna è come mostrato nell'immagine.

**Add Interface Mac Address** ⓘ

**Physical Interface:\***

Ethernet1/4 ▾

**Active Interface Mac Address:\***

aaaa.bbbb.1111

**Standby Interface Mac Address:\***

aaaa.bbbb.2222

ⓘ Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

Cancel OK

Passaggio 12. Ripetere l'operazione per l'interfaccia esterna.

Passaggio 13. Verificare il risultato come mostrato nell'immagine.

Interface MAC Addresses			
Physical Interface	Active Mac Address	Standby Mac Address	
Ethernet1/4	aaaa.bbbb.1111	aaaa.bbbb.2222	
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	

Passaggio 14. Dopo aver configurato le modifiche, scegliere Salva e distribuisci.

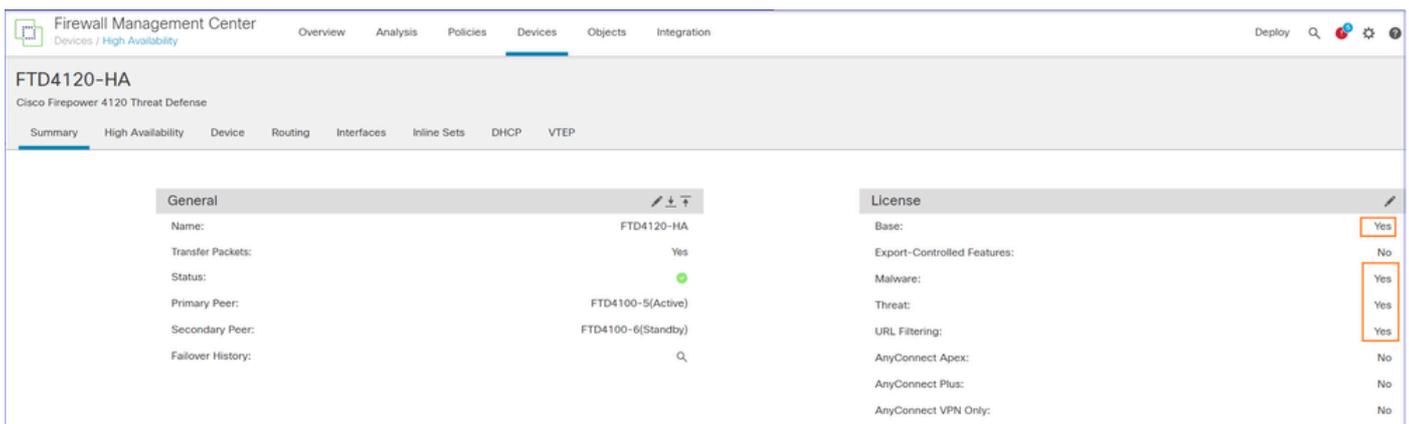
## Attività 3. Verifica FTD HA e licenza

Attività richiesta:

Verificare le impostazioni HA della coppia di FTD e le licenze abilitate dalla GUI dell'FMC e dalla CLI degli FTD.

Soluzione:

Passaggio 1. Passare a Riepilogo e controllare le impostazioni HA e le licenze abilitate come mostrato nell'immagine.



The screenshot shows the FMC interface for a Cisco Firepower 4120 Threat Defense device in High Availability mode. The 'License' section is expanded, showing the following settings:

License Feature	Status
Base	Yes
Export-Controlled Features	No
Malware	Yes
Threat	Yes
URL Filtering	Yes
AnyConnect Apex	No
AnyConnect Plus	No
AnyConnect VPN Only	No

Passaggio 2. Dalla CLI di FTD CLISH, eseguire il comando 'show high-availability config' o 'show failover':

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel3 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 1291 maximum
MAC Address Move Notification Interval not set
```

failover replication http  
Version: Ours 9.18(4)210, Mate 9.18(4)210  
Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG  
Last Failover at: 08:46:30 UTC Jul 18 2024

**This host: Primary - Active**

Active time: 1999 (sec)  
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)  
  Interface diagnostic (0.0.0.0): Normal (Waiting)  
  Interface Inside (192.168.75.10): Link Down (Shutdown)  
  Interface Outside (192.168.76.10): Normal (Not-Monitored)  
slot 1: snort rev (1.0) status (up)  
slot 2: diskstatus rev (1.0) status (up)

**Other host: Secondary - Standby Ready**

Active time: 1466 (sec)  
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)  
  Interface diagnostic (0.0.0.0): Normal (Waiting)  
  Interface Inside (192.168.75.11): Link Down (Shutdown)  
  Interface Outside (192.168.76.11): Normal (Not-Monitored)  
slot 1: snort rev (1.0) status (up)  
slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics  
<output omitted>

Passaggio 3. Eseguire la stessa operazione sul dispositivo secondario.

Passaggio 4. Eseguire il comando show failover state dalla CLI di LINA:

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016

====Configuration State====

  Sync Done

====Communication State====

  Mac set

firepower#

Passaggio 5. Verificare la configurazione dall'unità principale (LINA CLI):

```
<#root>
```

```
>  
  
show running-config failover  
  
failover  
failover lan unit primary  
failover lan interface FOVER Port-channel3  
failover replication http  
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222  
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444  
failover link FOVER Port-channel3  
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2
```

