Configurazione della funzionalità FTD High Availability nei dispositivi Firepower

Sommario

| Introduzione |
|---------------------------------------|
| Prerequisiti |
| Requisiti |
| <u>Componenti usati</u> |
| 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-F | PR9K-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-FP | R9K-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 Snort 3 10.62.148.188 - Routed | Firepower 4120 with FTD | 7.2.8 | EP4100-5:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | ¢۶ | 1 |
|---|-------------------------|-------|-------------------------------------|-----------------------|------------|----|----|
| FTD4100-6 Snort 3 10.62.148.191 - Routed | Firepower 4120 with FTD | 7.2.8 | III Security Module - 1 | Base, Threat (2 more) | acp_simple | 49 | 1: |

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

| | Deployme | ent History |
|---------------|----------|-------------|
| Q Search De | evice | Add 🔻 |
| | Device | |
| | High A | vailability |
| Auto RollBack | Cluster | r |
| | Group | |
| | | |

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

| ion Charole Henney | - |
|---|--|
| Add High Availability Pair | l |
| Name:* | |
| FTD4100-HA | at () |
| Device Type: | |
| Firewall Threat Defense 🔻 | a C |
| Primary Peer: | |
| FTD4100-5 v | |
| Secondary Peer: | |
| FTD4100-6 v | |
| 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 | |
| | Add High Availability Pair Name:* FTD4100-HA Device Type: Firewall Threat Defense Frimary Peer: FTD4100-5 Primary Peer: FTD4100-6 Secondary Peer: FTD4100-6 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.

| ligh Availabi | lity Link | State Link | |
|---------------------------------|---|---|--|
| Interface:* | Port-channel3 | Interface:* | Same as LAN Failover Link |
| ogical Name:* | FOVER | Logical Name:* | FOVER |
| Primary IP:* | 172.16.51.1 | Primary IP:* | 172.16.51.1 |
| Ì | Use IPv6 Address | | 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 |
| Psec Encryp | tion | | |
| (ey Generation: | Auto | v. | |
| LAN failover I etween peers. | ink is used to sync configuration, sta Selected interface links and encrypti | teful failover link is used on settings cannot be cl | t to sync application content hanged later. |

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

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

#

| V FTD4120-HA High Availability | | | | | | | 1 |
|---|-------------------------|-------|--------------------------------------|-----------------------|------------|----|----------|
| FTD4100-5(Primary, Active) Short 3 10.62.148.188 - Routed | Firepower 4120 with FTD | 7.2.8 | EP4100-5:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | c? | : |
| FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed | Firepower 4120 with FTD | 7.2.8 | EFP4100-6:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | P | : |

Passaggio 5. Configurare le impostazioni dell'interfaccia:

| Edit Physical Interface | | | 0 |
|-------------------------------|---------------------|--|-----------|
| General IPv4 IPv6 Pat | Monitoring Advanced | | |
| Name: | | | |
| Inside | | | |
| Enabled | | | |
| Management Only | | | |
| Description: | | | |
| | | | |
| Mode: | | | |
| None + | | | |
| Security Zone: | | | |
| | | | |
| Interface ID: | | | |
| Ethernet1/4 | | | |
| MTU: | | | |
| 1500 | | | |
| (64 - 9184) | | | |
| Priority: | | | |
| 0 | (0 - 65535) | | |
| Propagate Security Group Tag: | | | |
| NVE Only: | | | |
| U | | | |
| | | | Cancel OK |

| General | IPv4 | IPv6 | Path Monitoring | Advanced | | |
|-----------------|-------------|--------------|-----------------|----------|--|--|
| P Type: | | | | | | |
| Use Static | IP | | v | | | |
| Address: | | | | | | |
| 192.168.7 | 5.10/24 | | | | | |
| | | | | | | |
| g. 192.0.2.1/2 | 255.255.255 | 5.128 or 19 | 2.0.2.1/25 | | | |
| g. 192.0.2.1/3 | 255.255.255 | 5.128 or 19 | 2.0.2.1/25 | | | |
| 7. 192.0.2.1/2 | 255.255.255 | 5.128 or 19 | 2.0.2.1/25 | | | |
| g. 192.0.2.1/3 | 255 255 251 | 5.128 or 19. | 2.0.2.1/25 | | | |
| g. 192.0.2.1/2 | 255.255.255 | 5.128 or 19 | 2.0.2.1/25 | | | |
| g. 192.0.2.1/2 | 255.255.25 | i. 128 or 19 | 2.0.2.1/25 | | | |
| ig. 192.0.2.1/2 | 255.255.25 | 5.128 or 19 | 2.0.2.1/25 | | | |

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

| Edit Ether | Channe | el Interfa | ace | | 0 |
|------------|-----------|------------|-----------------|----------|---|
| General | IPv4 | IPv6 | Path Monitoring | Advanced | |
| Name: | nent Only | | | | |

