

# 在 Firepower 設備上設定 FTD 高可用性

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[任務1.驗證條件](#)

[任務2.設定FTD HA](#)

[狀況](#)

[任務3.驗證FTD HA和授權](#)

[任務4.切換容錯移轉角色](#)

[任務5.中斷HA對](#)

[任務6.刪除HA對](#)

[任務7.暫停HA](#)

[常見問題 \(FAQ\)](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何在Firepower裝置上配置和驗證Firepower威脅防禦(FTD)高可用性(HA) ( 主用/備用故障切換 )。

## 必要條件

### 需求

本文件沒有特定需求。


### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 2個Cisco Firepower 9300
- 2個Cisco Firepower 4100 (7.2.8)
- Firepower管理中心(FMC) (7.2.8)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 ( 預設 ) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

---

 註：在帶有FTD的FPR9300裝置上，您只能配置機箱間HA。HA 組態中的兩個裝置必須符合本文件提及的條件。

---

## 任務1. 驗證條件

工作需求：

確認兩台FTD裝置均符合備註要求，且可設定為HA裝置。

解決方案：

步驟 1. 連線到FPR9300管理IP並驗證模組硬體。

確認 FPR9300-1 硬體。

```
<#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#
```

確認 FPR9300-2 硬體。

```
<#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#
```

步驟 2. 登入到FPR9300-1機箱管理器，然後導航到邏輯裝置。

檢驗軟體版本、介面編號和型別。

## 任務2. 設定FTD HA

工作需求：

按照此圖表設定作用中/待命容錯移轉 (HA)。在這種情況下，使用41xx配對。

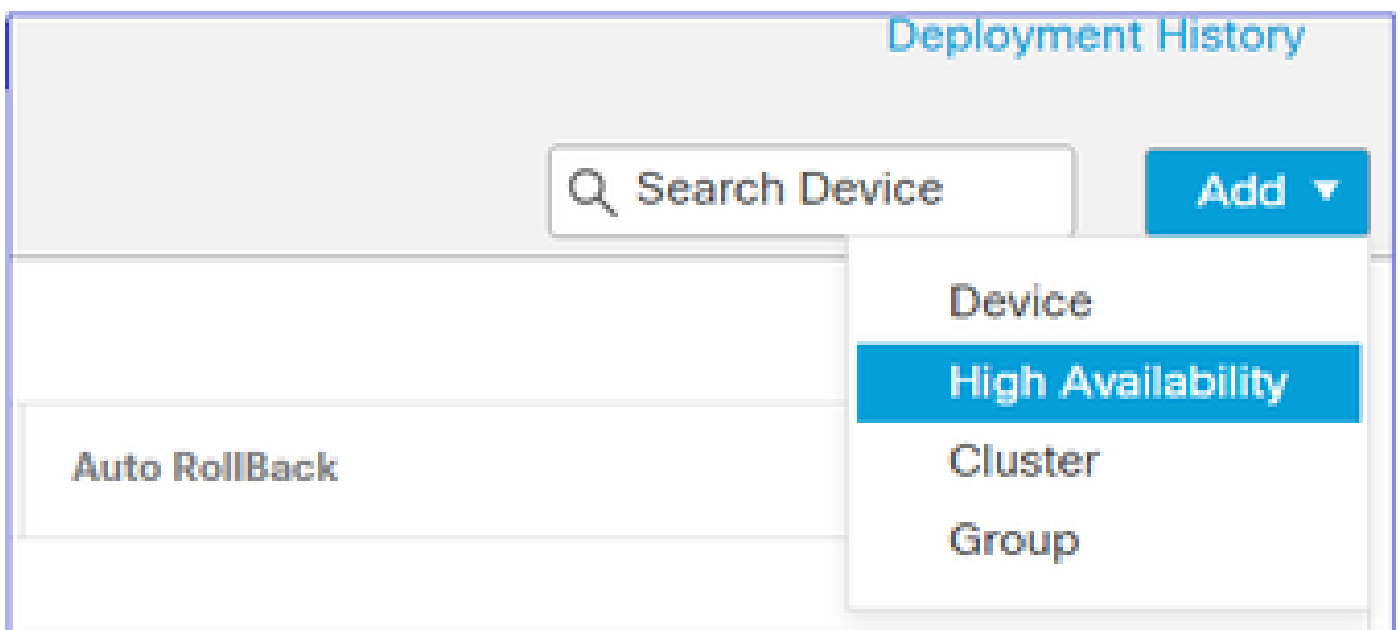


## 解決方案

兩個 FTD 裝置已在 FMC 註冊，如圖所示。

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	↔	✎

步驟 1. 若要設定 FTD 容錯移轉，請導覽至 Devices > Device Management，然後選擇 Add High Availability，如下圖所示。



