

# Configuración de alta disponibilidad de FTD en dispositivos Firepower

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Tarea 1. Verificar las condiciones](#)

[Tarea 2. Configuración de FTD HA](#)

[Condiciones](#)

[Tarea 3. Verificar HA y la licencia de FTD](#)

[Tarea 4. Cambiar los roles de conmutación por error](#)

[Tarea 5. Interrumpir el par de HA](#)

[Tarea 6. Eliminar un par HA](#)

[Tarea 7. Suspender HA](#)

[Preguntas frecuentes](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo configurar y verificar la alta disponibilidad (HA) de Firepower Threat Defense (FTD) (conmutación por fallo activa/en espera) en los dispositivos Firepower.

## Prerequisites

### Requirements

No hay requisitos específicos para este documento.

### Componentes Utilizados


La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

---

 Nota: En un dispositivo FPR9300 con FTD, solo puede configurar HA entre chasis. Las dos unidades en una configuración de HA deben cumplir con las condiciones mencionadas aquí.

---

## Tarea 1. Verificar las condiciones

Tarea requerida:

Verifique que ambos appliances FTD cumplan los requisitos de la nota y se puedan configurar como unidades HA.

Solución:

Paso 1. Conéctese a la IP de administración FPR9300 y verifique el hardware del módulo.

Verifique el 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#
```

Verifique el 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#
```

Paso 2. Inicie sesión en el administrador de chasis de FPR9300-1 y vaya hasta Dispositivos

lógicos.

Verifique la versión del software, el número y el tipo de interfaces.

## Tarea 2. Configuración de FTD HA

Tarea requerida:

Configure la conmutación por falla activa / en espera (HA) según este diagrama. En este caso, se utiliza un par 41xx.

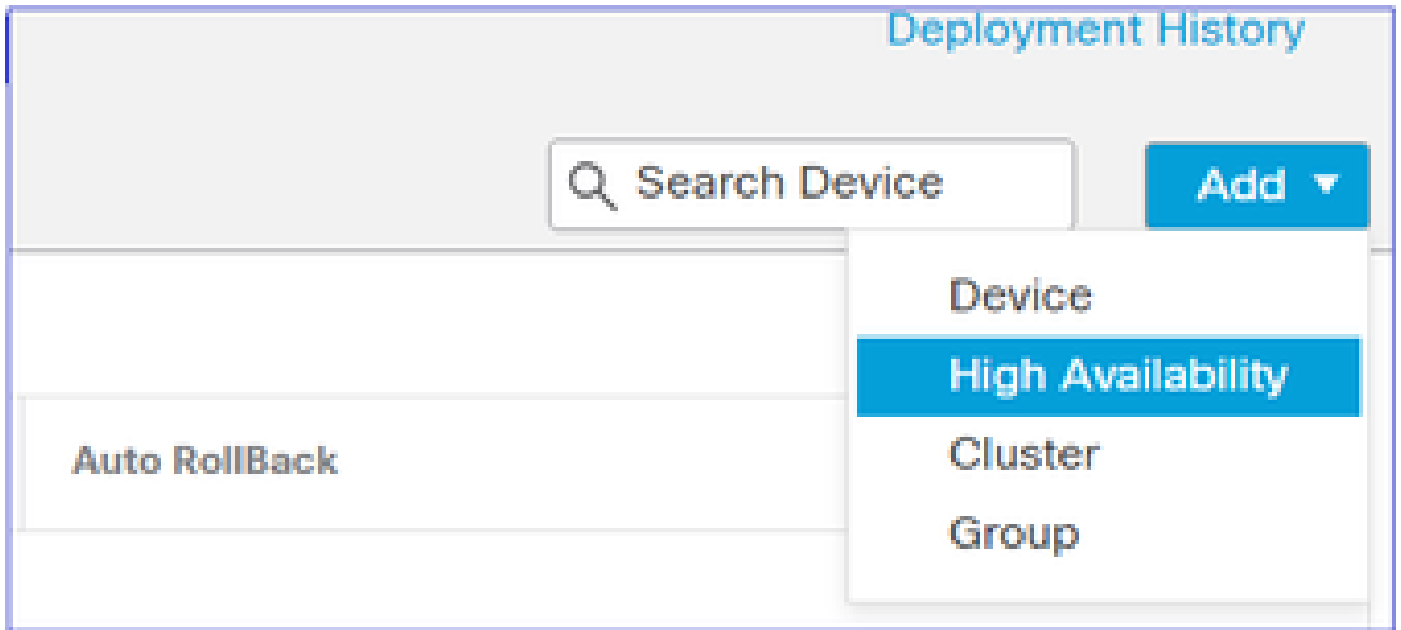


Solución

Ambos dispositivos FTD ya están registrados en el FMC, como se muestra en la imagen.

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	⏪	✎

Paso 1. Para configurar el failover FTD, navegue hasta Devices > Device Management y elija Add High Availability como se muestra en la imagen.



Paso 2. Ingrese el Peer Primario y el Peer Secundario y elija Continue como se muestra en la imagen.

Version: 7.2 Channel: 7.2 License:

## 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.

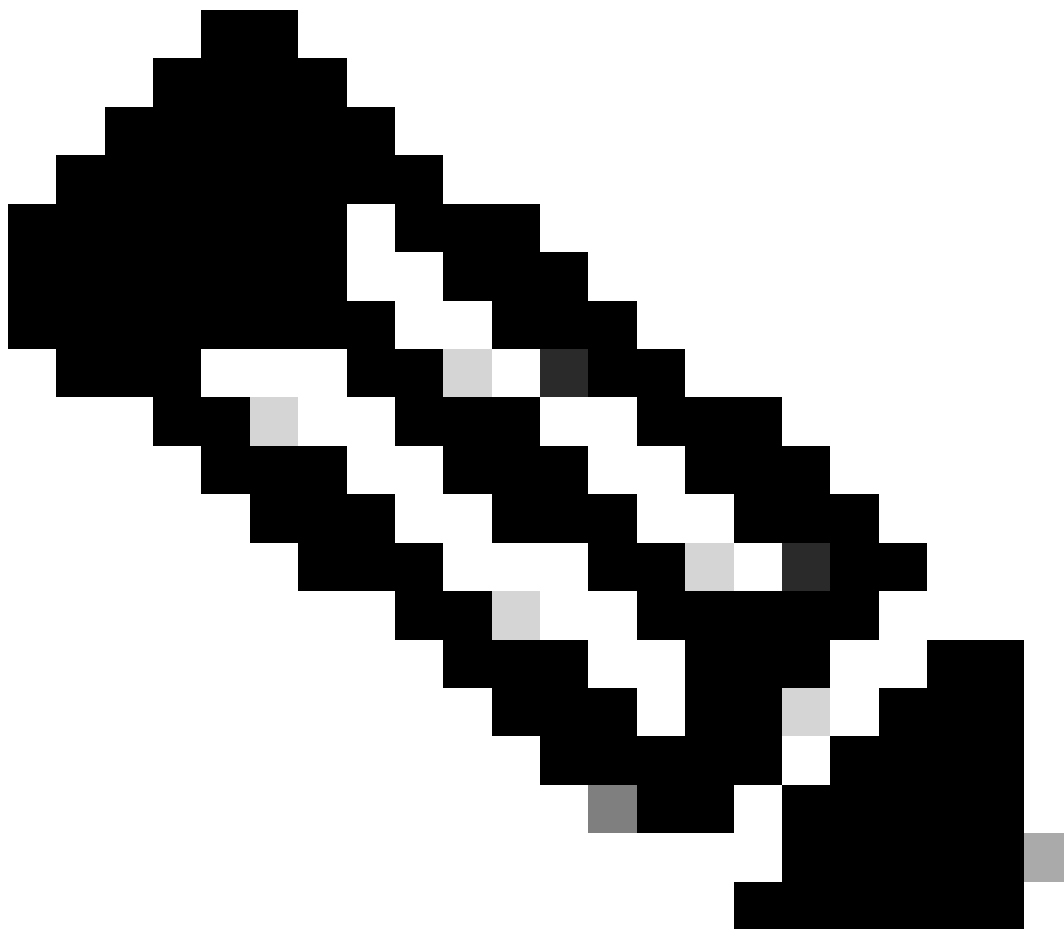
Cancel Continue

**⚠** Advertencia: Asegúrese de seleccionar la unidad correcta como la unidad principal. Todas las configuraciones de la unidad principal seleccionada se replican en la unidad FTD secundaria seleccionada. Como resultado de la replicación, se puede reemplazar la configuración actual en la unidad secundaria.