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

| Firewall Management Cen Devices / High Availability | ter _{Overview} | Analysis Policies | Devices Objects Integration | 'n | | | Deploy Q 💕 🌣 | 🛛 mzafeiro 🕶 | testes SECURE |
|--|-------------------------|--------------------|-----------------------------|----|--------------|------------------------|-------------------------|--------------|---------------|
| FTD4120-HA Cisco Firepower 4120 Threat Defense | | | | | | | | | e Cancel |
| Summary High Availability Device | e Routing Interfa- | ces Inline Sets DF | ICP VTEP | | | | | | |
| High Availability Configuration | | | | | | | | | |
| High Availability Link | | | | | State Link | | | | |
| Interface | | | Port-channel3 | | Interface | | | Port- | channel3 |
| Logical Name | | | FOVER | | Logical Name | | | | FOVER |
| Primary IP | | | 172.16.51.1 | | Primary IP | | | 172 | 2.16.51.1 |
| Secondary IP | | | 172.16.51.2 | | Secondary IP | | | 17: | 2.16.51.2 |
| Subnet Mask | | | 255.255.255.0 | | Subnet Mask | | | 255.2 | 55.255.0 |
| IPsec Encryption | | | Disabled | | Statistics | | | | Q |
| Monitored Interfaces | | | | | | | | | |
| Interface Name | Active IPv4 | Standby IPv4 | Active IPv6 - Standby IPv6 | | | Active Link-Local IPv6 | Standby Link-Local IPv6 | Monitoring | |
| Enside | 192.168.75.10 | | | | | | | • | 1 |
| diagnostic | | | | | | | | • | 1 |
| Outside | 192.168.76.10 | | | | | | | • | 1 |

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

| Edit Inside | 0 |
|---|----|
| 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 | ок |

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 IIPv6 - Standby IPv6 | Active Link-Local IPv6 | Standby Link-Local IPv6 | Monitoring | |
| 😭 Inside | 192.168.75.10 | 192.168.75.11 | | | | • | / |
| diagnostic | | | | | | • | / |
| Outside | 192.168.76.10 | 192.168.76.11 | | | | • | / |
| | | | | | | | |

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 | /1 |
| Port-channel2.202 | aaaa.bbbb.3333 | aaaa.bbbb.4444 | /1 |

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.

| Firewall Manage | gement Center Overview An | alysis Policies Devices | Objects Integratio | on | | Deploy Q | ¢ | 0 |
|---|--|-------------------------|--------------------|----|-----------------------------|----------|---|-----|
| FTD4120-HA Cisco Firepower 4120 Thre Summary High Avail | at Defense lability Device Routing Interfaces | Inline Sets DHCP VTEP | | | | | | |
| | | | | | | | | |
| | General | | /±∓ | | License | | | / |
| | Name: | | FTD4120-HA | | Base: | | 2 | fes |
| | Transfer Packets: | | Yes | | Export-Controlled Features: | | | No |
| | Status: | | • | | Malware: | | ٢ | /es |
| | Primary Peer: | | FTD4100-5(Active) | | Threat: | | ` | /es |
| | Secondary Peer: | | FTD4100-6(Standby) | | URL Filtering: | | 1 | /es |
| | Failover History: | | Q | | 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

| This host - | State Primary | Last Failure Reason | Date/Time |
|--|------------------------------|---------------------|---------------------------|
| Other host - | Active Secondary | None | |
| | Standby Ready | Comm Failure | 18:32:56 EEST Jul 21 2016 |
| ====Configurat Sync Done ====Communicat Mac set | ion State=== ion State=== | | |
| 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 1 interface Port-channel3 description LAN/STATE Failover Interface interface Ethernet1/1 management-only nameif diagnostic security-level 0 no ip address 1 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.

| FTD4120-HA High Availability | | | | | | | Switch Active Peer |
|--|-------------------------|-------|-------------------------------------|-----------------------|------------|----|---|
| FTD4100-5(Primary, Active) Short 3 10.62.148.188 - Routed | Firepower 4120 with FTD | 7.2.8 | ER Security Module - 1 | Base, Threat (2 more) | acp_simple | «Ø | Force refresh node status Delete Revert Upgrade |
| FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed | Firepower 4120 with FTD | 7.2.8 | EP4100-6:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | ¢9 | Health Monitor Troubleshoot Files |

Passaggio 2. Confermare l'azione.

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

| Sul nuovo Active Directory | | ll 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 config) | (Impostato con il comando | |
| 09:27:11 UTC lug 18 2024 Solo Active Drain L'altra unità mi vuole Active config) | (Impostato con il comando | > n ==: Da ==: |
| 09:27:11 UTC lug 18 2024 Active Drain Active Applying Config Other unit want me Active config) | (Impostato con il comando | 09: Att |
| 09:27:11 UTC lug 18 2024 Active Applying Config Active Config Applied Other unit want me Activ config) | e (Impostato con il comando | |
| 09:27:11 UTC lug 18 2024 Active Config Applied Active Other unit want me Active config) | (Impostato con il comando | |

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.

| × : |
|---------------------------|
| Switch Active Peer |
| Break |
| Force refresh node status |
| Delete |
| Revert Upgrade |
| Health Monitor |
| Troubleshoot Files |
| |

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



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

| Deployments Upgrades 0 Health 0 Tasks | how Notific | ation | s |
|--|-----------------|-------|---|
| 20+ total 0 waiting 0 running 0 retrying 20+ success 1 failure Q Filter | | |] |
| Policy Deployment Policy Deployment to FTD4100-5. Applied successfully | 47s | × | Í |
| Policy Pre-Deployment Pre-deploy Device Configuration for FTD4100-5 success | 3s | × | |
| Policy Pre-Deployment Pre-deploy Global Configuration Generation success | 4s | × | |
| High Availability HA pair has been broken successfully and all policies have been retained on active peer FTD4100-6. Standb peer FTD4100-5 policies are being deleted by an auto triggered deployment. Please allow this deployment to complete on FTD4100-5 before configuring its policies. | y <u>1m 59s</u> | × | |
| Remove completed tasks | | | |