步驟 2.輸入Primary Peer和Secondary Peer，然後選擇Continue，如下圖所示。

**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.

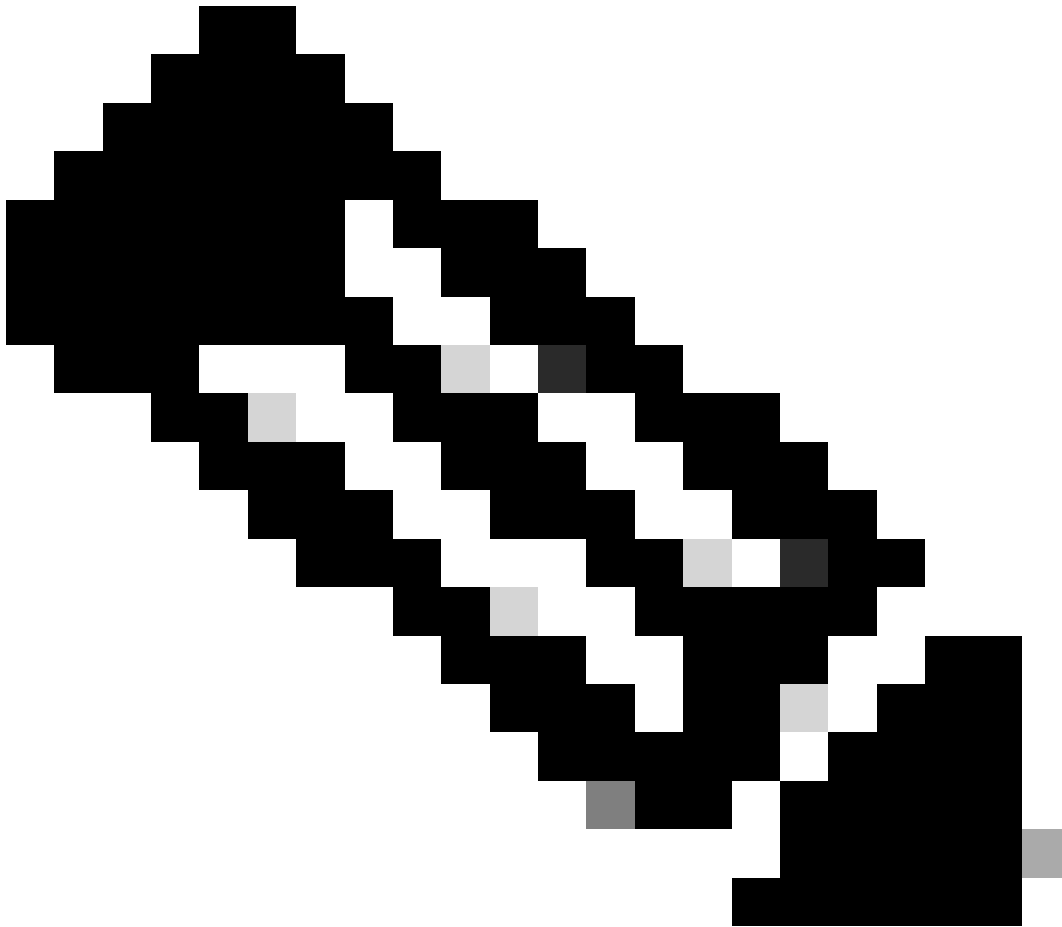
Cancel Continue

**警告：**請確定選取正確的單位作為主要單位。所選主要裝置上的所有組態都會複製到所選輔助FTD裝置。由於複製，可以替換輔助裝置上的當前配置。

## 狀況

若要在 2 個 FTD 裝置之間建立 HA，必須符合下列條件：

- 型號相同
  - 相同版本-適用於FXOS和FTD -主要 ( 第一個數字 )、次要 ( 第二個數字 ) 和維護 ( 第三個數字 ) 必須相等。
  - 介面數目相同
  - 介面類型相同
  - 兩台裝置作為FMC中同一組/域的一部分。
  - 具有相同的網路時間協定(NTP)配置。
  - 完全部署在FMC上，無需進行未提交的更改。
  - 處於相同的防火牆模式：路由或透明。
- 



附註：在FTD裝置和FMC GUI上都必須核取此專案，因為有時候FTD使用的是相同模式，但FMC並未反映此模式。

- 
- 在任何介面中沒有配置DHCP/乙太網點對點協定(PPPoE)。
  - 兩個機箱的主機名[完全限定域名(FQDN)]不同。要檢查機箱主機名，請導航到FTD CLI，然後運行此命令：

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

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

---

 注意：在6.3以後的FTD中，請使用show chassis detail命令。

---

```
<#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
```

如果兩個機箱的名稱相同，請使用下列命令變更其中一個機箱的名稱：

```
<#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
#
```

變更機箱名稱後，請從 FMC 取消註冊 FTD，然後再重新註冊。接著，繼續建立 HA 配對。

步驟 3. 配置 HA 並宣告鏈路設定。

依照您的情況，狀態連結的設定與高可用性相同。

選擇 Add，然後等待幾分鐘，以便部署 HA 對，如圖所示。

**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

**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

步驟 4. 配置資料介面 ( 主用 IP 地址和備用 IP 地址 )

在 FMC GUI 中，選擇 HA Edit，如下圖所示。

Interface	IP Address	Status	Device	Version	Security Module	Threat Policy	Actions
FTD4100-5(Primary, Active)	10.62.148.188	Routed	Firepower 4120 with FTD	7.2.8	FP4100-6.443 Security Module - 1	Base, Threat (2 more...)	acp_simple
FTD4100-6(Secondary, Standby)	10.62.148.191	Routed	Firepower 4120 with FTD	7.2.8	FP4100-6.443 Security Module - 1	Base, Threat (2 more...)	acp_simple

步驟 5. 配置介面設定：

### Edit Physical Interface

General IPv4 IPv6 Path Monitoring Advanced

Name:

Enabled  
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:  
  
(64 - 9184)

Priority:  
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

### Edit Physical Interface

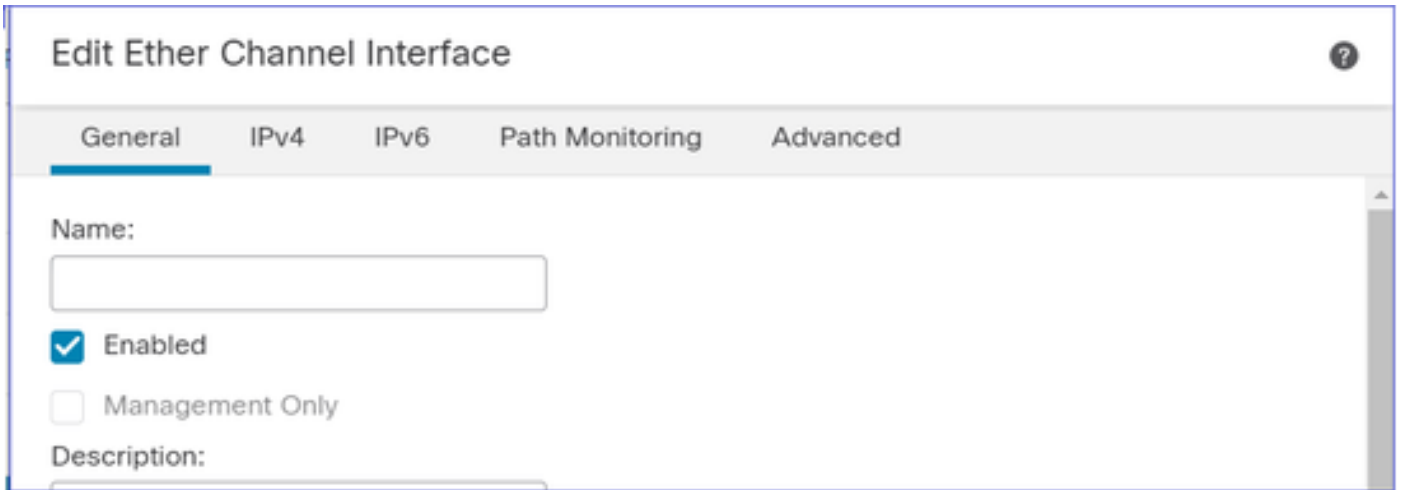
General IPv4 IPv6 Path Monitoring Advanced