Condiciones

Para crear una HA entre 2 dispositivos FTD, deben cumplirse estas condiciones:

- Mismo modelo
  - La misma versión: esto se aplica a FXOS y a FTD. Las versiones principal (primer número), secundaria (segundo número) y de mantenimiento (tercer número) deben ser iguales.
  - Misma cantidad de interfaces
  - El mismo tipo de interfaces
  - Ambos dispositivos forman parte del mismo grupo o dominio en FMC.
  - Tienen una configuración idéntica de protocolo de tiempo de red (NTP).
  - Estar completamente implementado en el FMC sin cambios no registrados.
  - Estar en el mismo modo de firewall: enrutado o transparente.
- 



Nota: Esto debe comprobarse tanto en los dispositivos FTD como en la GUI de FMC, ya que ha habido casos en los que los FTD tenían el mismo modo, pero FMC no lo refleja.

---

- No tiene DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configurado en ninguna de las interfaces.

- Nombre de host diferente [Nombre de dominio completamente calificado (FQDN)] para ambos chasis. Para verificar el nombre de host del chasis, navegue hasta FTD CLI y ejecute este comando:

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

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



Nota: En el FTD posterior a la versión 6.3, utilice el 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
```

Si ambos chasis tienen el mismo nombre, cambie el nombre en uno de ellos con el uso de estos comandos:

```
<#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

FPR9K-1new-A

#

Después de cambiar el nombre del chasis, anule el registro del FTD del FMC y vuelva a registrarlo. Luego, proceda con la creación del par de HA.

Paso 3. Configure la HA y establezca la configuración de los enlaces.

En su caso, el enlace de estado tiene la misma configuración que el enlace de alta disponibilidad.

Elija Add y espere unos minutos a que se implemente el par HA, como se muestra en la imagen.

**Add High Availability Pair**

**High Availability Link**

Interface:\* Port-channel3

Logical Name:\* FOVER

Primary IP:\* 172.16.51.1

Use IPv6 Address

Secondary IP:\* 172.16.51.2

Subnet Mask:\* 255.255.255.0

**State Link**

Interface:\* Same as LAN Failover Link

Logical Name:\* FOVER

Primary IP:\* 172.16.51.1

Use IPv6 Address

Secondary IP:\* 172.16.51.2

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

Paso 4. Configurar las interfaces de datos (direcciones IP principales y de reserva)

En la GUI de FMC, elija la edición de HA como se muestra en la imagen.

ID	Name	Status	Model	Version	Security Module	Base	Threat	Action
FTD4100-5	FTD4100-5(Primary, Active)	Short 3	Firepower 4120 with FTD	7.2.8	FP4100-6:443 Security Module - 1	Base, Threat (2 more...)	acp_simple	
FTD4100-6	FTD4100-6(Secondary, Standby)	Short 3	Firepower 4120 with FTD	7.2.8	FP4100-6:443 Security Module - 1	Base, Threat (2 more...)	acp_simple	

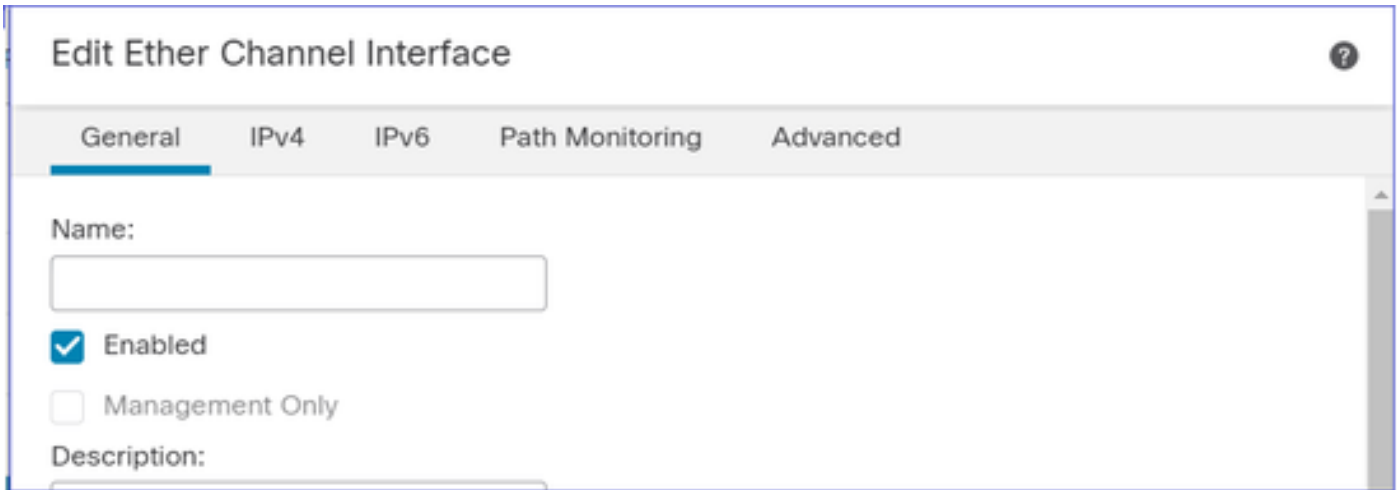


Paso 5. Configure los parámetros de la interfaz:

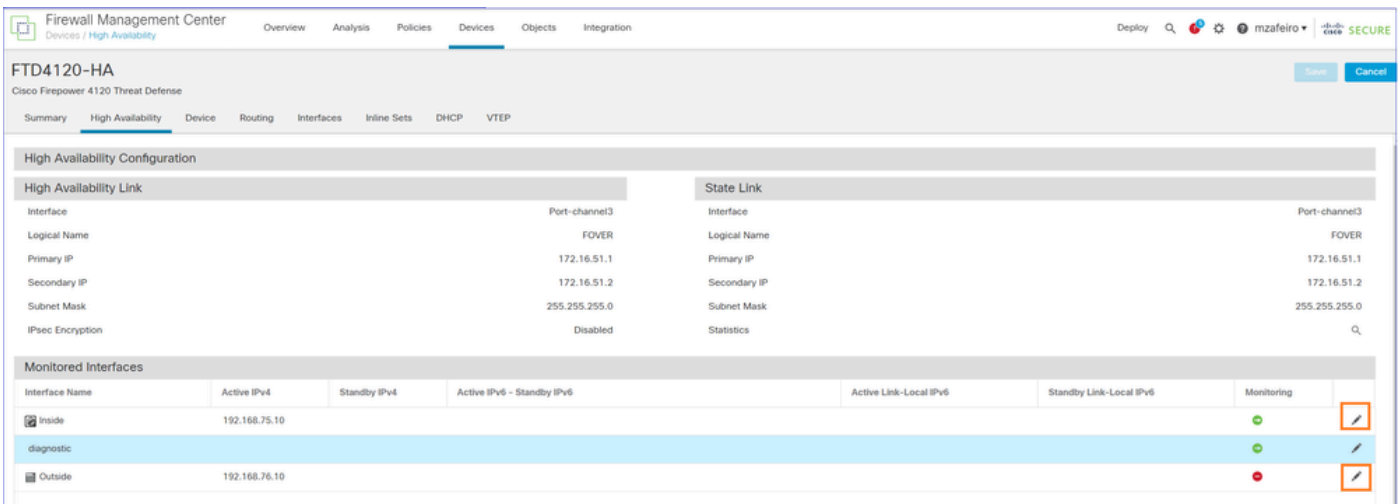
The screenshot shows the 'Edit Physical Interface' configuration window with the 'General' tab selected. The interface name is 'Inside'. There are checkboxes for 'Enabled' and 'Management Only', both of which are currently unchecked. The 'Description' field is empty. The 'Mode' is set to 'None'. The 'Security Zone' is set to an empty dropdown. The 'Interface ID' is 'Ethernet1/4'. The 'MTU' is set to '1500' with a range of '(64 - 9184)'. The 'Priority' is set to '0' with a range of '(0 - 65535)'. There is a checkbox for 'Propagate Security Group Tag' which is unchecked. There is also a checkbox for 'NVE Only' which is unchecked. At the bottom right, there are 'Cancel' and 'OK' buttons.

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' is set to 'Use Static IP'. The 'IP Address' field contains '192.168.75.10/24'. Below the field, there is a note: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'. At the bottom right, there are 'Cancel' and 'OK' buttons.