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 |
|---|--|
| > show running-config : salvato | > INFORMAZIONI: l'apparecchio è attualmente in stato di standby. Disattivando il failover, l'apparecchio rimane in stato di standby. |
| : numero di serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) | > show running-config : salvato : |
| NGFW versione 7.2.8 ! hostname firepower | : numero di serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) |
| abilita password **** crittografata | • |
| strong-encryption-disable | NGFW versione 7.2.8 |
| service-module 0 keepalive-timeout 4 | ! |
| modulo di servizio 0 keepalive-counter 6 | hostname firepower |
| nomi | abilita password **** crittografata |
| nessun indirizzo mac automatico | strong-encryption-disable |
| | service-module 0 keepalive-timeout 4 |
| ! intorface Port channel? | |
| | nessun indirizzo mac automatico |
| manuale cat | |
| propagazione di sgt preserve-untag | ! |
| criterio statico sgt disabilitato attendibile | interface Port-channel2 |
| nessun livello di protezione | shutdown |
| nessun indirizzo ip | no nameif |
| ! | nessun livello di protezione |
| interface Port-channel 2.202 | nessun indirizzo ip |
| vlan 202 | l interface Dart sharral? |
| nameif Esterno | Interface Port-channels |
| manuale cat | |
| propagazione di sgt preserve-untag | nessun livello di protezione |
| criterio statico sgt disabilitato attendibile | nessun indirizzo in |
| livello di protezione u lindirizzo in 102 168 76 10 255 255 255 0 standbu | ! |
| 102 168 76 11 | interfaccia Ethernet1/1 |
| 1 | solo gestione |
| interface Port-channel3 | shutdown |
| descrizione Interfaccia di failover LAN/STATE | no nameif |
| ! | nessun livello di protezione |
| interfaccia Ethernet1/1 | nessun indirizzo ip |
| solo gestione | |
| diagnostica nameif | Interfaccia Ethernet1/4 |

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

| intervallo di opzioni tcp 20-255 consentito consenti contrassegno urgente ! nessun cercapersone nessun messaggio di registrazione 106015 nessun messaggio di registrazione 313008 nessun messaggio di registrazione 106023 nessun messaggio di registrazione 710003 nessun messaggio di registrazione 302015 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 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 FOVER Port-channel3 http per la replica di failover FOVER Port-channel3 interfaccia di failover FOVER Port-channel3 interfaccia di failover ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <output omesso=""></output> | nessun messaggio di registrazione 106100 nessun messaggio di registrazione 302013 nessun messaggio di registrazione 302013 nessun messaggio di registrazione 302017 nessun messaggio di registrazione 302016 nessun messaggio di logging 302021 nessun messaggio di registrazione 302020 nessun failover <output omesso=""></output> |
|--|--|
| Unità secondaria/attiva prima dell'interruzione HA | Unità secondaria dopo l'interruzione HA |
| > show running-config : salvato : | > 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) | : : Numero di serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73850 MB RAM, |

| • | CPU Xeon serie E5 2200 MHz, 2 CPU (48 core) |
|---|---|
| NGFW versione 7.2.8 | : |
| ! | NGFW versione 7.2.8 |
| hostname firepower | ! |
| abilita password **** crittografata | hostname firepower |
| strong-encryption-disable | abilita password **** crittografata |
| service-module 0 keepalive-timeout 1 | strong-encryption-disable |
| service-module o keepalive-timeout 4 | subrig-encryption-disable |
| | service-module 0 keepalive-timeout 4 |
| nomi | modulo di servizio U keepalive-counter 6 |
| nessun indirizzo mac automatico | nomi |
| ! | nessun indirizzo mac automatico |
| interface Port-channel2 | 1 |
| no nameif | interface Port-channel2 |
| nessun livello di protezione | no nameif |
| | no namen possun livello di protoziono |
| | |
| ! interface Dart shows at 2,200 | |
| | |
| | Interface Port-channel 2.202 |
| nameif Esterno | vlan 202 |
| manuale cat | nameif Esterno |
| propagazione di sgt preserve-untag | manuale cat |
| criterio statico sgt disabilitato attendibile | propagazione di sgt preserve-untag |
| livello di protezione 0 | criterio statico sgt disabilitato attendibile |
| indirizzo ip 192.168.76.10 255.255.255.0 | livello di protezione 0 |
| standby 192.168.76.11 | indirizzo ip 192.168.76.10 255.255.255.0 |
| ! | standby 192.168.76.11 |
| interface Port-channel3 | ! |
| descrizione Interfaccia di failover LAN/STATE | interface Port-channel3 |
| ! | no nameif |
| interfaccia Ethernet1/1 | nessun livello di protezione |
| solo gestione | |
| diagnostica namoif | |
| | : interfaccio Ethornat1/1 |
| | |
| nessun indirizzo ip | |
| | |
| Interfaccia Ethernet1/4 | livello di protezione 0 |
| nameif Inside | nessun indirizzo ip |
| livello di protezione 0 | ! |
| indirizzo ip 192.168.75.10 255.255.255.0 | interfaccia Ethernet1/4 |
| standby 192.168.75.11 | nameif Inside |
| ! | livello di protezione 0 |
| modalità ftp passiva | indirizzo ip 192.168.75.10 255.255.255.0 |
| ngips conn-match vlan-id | standby 192.168.75.11 |
| controllo dell'accesso obiect group search | ! |
| access-group CSM FW ACL globale | modalità ftp passiva |
| | |