IP Type:

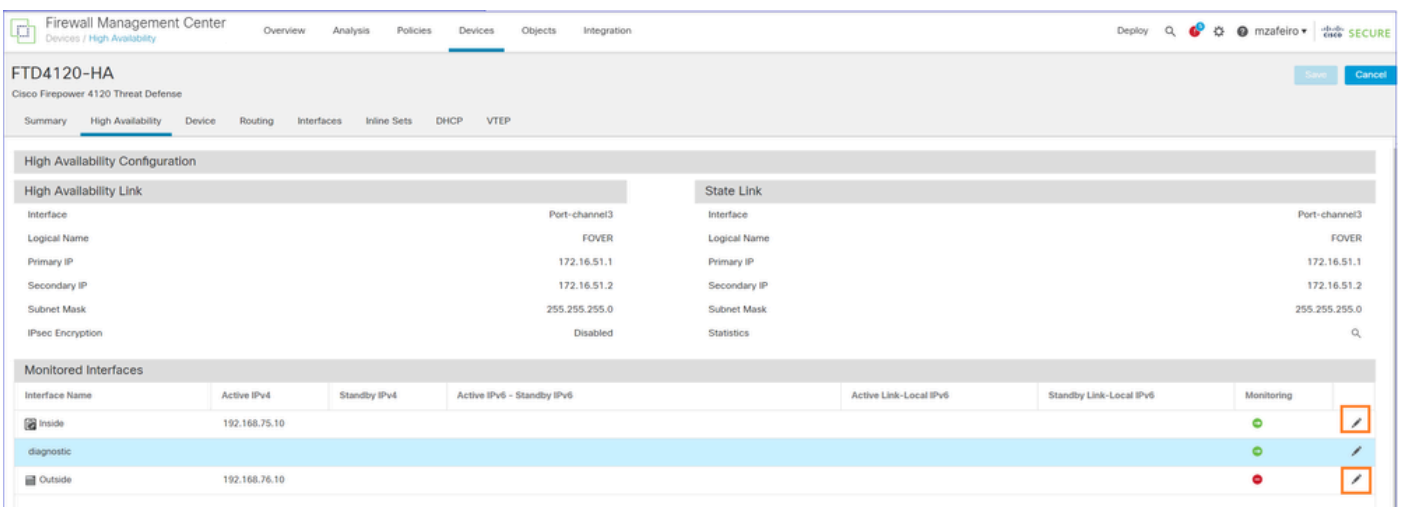
IP Address:  
  
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

在子介面的情況下，需要首先啟用父介面：





步驟 6. 導覽至High Availability，然後選擇Interface Name Edit以新增待命IP位址，如下圖所示。



步驟 7. 用於Inside介面，如圖所示。

## 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

步驟 8.對Outside介面執行相同的操作。

步驟 9.驗證結果如圖所示。

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				● /
diagnostic						● /
Outside	192.168.76.10	192.168.76.11				● /

步驟 10.保留「High Availability」索引標籤，並設定虛擬MAC位址，如圖所示。

### Interface MAC Addresses

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

+

步驟 11.如圖所示。

## 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

步驟 12.對Outside介面執行相同的操作。

步驟 13.驗證結果如圖所示。

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	

步驟 14. 配置更改後，請選擇Save和Deploy。

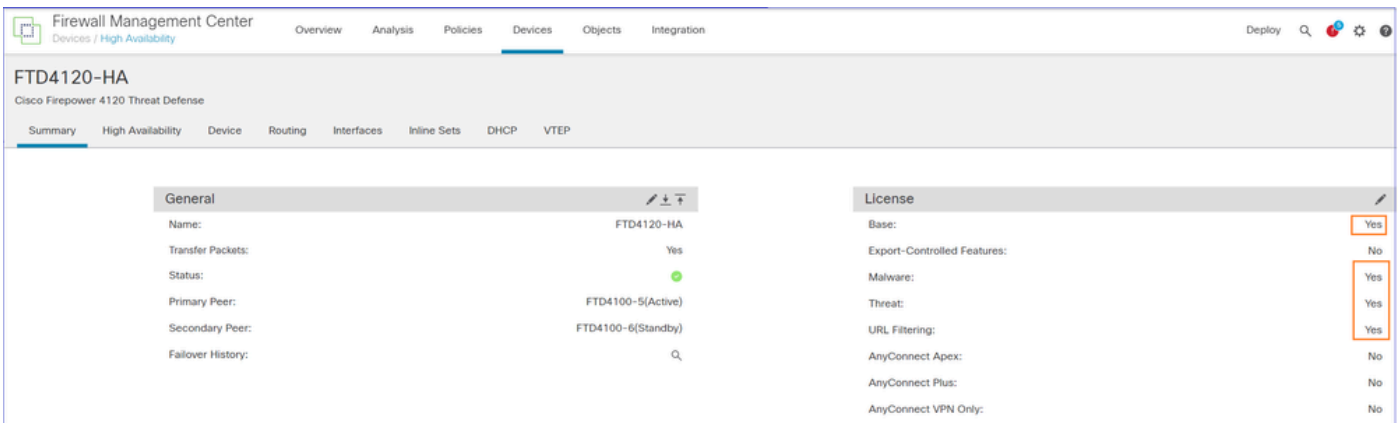
## 任務3. 驗證FTD HA和授權

工作需求：


透過 FMC GUI 和 FTD CLI 確認 FTD HA 設定和已啟用的授權。

解決方案：

步驟 1. 導航到摘要，檢查HA設定和已啟用的許可證，如下圖所示。



The screenshot shows the FMC GUI for a Cisco Firepower 4120 Threat Defense device in High Availability mode. The 'General' tab is active, displaying the following configuration:

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

The **License** section shows the following status:

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

步驟 2. 從FTD CLISH CLI，執行「show high-availability config」或「show failover」指令：

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-chnane13 (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>