En el caso de una subinterfaz, primero debe habilitar la interfaz principal:



Paso 6. Navegue hasta High Availability y elija el Interface Name Edit para agregar las direcciones IP standby como se muestra en la imagen.



Paso 7. Para la interfaz interna como se muestra en la imagen.

## 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

Paso 8. Haga lo mismo para la interfaz externa.

Paso 9. Verifique el resultado como se muestra en la imagen.

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

Paso 10. Permanezca en la ficha High Availability (Alta disponibilidad) y configure las direcciones MAC virtuales como se muestra en la imagen.

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

Paso 11. Para la interfaz interna es como se muestra en la imagen.

## Add Interface Mac Address ?

Physical Interface:\*

Ethernet1/4

Active Interface Mac Address:\*

aaaa.bbbb.1111

Standby Interface Mac Address:\*

aaaa.bbbb.2222

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

Cancel

OK

Paso 12. Haga lo mismo para la interfaz externa.

Paso 13. Verifique el resultado como se muestra en la imagen.

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	 

Paso 14. Después de configurar los cambios, elija Save and Deploy.

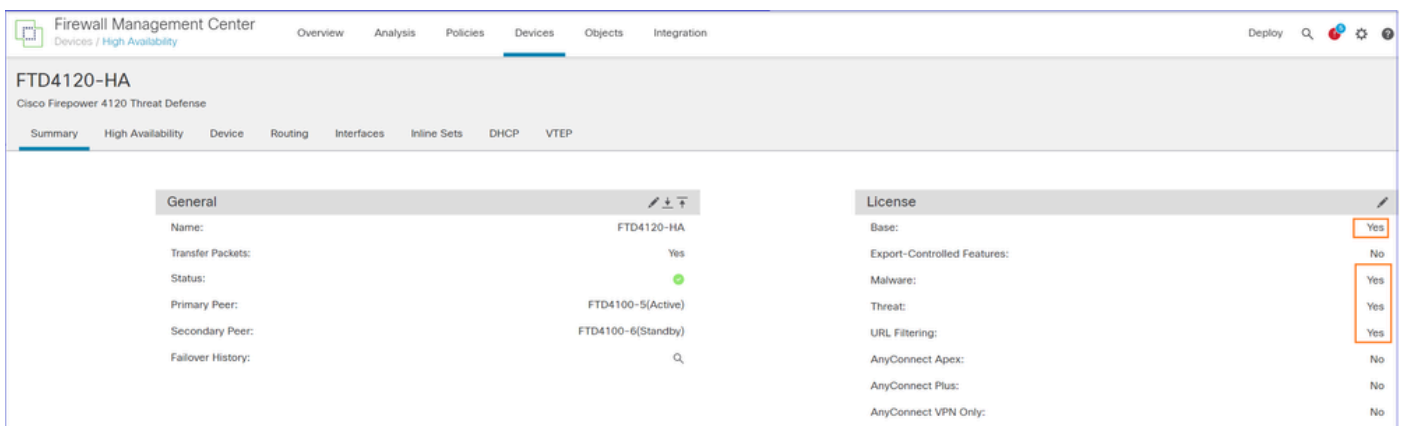
## Tarea 3. Verificar HA y la licencia de FTD

Tarea requerida:


Verifique la configuración de HA de FTD y las licencias activadas desde la GUI de FMC y desde la CLI de FTD.

Solución:

Paso 1. Vaya a Resumen y verifique la configuración de HA y las licencias activadas como se muestra en la imagen.



The screenshot shows the Firewall Management Center (FMC) interface for a device named 'FTD4120-HA'. The 'General' tab is active, displaying the following configuration:

- Name: FTD4120-HA
- Transfer Packets: Yes
- Status: ●
- Primary Peer: FTD4100-5(Active)
- Secondary Peer: FTD4100-6(Standby)
- Failover History: 

The 'License' tab is also visible, showing the following license settings:

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

Paso 2. Desde la CLI de FTD CLISH, ejecute el comando 'show high-availability config' o 'show failover':

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-chnnel3 (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>

Paso 3. Haga lo mismo en el dispositivo secundario.

Paso 4. Ejecute el comando show failover state desde la CLI de 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#

Paso 5. Verifique la configuración desde la unidad principal (CLI de LINA):

```
<#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  
>
```

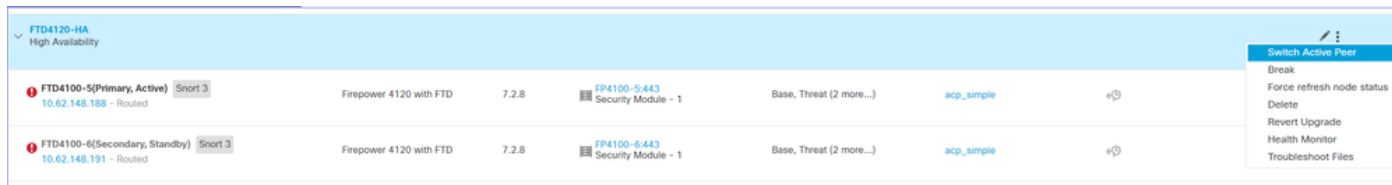
## Tarea 4. Cambiar los roles de conmutación por error

Tarea requerida:

Desde la FMC, cambie los roles de conmutación por error de Principal/Activo, Secundario/De reserva a Principal/De reserva, Secundario/Activo

Solución:

Paso 1. Seleccione el icono como se muestra en la imagen.



Paso 2. Confirme la acción.

Puede utilizar el resultado del comando show failover history:

En el nuevo Active	En el n
> show failover history =====	
De Estado A Estado Motivo =====	
09:27:11 UTC 18 de julio de 2024 Standby Ready Just Active La otra unidad me quiere activo comando config) (Establecido por el	
09:27:11 UTC 18 de julio de 2024 Solo Activo Drenaje Activo Otra unidad me quiere Activo comando config) (Establecido por el	> show =====
09:27:11 UTC 18 de julio de 2024 Drenaje activo Aplicando configuración Otra unidad me quiere activo comando config) (Establecido por el	De Est =====
09:27:11 UTC 18 de julio de 2024 Activa Aplicando configuración Activa Config Aplicada Otra unidad me desea activo comando config) (Establecido por el	09:27:1 Active s
09:27:11 UTC 18 de julio de 2024 Active Config Applied Active Otra unidad me quiere activo comando config) (Establecido por el	

Paso 4. Después de la verificación, vuelva a activar la unidad principal.