```
>  
  
show running-config interface  
  
!  
interface Port-channel2  
no nameif  
no security-level  
no ip address  
!  
interface Port-channel2.202  
vlan 202  
nameif Outside  
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0  
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11  
!  
interface Port-channel3  
description LAN/STATE Failover Interface  
!  
interface Ethernet1/1  
management-only  
nameif diagnostic  
security-level 0  
no ip address  
!  
interface Ethernet1/4  
shutdown  
nameif Inside  
security-level 0  
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11  
>
```

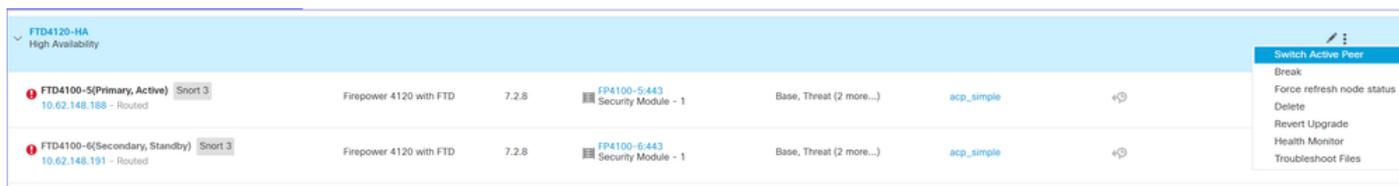
## Attività 4. Cambia ruoli di failover

Attività richiesta:

Dall'FMC, invertire i ruoli di failover da Principale/Attivo, Secondario/Standby a Principale/Standby, Secondario/Attivo

Soluzione:

Passaggio 1. Selezionate l'icona come mostrato nell'immagine.



Passaggio 2. Confermare l'azione.

È possibile utilizzare l'output del comando show failover history:

Sul nuovo Active Directory	Il n
> mostra cronologia failover	
=====	
Da Stato A Stato Motivo	
=====	
09:27:11 UTC lug 18 2024 Pronto per lo standby Solo Attivo L'altra unità mi vuole Attivo	(Impostato con il comando
config)	
09:27:11 UTC lug 18 2024 Solo Active Drain L'altra unità mi vuole Active	(Impostato con il comando
config)	
09:27:11 UTC lug 18 2024 Active Drain Active Applying Config Other unit want me Active	(Impostato con il comando
config)	
09:27:11 UTC lug 18 2024 Active Applying Config Active Config Applied Other unit want me Active	(Impostato con il comando
config)	
09:27:11 UTC lug 18 2024 Active Config Applied Active Other unit want me Active	(Impostato con il comando
config)	

Passaggio 4. Dopo la verifica, riattivare l'unità principale.

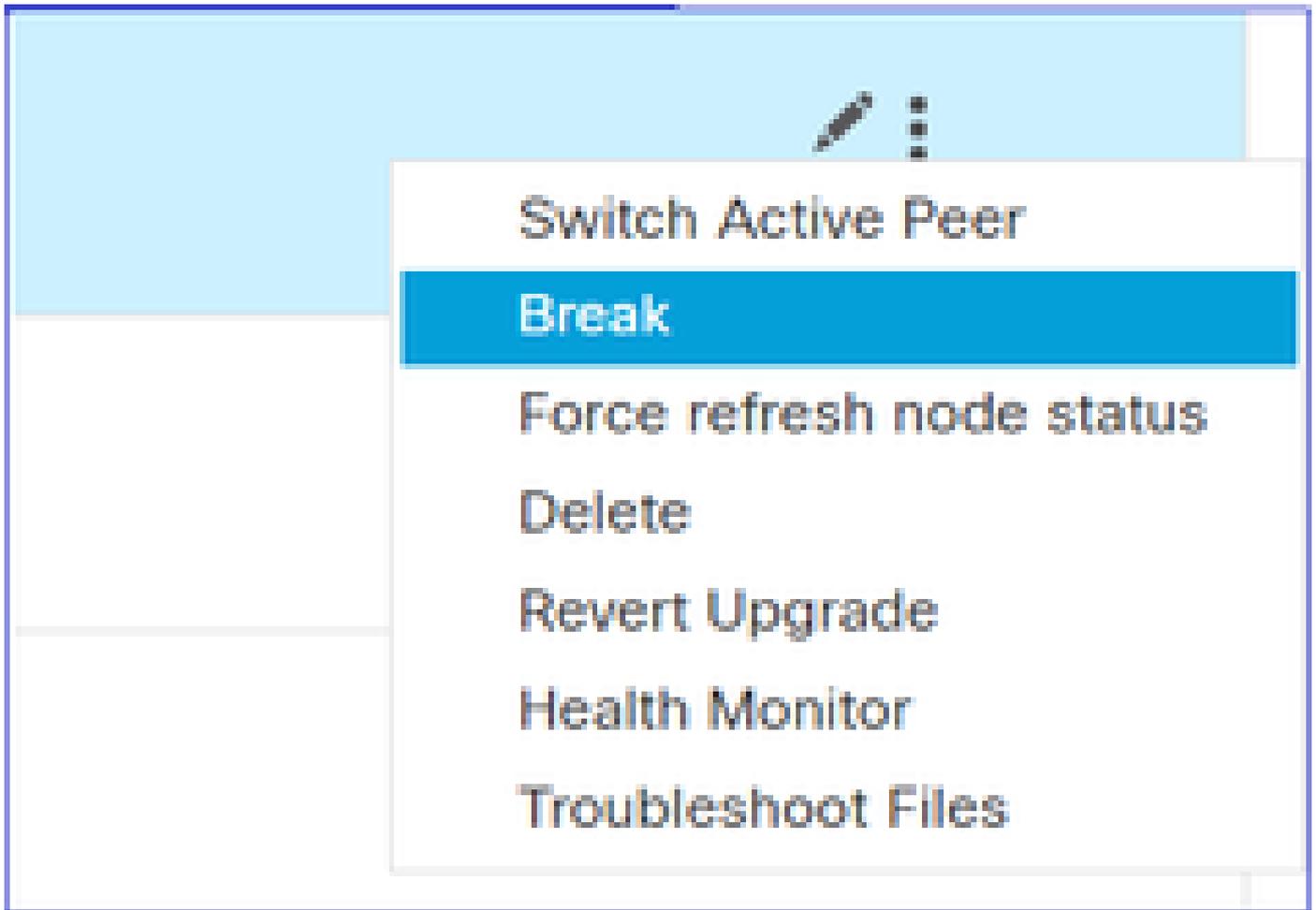
## Attività 5. Interrompere la coppia HA

Attività richiesta:

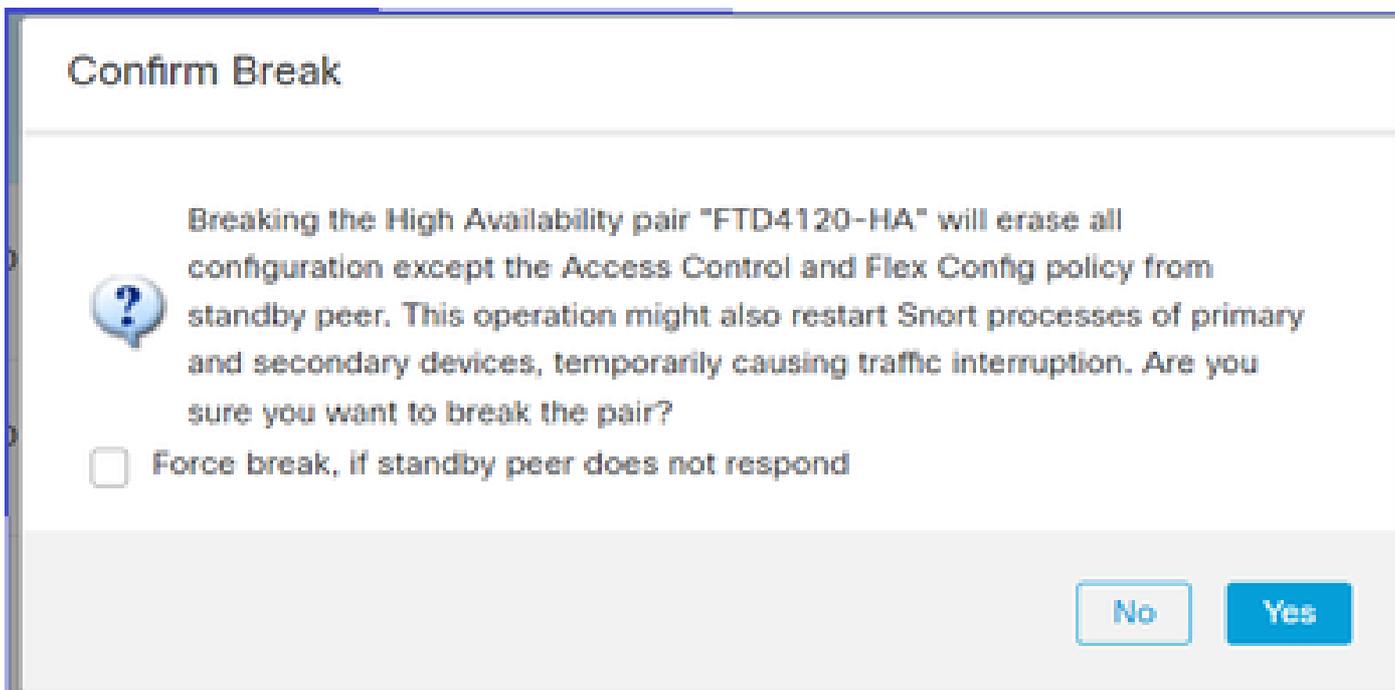
Dall'FMC, separare la coppia di failover.

Soluzione:

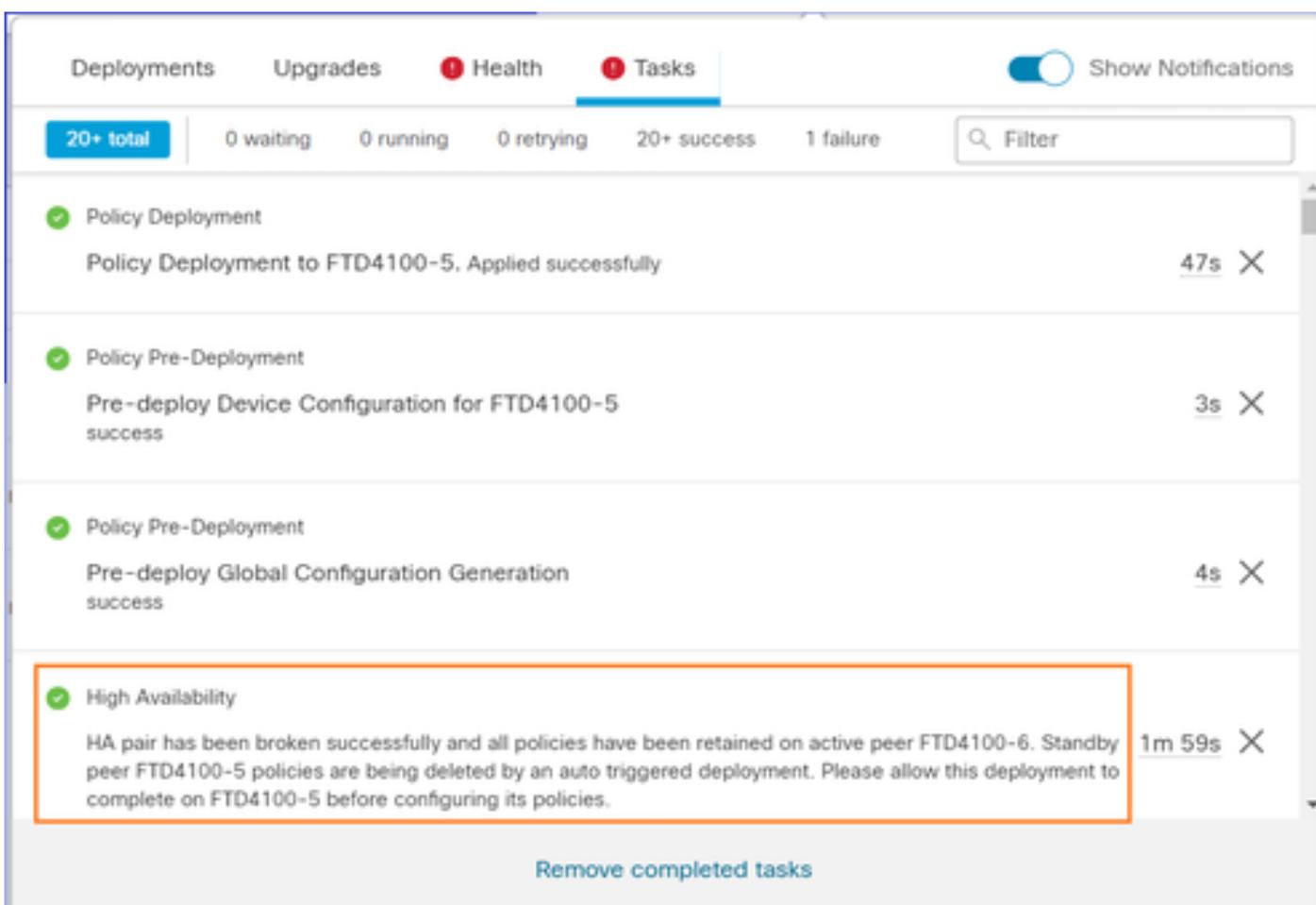
Passaggio 1. Selezionate l'icona come mostrato nell'immagine.



Passaggio 2. Controllare la notifica come mostrato nell'immagine.



Passaggio 3. Osservate il messaggio come mostrato nell'immagine.



Passaggio 4. Verificare il risultato dalla GUI del FMC o dalla CLI

Output del comando show running-config sull'unità Principale prima e dopo la separazione della coppia HA:

Unità principale/standby prima dell'interruzione HA	Unità principale dopo l'interruzione HA
<pre> &gt; show running-config : salvato : : numero di serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) : NGFW versione 7.2.8 ! hostname firepower abilita password **** crittografata strong-encryption-disable service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico ! interface Port-channel2 no nameif manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile nessun livello di protezione nessun indirizzo ip ! interface Port-channel 2.202 vlan 202 nameif Esterno manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 descrizione Interfaccia di failover LAN/STATE ! interfaccia Ethernet1/1 solo gestione diagnostica nameif </pre>	<pre> &gt; INFORMAZIONI: l'apparecchio è attualmente in stato di standby. Disattivando il failover, l'apparecchio rimane in stato di standby. &gt; show running-config : salvato : : numero di serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) : NGFW versione 7.2.8 ! hostname firepower abilita password **** crittografata strong-encryption-disable service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico ! interface Port-channel2 shutdown no nameif nessun livello di protezione nessun indirizzo ip ! interface Port-channel3 shutdown no nameif nessun livello di protezione nessun indirizzo ip ! interfaccia Ethernet1/1 solo gestione shutdown no nameif nessun livello di protezione nessun indirizzo ip ! interfaccia Ethernet1/4 </pre>

<p>manuale cat  propagazione di sgt preserve-untag  criterio statico sgt disabilitato attendibile  livello di protezione 0  nessun indirizzo ip  !  interfaccia Ethernet1/4  nameif Inside  manuale cat  propagazione di sgt preserve-untag  criterio statico sgt disabilitato attendibile  livello di protezione 0  indirizzo ip 192.168.75.10 255.255.255.0 standby  192.168.75.11  !  modalità ftp passiva  ngips conn-match vlan-id  controllo dell'accesso object group search  access-group CSM_FW_ACL_ globale  access-list CSM_FW_ACL_ note rule-id 9998:  PREFIXER POLICY: Criterio di priorità e tunnel  predefinito  access-list CSM_FW_ACL_ note rule-id 9998:  RULE: DEFAULT TUNNEL ACTION RULE  access-list CSM_FW_ACL_ advanced allow  ipinip any rule-id 9998  access-list CSM_FW_ACL_ advanced allow udp  any eq 3544 any range 1025 65535 rule-id 9998  access-list CSM_FW_ACL_ advanced allow udp  qualsiasi intervallo 1025 65535 any eq 3544 rule-  id 9998  access-list CSM_FW_ACL_ advanced allow 41  qualsiasi rule-id 9998  access-list CSM_FW_ACL_ advanced allow gre  any rule-id 9998  access-list CSM_FW_ACL_ note rule-id  268434433: ACCESS POLICY: acp_simple -  Default  access-list CSM_FW_ACL_ note rule-id  268434433: L4 RULE: DEFAULT ACTION RULE  access-list CSM_FW_ACL_ advanced  permission ip any rule-id 268434433  !  tcp-map UM_STATIC_TCP_MAP  intervallo di opzioni tcp 6/7 consentito  intervallo di opzioni tcp 9 18 consentito</p>	<p>shutdown  no nameif  nessun livello di protezione  nessun indirizzo ip  !  modalità ftp passiva  ngips conn-match vlan-id  controllo dell'accesso object group search  access-group CSM_FW_ACL_ globale  access-list CSM_FW_ACL_ note rule-id 9998:  PREFIXER POLICY: Criterio di priorità e  tunnel predefinito  access-list CSM_FW_ACL_ note rule-id 9998:  RULE: DEFAULT TUNNEL ACTION RULE  access-list CSM_FW_ACL_ advanced allow  ipinip any rule-id 9998  access-list CSM_FW_ACL_ advanced allow udp  any eq 3544 any range 1025 65535 rule-id  9998  access-list CSM_FW_ACL_ advanced allow udp  qualsiasi intervallo 1025 65535 any eq 3544  rule-id 9998  access-list CSM_FW_ACL_ advanced allow 41  qualsiasi rule-id 9998  access-list CSM_FW_ACL_ advanced allow gre  any rule-id 9998  access-list CSM_FW_ACL_ note rule-id  268439552: ACCESS POLICY: acp_simple -  Obbligatorio  access-list CSM_FW_ACL_ note rule-id  268439552: L7 RULE: rule1  access-list CSM_FW_ACL_ advanced  permission ip any rule-id 268439552  !  tcp-map UM_STATIC_TCP_MAP  intervallo di opzioni tcp 6/7 consentito  intervallo di opzioni tcp 9 18 consentito  intervallo di opzioni tcp 20-255 consentito  consenti contrassegno urgente  !  nessun cercapersone  nessun messaggio di registrazione 106015  nessun messaggio di logging 313001  nessun messaggio di registrazione 313008  nessun messaggio di registrazione 106023  nessun messaggio di registrazione 710003</p>
---	---