步驟 3.在輔助裝置上執行相同的操作。

步驟 4.從LINA CLI運行show failover state命令：

<#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#

步驟 5.從主要單元(LINA CLI)驗證設定：

<#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
>
```

## 任務4. 切換容錯移轉角色

工作需求：

在 FMC 中，將容錯移轉角色從「主要/作用中」、「次要/待命」切換成「主要/待命」、「次要/作用中」

解決方案：

步驟 1. 選取圖示 ( 如圖所示 ) 。



步驟 2. 確認操作。

可以使用 show failover history 命令輸出：

<p>在新的使用中</p>	<p>在新待</p>
<pre> &gt; show failover history ===== 從狀態到狀態原因 =====  世界協調時2024年7月18日09時27分11秒 備用就緒僅啟用其他裝置希望我啟用 ( 透過config命令設定 )  世界協調時2024年7月18日09時27分11秒 僅使用主動式主動式排水其他裝置想要我使用主動式 ( 透過config命令設定 )  世界協調時2024年7月18日09時27分11秒 主用漏極主用應用配置其他單元想要我主用 ( 透過config命令設定 )  世界協調時2024年7月18日09時27分11秒 Active Applying Config Active Config Applied Other unit deses me Active ( 透過config命令設定 )  世界協調時2024年7月18日09時27分11秒 Active Config Applied Active Other Unit希望我處於活動狀態 ( 透過config命令設定 ) </pre>	<p>&gt; show ===== 從狀態 ===== 世界協 Active :</p>

步驟 4. 驗證後，請再次啟用主裝置。

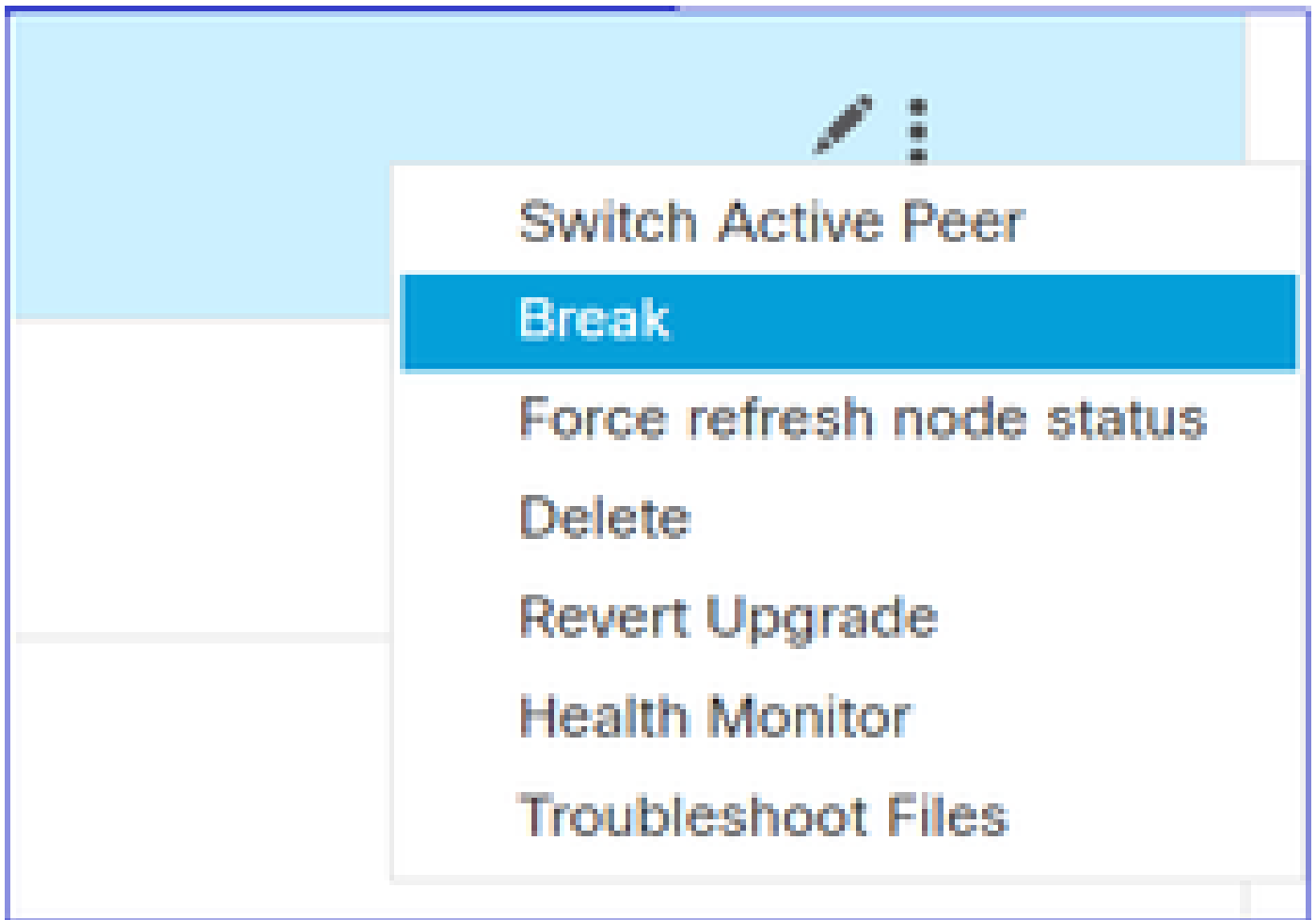
## 任務5. 中斷HA對

工作需求：

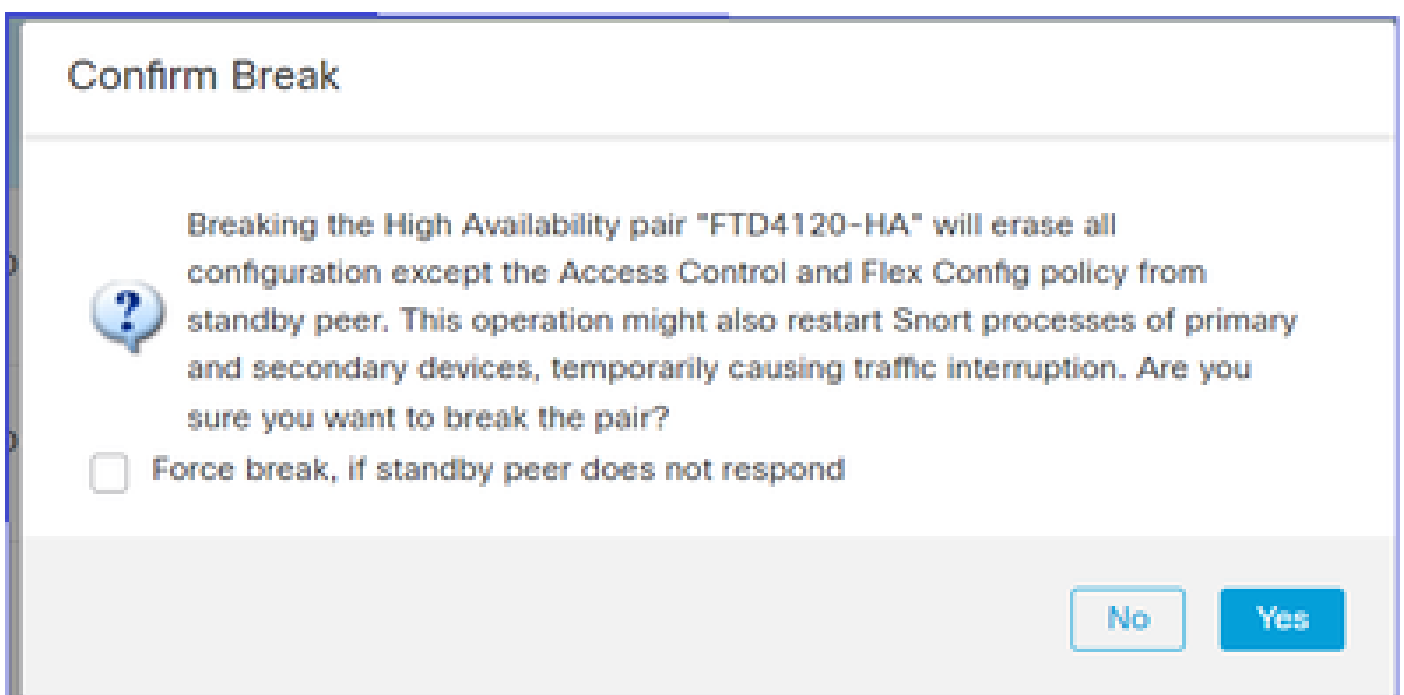
在 FMC 中分割容錯移轉配對。

解決方案：

步驟 1. 選取圖示（如圖所示）。

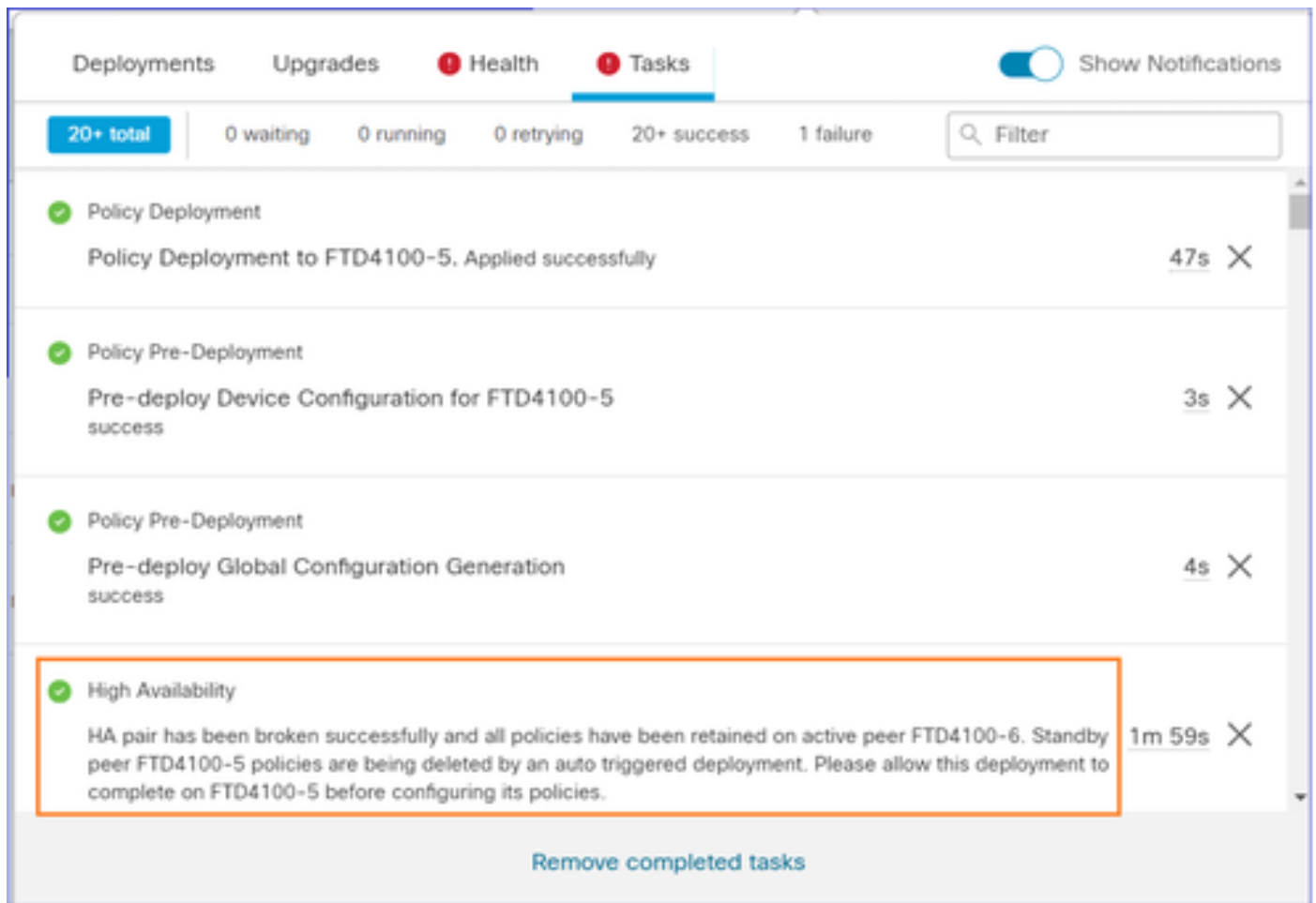


步驟 2. 請檢查圖中所示的通知。





步驟 3.請注意如下圖所示的消息。



步驟 4.從FMC GUI或CLI驗證結果

在執行 HA 分割之前和之後，主要裝置上的 show running-config：

HA中斷前的主/備用裝置	HA中斷後的主裝置
<pre>&gt; show running-config : 已儲存 : : 序列號 : FLM1949C5RR : 硬體 : FPR4K-SM-24 , 73850 MB RAM , CPU Xeon E5系列2200 MHz , 2個CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4</pre>	<pre>&gt;資訊：此裝置當前處於備用狀態。透過停用故障轉移，此裝置將保持備用狀態。 &gt; show running-config : 已儲存 : : 序列號 : FLM1949C5RR : 硬體 : FPR4K-SM-24 , 73850 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 !</pre>

<pre> service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 無名稱 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 無安全等級 無ip地址 ! interface Port-channel2.202 vlan 202 nameif Outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 說明LAN/狀態故障切換介面 ! interface Ethernet1/1 僅管理 nameif diagnostic cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif Inside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11 ! ftp mode passive ngips conn-match vlan-id </pre>	<pre> 主機名firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 關機 無名稱 無安全等級 無ip地址 ! interface Port-channel3 關機 無名稱 無安全等級 無ip地址 ! interface Ethernet1/1 僅管理 關機 無名稱 無安全等級 無ip地址 ! interface Ethernet1/4 關機 無名稱 無安全等級 無ip地址 ! 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 </pre>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<pre> 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 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : ACCESS POLICY : acp_simple - 預設 access-list CSM_FW_ACL_ remark rule-id 268434433 : L4 RULE : 預設操作規則 access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp選項範圍6 7允許 tcp-options範圍9 18 allow tcp-options range 20 255 allow urgent-flag allow ! 