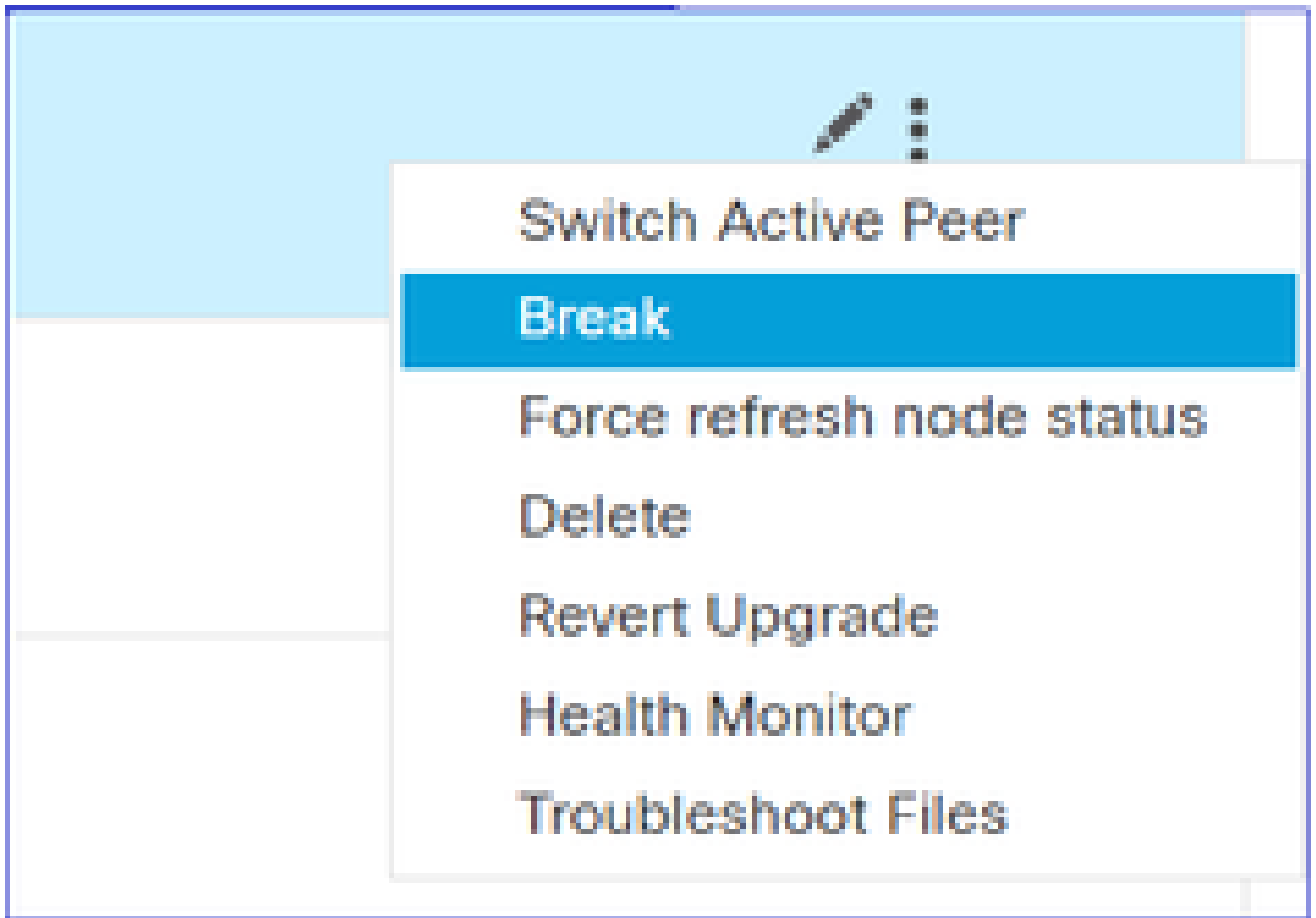
## Tarea 5. Interrumpir el par de HA

Tarea requerida:

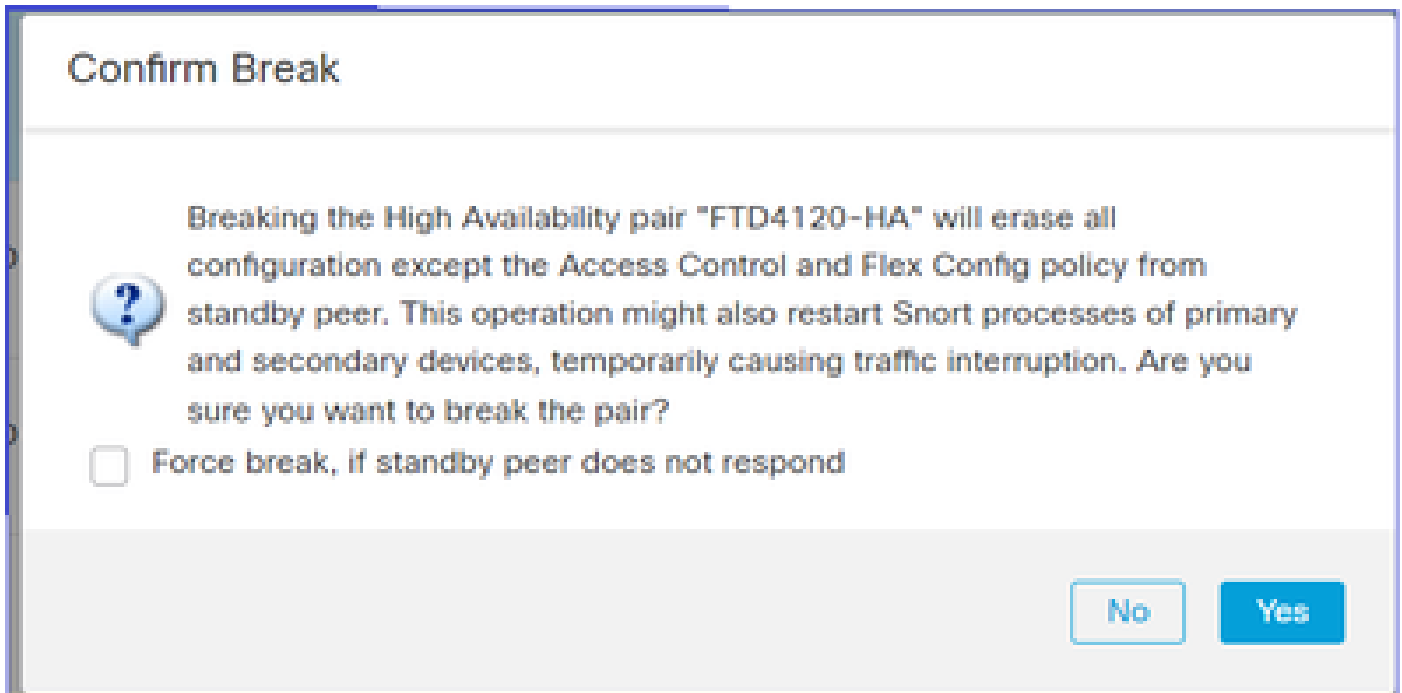
Desde el FMC, interrumpa el par de conmutación por error.

Solución:

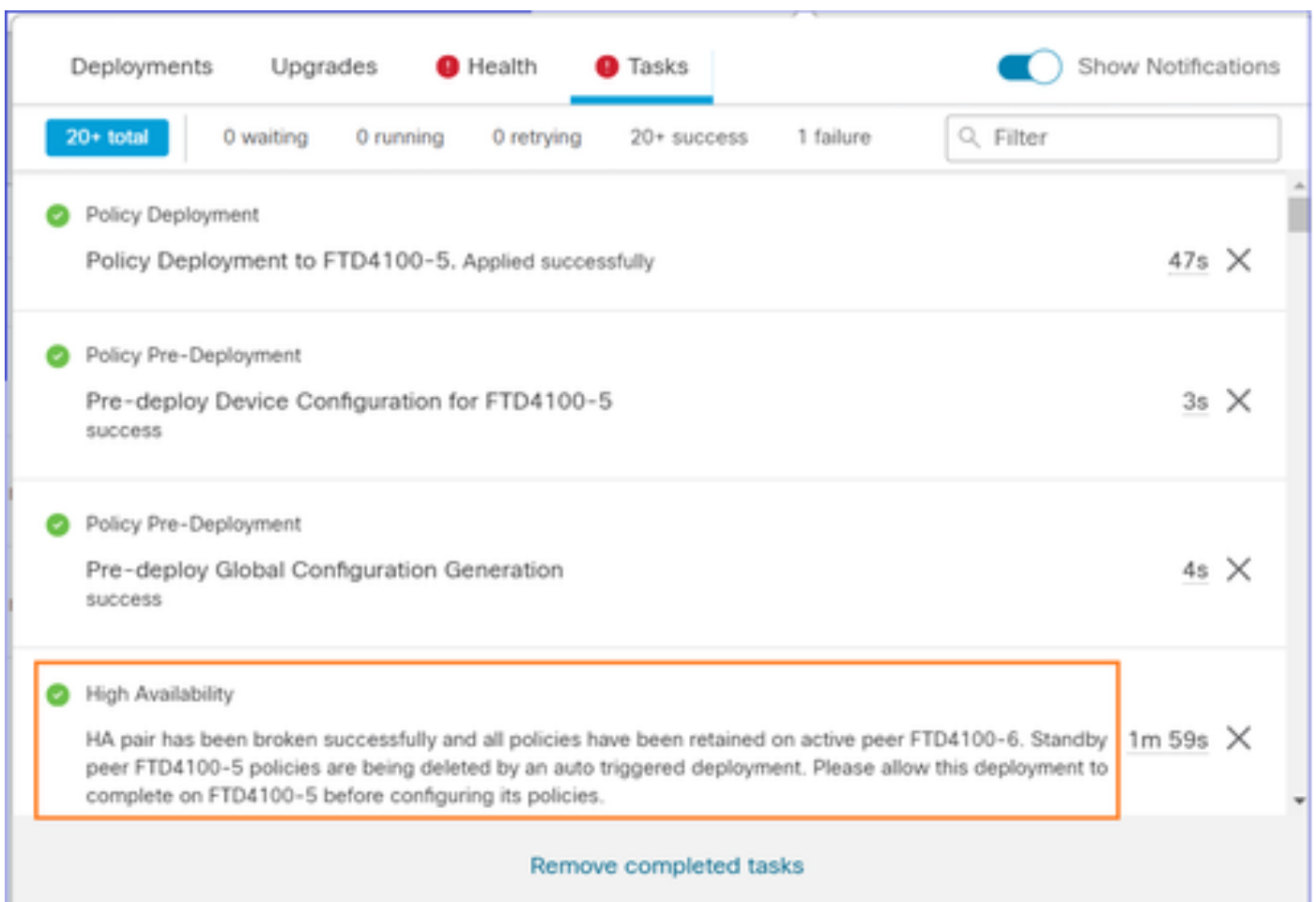
Paso 1. Seleccione el icono como se muestra en la imagen.