<p>intervallo di opzioni tcp 20-255 consentito  consenti contrassegno urgente  !  nessun cercapersone  nessun messaggio di registrazione 106015  nessun messaggio di logging 313001  nessun messaggio di registrazione 313008  nessun messaggio di registrazione 106023  nessun messaggio di registrazione 710003  nessun messaggio di registrazione 106100  nessun messaggio di registrazione 302015  nessun messaggio di registrazione 302014  nessun messaggio di registrazione 302013  nessun messaggio di registrazione 302018  nessun messaggio di registrazione 302017  nessun messaggio di registrazione 302016  nessun messaggio di logging 302021  nessun messaggio di registrazione 302020  mtu esterna a 1500  mtu diagnostic 1500  mtu all'interno di 1500  failover  unità lan di failover principale  failover interfaccia lan FOVER Port-channel3  http per la replica di failover  indirizzo mac di failover Ethernet1/4  aaaa.bbbb.1111 aaaa.bbbb.2222  indirizzo mac di failover Port-channel2.202  aaaa.bbbb.3333 aaaa.bbbb.4444  collegamento di failover FOVER Port-channel3  interfaccia di failover ip FOVER 172.16.51.1  255.255.255.0 standby 172.16.51.2</p> <p>&lt;output omezzo&gt;</p>	<p>nessun messaggio di registrazione 106100  nessun messaggio di registrazione 302015  nessun messaggio di registrazione 302014  nessun messaggio di registrazione 302013  nessun messaggio di registrazione 302018  nessun messaggio di registrazione 302017  nessun messaggio di registrazione 302016  nessun messaggio di logging 302021  nessun messaggio di registrazione 302020  nessun failover</p> <p>&lt;output omezzo&gt;</p>
<p>Unità secondaria/attiva prima dell'interruzione HA</p>	<p>Unità secondaria dopo l'interruzione HA</p>
<pre>&gt; show running-config : salvato : : Numero di serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core)</pre>	<pre>&gt; show running-config : salvato : : Numero di serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73850 MB RAM,</pre>

<pre> : NGFW versione 7.2.8 ! hostname firepower abilita password **** crittografata strong-encryption-disable service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico  ! interface Port-channel2 no nameif nessun livello di protezione nessun indirizzo ip  ! interface Port-channel 2.202 vlan 202 nameif Esterno manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 192.168.76.10 255.255.255.0 standby 192.168.76.11  ! interface Port-channel3 descrizione Interfaccia di failover LAN/STATE  ! interfaccia Ethernet1/1 solo gestione diagnostica nameif livello di protezione 0 nessun indirizzo ip  ! interfaccia Ethernet1/4 nameif Inside livello di protezione 0 indirizzo ip 192.168.75.10 255.255.255.0 standby 192.168.75.11  ! modalità ftp passiva ngips conn-match vlan-id controllo dell'accesso object group search access-group CSM_FW_ACL_ globale </pre>	<pre> CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) : NGFW versione 7.2.8 ! hostname firepower abilita password **** crittografata strong-encryption-disable service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico  ! interface Port-channel2 no nameif nessun livello di protezione nessun indirizzo ip  ! interface Port-channel 2.202 vlan 202 nameif Esterno manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 192.168.76.10 255.255.255.0 standby 192.168.76.11  ! interface Port-channel3 no nameif nessun livello di protezione nessun indirizzo ip  ! interfaccia Ethernet1/1 solo gestione diagnostica nameif livello di protezione 0 nessun indirizzo ip  ! interfaccia Ethernet1/4 nameif Inside livello di protezione 0 indirizzo ip 192.168.75.10 255.255.255.0 standby 192.168.75.11  ! modalità ftp passiva </pre>
--	--

<p>access-list CSM_FW_ACL_ note rule-id 9998:          PREFILTER POLICY: Criterio di priorità e tunnel          predefinito</p> <p>access-list CSM_FW_ACL_ note rule-id 9998:          RULE: DEFAULT TUNNEL ACTION RULE</p> <p>access-list CSM_FW_ACL_ advanced allow          ipinip any rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp          any eq 3544 any range 1025 65535 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp          qualsiasi intervallo 1025 65535 any eq 3544          rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow 41          qualsiasi rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow gre          any rule-id 9998</p> <p>access-list CSM_FW_ACL_ note rule-id          268439552: ACCESS POLICY: acp_simple -          Obbligatorio</p> <p>access-list CSM_FW_ACL_ note rule-id          268439552: L7 RULE: rule1</p> <p>access-list CSM_FW_ACL_ advanced          permission ip any rule-id 268439552          !</p> <p>tcp-map UM_STATIC_TCP_MAP          intervallo di opzioni tcp 6/7 consentito          intervallo di opzioni tcp 9 18 consentito          intervallo di opzioni tcp 20-255 consentito          consenti contrassegno urgente          !</p> <p>nessun cercapersone</p> <p>nessun messaggio di registrazione 106015</p> <p>nessun messaggio di logging 313001</p> <p>nessun messaggio di registrazione 313008</p> <p>nessun messaggio di registrazione 106023</p> <p>nessun messaggio di registrazione 710003</p> <p>nessun messaggio di registrazione 106100</p> <p>nessun messaggio di registrazione 302015</p> <p>nessun messaggio di registrazione 302014</p> <p>nessun messaggio di registrazione 302013</p> <p>nessun messaggio di registrazione 302018</p> <p>nessun messaggio di registrazione 302017</p> <p>nessun messaggio di registrazione 302016</p> <p>nessun messaggio di logging 302021</p> <p>nessun messaggio di registrazione 302020</p>	<p>ngips conn-match vlan-id</p> <p>controllo dell'accesso object group search</p> <p>access-group CSM_FW_ACL_ globale</p> <p>access-list CSM_FW_ACL_ note rule-id 9998:          PREFILTER POLICY: Criterio di priorità e tunnel          predefinito</p> <p>access-list CSM_FW_ACL_ note rule-id 9998:          RULE: DEFAULT TUNNEL ACTION RULE</p> <p>access-list CSM_FW_ACL_ advanced allow          ipinip any rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp          any eq 3544 any range 1025 65535 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp          qualsiasi intervallo 1025 65535 any eq 3544          rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow 41          qualsiasi rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow gre          any rule-id 9998</p> <p>access-list CSM_FW_ACL_ note rule-id          268439552: ACCESS POLICY: acp_simple -          Obbligatorio</p> <p>access-list CSM_FW_ACL_ note rule-id          268439552: L7 RULE: rule1</p> <p>access-list CSM_FW_ACL_ advanced          permission ip any rule-id 268439552          !</p> <p>tcp-map UM_STATIC_TCP_MAP          intervallo di opzioni tcp 6/7 consentito          intervallo di opzioni tcp 9 18 consentito          intervallo di opzioni tcp 20-255 consentito          consenti contrassegno urgente          !</p> <p>nessun cercapersone</p> <p>nessun messaggio di registrazione 106015</p> <p>nessun messaggio di logging 313001</p> <p>nessun messaggio di registrazione 313008</p> <p>nessun messaggio di registrazione 106023</p> <p>nessun messaggio di registrazione 710003</p> <p>nessun messaggio di registrazione 106100</p> <p>nessun messaggio di registrazione 302015</p> <p>nessun messaggio di registrazione 302014</p> <p>nessun messaggio di registrazione 302013</p> <p>nessun messaggio di registrazione 302018</p> <p>nessun messaggio di registrazione 302017</p>
--	--

mtu esterna a 1500 mtu diagnostic 1500 mtu all'interno di 1500 failover unità lan di failover secondaria failover interfaccia lan FOVER Port-channel3 http per la replica di failover collegamento di failover FOVER Port-channel3 interfaccia di failover ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2  <output omissa>	nessun messaggio di registrazione 302016 nessun messaggio di logging 302021 nessun messaggio di registrazione 302020 mtu esterna a 1500 mtu diagnostic 1500 mtu all'interno di 1500 nessun failover nessuna interfaccia monitor esterna no monitor-interface service-module  <output omissa>