| | 1 |
|--|---|
| Concerns list CSM EW/ ACL - pote rule id 0008: | nging conn match ylon id |
| DEEL TED DOLLOV: Critorio di priorità o tuppol | Ingips conn-match vian-id |
| PREFILIER FOLICE: Chieno di priorita e turiner | access group CSM EW ACL globalo |
| access list CSM EW/ ACL pote rule id 0008: | access-group CSIM_FW_ACL_ globale |
| | DEFILITED DOLLOV: Criteria di priorità a tuppol |
| ROLE. DEFAULT TUNNEL ACTION ROLE | PREFILIER FOLICIT. Chieno di priorita e turirer |
| lininin any rule id 0008 | access list CSM EW ACL noto rule id 0008: |
| Ipinip any rule-id 9990 | |
| access-list CSIVI_FVV_ACL_ advanced allow uup | ROLE. DEFAULT TOINNEL ACTION ROLE |
| | lininin any rule id 0008 |
| access list CSM_EW/ACL_advanced allow udp | access list CSM EW ACL advanced allow udp |
| access-list Colvi_1 W_ACL_ advanced allow dup | access-list COM_I W_ACL_ advanced allow dup |
| | |
| access-list CSM_EW_ACL_advanced allow 41 | access-list CSM_EW_ACL_advanced allow udp |
| qualsiasi rule-id 9998 | gualsiasi intervallo 1025 65535 any eg 3544 |
| access-list CSM_EW_ACL_advanced allow are | rule-id 9998 |
| any rule-id 9998 | access-list CSM_EW_ACL_advanced allow 41 |
| access-list CSM_EW_ACLnote rule-id | gualsiasi rule-id 9998 |
| 268439552: ACCESS POLICY: acp_simple - | access-list CSM_FW_ACL_advanced allow gre |
| Obbligatorio | any rule-id 9998 |
| access-list CSM FW ACL note rule-id | access-list CSM FW ACL note rule-id |
| 268439552: L7 RULE: rule1 | 268439552: ACCESS POLICY: acp simple - |
| access-list CSM_FW_ACL_ advanced | Obbligatorio |
| permission ip any rule-id 268439552 | access-list CSM_FW_ACL_ note rule-id |
| ! | 268439552: L7 RULE: rule1 |
| tcp-map UM_STATIC_TCP_MAP | access-list CSM_FW_ACL_ advanced |
| intervallo di opzioni tcp 6/7 consentito | permission ip any rule-id 268439552 |
| intervallo di opzioni tcp 9 18 consentito | ! |
| intervallo di opzioni tcp 20-255 consentito | tcp-map UM_STATIC_TCP_MAP |
| consenti contrassegno urgente | intervallo di opzioni tcp 6/7 consentito |
| ! | intervallo di opzioni tcp 9 18 consentito |
| nessun cercapersone | intervallo di opzioni tcp 20-255 consentito |
| nessun messaggio di registrazione 106015 | consenti contrassegno urgente |
| nessun messaggio di logging 313001 | 1 |
| nessun messaggio di registrazione 313008 | nessun cercapersone |
| nessun messaggio di registrazione 106023 | nessun messaggio di registrazione 106015 |
| nessun messaggio di registrazione 710003 | nessun messaggio di logging 313001 |
| nessun messaggio di registrazione 106100 | nessun messaggio di registrazione 313008 |
| nessun messaggio di registrazione 302015 | nessun messaggio di registrazione 106023 |
| nessun messaggio di registrazione 302014 | nessun messaggio di registrazione 710003 |
| nessun messaggio di registrazione 302013 | nessun messaggio di registrazione 100100 |
| nessun messaggio di registrazione 302018 | nessun messaggio di registrazione 302013 |
| nessun messaggio di registrazione 302017 | nessun messaggio di registraziono 302013 |
| nessun messaggio di loggina 202010 | nessun messaggio di registrazione 302013 |
| nessun messaggio di registrazione 302020 | nessun messangio di registrazione 302017 |
| nessun messayyin ui registrazione suzuzu | 10000111000000000000000000000000000000 |

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

Considerazioni principali per la separazione della coppia HA:

| Unità principale/standby | Unità secondaria/attiva |
|---|---|
| Tutta la configurazione di failover è stata rimossa Tutta la configurazione IP è stata rimossa | Tutta la configurazione di failover è stata rimossa Gli IP in standby rimangono, ma vengono rimossi nella distribuzione successiva |

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:

| FTD4120-HA High Availability | | | | | | | Switch Active Peer |
|--|-------------------------|-------|-------------------------------------|-----------------------|------------|-----|--|
| FTD4100-5(Primary, Standby) Snort 3 10.62.148.188 - Routed | Firepower 4120 with FTD | 7.2.8 | EP4100-5:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | *\$ | Force refresh node status Delete Devent Unescole |
| FTD4100-6(Secondary, Active) Snort 3 10.62.148.191 - Routed | Firepower 4120 with FTD | 7.2.8 | FP4100-6:443 Security Module - 1 | Base, Threat (2 more) | acp_simple | 45 | Health Monitor Troubleshoot Files |