Paso 2. Verifique la notificación como se muestra en la imagen.



Paso 3. Observe el mensaje como se muestra en la imagen.



Paso 4. Verifique el resultado desde la GUI de FMC o desde la CLI

show running-config en la unidad principal antes y después de la interrupción de HA:

Unidad primaria/en espera antes de la interrupción de HA	Unidad primaria después de la interrupción de HA
<pre> &gt; show running-config : Guardado : : Número de serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname firepower enable password ***** encryption strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 no name if manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted no security-level sin dirección de IP ! interface Port-channel2.202 vlan 202 nameif Outside manual de CTS 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 ! interfaz Ethernet1/1 solo de administración </pre>	<pre> &gt; INFO: Esta unidad se encuentra actualmente en estado de espera. Al inhabilitar la conmutación por fallas, esta unidad permanecerá en estado de espera. &gt; show running-config : Guardado : : Número de serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname firepower enable password ***** encryption strong-encryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 apagado no name if no security-level sin dirección de IP ! interface Port-channel3 apagado no name if no security-level sin dirección de IP ! interfaz Ethernet1/1 solo de administración apagado no name if no security-level sin dirección de IP </pre>

<pre> nameif diagnostic manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 sin dirección de IP ! interface Ethernet1/4 nameif Inside manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11 ! ftp mode passive ngips conn-match vlan-id object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow </pre>	<pre> ! interface Ethernet1/4 apagado no name if no security-level sin dirección de IP ! ftp mode passive ngips conn-match vlan-id object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268439552: ACCESS POLICY: acp_simple - Obligatorio access-list CSM_FW_ACL_remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_advanced permit ip any any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 </pre>
---	--

<pre> tcp-options range 20 255 allow urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 ningún mensaje de registro 302018 ningún mensaje de registro 302017 ningún mensaje de registro 302016 ningún mensaje de registro 302021 ningún mensaje de registro 302020 mtu Outside 1500 mtu diagnostic 1500 mtu Inside 1500 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.bbb.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  &lt;salida omitida&gt; </pre>	<pre> ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 ningún mensaje de registro 302018 ningún mensaje de registro 302017 ningún mensaje de registro 302016 ningún mensaje de registro 302021 ningún mensaje de registro 302020 ningún failover &lt;salida omitida&gt; </pre>
<p>Unidad secundaria/activa antes de la interrupción de HA</p>	<p>Unidad secundaria después de la interrupción de HA</p>
<pre> &gt; show running-config : Guardado : : Número de serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73850 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 </pre>	<pre> &gt; show running-config : Guardado : : Número de serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73850 MB de RAM, </pre>

```
núcleos)
:
NGFW versión 7.2.8
!
hostname firepower
enable password ***** encryption
strong-encryption-disable
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto
!
interface Port-channel2
no name if
no security-level
sin dirección de IP
!
interface Port-channel2.202
vlan 202
nameif Outside
manual de CTS
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
!
interfaz Ethernet1/1
solo de administración
nameif diagnostic
security-level 0
sin dirección de IP
!
interface Ethernet1/4
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0
standby 192.168.75.11
!
ftp mode passive
ngips conn-match vlan-id
object-group-search access-control
```

```
CPU Xeon serie E5 2200 MHz, 2 CPU (48
núcleos)
:
NGFW versión 7.2.8
!
hostname firepower
enable password ***** encryption
strong-encryption-disable
service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6
names
no mac-address auto
!
interface Port-channel2
no name if
no security-level
sin dirección de IP
!
interface Port-channel2.202
vlan 202
nameif Outside
manual de CTS
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
no name if
no security-level
sin dirección de IP
!
interfaz Ethernet1/1
solo de administración
nameif diagnostic
security-level 0
sin dirección de IP
!
interface Ethernet1/4
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0
standby 192.168.75.11
!
```

<pre> access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIX POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268439552: ACCESS POLICY: acp_simple - Obligatorio access-list CSM_FW_ACL_remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_advanced permit ip any any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 ningún mensaje de registro 302018 ningún mensaje de registro 302017 ningún mensaje de registro 302016 ningún mensaje de registro 302021 </pre>	<pre> ftp mode passive ngips conn-match vlan-id object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIX POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268439552: ACCESS POLICY: acp_simple - Obligatorio access-list CSM_FW_ACL_remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_advanced permit ip any any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 ningún mensaje de registro 302018 </pre>
---	---

ningún mensaje de registro 302020 mtu Outside 1500 mtu diagnostic 1500 mtu Inside 1500 failover failover lan unit secondary failover lan interface FOVER Port-channel3 failover replication http failover link FOVER Port-channel3 failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <salida omitida>	ningún mensaje de registro 302017 ningún mensaje de registro 302016 ningún mensaje de registro 302021 ningún mensaje de registro 302020 mtu Outside 1500 mtu diagnostic 1500 mtu Inside 1500 ningún failover no monitor-interface Outside no monitor-interface service-module <salida omitida>
--	--

Puntos principales a tener en cuenta para la interrupción de HA:

Unidad principal/en espera	Unidad secundaria/activa
<ul style="list-style-type: none"> <li>• Se elimina toda la configuración de conmutación por error.</li> <li>• Se elimina toda la configuración IP</li> </ul>	<ul style="list-style-type: none"> <li>• Se elimina toda la configuración de conmutación por error.</li> <li>• Las IP en espera permanecen, pero se eliminan en la siguiente implementación</li> </ul>

Paso 5. Después de finalizar esta tarea, vuelva a crear el par de HA.

## Tarea 6. Eliminar un par HA

Esta tarea se basa en una configuración de HA en 41xx con el software 7.2.8. En este caso, inicialmente los dispositivos se encontraban en estos estados:

- Principal/En espera
- Secundario/Activo

Tarea requerida:

En el FMC, elimine el par de conmutación por fallo.

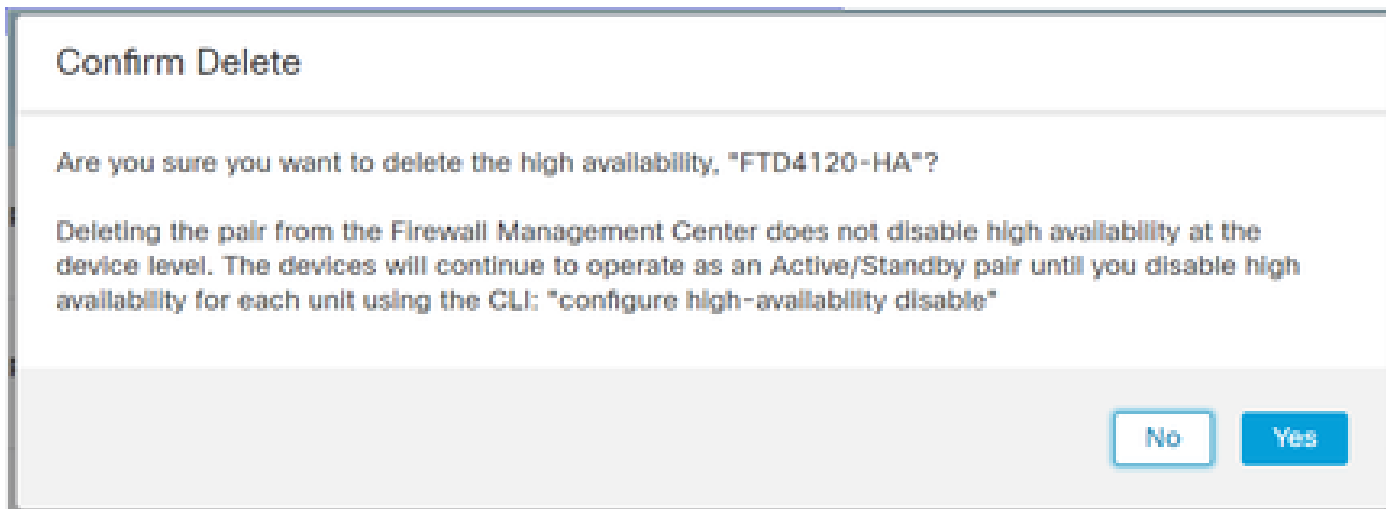
Solución:

Paso 1. Elija el icono como se muestra en la imagen:





Paso 2. Verifique la notificación y confirme como se muestra en la imagen:



Paso 3. Después de eliminar la HA, ambos dispositivos no están registrados (se eliminan) de la FMC.