無尋呼機 no logging message 106015 -無記錄訊息 no logging message 313001 -無記錄訊息 no logging message 313008 -無記錄訊息 no logging message 106023 -無記錄訊息 no logging message 710003 -無記錄訊息 no logging message 106100 -無記錄訊息 no logging message 302015 -無記錄訊息 no logging message 302014 -無記錄訊息 no logging message 302013 -無記錄訊息 no logging message 302018 -無記錄訊息 no logging message 302017 -無記錄訊息 no logging message 302016 -無記錄訊息 no logging message 302021 -無記錄訊息 no logging message 302020 -無記錄訊息 </pre>	<pre> 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 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268439552 : ACCESS POLICY : acp_simple - 必備 access-list CSM_FW_ACL_ remark rule-id 268439552 : L7規則 : rule1 access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268439552 ! tcp-map UM_STATIC_TCP_MAP tcp選項範圍6 7允許 tcp-options範圍9 18 allow tcp-options range 20 255 allow urgent-flag allow ! 無尋呼機 no logging message 106015 -無記錄訊息 no logging message 313001 -無記錄訊息 no logging message 313008 -無記錄訊息 no logging message 106023 -無記錄訊息 no logging message 710003 -無記錄訊息 no logging message 106100 -無記錄訊息 no logging message 302015 -無記錄訊息 no logging message 302014 -無記錄訊息 no logging message 302013 -無記錄訊息 no logging message 302018 -無記錄訊息 no logging message 302017 -無記錄訊息 no logging message 302016 -無記錄訊息 no logging message 302021 -無記錄訊息 no logging message 302020 -無記錄訊息 無故障轉移 &lt;省略部分輸出&gt; </pre>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<pre> no logging message 302020 -無記錄訊息 1500以外的MTU mtu diagnostic 1500 mtu Inside 1500 容錯移轉 主要容錯移轉lan裝置 failover lan interface FOVER Port-channel3 故障切換複製http 故障轉移mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222 故障轉移mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444 故障切換鏈路FOVER Port-channel3 故障切換介面IP FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2  &lt;省略部分輸出&gt; </pre>	
<p>高可用性中斷前的輔助/主用裝置</p>	<p>HA中斷之後的輔助裝置</p>
<pre> &gt; show running-config : 已儲存 : : 序列號 : FLM2108V9YG : 硬體 : FPR4K-SM-24 , 73850 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto ! interface Port-channel2 無名稱 無安全等級 無ip地址 ! </pre>	<pre> &gt; show running-config : 已儲存 : : 序列號 : FLM2108V9YG : 硬體 : FPR4K-SM-24 , 73850 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名firepower enable password ***** encrypted strong-cryption-disable service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto ! interface Port-channel2 無名稱 無安全等級 無ip地址 ! </pre>

<pre> interface Port-channel2.202 vlan 202 nameif Outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 說明LAN/狀態故障切換介面 ! interface Ethernet1/1 僅管理 nameif diagnostic 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif Inside 安全性層級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 </pre>	<pre> ! interface Port-channel2.202 vlan 202 nameif Outside cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11 ! interface Port-channel3 無名稱 無安全等級 無ip地址 ! interface Ethernet1/1 僅管理 nameif diagnostic 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif Inside 安全性層級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 </pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>any rule-id 9998  access-list CSM_FW_ACL_ remark rule-id  268439552 : ACCESS POLICY : acp_simple -  必備  access-list CSM_FW_ACL_ remark rule-id  268439552 : L7規則 : rule1  access-list CSM_FW_ACL_ advanced permit ip  any any rule-id 268439552  !  tcp-map UM_STATIC_TCP_MAP  tcp選項範圍6 7允許  tcp-options範圍9 18 allow  tcp-options range 20 255 allow  urgent-flag allow  !  