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

| interface Port-channel 2.202 | interface Port-channel 2.202 |
|---|---|
| vlan 202 | vlan 202 |
| nameif NET202 | nameif NET202 |
| manuale cat | manuale cat |
| propagazione di sgt preserve-untag | propagazione di sat preserve-untag |
| criterio statico sot disabilitato attendibile | criterio statico sot disabilitato attendibile |
| livello di protezione 0 | livello di protezione 0 |
| indirizzo in 172 16 202 1 255 255 255 0 standby | indirizzo in 172 16 202 1 255 255 255 0 standby |
| 172 16 202 2 | 172 16 202 2 |
| 1 | 1 |
| interface Port₋channel 2 203 | l [:] Interface Port-channel 2 203 |
| vlan 203 | vlan 203 |
| | |
| | |
| | inanuale cal |
| propagazione di sgi preserve-unitag | propagazione di sgi preserve-untag |
| | |
| | |
| Indirizzo ip 172.16.203.1 255.255.255.0 standby | Indirizzo ip 172.16.203.1 255.255.255.0 standby |
| 172.16.203.2 | 172.16.203.2 |
| | |
| Interface Port-channel3 | Interface Port-channel3 |
| descrizione Interfaccia di failover LAN/STATE | descrizione Interfaccia di failover LAN/STATE |
| interfaccia Ethernet1/1 | interfaccia Ethernet1/1 |
| solo gestione | solo gestione |
| diagnostica nameif | diagnostica nameif |
| manuale cat | manuale cat |
| propagazione di sgt preserve-untag | propagazione di sgt preserve-untag |
| criterio statico sgt disabilitato attendibile | criterio statico sgt disabilitato attendibile |
| livello di protezione 0 | livello di protezione 0 |
| nessun indirizzo ip | nessun indirizzo ip |
| ! | ! |
| interfaccia Ethernet1/4 | interfaccia Ethernet1/4 |
| nameif NET204 | nameif NET204 |
| manuale cat | manuale cat |
| propagazione di sgt preserve-untag | propagazione di sgt preserve-untag |
| criterio statico sgt disabilitato attendibile | criterio statico sgt disabilitato attendibile |
| livello di protezione 0 | livello di protezione 0 |
| indirizzo ip 172.16.204.1 255.255.255.0 standby | indirizzo ip 172.16.204.1 255.255.255.0 standby |
| 172.16.204.2 | 172.16.204.2 |
| ! | ! |
| modalità ftp passiva | modalità ftp passiva |
| ngips conn-match vlan-id | ngips conn-match vlan-id |
| nessun controllo di accesso obiect-group-search | nessun controllo di accesso obiect-group-search |
| access-group CSM FW ACL globale | access-group CSM FW ACL dlobale |
| access-list CSM FW ACL note rule-id 9998: | access-list CSM FW ACL note rule-id 9998: |
| | |

| PREFILTER POLICY: Criterio di priorità e tunnel | PREFILTER POLICY: Criterio di priorità e tunnel |
|---|---|
| access-list CSM_EW_ACLnote rule-id 9998 | access-list CSM_EW_ACLnote rule-id 9998 |
| | |
| access list CSM EW ACL advanced allow | access-list CSM EW ACL advanced allow |
| lininin any rule id 0008 | lininin any rule id 9008 |
| access list CSM EW ACL advanced allow up | access list CSM EW ACL advanced allow udp |
| access-list CSIVI_FVV_ACL_ advanced allow dup | access-list CSIM_FW_ACL_ advanced allow up |
| | |
| cases list CSM EW/ ACL advanced allow udp | access list CSM EW ACL advanced allow udp |
| access-list CSIVI_FVV_ACL_ advanced allow dup | access-list CSIM_FW_ACL_ advanced allow up |
| | |
| access list CSM EW/ ACL advanced allow 41 | access list CSM EW ACL advanced allow 41 |
| access-list CSIVI_FVV_ACL_ advanced allow 41 | access-list CSIM_FW_ACL_ advanced allow 41 |
| qualsiasi Tule-lu 9990 | qualsiasi Tule-IU 9990 |
| access-list CSIVI_FVV_ACL_ advanced allow gre | access-list CSIM_FW_ACL_ advanced allow gre |
| access list CSM EW ACL pote rule id | access list CSM EW ACL noto rule id |
| 268434433: ACCESS DOLICY: acc. simple | 269434432: ACCESS DOLICY: app. simple |
| Default | Dofault |
| access list CSM EW/ ACL poto rulo id | access list CSM EW ACL noto rule id |
| | |
| | |
| ROLE | ROLE |
| nermission in any rule-id 268/3//33 | nermission in any rule-id 268/3//33 |
| | |
| tcp-map UM STATIC TCP MAP | tcp-map UM STATIC TCP MAP |
| intervallo di opzioni tcp 6/7 consentito | intervallo di opzioni tcp 6/7 consentito |
| intervallo di opzioni tcp 9 18 consentito | intervallo di opzioni tcp 9 18 consentito |
| intervallo di opzioni tcp 20-255 consentito | intervallo di opzioni tcp 20-255 consentito |
| tcp-options md5 clear | tcp-options md5 clear |
| consenti contrassegno urgente | consenti contrassegno urgente |
| ! | ! |
| nessun cercapersone | nessun cercapersone |
| nessun messaggio di registrazione 106015 | nessun messaggio di registrazione 106015 |
| nessun messaggio di logging 313001 | nessun messaggio di logging 313001 |
| nessun messaggio di registrazione 313008 | nessun messaggio di registrazione 313008 |
| nessun messaggio di registrazione 106023 | nessun messaggio di registrazione 106023 |
| nessun messaggio di registrazione 710003 | nessun messaggio di registrazione 710003 |
| nessun messaggio di registrazione 106100 | nessun messaggio di registrazione 106100 |
| nessun messaggio di registrazione 302015 | nessun messaggio di registrazione 302015 |
| nessun messaggio di registrazione 302014 | nessun messaggio di registrazione 302014 |
| nessun messaggio di registrazione 302013 | nessun messaggio di registrazione 302013 |
| nessun messaggio di registrazione 302018 | nessun messaggio di registrazione 302018 |
| nessun messaggio di registrazione 302017 | nessun messaggio di registrazione 302017 |
| nessun messaggio di registrazione 302016 | nessun messaggio di registrazione 302016 |
| nessun messaggio di logging 302021 | nessun messaggio di logging 302021 |
| | 1 |