El resultado de show running-config de la CLI de LINA es el que se muestra en la siguiente tabla:

Unidad principal (en espera)	Unidad secundaria (activa)
<pre>&gt; show running-config : Guardado : : Número de serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname Firepower-module1 enable password ***** encryption strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names</pre>	<pre>&gt; show running-config : Guardado : : Número de serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname Firepower-module1 enable password ***** encryption strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names</pre>

```
no mac-address auto
!
interface Port-channel2
no name if
no security-level
sin dirección de IP
!
interface Port-channel2.202
vlan 202
nameif NET202
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.202.1 255.255.255.0 standby
172.16.202.2
!
interface Port-channel2.203
vlan 203
nameif NET203
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.203.1 255.255.255.0 standby
172.16.203.2
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interfaz Ethernet1/1
solo de administración
nameif diagnostic
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
sin dirección de IP
!
interface Ethernet1/4
nameif NET204
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
```

```
no mac-address auto
!
interface Port-channel2
no name if
no security-level
sin dirección de IP
!
interface Port-channel2.202
vlan 202
nameif NET202
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.202.1 255.255.255.0 standby
172.16.202.2
!
interface Port-channel2.203
vlan 203
nameif NET203
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 172.16.203.1 255.255.255.0 standby
172.16.203.2
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interfaz Ethernet1/1
solo de administración
nameif diagnostic
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
sin dirección de IP
!
interface Ethernet1/4
nameif NET204
manual de CTS
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
```

<pre>ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIXER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003</pre>	<pre>ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIXER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003</pre>
--	--

ningún mensaje de registro 106100  
ningún mensaje de registro 302015  
ningún mensaje de registro 302014  
ningún mensaje de registro 302013  
ningún mensaje de registro 302018  
ningún mensaje de registro 302017  
ningún mensaje de registro 302016  
ningún mensaje de registro 302021  
ningún mensaje de registro 302020  
mtu NET202 1500  
mtu NET203 1500  
mtu diagnostic 1500  
mtu NET204 1500  
failover  
failover lan unit primary  
failover lan interface FOVER Port-channel3  
failover replication http  
failover link FOVER Port-channel3  
failover interface ip FOVER 172.16.51.1  
255.255.255.0 standby 172.16.51.2  
monitor-interface NET202  
monitor-interface NET203  
icmp unreachable rate-limit 1 burst-size 1

<salida omitida>

> show ip

Direcciones IP del sistema:

Nombre de interfaz Dirección IP Método de  
máscara de subred

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

Port-channel3 FOVER 172.16.51.1  
255.255.255.0 unset

Ethernet1/4 NET204 172.16.204.1  
255.255.255.0 CONFIG

Direcciones IP actuales:

Nombre de interfaz Dirección IP Método de  
máscara de subred

Port-channel2.202 NET202 172.16.202.2  
255.255.255.0 CONFIG

Port-channel2.203 NET203 172.16.203.2  
255.255.255.0 CONFIG

ningún mensaje de registro 106100  
ningún mensaje de registro 302015  
ningún mensaje de registro 302014  
ningún mensaje de registro 302013  
ningún mensaje de registro 302018  
ningún mensaje de registro 302017  
ningún mensaje de registro 302016  
ningún mensaje de registro 302021  
ningún mensaje de registro 302020  
mtu NET202 1500  
mtu NET203 1500  
mtu diagnostic 1500  
mtu NET204 1500  
failover  
failover lan unit secondary  
failover lan interface FOVER Port-channel3  
failover replication http  
failover link FOVER Port-channel3  
failover interface ip FOVER 172.16.51.1  
255.255.255.0 standby 172.16.51.2  
monitor-interface NET202  
monitor-interface NET203  
icmp unreachable rate-limit 1 burst-size 1

<salida omitida>

> show ip

Direcciones IP del sistema:

Nombre de interfaz Dirección IP Método de  
máscara de subred

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

Port-channel3 FOVER 172.16.51.1  
255.255.255.0 unset

Ethernet1/4 NET204 172.16.204.1  
255.255.255.0 CONFIG

Direcciones IP actuales:

Nombre de interfaz Dirección IP Método de  
máscara de subred

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

<p>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.2 255.255.255.0 CONFIG</p> <p>&gt; show failover Conmutación por error activada Unidad de conmutación por error principal Failover LAN Interface: FOVER Port-channel3 (up) Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1 Interfaces supervisadas 4 de 1291 como máximo Intervalo de notificación de movimiento de dirección MAC no definido failover replication http Versión: Nuestra 9.18(4)210, Mate 9.18(4)210 Número de serie: Nuestro FLM1949C5RR, Mate FLM2108V9YG Última conmutación por error a las: 13:56:37 UTC 16 de julio de 2024 Este host: principal - preparado para el modo de espera Tiempo activo: 0 (s) Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys) Interfaz NET202 (172.16.202.2): Normal (supervisada) Interface NET203 (172.16.203.2): Normal (Monitored) Diagnóstico de interfaz (0.0.0.0): Normal (en espera) Interfaz NET204 (172.16.204.2): Normal (supervisada) slot 1: estado de snort rev (1.0) (up) slot 2: diskstatus rev (1.0) status (up) Otro host: secundario - Activo Tiempo activo: 70293 (s) Interfaz NET202 (172.16.202.1): Normal (supervisada) Interfaz NET203 (172.16.203.1): Normal</p>	<p>Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG</p> <p>&gt; show failover Conmutación por error activada Unidad de failover secundaria Failover LAN Interface: FOVER Port-channel3 (up) Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1 Interfaces supervisadas 4 de 1291 como máximo Intervalo de notificación de movimiento de dirección MAC no definido failover replication http Versión: Nuestra 9.18(4)210, Mate 9.18(4)210 Número de serie: Nuestro FLM2108V9YG, Mate FLM1949C5RR Última conmutación por error a las: 13:42:35 UTC 16 de julio de 2024 Este host: Secundario - Activo Tiempo activo: 70312 (s) Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys) Interfaz NET202 (172.16.202.1): Normal (supervisada) Interfaz NET203 (172.16.203.1): Normal (supervisada) Diagnóstico de interfaz (0.0.0.0): Normal (en espera) Interfaz NET204 (172.16.204.1): Normal (supervisada) slot 1: estado de snort rev (1.0) (up) slot 2: diskstatus rev (1.0) status (up) Otro host: principal - preparado para el modo de espera Tiempo activo: 0 (s) Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys) Interfaz NET202 (172.16.202.2): Normal</p>
--	---

(supervisada) Diagnóstico de interfaz (0.0.0.0): Normal (en espera) Interfaz NET204 (172.16.204.1): Normal (supervisada) slot 1: estado de snort rev (1.0) (up) slot 2: diskstatus rev (1.0) status (up)  <salida omitida>	(supervisada) Interface NET203 (172.16.203.2): Normal (Monitored) Diagnóstico de interfaz (0.0.0.0): Normal (en espera) Interfaz NET204 (172.16.204.2): Normal (supervisada) slot 1: estado de snort rev (1.0) (up) slot 2: diskstatus rev (1.0) status (up)  <salida omitida>
--	---

Paso 4. Ambos dispositivos FTD no estaban registrados en el FMC:

```
<#root>
```

```
> show managers
```

```
No managers configured.
```

Principales puntos a tener en cuenta para la opción Desactivar HA en FMC:

Unidad primaria	Unidad secundaria
El dispositivo se elimina de la FMC.  No se ha eliminado ninguna configuración del dispositivo FTD.	El dispositivo se elimina de la FMC.  No se ha eliminado ninguna configuración del dispositivo FTD.