無尋呼機  no logging message 106015 -無記錄訊息  no logging message 313001 -無記錄訊息  no logging message 313008 -無記錄訊息  no logging message 106023 -無記錄訊息  no logging message 710003 -無記錄訊息  no logging message 106100 -無記錄訊息  no logging message 302015 -無記錄訊息  no logging message 302014 -無記錄訊息  no logging message 302013 -無記錄訊息  no logging message 302018 -無記錄訊息  no logging message 302017 -無記錄訊息  no logging message 302016 -無記錄訊息  no logging message 302021 -無記錄訊息  no logging message 302020 -無記錄訊息  1500以外的MTU  mtu diagnostic 1500  mtu Inside 1500  容錯移轉  故障轉移lan單元輔助  failover lan interface FOVER Port-channel3  故障切換複製http  故障切換鏈路FOVER Port-channel3  故障切換介面IP FOVER 172.16.51.1  255.255.255.0 standby 172.16.51.2  &lt;省略部分輸出&gt;</p>	<p>access-list CSM_FW_ACL_ advanced permit 41  any any rule-id 9998  access-list CSM_FW_ACL_ advanced permit gre  any rule-id 9998  access-list CSM_FW_ACL_ remark rule-id  268439552 : ACCESS POLICY : acp_simple -  必備  access-list CSM_FW_ACL_ remark rule-id  268439552 : L7規則 : rule1  access-list CSM_FW_ACL_ advanced permit ip  any any rule-id 268439552  !  tcp-map UM_STATIC_TCP_MAP  tcp選項範圍6 7允許  tcp-options範圍9 18 allow  tcp-options range 20 255 allow  urgent-flag allow  !  無尋呼機  no logging message 106015 -無記錄訊息  no logging message 313001 -無記錄訊息  no logging message 313008 -無記錄訊息  no logging message 106023 -無記錄訊息  no logging message 710003 -無記錄訊息  no logging message 106100 -無記錄訊息  no logging message 302015 -無記錄訊息  no logging message 302014 -無記錄訊息  no logging message 302013 -無記錄訊息  no logging message 302018 -無記錄訊息  no logging message 302017 -無記錄訊息  no logging message 302016 -無記錄訊息  no logging message 302021 -無記錄訊息  no logging message 302020 -無記錄訊息  1500以外的MTU  mtu diagnostic 1500  mtu Inside 1500  無故障轉移  no monitor-interface外部  no monitor-interface service-module  &lt;省略部分輸出&gt;</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

HA 分割的主要注意事項 :

主/備用裝置	輔助/主用裝置
<ul style="list-style-type: none"> <li>會移除所有容錯移轉組態</li> <li>刪除所有IP配置</li> </ul>	<ul style="list-style-type: none"> <li>會移除所有容錯移轉組態</li> <li>備用IP將保留，但在下次部署時刪除</li> </ul>

步驟 5.完成此任務後，重新建立HA對。

## 任務6.刪除HA對

此任務基於使用7.2.8軟體在41xx上進行的HA設定。在本例中，裝置最初處於以下狀態：

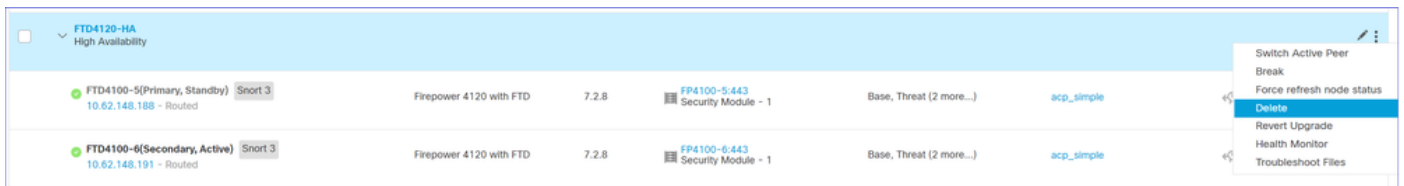
- 主要/標準
- 輔助/主用

工作需求：

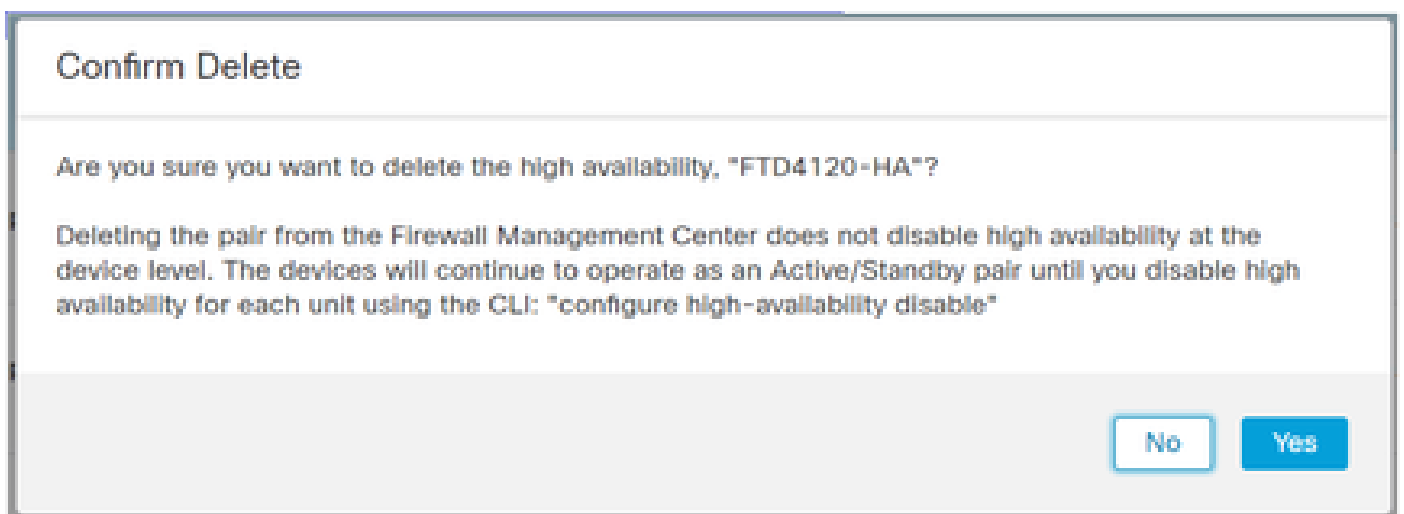
從FMC中刪除故障轉移對。

解決方案：

步驟 1.選擇圖示，如下圖所示：



步驟 2.檢查通知並進行確認，如下圖所示：



步驟 3.刪除HA後，兩個裝置都將從FMC中註銷（刪除）。

LINA CLI 傳回的 show running-config 結果，如下表所示：

主裝置 ( 備用 )	輔助裝置 ( 活動 )
<pre> &gt; show running-config : 已儲存  : : 序列號 : FLM1949C5RR : 硬體 : FPR4K-SM-24 , 73853 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名Firepower-module1 enable password ***** encrypted strong-cryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 無名稱 無安全等級 無ip地址 ! interface Port-channel2.202 vlan 202 nameif NET202 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 172.16.203.1 255.255.255.0 standby </pre>	<pre> &gt; show running-config : 已儲存  : : 序列號 : FLM2108V9YG : 硬體 : FPR4K-SM-24 , 73853 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名Firepower-module1 enable password ***** encrypted strong-cryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 無名稱 無安全等級 無ip地址 ! interface Port-channel2.202 vlan 202 nameif NET202 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 172.16.203.1 255.255.255.0 standby </pre>