| nessun messaggio di registrazione 302020 | nessun messaggio di registrazione 302020 |
|--|--|
| mtu NET 202 1500 | mtu NET 202 1500 |
| mtu NET 203 1500 | mtu NET 203 1500 |
| mtu diagnostic 1500 | mtu NET 203 1500 |
| mtu NET 204 1500 | mtu NET 204 1500 |
| failover | failover |
| unità lan di failover principale | unità lan di failover secondaria |
| failover interfaccia lan FOVER Port-channel3 | failover interfaccia lan FOVER Port-channel3 |
| http per la replica di failover | http per la replica di failover |
| collegamento di failover FOVER Port-channel3 | collegamento di failover FOVER Port-channel3 |
| interfaccia di failover ip FOVER 172.16.51.1 | interfaccia di failover ip FOVER 172.16.51.1 |
| 255.255.255.0 standby 172.16.51.2 | 255.255.255.0 standby 172.16.51.2 |
| monitor-interface NET202 | monitor-interface NET202 |
| interfaccia monitor NET203 | interfaccia monitor NET203 |
| icmp unreachable rate-limit 1 burst-size 1 | icmp unreachable rate-limit 1 burst-size 1 |
| <output omesso=""></output> | <output omesso=""></output> |
| > mostra ip | > mostra ip |
| Indirizzi IP di sistema: | Indirizzi IP di sistema: |
| Nome interfaccia Indirizzo IP Subnet mask, | Nome interfaccia Indirizzo IP Subnet mask, |
| metodo | metodo |
| Port-channel 2.202 NET20 172.16.202.1 | Port-channel 2.202 NET20 172.16.202.1 |
| 255.255.255.0 CONFIG | 255.255.255.0 CONFIG |
| Port-channel 2.203 NET203 172.16.203.1 | Port-channel 2.203 NET203 172.16.203.1 |
| 255.255.255.0 CONFIG | 255.255.255.0 CONFIG |
| Port-channel3 FOVER 172.16.51.1 | Port-channel3 FOVER 172.16.51.1 |
| 255.255.255.0 unset | 255.255.255.0 unset |
| Ethernet1/4 NET204 172.16.204.1 | Ethernet1/4 NET204 172.16.204.1 |
| 255.255.255.0 CONFIG | 255.255.255.0 CONFIG |
| Indirizzi IP correnti: | Indirizzi IP correnti: |
| Nome interfaccia Indirizzo IP Subnet mask, | Nome interfaccia Indirizzo IP Subnet mask, |
| metodo | metodo |
| Port-channel 2.202 NET20 172.16.202.2 | Port-channel 2.202 NET20 172.16.202.1 |
| 255.255.255.0 CONFIG | 255.255.255.0 CONFIG |
| Port-channel 2.203 NET203 172.16.203.2 | Port-channel 2.203 NET203 172.16.203.1 |
| 255.255.255.0 CONFIG | 255.255.255.0 CONFIG |
| Port-channel 3 FOVER 172.16.51.1 | Port-channel 3 FOVER 172.16.51.2 |
| 255.255.255.0 unset | 255.255.255.0 non impostato |
| Ethernet1/4 NET204 172.16.204.2 | Ethernet1/4 NET204 172.16.204.1 |
| 255.255.255.0 unset | 255.255.255.0 CONFIG |
| > mostra failover | > mostra failover |
| Failover attivato | Failover attivato |
| Unità di failover primaria | Unità di failover secondaria |
| Interfaccia LAN di failover: FOVER Port- | Interfaccia LAN di failover: FOVER Port- |

ſ

| channel3 (up) | channel3 (up) |
|---|---|
| Timeout riconnessione 0:00:00 | Timeout riconnessione 0:00:00 |
| Frequenza Unit Poll 1 secondi tempo di attesa | Frequenza I Init Poll 1 secondi, tempo di attesa |
| 15 secondi | 15 secondi |
| Frequenza di polling interfaccia 5 secondi. | Frequenza di polling interfaccia 5 secondi. |
| tempo di attesa 25 secondi | tempo di attesa 25 secondi |
| Criterio interfaccia 1 | Criterio interfaccia 1 |
| Interfacce monitorate 4 di 1291 massimo | Interfacce monitorate 4 di 1291 massimo |
| Intervallo di notifica spostamento indirizzo MAC | Intervallo di notifica spostamento indirizzo MAC |
| non impostato | non impostato |
| http per la replica di failover | http per la replica di failover |
| Versione: 9 18(4)210 Mate 9 18(4)210 | $V_{ersione} = 9.18(4)210$ Mate 9.18(4)210 |
| Numero di serie: El M1949C5RR Mate | Numero di serie: El M2108\/9YG_Mate |
| | FI M19/9C5RR |
| I litimo failover alle: 13:56:37 LITC lug 16 2024 | I litimo failover alle: 13:42:35 LITC lug 16 2024 |
| Host: primario - pronto per lo standby | Host corrente: secondario - attivo |
| Tempo di attività: 0 (sec) | Tempo di attività: 70312 (sec) |
| Slot 0: UCSB-B200-M3-U bw/sw rev | Slot 0: UCSB-B200-M3-U bw/sw rev |
| (0.0/9.18(4)210) status (Un Sys) | (0.0/9.18(4)210) status (Up Sys) |
| Interfaccia NET202 (172 16 202 2): normale | Interfaccia NET202 (172 16 202 1): normale |
| (monitorata) | (monitorata) |
| Interfaccia NET203 (172.16.203.2): normale | Interfaccia NET203 (172.16.203.1): normale |
| (monitorata) | (monitorata) |
| Diagnostica interfaccia (0.0.0.0): normale (in | Diagnostica interfaccia (0.0.0.0): normale (in |
| attesa) | attesa) |
| Interfaccia NET204 (172.16.204.2): normale | Interfaccia NET204 (172.16.204.1): normale |
| (monitorata) | (monitorata) |
| slot 1: stato snort rev (1.0) (su) | slot 1: stato snort rev (1.0) (su) |
| slot 2: stato rev diskstatus (1.0) (su) | slot 2: stato rev diskstatus (1.0) (su) |
| Altro host: secondario - attivo | Altro host: primario - pronto per lo standby |
| Tempo di attività: 70293 (sec) | Tempo di attività: 0 (sec) |
| Interfaccia NET202 (172.16.202.1): normale | Slot 0: UCSB-B200-M3-U hw/sw rev |
| (monitorata) | (0,0/9,18(4)210) status (Up Sys) |
| Interfaccia NET203 (172.16.203.1): normale | Interfaccia NET202 (172.16.202.2): normale |
| (monitorata) | (monitorata) |
| Diagnostica interfaccia (0.0.0.0): normale (in | Interfaccia NET203 (172.16.203.2): normale |
| attesa) | (monitorata) |
| Interfaccia NET204 (172.16.204.1): normale | Diagnostica interfaccia (0.0.0.0): normale (in |
| (monitorata) | attesa) |
| slot 1: stato snort rev (1.0) (su) | Interfaccia NET204 (172.16.204.2): normale |
| slot 2: stato rev diskstatus (1.0) (su) | (monitorata) |
| | slot 1: stato snort rev (1.0) (su) |
| | slot 2: stato rev diskstatus (1.0) (su) |
| | <output omesso=""></output> |
| | |