Escenario 1

Ejecute el comando 'configure high-availability disable' para quitar la configuración de failover del dispositivo FTD activo:

```
<#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.

El resultado:

Unidad principal (ex-Standby)	Unidad secundaria (exactiva)
<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>

Principal (antiguo en espera)	Secundario (ex activo)
<pre> &gt; show running-config : Guardado : : Número de serie: FLM1949C5RR : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname Firepower-module1 enable password ***** encryption strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 apagado no name if no security-level no ip address &lt;- Se eliminan las IP ! interface Port-channel3 description LAN/STATE Failover Interface ! interfaz Ethernet1/1 solo de administración apagado no name if no security-level sin dirección de IP ! interface Ethernet1/4 apagado no name if no security-level sin dirección de IP ! ftp mode passive </pre>	<pre> &gt; show running-config : Guardado : : Número de serie: FLM2108V9YG : Hardware: FPR4K-SM-24, 73853 MB de RAM, CPU Xeon serie E5 2200 MHz, 2 CPU (48 núcleos) : NGFW versión 7.2.8 ! hostname Firepower-module1 enable password ***** encryption strong-encryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 names no mac-address auto ! interface Port-channel2 no name if no security-level sin dirección de IP ! interface Port-channel2.202 vlan 202 nameif NET202 manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 172.16.203.1 255.255.255.0 standby </pre>



<pre> ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIXER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 </pre>	<pre> 172.16.203.2 ! interface Port-channel3 no name if no security-level sin dirección de IP ! interfaz Ethernet1/1 solo de administración nameif diagnostic manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 sin dirección de IP ! interface Ethernet1/4 nameif NET204 manual de CTS propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 172.16.204.1 255.255.255.0 standby 172.16.204.2 ! ftp mode passive ngips conn-match vlan-id no object-group-search access-control access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIXER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 access-list CSM_FW_ACL_advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_advanced permit gre any any rule-id 9998 </pre>
--	---

<p>ningún mensaje de registro 302018  ningún mensaje de registro 302017  ningún mensaje de registro 302016  ningún mensaje de registro 302021  ningún mensaje de registro 302020  ningún failover  failover lan unit primary  failover lan interface FOVER Port-channel3  failover replication http  failover link FOVER Port-channel3  failover interface ip FOVER 172.16.51.1  255.255.255.0 standby 172.16.51.2  no monitor-interface service-module</p> <p>&lt;salida omitida&gt;</p>	<pre> access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY: acp_simple - Default access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgente-flag allow ! no pager ningún mensaje de registro 106015 ningún mensaje de registro 313001 ningún mensaje de registro 313008 ningún mensaje de registro 106023 ningún mensaje de registro 710003 ningún mensaje de registro 106100 ningún mensaje de registro 302015 ningún mensaje de registro 302014 ningún mensaje de registro 302013 ningún mensaje de registro 302018 ningún mensaje de registro 302017 ningún mensaje de registro 302016 ningún mensaje de registro 302021 ningún mensaje de registro 302020 mtu NET202 1500 mtu NET203 1500 mtu diagnostic 1500 mtu NET204 1500 ningún failover monitor-interface NET202 monitor-interface NET203 no monitor-interface service-module </pre>
---	--

Puntos principales que deben tenerse en cuenta para la desactivación de HA de la CLI de FTD activa:

Unidad activa	Unidad en espera
---------------	------------------

<ul style="list-style-type: none"> <li>• Se quita la configuración de conmutación por error</li> <li>• Las IP en espera no se eliminan</li> </ul>	<ul style="list-style-type: none"> <li>• Se eliminan las configuraciones de interfaz.</li> <li>• La configuración de failover no se quita, pero el failover se inhabilita (pseudo-Standby)</li> </ul>
---	---

En este momento, puede desactivar el HA también en la unidad ex-Standby.

## Situación 2 (no recomendado)



Advertencia: Este escenario conduce a una situación Activo/Activo, por lo que no se recomienda. Se muestra solo para la conciencia.

Ejecute el comando 'configure high-availability disable' para quitar la configuración de failover del dispositivo FTD en espera:

```
<#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.
```

El resultado:

Principal (antiguo en espera)	Secundario (activo)
<pre>&gt; show failover Conmutación por error desactivada Unidad de failover secundaria Interfaz LAN de conmutación por error: no configurada Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds</pre>	<pre>&gt; show failover Failover On &lt;- Failover no está inhabilitado Unidad de failover secundaria Failover LAN Interface: FOVER Port-channel3 (up) Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds</pre>

Política de interfaz 1  
Interfaces supervisadas 4 de 1291 como máximo  
Intervalo de notificación de movimiento de dirección MAC no definido

> show ip  
Direcciones IP del sistema:  
Nombre de interfaz Dirección IP Método de máscara de subred  
Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- El dispositivo utiliza las mismas IP que el ex-Active!  
Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual  
Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual  
Direcciones IP actuales:  
Nombre de interfaz Dirección IP Método de máscara de subred  
Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual  
Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual  
Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual

Política de interfaz 1  
Interfaces supervisadas 4 de 1291 como máximo  
Intervalo de notificación de movimiento de dirección MAC no definido  
failover replication http  
Versión: Nuestra 9.18(4)210, Mate 9.18(4)210  
Número de serie: Nuestro FLM2108V9YG, Mate FLM1949C5RR  
Última conmutación por error a las: 12:44:06 UTC 17 de julio de 2024  
Este host: Secundario - Activo  
Tiempo activo: 632 (s)  
Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys)  
Diagnóstico de interfaz (0.0.0.0): Normal (en espera)  
Interfaz NET204 (172.16.204.1): Normal (supervisada)  
Interfaz NET203 (172.16.203.1): Normal (supervisada)  
Interfaz NET202 (172.16.202.1): Normal (supervisada)  
slot 1: estado de snort rev (1.0) (up)  
slot 2: diskstatus rev (1.0) status (up)  
Otro host: principal - deshabilitado  
Tiempo activo: 932 (s)  
Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys)  
Diagnóstico de interfaz (0.0.0.0): Desconocido (en espera)  
Interfaz NET204 (172.16.204.2): Desconocido (supervisado)  
Interfaz NET203 (172.16.203.2): Desconocido (supervisado)  
Interfaz NET202 (172.16.202.2): Desconocido (supervisado)  
slot 1: estado de snort rev (1.0) (up)  
slot 2: diskstatus rev (1.0) status (up)

> show ip  
Direcciones IP del sistema:  
Nombre de interfaz Dirección IP Método de máscara de subred  
Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual <- El dispositivo utiliza

	<p>las mismas IP que el ex-Standby!</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual</p> <p>Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset</p> <p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual</p> <p>Direcciones IP actuales: Nombre de interfaz Dirección IP Método de máscara de subred</p> <p>Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual</p> <p>Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset</p> <p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual</p>
--	---

Puntos principales que deben tenerse en cuenta para la desactivación de HA de la CLI de FTD activa:

Unidad activa	Unidad en espera
<ul style="list-style-type: none"> <li>• La configuración de failover no se quita y permanece habilitada</li> <li>• El dispositivo utiliza las mismas direcciones IP que la unidad en espera</li> </ul>	<ul style="list-style-type: none"> <li>• Se quita la configuración de conmutación por error</li> <li>• El dispositivo utiliza las mismas direcciones IP que la unidad activa</li> </ul>

### Escenario 3

Ejecute el comando 'configure high-availability disable clear-interfaces' para quitar la configuración de failover del dispositivo FTD activo:

```
<#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.