<pre> 172.16.203.2 ! interface Port-channel3 說明LAN/狀態故障切換介面 ! interface Ethernet1/1 僅管理 nameif diagnostic cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif NET204 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級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 : 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 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id </pre>	<pre> 172.16.203.2 ! interface Port-channel3 說明LAN/狀態故障切換介面 ! interface Ethernet1/1 僅管理 nameif diagnostic cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif NET204 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級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 : 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 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id </pre>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

268434433 : ACCESS POLICY : acp\_simple -  
預設  
access-list CSM\_FW\_ACL\_ remark rule-id  
268434433 : L4 RULE : 預設操作規則  
access-list CSM\_FW\_ACL\_ advanced permit ip  
any any rule-id 268434433  
!  
tcp-map UM\_STATIC\_TCP\_MAP  
tcp選項範圍6 7允許  
tcp-options範圍9 18 allow  
tcp-options range 20 255 allow  
tcp-options md5 clear  
urgent-flag allow  
!  
無尋呼機  
no logging message 106015 -無記錄訊息  
no logging message 313001 -無記錄訊息  
no logging message 313008 -無記錄訊息  
no logging message 106023 -無記錄訊息  
no logging message 710003 -無記錄訊息  
no logging message 106100 -無記錄訊息  
no logging message 302015 -無記錄訊息  
no logging message 302014 -無記錄訊息  
no logging message 302013 -無記錄訊息  
no logging message 302018 -無記錄訊息  
no logging message 302017 -無記錄訊息  
no logging message 302016 -無記錄訊息  
no logging message 302021 -無記錄訊息  
no logging message 302020 -無記錄訊息  
mtu NET202 1500  
mtu NET203 1500  
mtu diagnostic 1500  
mtu NET204 1500  
容錯移轉  
主要容錯移轉lan裝置  
failover lan interface FOVER Port-channel3  
故障切換複製http  
故障切換鏈路FOVER Port-channel3  
故障切換介面IP FOVER 172.16.51.1  
255.255.255.0 standby 172.16.51.2  
監控介面NET202  
監控介面NET203  
icmp unreachable rate-limit 1 burst-size 1  
  
<省略部分輸出>

268434433 : ACCESS POLICY : acp\_simple -  
預設  
access-list CSM\_FW\_ACL\_ remark rule-id  
268434433 : L4 RULE : 預設操作規則  
access-list CSM\_FW\_ACL\_ advanced permit ip  
any any rule-id 268434433  
!  
tcp-map UM\_STATIC\_TCP\_MAP  
tcp選項範圍6 7允許  
tcp-options範圍9 18 allow  
tcp-options range 20 255 allow  
tcp-options md5 clear  
urgent-flag allow  
!  
無尋呼機  
no logging message 106015 -無記錄訊息  
no logging message 313001 -無記錄訊息  
no logging message 313008 -無記錄訊息  
no logging message 106023 -無記錄訊息  
no logging message 710003 -無記錄訊息  
no logging message 106100 -無記錄訊息  
no logging message 302015 -無記錄訊息  
no logging message 302014 -無記錄訊息  
no logging message 302013 -無記錄訊息  
no logging message 302018 -無記錄訊息  
no logging message 302017 -無記錄訊息  
no logging message 302016 -無記錄訊息  
no logging message 302021 -無記錄訊息  
no logging message 302020 -無記錄訊息  
mtu NET202 1500  
mtu NET203 1500  
mtu diagnostic 1500  
mtu NET204 1500  
容錯移轉  
故障轉移lan單元輔助  
failover lan interface FOVER Port-channel3  
故障切換複製http  
故障切換鏈路FOVER Port-channel3  
故障切換介面IP FOVER 172.16.51.1  
255.255.255.0 standby 172.16.51.2  
監控介面NET202  
監控介面NET203  
icmp unreachable rate-limit 1 burst-size 1  
  
<省略部分輸出>