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. | II dispositivo viene rimosso dall'FMC. |
| Nessuna configurazione rimossa dal dispositivo FTD. | 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 <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:

| | 1 |
|--|--|
| Unità primaria (ex standby) | Unità secondaria (ex attiva) |
| > INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > show failover Failover Off (pseudo-Standby) Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 | > show failover Failover Off Failover unit Secondary Failover LAN Interface: not Configured 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 4 of 1291 maximum MAC Address Move Notification Interval not set |
| seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http > show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset | > show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG |
| Principale (ex standby) | Secondario (ex attivo) |
| > show running-config : salvato | > 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) : | : : 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 | NGFW versione 7.2.8 |
|--|--|
| bostname Firenower-module1 | ¦. Ibostname Firenower₋module1 |
| abilita password **** crittografata | abilita password **** crittografata |
| abilita passivoru chilografata | abilita passivoru crittografata |
| | strong-encryption-disable |
| no asp inspect-dp ack-passtnrougn | no asp inspect-dp ack-passtnrough |
| service-module 0 keepalive-timeout 4 | service-module 0 keepalive-timeout 4 |
| modulo di servizio 0 keepalive-counter 6 nomi | modulo di servizio 0 keepalive-counter 6 nomi |
| nessun indirizzo mac automatico | nessun indirizzo mac automatico |
| ! | ! |
| interface Port-channel2 | interface Port-channel2 |
| shutdown | no nameif |
| no nameif | nessun livello di protezione |
| nessun livello di protezione | nessun indirizzo ip |
| nessun indirizzo ip <- gli IP vengono rimossi | ! |
| ! | interface Port-channel 2.202 |
| interface Port-channel3 | vlan 202 |
| descrizione Interfaccia di failover LAN/STATE | nameif NET202 |
| ! | manuale cat |
| interfaccia Ethernet1/1 | propagazione di sat preserve-untag |
| solo gestione | criterio statico sot disabilitato attendibile |
| shutdown | livello di protezione 0 |
| no nameif | indirizzo in 172 16 202 1 255 255 255 0 standby |
| nessun livello di protezione | 172 16 202 2 |
| nessun indirizzo in | 172.10.202.2 |
| | interface Port channel 2 203 |
| ! interfaceia Ethernat1// | vian 202 |
| | |
| | |
| | |
| nessun livello di protezione | propagazione di sgt preserve-untag |
| nessun indirizzo ip | criterio statico sgt disabilitato attendibile |
| ! | livello di protezione 0 |
| modalità ftp passiva | indirizzo ip 172.16.203.1 255.255.255.0 standby |
| ngips conn-match vlan-id | 172.16.203.2 |
| nessun controllo di accesso object-group-search | ! |
| access-group CSM_FW_ACL_ globale | interface Port-channel3 |
| access-list CSM_FW_ACL_ note rule-id 9998: | no nameif |
| PREFILTER POLICY: Criterio di priorità e tunnel | nessun livello di protezione |
| predefinito | nessun indirizzo ip |
| access-list CSM_FW_ACL_ note rule-id 9998: | ! |
| RULE: DEFAULT TUNNEL ACTION RULE | interfaccia Ethernet1/1 |
| access-list CSM_FW_ACL_ advanced allow | solo gestione |
| ipinip any rule-id 9998 | diagnostica nameif |
| access-list CSM_FW ACL advanced allow udp | manuale cat |
| | |

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

| 255.255.255.0 standby 172.16.51.2 | intervallo di opzioni tcp 9 18 consentito |
|-------------------------------------|---|
| no monitor-interface service-module | intervallo di opzioni tcp 20-255 consentito |
| | tcp-options md5 clear |
| <output omesso=""></output> | 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 |
| | |