>

El resultado:

Principal (antiguo en espera)	Secundario (ex activo)
<pre>&gt; show failover Conmutación por error desactivada (pseudoen espera) Unidad de conmutación por error principal Failover LAN Interface: FOVER Port-channel3 (up) Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1 Interfaces supervisadas 0 de 1291 como máximo Intervalo de notificación de movimiento de dirección MAC no definido failover replication http  &gt; show ip Direcciones IP del sistema: Nombre de interfaz Dirección IP Método de máscara de subred Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Direcciones IP actuales: Nombre de interfaz Dirección IP Método de máscara de subred Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset &gt;</pre>	<pre>&gt; show failover Conmutación por error desactivada Unidad de failover secundaria Interfaz LAN de conmutación por error: no configurada Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1 Interfaces supervisadas 0 de 1291 como máximo Intervalo de notificación de movimiento de dirección MAC no definido  &gt; show ip Direcciones IP del sistema: Nombre de interfaz Dirección IP Método de máscara de subred Direcciones IP actuales: Nombre de interfaz Dirección IP Método de máscara de subred &gt;</pre>

Puntos principales a tener en cuenta para la desactivación de HA junto con 'clear-interfaces' de la CLI de FTD activo:

Unidad activa	Unidad en espera
<ul style="list-style-type: none"> <li>• Se quita la configuración de conmutación por error</li> <li>• Se eliminan las direcciones IP</li> </ul>	<ul style="list-style-type: none"> <li>• La configuración de failover no se quita, pero el failover se inhabilita (pseudo-Standby)</li> <li>• Se eliminan las direcciones IP</li> </ul>

#### Situación 4

Ejecute el comando 'configure high-availability disable clear-interfaces' para quitar la configuración de failover del dispositivo FTD en espera:

```
<#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.
```

```
>
```

El resultado:

Principal (antiguo en espera)	Secundario (activo)
<pre>&gt; show failover Conmutación por error desactivada Unidad de failover secundaria Interfaz LAN de conmutación por error: no configurada Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1</pre>	<pre>&gt; show failover Conmutación por error activada Unidad de failover secundaria Failover LAN Interface: FOVER Port-channel3 (up) Volver a conectar el tiempo de espera 0:00:00 Frecuencia de sondeo de unidad 1 segundos, tiempo de espera 15 segundos Interface Poll frequency 5 seconds, holdtime 25 seconds Política de interfaz 1</pre>

Interfaces supervisadas 0 de 1291 como máximo  
Intervalo de notificación de movimiento de dirección MAC no definido

> show ip

Direcciones IP del sistema:

Nombre de interfaz Dirección IP Método de máscara de subred

Direcciones IP actuales:

Nombre de interfaz Dirección IP Método de máscara de subred

>

Interfaces supervisadas 4 de 1291 como máximo

Intervalo de notificación de movimiento de dirección MAC no definido

failover replication http

Versión: Nuestra 9.18(4)210, Mate 9.18(4)210

Número de serie: Nuestro FLM2108V9YG, Mate FLM1949C5RR

Última conmutación por error a las: 07:06:56

UTC 18 de julio de 2024

Este host: Secundario - Activo

Tiempo activo: 1194 (s)

Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys)

Diagnóstico de interfaz (0.0.0.0): Normal (en espera)

Interfaz NET204 (172.16.204.1): Normal (supervisada)

Interfaz NET202 (172.16.202.1): Normal (supervisada)

Interfaz NET203 (172.16.203.1): Normal (supervisada)

slot 1: estado de snort rev (1.0) (up)

slot 2: diskstatus rev (1.0) status (up)

Otro host: principal - deshabilitado

Tiempo activo: 846 (s)

Ranura 0: estado de UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) (Up Sys)

Diagnóstico de interfaz (0.0.0.0): Desconocido (en espera)

Interfaz NET204 (172.16.204.2): Desconocido (supervisado)

Interfaz NET202 (172.16.202.2): Desconocido (supervisado)

Interfaz NET203 (172.16.203.2): Desconocido (supervisado)

slot 1: estado de snort rev (1.0) (up)

slot 2: diskstatus rev (1.0) status (up)

> show ip

Direcciones IP del sistema:

Nombre de interfaz Dirección IP Método de máscara de subred

Port-channel2.202 NET202 172.16.202.1  
255.255.255.0 manual

Port-channel2.203 NET203 172.16.203.1



	255.255.255.0 manual Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual Direcciones IP actuales: Nombre de interfaz Dirección IP Método de máscara de subred Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual Port-channel2.203 NET203 172.16.203.1 255.255.255.0 manual Port-channel3 FOVER 172.16.51.2 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0 manual
--	---

Puntos principales a tener en cuenta para la desactivación de HA junto con 'clear-interfaces' de la CLI de FTD activo:

Unidad activa	Unidad en espera
<ul style="list-style-type: none"> <li>• La configuración de failover no se quita</li> <li>• Las direcciones IP no se quitan</li> </ul>	<ul style="list-style-type: none"> <li>• Se quita la configuración de conmutación por error</li> <li>• Se eliminan las direcciones IP</li> </ul>

Paso 6. Después de finalizar la tarea, registre los dispositivos en la FMC y active el par de HA.

## Tarea 7. Suspend HA

Tarea requerida:

Suspend la HA de la CLI de CLISH de FTD

Solución:

Paso 1. En el FTD principal, ejecute el comando y confirme (escriba 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.

Paso 2. Verifique los cambios en la unidad principal:

```
<#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
```

Paso 3. El resultado en la unidad secundaria:

```
<#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
```

Paso 4. Reanudar HA en la unidad principal:

```
<#root>
```

```
>
```

```
configure high-availability resume
```

```
Successfully resumed high-availability.
```

```
> .  
  
No Active mate detected  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
Beginning configuration replication: Sending to mate.  
End Configuration Replication to mate
```

```
>
```

```
<#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
```

Paso 5. El resultado en la unidad secundaria después de reanudar 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
>
```

## Preguntas frecuentes

Cuando se replica la configuración, ¿se guarda inmediatamente (línea por línea) o al final de la replicación?

Al final de la replicación. La evidencia se encuentra al final del resultado del comando debug fover sync que muestra la réplica de comando/configuración:

```
<#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      <--
```

¿Qué sucede si una unidad se encuentra en un estado pseudoen espera (conmutación por error deshabilitada) y luego la recarga mientras la otra unidad tiene la conmutación por error habilitada y está activa?

Usted termina en un escenario Activo/Activo (aunque técnicamente es un escenario Activo/Failover-off). Específicamente, una vez que esté ACTIVA, la conmutación por error se deshabilita, pero la unidad utiliza las mismas IP que la unidad activa. Así que efectivamente, tiene:

- Unidad-1: activa
- Unidad 2: la conmutación por error está desactivada. La unidad utiliza las mismas IP de datos que la Unidad 1, pero diferentes direcciones MAC.

¿Qué sucede con la configuración de conmutación por error si deshabilita manualmente la conmutación por error (configurar suspensión de alta disponibilidad) y, a continuación, recarga el dispositivo?

Cuando inhabilita el failover, no es un cambio permanente (no se guarda en startup-config a menos que decida hacer esto explícitamente). Puede reiniciar/recargar la unidad de 2 maneras diferentes y con la segunda debe tener cuidado:

#### Caso 1. Reiniciar desde CLISH

El reinicio desde CLISH no requiere confirmación. Por lo tanto, el cambio de configuración no se guarda en startup-config:

```
<#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.
```

El running-config tiene el failover inhabilitado. En este caso, la unidad estaba en espera y entró en el estado pseudo-en espera como se esperaba para evitar un escenario Activo/Activo:

```
<#root>
```

```
firepower#
```

```
show failover | include Failover
```

```
Failover Off (
```

```
pseudo-standby
```

```
)
```

```
Failover unit Secondary
```

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

La configuración de inicio tiene la conmutación por fallas aún habilitada:

```
<#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 *****
```

Reinicie el dispositivo desde 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 vez que la unidad está ACTIVA, dado que la conmutación por error esté activada, el dispositivo ingresa en la fase de negociación de conmutación por error e intenta detectar el par 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. Reiniciar desde LINA de CLI

Reiniciar desde LINA (comando reload) requiere confirmación. Por lo tanto, en caso de que seleccione Y (Sí), el cambio de configuración se guarda en startup-config:

```
<#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 *****
```

Una vez que la unidad está ACTIVA, la conmutación por error se desactiva:

```
<#root>
firepower#

show failover | include Fail

Failover Off

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



Nota: Para evitar este escenario, asegúrese de que cuando se le solicite, no guarde los cambios en startup-config.

---

## Información Relacionada

- Todas las versiones de la guía de configuración del Centro de administración Firepower se pueden encontrar aquí.

[Navegación por la documentación de Cisco Secure Firewall Threat Defence](#)

- Todas las versiones de las guías de configuración de la CLI y el administrador de chasis FXI se pueden encontrar aquí

## [Navegación por la documentación de Cisco Firepower 4100/9300 FXOS](#)

- Cisco Global Technical Assistance Center (TAC) recomienda encarecidamente esta guía visual para obtener un conocimiento práctico en profundidad de las tecnologías de seguridad de última generación de Cisco Firepower:

[Cisco Firepower Threat Defence \(FTD\): configuración y solución de problemas de prácticas recomendadas para el firewall de última generación \(NGFW\), el sistema de prevención de intrusiones de última generación \(NGIPS\) y la protección frente a malware avanzado \(AMP\)](#)

- Para todas las notas técnicas de configuración y solución de problemas relacionadas con las tecnologías Firepower

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

- [Soporte Técnico y Documentación - Cisco Systems](#)



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).