---	--

Considerazioni principali per la separazione della coppia HA:

Unità principale/standby	Unità secondaria/attiva
<ul style="list-style-type: none"> <li>• Tutta la configurazione di failover è stata rimossa</li> <li>• Tutta la configurazione IP è stata rimossa</li> </ul>	<ul style="list-style-type: none"> <li>• Tutta la configurazione di failover è stata rimossa</li> <li>• Gli IP in standby rimangono, ma vengono rimossi nella distribuzione successiva</li> </ul>

Passaggio 5. Al termine dell'operazione, ricreare la coppia HA.

## Attività 6. Eliminare una coppia HA

Questa attività si basa su un'installazione HA su 41xx con software 7.2.8. In questo caso, inizialmente i dispositivi si trovavano nei seguenti stati:

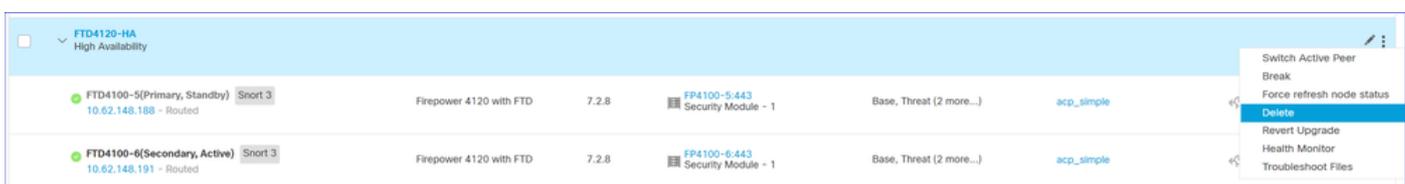
- Principale/Standby
- Secondario/Attivo

Attività richiesta:

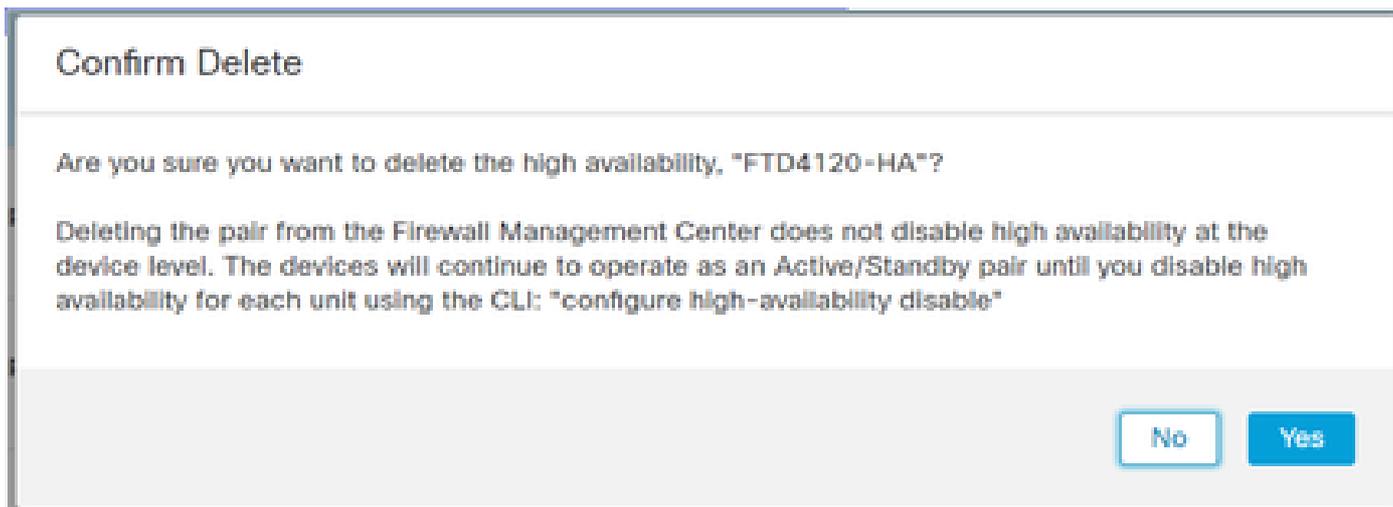
Eliminare la coppia di failover dal FMC.

Soluzione:

Passaggio 1. Scegliere l'icona come illustrato nell'immagine:



Passaggio 2. Controllare la notifica e confermare come mostrato nell'immagine:



Passaggio 3. Dopo aver eliminato l'HA, entrambe le periferiche vengono rimosse dalla FMC.

Output del comando show running-config dalla CLI LINA:

Unità principale (standby)	Unità secondaria (attiva)
<pre>&gt; show running-config : salvato : : numero di serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB di RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) : NGFW versione 7.2.8 ! hostname Firepower-module1 abilita password **** crittografata strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico ! interface Port-channel2 no nameif nessun livello di protezione nessun indirizzo ip !</pre>	<pre>&gt; show running-config : salvato : : Numero di serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB di RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) : NGFW versione 7.2.8 ! hostname Firepower-module1 abilita password **** crittografata strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 modulo di servizio 0 keepalive-counter 6 nomi nessun indirizzo mac automatico ! interface Port-channel2 no nameif nessun livello di protezione nessun indirizzo ip !</pre>

<pre> interface Port-channel 2.202 vlan 202 nameif NET202 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel 2.203 vlan 203 nameif NET203 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.203.1 255.255.255.0 standby 172.16.203.2 ! interface Port-channel3 descrizione Interfaccia di failover LAN/STATE ! interfaccia Ethernet1/1 solo gestione diagnostica nameif manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 nessun indirizzo ip ! interfaccia Ethernet1/4 nameif NET204 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! modalità ftp passiva ngips conn-match vlan-id nessun controllo di accesso object-group-search access-group CSM_FW_ACL_ globale access-list CSM_FW_ACL_ note rule-id 9998: </pre>	<pre> interface Port-channel 2.202 vlan 202 nameif NET202 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel 2.203 vlan 203 nameif NET203 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.203.1 255.255.255.0 standby 172.16.203.2 ! interface Port-channel3 descrizione Interfaccia di failover LAN/STATE ! interfaccia Ethernet1/1 solo gestione diagnostica nameif manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 nessun indirizzo ip ! interfaccia Ethernet1/4 nameif NET204 manuale cat propagazione di sgt preserve-untag criterio statico sgt disabilitato attendibile livello di protezione 0 indirizzo ip 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! modalità ftp passiva ngips conn-match vlan-id nessun controllo di accesso object-group-search access-group CSM_FW_ACL_ globale access-list CSM_FW_ACL_ note rule-id 9998: </pre>
--	--

PREFILTER POLICY: Criterio di priorità e tunnel predefinito  
access-list CSM\_FW\_ACL\_ note rule-id 9998:  
RULE: DEFAULT TUNNEL ACTION RULE  
access-list CSM\_FW\_ACL\_ advanced allow ipinip any rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow udp any eq 3544 any range 1025 65535 rule-id 9998  
  
access-list CSM\_FW\_ACL\_ advanced allow udp qualsiasi intervallo 1025 65535 any eq 3544 rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow 41 qualsiasi rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow gre any rule-id 9998  
access-list CSM\_FW\_ACL\_ note rule-id 268434433: ACCESS POLICY: acp\_simple - Default  
access-list CSM\_FW\_ACL\_ note rule-id 268434433: L4 RULE: DEFAULT ACTION RULE  
access-list CSM\_FW\_ACL\_ advanced permission ip any rule-id 268434433  
!  
tcp-map UM\_STATIC\_TCP\_MAP  
intervallo di opzioni tcp 6/7 consentito  
intervallo di opzioni tcp 9 18 consentito  
intervallo di opzioni tcp 20-255 consentito  
tcp-options md5 clear  
consenti contrassegno urgente  
!  
nessun cercapersone  
nessun messaggio di registrazione 106015  
nessun messaggio di logging 313001  
nessun messaggio di registrazione 313008  
nessun messaggio di registrazione 106023  
nessun messaggio di registrazione 710003  
nessun messaggio di registrazione 106100  
nessun messaggio di registrazione 302015  
nessun messaggio di registrazione 302014  
nessun messaggio di registrazione 302013  
nessun messaggio di registrazione 302018  
nessun messaggio di registrazione 302017  
nessun messaggio di registrazione 302016  
nessun messaggio di logging 302021

PREFILTER POLICY: Criterio di priorità e tunnel predefinito  
access-list CSM\_FW\_ACL\_ note rule-id 9998:  
RULE: DEFAULT TUNNEL ACTION RULE  
access-list CSM\_FW\_ACL\_ advanced allow ipinip any rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow udp any eq 3544 any range 1025 65535 rule-id 9998  
  
access-list CSM\_FW\_ACL\_ advanced allow udp qualsiasi intervallo 1025 65535 any eq 3544 rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow 41 qualsiasi rule-id 9998  
access-list CSM\_FW\_ACL\_ advanced allow gre any rule-id 9998  
access-list CSM\_FW\_ACL\_ note rule-id 268434433: ACCESS POLICY: acp\_simple - Default  
access-list CSM\_FW\_ACL\_ note rule-id 268434433: L4 RULE: DEFAULT ACTION RULE  
access-list CSM\_FW\_ACL\_ advanced permission ip any rule-id 268434433  
!  
tcp-map UM\_STATIC\_TCP\_MAP  
intervallo di opzioni tcp 6/7 consentito  
intervallo di opzioni tcp 9 18 consentito  
intervallo di opzioni tcp 20-255 consentito  
tcp-options md5 clear  
consenti contrassegno urgente  
!  
nessun cercapersone  
nessun messaggio di registrazione 106015  
nessun messaggio di logging 313001  
nessun messaggio di registrazione 313008  
nessun messaggio di registrazione 106023  
nessun messaggio di registrazione 710003  
nessun messaggio di registrazione 106100  
nessun messaggio di registrazione 302015  
nessun messaggio di registrazione 302014  
nessun messaggio di registrazione 302013  
nessun messaggio di registrazione 302018  
nessun messaggio di registrazione 302017  
nessun messaggio di registrazione 302016  
nessun messaggio di logging 302021