Note principali per Disabilitare HA dalla CLI FTD attiva:

| Unità attiva | Unità di standby |
|---|---|
| Configurazione di failover rimossa Gli IP in standby non vengono rimossi | Le configurazioni delle interfacce sono state rimosse. La configurazione di failover non viene rimossa, ma il failover è disabilitato (pseudo-standby) |

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) |
|--|--|
| > 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 | > mostra failover Failover su <- 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 |
| > 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 <- II dispositivo utilizza | 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) |

| 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-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 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) Interfaccia NET202 (172.16.202.2): sconosciuta (monitorata) Interfaccia NET202 (172.16.202.1) slot 1: stato snort rev (1.0) (su) slot 2: stato rev diskstatus (1.0) (su) Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manuale <- II dispositivo utilizza gli stessi IP dell'ex-standby! Port-channel 2.203 NET203 172.16.203.1 255.255.255.0 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 Indirizzi IP correnti: Nome interfaccia Indirizzo IP Subnet mask, metodo Port-channel2.203 NET203 172.16.203.1 |
|--|--|

٦

| 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 |
|--|---|
| La configurazione di failover non viene rimossa e rimane abilitata Il dispositivo usa gli stessi IP dell'unità ex-Standby | Configurazione di failover rimossa Il dispositivo utilizza gli stessi IP dell'unità attiva |

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) |
|---------------------------------------|------------------------------|
| > mostra failover | > mostra failover |
| Failover disattivato (pseudo standby) | Failover disattivato |
| Unità di failover primaria | Unità di failover secondaria |

| Interfaccia LAN di failover: FOVER Port- | Interfaccia LAN di failover: non configurata |
|--|--|
| channel3 (up) | Timeout riconnessione 0:00:00 |
| Timeout riconnessione 0:00:00 | Frequenza Unit Poll 1 secondi, tempo di attesa |
| Frequenza Unit Poll 1 secondi, tempo di attesa | 15 secondi |
| 15 secondi | Frequenza di polling interfaccia 5 secondi, |
| Frequenza di polling interfaccia 5 secondi, | tempo di attesa 25 secondi |
| tempo di attesa 25 secondi | Criterio interfaccia 1 |
| Criterio interfaccia 1 | Interfacce monitorate 0 di 1291 massimo |
| Interfacce monitorate 0 di 1291 massimo | Intervallo di notifica spostamento indirizzo MAC |
| Intervallo di notifica spostamento indirizzo MAC | non impostato |
| non impostato | |
| http per la replica di failover | |
| | > mostra ip |
| | Indirizzi IP di sistema: |
| > mostra ip | Nome interfaccia Indirizzo IP Subnet mask, |
| Indirizzi IP di sistema: | metodo |
| Nome interfaccia Indirizzo IP Subnet mask, | Indirizzi IP correnti: |
| metodo | Nome interfaccia Indirizzo IP Subnet mask, |
| Port-channel3 FOVER 172.16.51.1 | metodo |
| 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 | |
| > | |
| | |

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

| Unità attiva | Unità di standby |
|--|---|
| Configurazione di failover rimossa Gli IP vengono rimossi | La configurazione di failover non viene rimossa, ma il failover è disabilitato (pseudo-standby) Gli IP vengono rimossi |

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 attivato |
| | Unità di failover secondaria |
| > mostra failover | Interfaccia LAN di failover: FOVER Port- |
| Failover disattivato | channel3 (up) |
| Unità di failover secondaria | Timeout riconnessione 0:00:00 |
| Interfaccia LAN di failover: non configurata | Frequenza Unit Poll 1 secondi, tempo di attesa |
| Timeout riconnessione 0:00:00 | 15 secondi |
| Frequenza Unit Poll 1 secondi, tempo di attesa | Frequenza di polling interfaccia 5 secondi, |
| 15 secondi | tempo di attesa 25 secondi |
| Frequenza di polling interfaccia 5 secondi, | Criterio interfaccia 1 |
| tempo di attesa 25 secondi | Interfacce monitorate 4 di 1291 massimo |
| Criterio interfaccia 1 | Intervallo di notifica spostamento indirizzo MAC |
| Interfacce monitorate 0 di 1291 massimo | non impostato |
| Intervallo di notifica spostamento indirizzo MAC | http per la replica di failover |
| non impostato | Versione: 9.18(4)210, Mate 9.18(4)210 |
| | Numero di serie: FLM2108V9YG, Mate |
| | FLM1949C5RR |
| > mostra ip Indirizzi ID di cictomo: | Ultimo failover alle: 07:06:56 UTC lug 18 2024 |
| Momo interfaccio Indirizzo ID Subnet maak | Host corrente: secondario - attivo |
| motodo | l empo di attivita: 1194 (sec) |
| Indirizzi ID corronti: | |
| Nome interfaccia Indirizzo IP Subnet mask | (0,0/9,18(4)210) status (Op Sys) |
| metodo | |
| > | allesa) |
| | (monitorata) |
| | Interfaceia NET202 (172 16 202 1): permale |
| | (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 |
| indinzzi ip di sistema: |
| Nome Interfaccia Indirizzo IP Subnet mask, |
| Melodo 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 |
|--|--|
| Configurazione di failover non rimossa Gli indirizzi IP non vengono rimossi | Configurazione di failover rimossa Gli IP vengono rimossi |

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 3. Risultato sull'unità secondaria:

<#root>

```
>
```

show high-availability config
Failover Off (pseudo-Standby)

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

Passaggio 4. Riprendere HA sull'unità primaria:

<#root>

>

configure high-availability resume

Successfully resumed high-availablity.

> .

>

<#root>

>

show high-availability config

Failover On

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
```

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 192.0.2.1 255.255.0 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:

<u>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)</u>

 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).