```
nessun messaggio di registrazione 302020
mtu NET 202 1500
mtu NET 203 1500
mtu diagnostic 1500
mtu NET 204 1500
failover
unità lan di failover principale
failover interfaccia lan FOVER Port-channel3
http per la replica di failover
collegamento di failover FOVER Port-channel3
interfaccia di failover ip FOVER 172.16.51.1
255.255.255.0 standby 172.16.51.2
monitor-interface NET202
interfaccia monitor NET203
icmp unreachable rate-limit 1 burst-size 1

<output omissa>
```

```
> mostra ip
Indirizzi IP di sistema:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel 2.202 NET20 172.16.202.1
255.255.255.0 CONFIG
Port-channel 2.203 NET203 172.16.203.1
255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1
255.255.255.0 CONFIG
Indirizzi IP correnti:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel 2.202 NET20 172.16.202.2
255.255.255.0 CONFIG
Port-channel 2.203 NET203 172.16.203.2
255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.2
255.255.255.0 CONFIG
```

```
> mostra failover
Failover attivato
Unità di failover primaria
Interfaccia LAN di failover: FOVER Port-
```

```
nessun messaggio di registrazione 302020
mtu NET 202 1500
mtu NET 203 1500
mtu diagnostic 1500
mtu NET 204 1500
failover
unità lan di failover secondaria
failover interfaccia lan FOVER Port-channel3
http per la replica di failover
collegamento di failover FOVER Port-channel3
interfaccia di failover ip FOVER 172.16.51.1
255.255.255.0 standby 172.16.51.2
monitor-interface NET202
interfaccia monitor NET203
icmp unreachable rate-limit 1 burst-size 1

<output omissa>
```

```
> mostra ip
Indirizzi IP di sistema:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel 2.202 NET20 172.16.202.1
255.255.255.0 CONFIG
Port-channel 2.203 NET203 172.16.203.1
255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1
255.255.255.0 CONFIG
Indirizzi IP correnti:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel 2.202 NET20 172.16.202.1
255.255.255.0 CONFIG
Port-channel 2.203 NET203 172.16.203.1
255.255.255.0 CONFIG
Port-channel3 FOVER 172.16.51.2
255.255.255.0 non impostato
Ethernet1/4 NET204 172.16.204.1
255.255.255.0 CONFIG
```

```
> mostra failover
Failover attivato
Unità di failover secondaria
Interfaccia LAN di failover: FOVER Port-
```

channel3 (up)  
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 1291 massimo  
Intervallo di notifica spostamento indirizzo MAC non impostato  
http per la replica di failover  
Versione: 9.18(4)210, Mate 9.18(4)210  
Numero di serie: FLM1949C5RR, Mate FLM2108V9YG  
Ultimo failover alle: 13:56:37 UTC lug 16 2024  
Host: primario - pronto per lo standby  
Tempo di attività: 0 (sec)  
Slot 0: UCSB-B200-M3-U hw/sw rev (0,0/9,18(4)210) status (Up Sys)  
Interfaccia NET202 (172.16.202.2): normale (monitorata)  
Interfaccia NET203 (172.16.203.2): normale (monitorata)  
Diagnostica interfaccia (0.0.0.0): normale (in attesa)  
Interfaccia NET204 (172.16.204.2): normale (monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)  
Altro host: secondario - attivo  
Tempo di attività: 70293 (sec)  
Interfaccia NET202 (172.16.202.1): normale (monitorata)  
Interfaccia NET203 (172.16.203.1): normale (monitorata)  
Diagnostica interfaccia (0.0.0.0): normale (in attesa)  
Interfaccia NET204 (172.16.204.1): normale (monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)

<output omissa>

channel3 (up)  
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 1291 massimo  
Intervallo di notifica spostamento indirizzo MAC non impostato  
http per la replica di failover  
Versione: 9.18(4)210, Mate 9.18(4)210  
Numero di serie: FLM2108V9YG, Mate FLM1949C5RR  
Ultimo failover alle: 13:42:35 UTC lug 16 2024  
Host corrente: secondario - attivo  
Tempo di attività: 70312 (sec)  
Slot 0: UCSB-B200-M3-U hw/sw rev (0,0/9,18(4)210) status (Up Sys)  
Interfaccia NET202 (172.16.202.1): normale (monitorata)  
Interfaccia NET203 (172.16.203.1): normale (monitorata)  
Diagnostica interfaccia (0.0.0.0): normale (in attesa)  
Interfaccia NET204 (172.16.204.1): normale (monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)  
Altro host: primario - pronto per lo standby  
Tempo di attività: 0 (sec)  
Slot 0: UCSB-B200-M3-U hw/sw rev (0,0/9,18(4)210) status (Up Sys)  
Interfaccia NET202 (172.16.202.2): normale (monitorata)  
Interfaccia NET203 (172.16.203.2): normale (monitorata)  
Diagnostica interfaccia (0.0.0.0): normale (in attesa)  
Interfaccia NET204 (172.16.204.2): normale (monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)

<output omissa>

Passaggio 4. La registrazione di entrambi i dispositivi FTD è stata annullata dal CCP:

```
<#root>
```

```
> show managers
```

```
No managers configured.
```

Considerazioni principali per la disabilitazione della coppia HA nell'FMC:

Unità Principale	Unità Secondaria
Il dispositivo viene rimosso dall'FMC. Nessuna configurazione rimossa dal dispositivo FTD.	Il dispositivo viene rimosso dall'FMC. Nessuna configurazione rimossa dal dispositivo FTD.

Scenario 1

Eseguire il comando 'configure high-availability disable' per rimuovere la configurazione di failover dal dispositivo FTD attivo:

```
<#root>
```

```
>
```

```
configure high-availability disable
```

```
?
```

```
Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear-interfaces)  
<cr>
```

```
<#root>
```

```
>
```

```
configure high-availability disable
```

```
High-availability will be disabled. Do you really want to continue?  
Please enter 'YES' or 'NO':
```

```
yes
```

```
Successfully disabled high-availability.
```

Il risultato:

Unità primaria (ex standby)	Unità secondaria (ex attiva)
<p>&gt; <b>INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state.</b></p> <p>&gt; show failover  <b>Failover Off (pseudo-Standby)</b>  <b>Failover unit Primary</b>  <b>Failover LAN Interface: FOVER Port-channel3 (up)</b>  <b>Reconnect timeout 0:00:00</b>  <b>Unit Poll frequency 1 seconds, holdtime 15 seconds</b>  <b>Interface Poll frequency 5 seconds, holdtime 25 seconds</b>  <b>Interface Policy 1</b>  <b>Monitored Interfaces 0 of 1291 maximum</b>  <b>MAC Address Move Notification Interval not set</b>  <b>failover replication http</b></p> <p>&gt; show ip  <b>System IP Addresses:</b>  <b>Interface Name IP address Subnet mask Method</b>  <b>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset</b>  <b>Current IP Addresses:</b>  <b>Interface Name IP address Subnet mask Method</b>  <b>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset</b></p>	<p>&gt; show failover  <b>Failover Off</b>  <b>Failover unit Secondary</b>  <b>Failover LAN Interface: not Configured</b>  <b>Reconnect timeout 0:00:00</b>  <b>Unit Poll frequency 1 seconds, holdtime 15 seconds</b>  <b>Interface Poll frequency 5 seconds, holdtime 25 seconds</b>  <b>Interface Policy 1</b>  <b>Monitored Interfaces 4 of 1291 maximum</b>  <b>MAC Address Move Notification Interval not set</b></p> <p>&gt; show ip  <b>System IP Addresses:</b>  <b>Interface Name IP address Subnet mask Method</b>  <b>Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG</b>  <b>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG</b>  <b>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG</b>  <b>Current IP Addresses:</b>  <b>Interface Name IP address Subnet mask Method</b>  <b>Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG</b>  <b>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG</b>  <b>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG</b></p>
Principale (ex standby)	Secondario (ex attivo)
<p>&gt; show running-config  : salvato</p> <p>:</p> <p>: numero di serie: FLM1949C5RR</p> <p>: Hardware: FPR4K-SM-24, 73853 MB di RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core)</p> <p>:</p>	<p>&gt; show running-config  : salvato</p> <p>:</p> <p>: Numero di serie: FLM2108V9YG</p> <p>: Hardware: FPR4K-SM-24, 73853 MB di RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core)</p> <p>:</p>

```

NGFW versione 7.2.8
!
hostname Firepower-module1
abilita password **** crittografata
strong-encryption-disable
no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4
modulo di servizio 0 keepalive-counter 6
nomi
nessun indirizzo mac automatico

!
interface Port-channel2
shutdown
no nameif
nessun livello di protezione
nessun indirizzo ip <- gli IP vengono rimossi
!
interface Port-channel3
descrizione Interfaccia di failover LAN/STATE
!
interfaccia Ethernet1/1
solo gestione
shutdown
no nameif
nessun livello di protezione
nessun indirizzo ip
!
interfaccia Ethernet1/4
shutdown
no nameif
nessun livello di protezione
nessun indirizzo ip
!
modalità ftp passiva
ngips conn-match vlan-id
nessun controllo di accesso object-group-search
access-group CSM_FW_ACL_ globale
access-list CSM_FW_ACL_ note rule-id 9998:
PREFIXER POLICY: Criterio di priorità e tunnel
predefinito
access-list CSM_FW_ACL_ note rule-id 9998:
RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced allow
ipinip any rule-id 9998
access-list CSM_FW_ACL_ advanced allow udp

```

```

NGFW versione 7.2.8
!
hostname Firepower-module1
abilita password **** crittografata
strong-encryption-disable
no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4
modulo di servizio 0 keepalive-counter 6
nomi
nessun indirizzo mac automatico

!
interface Port-channel2
no nameif
nessun livello di protezione
nessun indirizzo ip
!
interface Port-channel 2.202
vlan 202
nameif NET202
manuale cat
propagazione di sgt preserve-untag
criterio statico sgt disabilitato attendibile
livello di protezione 0
indirizzo ip 172.16.202.1 255.255.255.0 standby
172.16.202.2
!
interface Port-channel 2.203
vlan 203
nameif NET203
manuale cat
propagazione di sgt preserve-untag
criterio statico sgt disabilitato attendibile
livello di protezione 0
indirizzo ip 172.16.203.1 255.255.255.0 standby
172.16.203.2
!
interface Port-channel3
no nameif
nessun livello di protezione
nessun indirizzo ip
!
interfaccia Ethernet1/1
solo gestione
diagnostica nameif
manuale cat

```

<p>any eq 3544 any range 1025 65535 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp qualsiasi intervallo 1025 65535 any eq 3544 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow 41 qualsiasi rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow gre any rule-id 9998</p> <p>access-list CSM_FW_ACL_ note rule-id 268434433: ACCESS POLICY: acp_simple - Default</p> <p>access-list CSM_FW_ACL_ note rule-id 268434433: L4 RULE: DEFAULT ACTION RULE</p> <p>access-list CSM_FW_ACL_ advanced permission ip any rule-id 268434433</p> <p>!</p> <p>tcp-map UM_STATIC_TCP_MAP intervallo di opzioni tcp 6/7 consentito intervallo di opzioni tcp 9 18 consentito intervallo di opzioni tcp 20-255 consentito tcp-options md5 clear consenti contrassegno urgente</p> <p>!</p> <p>nessun cercapersone</p> <p>nessun messaggio di registrazione 106015</p> <p>nessun messaggio di logging 313001</p> <p>nessun messaggio di registrazione 313008</p> <p>nessun messaggio di registrazione 106023</p> <p>nessun messaggio di registrazione 710003</p> <p>nessun messaggio di registrazione 106100</p> <p>nessun messaggio di registrazione 302015</p> <p>nessun messaggio di registrazione 302014</p> <p>nessun messaggio di registrazione 302013</p> <p>nessun messaggio di registrazione 302018</p> <p>nessun messaggio di registrazione 302017</p> <p>nessun messaggio di registrazione 302016</p> <p>nessun messaggio di logging 302021</p> <p>nessun messaggio di registrazione 302020</p> <p>nessun failover</p> <p>unità lan di failover principale</p> <p>failover interfaccia lan FOVER Port-channel3 http per la replica di failover</p> <p>collegamento di failover FOVER Port-channel3</p> <p>interfaccia di failover ip FOVER 172.16.51.1</p>	<p>propagazione di sgt preserve-untag</p> <p>criterio statico sgt disabilitato attendibile</p> <p>livello di protezione 0</p> <p>nessun indirizzo ip</p> <p>!</p> <p>interfaccia Ethernet1/4</p> <p>nameif NET204</p> <p>manuale cat</p> <p>propagazione di sgt preserve-untag</p> <p>criterio statico sgt disabilitato attendibile</p> <p>livello di protezione 0</p> <p>indirizzo ip 172.16.204.1 255.255.255.0 standby 172.16.204.2</p> <p>!</p> <p>modalità ftp passiva</p> <p>ngips conn-match vlan-id</p> <p>nessun controllo di accesso object-group-search</p> <p>access-group CSM_FW_ACL_ globale</p> <p>access-list CSM_FW_ACL_ note rule-id 9998: PREFILTER POLICY: Criterio di priorità e tunnel predefinito</p> <p>access-list CSM_FW_ACL_ note rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE</p> <p>access-list CSM_FW_ACL_ advanced allow ipinip any rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp any eq 3544 any range 1025 65535 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow udp qualsiasi intervallo 1025 65535 any eq 3544 rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow 41 qualsiasi rule-id 9998</p> <p>access-list CSM_FW_ACL_ advanced allow gre any rule-id 9998</p> <p>access-list CSM_FW_ACL_ note rule-id 268434433: ACCESS POLICY: acp_simple - Default</p> <p>access-list CSM_FW_ACL_ note rule-id 268434433: L4 RULE: DEFAULT ACTION RULE</p> <p>access-list CSM_FW_ACL_ advanced permission ip any rule-id 268434433</p> <p>!</p> <p>tcp-map UM_STATIC_TCP_MAP intervallo di opzioni tcp 6/7 consentito</p>
---	---

<p>255.255.255.0 standby 172.16.51.2 no monitor-interface service-module</p> <p>&lt;output omissa&gt;</p>	<p>intervallo di opzioni tcp 9 18 consentito intervallo di opzioni tcp 20-255 consentito tcp-options md5 clear consenti contrassegno urgente ! nessun cercapersone nessun messaggio di registrazione 106015 nessun messaggio di logging 313001 nessun messaggio di registrazione 313008 nessun messaggio di registrazione 106023 nessun messaggio di registrazione 710003 nessun messaggio di registrazione 106100 nessun messaggio di registrazione 302015 nessun messaggio di registrazione 302014 nessun messaggio di registrazione 302013 nessun messaggio di registrazione 302018 nessun messaggio di registrazione 302017 nessun messaggio di registrazione 302016 nessun messaggio di logging 302021 nessun messaggio di registrazione 302020 mtu NET 202 1500 mtu NET 203 1500 mtu diagnostic 1500 mtu NET 204 1500 nessun failover monitor-interface NET202 interfaccia monitor NET203 no monitor-interface service-module</p>
---	---

Note principali per Disabilitare HA dalla CLI FTD attiva:

Unità attiva	Unità di standby
<ul style="list-style-type: none"> <li>• Configurazione di failover rimossa</li> <li>• Gli IP in standby non vengono rimossi</li> </ul>	<ul style="list-style-type: none"> <li>• Le configurazioni delle interfacce sono state rimosse.</li> <li>• La configurazione di failover non viene rimossa, ma il failover è disabilitato (pseudo-standby)</li> </ul>

A questo punto è possibile disattivare HA anche sull'unità ex-Standby.

Scenario 2 (non consigliato)

 **Avviso:** questo scenario determina una situazione di attività/attività, pertanto non è consigliato. È mostrato solo per la consapevolezza.

Eseguire il comando 'configure high-availability disable' per rimuovere la configurazione del failover dal dispositivo FTD in standby:

```
<#root>
```

```
>
```

```
configure high-availability disable
```

```
High-availability will be disabled. Do you really want to continue?  
Please enter 'YES' or 'NO':
```

```
YES
```

```
Successfully disabled high-availability.
```

Il risultato:

Principale (ex standby)	Secondario (attivo)
<pre>&gt; mostra failover Failover disattivato Unità di failover secondaria Interfaccia LAN di failover: non configurata 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 1291 massimo Intervallo di notifica spostamento indirizzo MAC non impostato  &gt; mostra ip Indirizzi IP di sistema: Nome interfaccia Indirizzo IP Subnet mask, metodo Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuale &lt;- Il dispositivo utilizza</pre>	<pre>&gt; mostra failover Failover su &lt;- Failover non disabilitato Unità di failover secondaria Interfaccia LAN di failover: FOVER Port- channel3 (up) 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 1291 massimo Intervallo di notifica spostamento indirizzo MAC non impostato http per la replica di failover Versione: 9.18(4)210, Mate 9.18(4)210 Numero di serie: FLM2108V9YG, Mate FLM1949C5RR Ultimo failover alle: 12:44:06 UTC lug 17 2024 Host corrente: secondario - attivo Tempo di attività: 632 (sec)</pre>

gli stessi indirizzi IP dell'ex-Active!  
Port-channel 2.203 NET203 172.16.203.1  
255.255.255.0 manuale  
Manuale Ethernet1/4 NET204 172.16.204.1  
255.255.255.0  
Indirizzi IP correnti:  
Nome interfaccia Indirizzo IP Subnet mask,  
metodo  
Port-channel 2.202 NET20 172.16.202.1  
255.255.255.0 manuale  
Port-channel 2.203 NET203 172.16.203.1  
255.255.255.0 manuale  
Manuale Ethernet1/4 NET204 172.16.204.1  
255.255.255.0

Slot 0: UCSB-B200-M3-U hw/sw rev  
(0,0/9,18(4)210) status (Up Sys)  
Diagnostica interfaccia (0.0.0.0): normale (in  
attesa)  
Interfaccia NET204 (172.16.204.1): normale  
(monitorata)  
Interfaccia NET203 (172.16.203.1): normale  
(monitorata)  
Interfaccia NET202 (172.16.202.1): normale  
(monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)  
Altro host: Primario - Disabilitato  
Tempo di attività: 932 (sec)  
Slot 0: UCSB-B200-M3-U hw/sw rev  
(0,0/9,18(4)210) status (Up Sys)  
Diagnostica interfaccia (0.0.0.0): sconosciuta (in  
attesa)  
Interfaccia NET204 (172.16.204.2): sconosciuta  
(monitorata)  
Interfaccia NET203 (172.16.203.2): sconosciuta  
(monitorata)  
Interfaccia NET202 (172.16.202.2): sconosciuta  
(monitorata)  
slot 1: stato snort rev (1.0) (su)  
slot 2: stato rev diskstatus (1.0) (su)  
  
> mostra ip  
Indirizzi IP di sistema:  
Nome interfaccia Indirizzo IP Subnet mask,  
metodo  
Port-channel 2.202 NET202 172.16.202.1  
255.255.255.0 manuale <- Il dispositivo utilizza  
gli stessi IP dell'ex-standby!  
Port-channel 2.203 NET203 172.16.203.1  
255.255.255.0 manuale  
Port-channel 3 FOVER 172.16.51.1  
255.255.255.0 unset  
Manuale Ethernet1/4 NET204 172.16.204.1  
255.255.255.0  
Indirizzi IP correnti:  
Nome interfaccia Indirizzo IP Subnet mask,  
metodo  
Port-channel 2.202 NET20 172.16.202.1  
255.255.255.0 manuale  
Port-channel 2.203 NET203 172.16.203.1

	255.255.255.0 manuale Port-channel3 FOVER 172.16.51.2 255.255.255.0 non impostato Manuale Ethernet1/4 NET204 172.16.204.1 255.255.255.0
--	---

Note principali per Disabilitare HA dalla CLI FTD attiva:

Unità attiva	Unità di standby
<ul style="list-style-type: none"> <li>• La configurazione di failover non viene rimossa e rimane abilitata</li> <li>• Il dispositivo usa gli stessi IP dell'unità ex-Standby</li> </ul>	<ul style="list-style-type: none"> <li>• Configurazione di failover rimossa</li> <li>• Il dispositivo utilizza gli stessi IP dell'unità attiva</li> </ul>

### Scenario 3

Eseguire il comando 'configure high-availability disable clear-interfaces' per rimuovere la configurazione di failover dal dispositivo FTD attivo:

```
<#root>
```

```
>
```

```
configure high-availability disable clear-interfaces
```

```
High-availability will be disabled. Do you really want to continue?  
Please enter 'YES' or 'NO':
```

```
yes
```

```
Successfully disabled high-availability.
```

```
>
```

Il risultato:

Principale (ex standby)	Secondario (ex attivo)
<pre>&gt; mostra failover Failover disattivato (pseudo standby) Unità di failover primaria</pre>	<pre>&gt; mostra failover Failover disattivato Unità di failover secondaria</pre>

<p>Interfaccia LAN di failover: FOVER Port-channel3 (up)  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 0 di 1291 massimo  Intervallo di notifica spostamento indirizzo MAC non impostato  http per la replica di failover</p> <p>&gt; mostra ip  Indirizzi IP di sistema:  Nome interfaccia Indirizzo IP Subnet mask, metodo  Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset  Indirizzi IP correnti:  Nome interfaccia Indirizzo IP Subnet mask, metodo  Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset  &gt;</p>	<p>Interfaccia LAN di failover: non configurata  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 0 di 1291 massimo  Intervallo di notifica spostamento indirizzo MAC non impostato</p> <p>&gt; mostra ip  Indirizzi IP di sistema:  Nome interfaccia Indirizzo IP Subnet mask, metodo  Indirizzi IP correnti:  Nome interfaccia Indirizzo IP Subnet mask, metodo  &gt;</p>
--	--

Principali punti da notare per Disable HA insieme a 'clear-interfaces' da Active FTD CLI:

Unità attiva	Unità di standby
<ul style="list-style-type: none"> <li>• Configurazione di failover rimossa</li> <li>• Gli IP vengono rimossi</li> </ul>	<ul style="list-style-type: none"> <li>• La configurazione di failover non viene rimossa, ma il failover è disabilitato (pseudo-standby)</li> <li>• Gli IP vengono rimossi</li> </ul>

#### Scenario 4

Eseguire il comando 'configure high-availability disable clear-interfaces' per rimuovere la configurazione del failover dal dispositivo FTD in standby:

<#root>

>

```
configure high-availability disable clear-interfaces
```

High-availability will be disabled. Do you really want to continue?  
Please enter 'YES' or 'NO':

YES

Successfully disabled high-availability.

>

Il risultato:

Principale (ex standby)	Secondario (attivo)
> mostra failover Failover disattivato Unità di failover secondaria Interfaccia LAN di failover: non configurata 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 0 di 1291 massimo Intervallo di notifica spostamento indirizzo MAC non impostato	> mostra failover Failover attivato Unità di failover secondaria Interfaccia LAN di failover: FOVER Port-channel3 (up) 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 1291 massimo Intervallo di notifica spostamento indirizzo MAC non impostato http per la replica di failover Versione: 9.18(4)210, Mate 9.18(4)210 Numero di serie: FLM2108V9YG, Mate FLM1949C5RR
> mostra ip Indirizzi IP di sistema: Nome interfaccia Indirizzo IP Subnet mask, metodo Indirizzi IP correnti: Nome interfaccia Indirizzo IP Subnet mask, metodo	Ultimo failover alle: 07:06:56 UTC lug 18 2024 Host corrente: secondario - attivo Tempo di attività: 1194 (sec) Slot 0: UCSB-B200-M3-U hw/sw rev (0,0/9,18(4)210) status (Up Sys) Diagnostica interfaccia (0.0.0.0): normale (in attesa) Interfaccia NET204 (172.16.204.1): normale (monitorata) Interfaccia NET202 (172.16.202.1): normale (monitorata)

```

Interfaccia NET203 (172.16.203.1): normale
(monitorata)
slot 1: stato snort rev (1.0) (su)
slot 2: stato rev diskstatus (1.0) (su)
Altro host: Primario - Disabilitato
Tempo di attività: 846 (sec)
Slot 0: UCSB-B200-M3-U hw/sw rev
(0,0/9,18(4)210) status (Up Sys)
Diagnostica interfaccia (0.0.0.0): sconosciuta (in
attesa)
Interfaccia NET204 (172.16.204.2): sconosciuta
(monitorata)
Interfaccia NET202 (172.16.202.2): sconosciuta
(monitorata)
Interfaccia NET203 (172.16.203.2): sconosciuta
(monitorata)
slot 1: stato snort rev (1.0) (su)
slot 2: stato rev diskstatus (1.0) (su)

> mostra ip
Indirizzi IP di sistema:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel2.202 NET20 172.16.202.1
255.255.255.0 manuale
Port-channel 2.203 NET203 172.16.203.1
255.255.255.0 manuale
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Manuale Ethernet1/4 NET204 172.16.204.1
255.255.255.0
Indirizzi IP correnti:
Nome interfaccia Indirizzo IP Subnet mask,
metodo
Port-channel2.202 NET20 172.16.202.1
255.255.255.0 manuale
Port-channel 2.203 NET203 172.16.203.1
255.255.255.0 manuale
Port-channel3 FOVER 172.16.51.2
255.255.255.0 non impostato
Manuale Ethernet1/4 NET204 172.16.204.1
255.255.255.0

```

Principali punti da notare per Disable HA insieme a 'clear-interfaces' da Active FTD CLI:

Unità attiva	Unità di standby
<ul style="list-style-type: none"> <li>• Configurazione di failover non rimossa</li> <li>• Gli indirizzi IP non vengono rimossi</li> </ul>	<ul style="list-style-type: none"> <li>• Configurazione di failover rimossa</li> <li>• Gli IP vengono rimossi</li> </ul>

Passaggio 6. Al termine dell'operazione, registrare i dispositivi nel FMC e abilitare la coppia HA.

## Attività 7. Sospendi HA

Attività richiesta:

Sospendere la coppia HA dalla CLI CLISH dell'FTD

Soluzione:

Passaggio 1. Nell'FTD principale eseguire il comando e confermare (digitare YES).

```
<#root>
```

```
> configure high-availability suspend
```

```
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to
```

```
YES
```

```
Successfully suspended high-availability.
```

Passaggio 2. Verificare le modifiche sull'unità principale:

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover Off
```

```
Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```



Passaggio 5. Il risultato sull'unità secondaria dopo la ripresa di HA:

```
<#root>
```

```
> ..
```

```
Detected an Active mate
```

```
Beginning configuration replication from mate.
```

```
WARNING: Failover is enabled but standby IP address is not configured for this interface.  
WARNING: Failover is enabled but standby IP address is not configured for this interface.  
End configuration replication from mate.
```

```
>
```

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
```

```
Failover unit Secondary  
Failover LAN Interface: fover_link Ethernet1/4 (up)  
Reconnect timeout 0:00:00  
Unit Poll frequency 1 seconds, holdtime 15 seconds  
Interface Poll frequency 5 seconds, holdtime 25 seconds  
Interface Policy 1  
Monitored Interfaces 1 of 1041 maximum  
MAC Address Move Notification Interval not set  
failover replication http  
>
```

## Domande frequenti (FAQ)

Quando la configurazione viene replicata, viene salvata immediatamente (riga per riga) o al termine della replica?

Alla fine della replica. Fare riferimento alla fine dell'output del comando `debug fover sync` che mostra la replica della configurazione/del comando:

```
<#root>
```

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL  
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group  
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
```

```

cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:

write memory      <--

```

Cosa succede se un'unità si trova in uno stato di pseudo-standby (failover disabilitato) e viene ricaricata mentre l'altra unità ha il failover abilitato ed è attiva?

Si finisce in uno scenario Attivo/Attivo (anche se tecnicamente si tratta di uno scenario Attivo/Failover-off). In particolare, dopo aver attivato l'unità, il failover viene disabilitato, ma l'unità utilizza gli stessi IP dell'unità Attiva. In realtà, si ha quindi:

- Unità-1: attiva
- Unità 2: failover disattivato. L'unità utilizza gli stessi IP dati dell'unità 1, ma indirizzi MAC diversi.

Cosa succede alla configurazione del failover se il failover viene disabilitato manualmente (configurazione della sospensione a disponibilità elevata) e il dispositivo viene ricaricato? Quando si disabilita il failover, non si tratta di una modifica permanente (non viene salvata nella configurazione di avvio a meno che non si decida di farlo in modo esplicito). È possibile riavviare/ricaricare l'unità in due modi diversi e con il secondo occorre prestare attenzione:

### Caso 1. Riavvio da CLISH

Il riavvio dalla CLISH non richiede conferma. Pertanto, la modifica alla configurazione non viene salvata nella configurazione di avvio:

```
<#root>
```

```
>
```

```
configure high-availability suspend
```

```
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to
```

```
YES
```

```
Successfully suspended high-availability.
```

Failover disabilitato in running-config. In questo caso, l'unità era in modalità Standby ed è entrata nello stato pseudo-Standby come previsto per evitare uno scenario Attivo/Attivo:

```
<#root>
firepower#
show failover | include Failover

Failover Off (
pseudo-Standby
)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Il failover è ancora abilitato nella configurazione di avvio:

```
<#root>
firepower#
show startup | include failover

failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Riavviare il dispositivo dalla CLISH (comando reboot):

```
<#root>
>
reboot

This command will reboot the system. Continue?
Please enter 'YES' or 'NO':

YES

Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=' '
Cisco FTD stopping ...
```

Una volta attivata l'unità, poiché il failover è abilitato, il dispositivo passa nella fase di negoziazione del failover e tenta di rilevare il peer remoto:

```
<#root>
```

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

```
Detected an Active mate
```

## Caso 2. Riavvio dalla CLI di LINA

Il riavvio dalla CLI LINA con il comando reload deve essere confermato. Pertanto, se si seleziona Y (Sì), la modifica della configurazione viene salvata nella configurazione di avvio:

```
<#root>
```

```
firepower#
```

```
reload
```

```
System config has been modified. Save? [Y]es/[N]o:
```

```
Y <-- Be careful. This disables the failover in the startup-config
```

```
Cryptochecksum: 31857237 8658f618 3234be7c 854d583a
```

```
8781 bytes copied in 0.940 secs
```

```
Proceed with reload? [confirm]
```

```
firepower#
```

```
show startup | include failover
```

```
no failover
```

```
failover lan unit secondary
```

```
failover lan interface FOVER Ethernet1/1
```

```
failover replication http
```

```
failover link FOVER Ethernet1/1
```

```
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
```

```
failover ipsec pre-shared-key *****
```

Dopo l'attivazione dell'unità, il failover viene disabilitato:

```
<#root>
```

```
firepower#
```

```
show failover | include Fail
```

```
Failover Off
```

```
Failover unit Secondary
```

```
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

---

 Nota: per evitare questo scenario, accertarsi di non salvare le modifiche alla configurazione di avvio quando richiesto.

---

## Informazioni correlate

- Per le versioni della guida alla configurazione di Cisco Firepower Management Center, usare questo link:

### [Navigazione nella documentazione di Cisco Secure Firewall Threat Defense](#)

- Per le versioni delle guide alla configurazione di FXOS Chassis Manager e della CLI, usare questo link:

### [Navigazione nella documentazione di Cisco Firepower 4100/9300 FXOS](#)

- Cisco Global Technical Assistance Center (TAC) consiglia vivamente questa guida visiva per una conoscenza pratica e approfondita delle tecnologie di sicurezza di nuova generazione di Cisco Firepower:

### [Cisco Firepower Threat Defense \(FTD\): best practice per la configurazione e la risoluzione dei problemi per il firewall di nuova generazione \(NGFW\), il NGIPS \(Next-Generation Intrusion Prevention System\) e l'AMP \(Advanced Malware Protection\)](#)

- Note tecniche relative alle tecnologie Firepower per la configurazione e la risoluzione dei problemi

### [Cisco Secure Firewall Management Center](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)

## 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).