```
> show ip
系統IP位址：
介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置
當前IP地址：
介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.2
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.2
255.255.255.0配置
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.2
255.255.255.0配置

> show failover
容錯移轉開啟
主要容錯移轉單元
容錯移轉LAN介面：FOVER Port-channel3 (up)
重新連線超時0:00:00
單位輪詢頻率1秒，保持時間15秒
介面輪詢頻率5秒，保持時間25秒
介面策略1
受監控的介面4 ( 最多1291個 )
未設定MAC地址移動通知間隔
故障切換複製http
版本：Ours 9.18(4)210、Mate 9.18(4)210
序號：我們的FLM1949C5RR、配對
FLM2108V9YG
上次故障切換時間：UTC 2024年7月16日
13:56:37
此主機：主要-待命就緒
活動時間：0 ( 秒 )
插槽0：UCSB-B200-M3-U硬體/軟體版本
(0.0/9.18(4)210)狀態 ( 啟動系統 )
NET202介面(172.16.202.2)：正常 ( 受監控 )
NET203介面(172.16.203.2)：正常 ( 受監控 )
介面診斷(0.0.0.0)：正常 ( 等待 )
NET204介面(172.16.204.2)：正常 ( 受監控 )
```

```
> show ip
系統IP位址：
介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置
Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置
當前IP地址：
介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置
Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置
Port-channel3 FOVER 172.16.51.2
255.255.255.0 ( 未設定 )
Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置

> show failover
容錯移轉開啟
故障轉移裝置輔助
容錯移轉LAN介面：FOVER Port-channel3 (up)
重新連線超時0:00:00
單位輪詢頻率1秒，保持時間15秒
介面輪詢頻率5秒，保持時間25秒
介面策略1
受監控的介面4 ( 最多1291個 )
未設定MAC地址移動通知間隔
故障切換複製http
版本：Ours 9.18(4)210、Mate 9.18(4)210
序號：我們的FLM2108V9YG、配對
FLM1949C5RR
上次故障切換時間：UTC 2024年7月16日
13:42:35
此主機：次要-活動
使用中時間：70312 ( 秒 )
插槽0：UCSB-B200-M3-U硬體/軟體版本
(0.0/9.18(4)210)狀態 ( 啟動系統 )
NET202介面(172.16.202.1)：正常 ( 受監控 )
NET203介面(172.16.203.1)：正常 ( 受監控 )
介面診斷(0.0.0.0)：正常 ( 等待 )
NET204介面(172.16.204.1)：正常 ( 受監控 )
```

插槽1 : snort rev (1.0)狀態(up) 插槽2 : diskstatus rev (1.0)狀態(up) 其他主機 : 次要-活動 使用中時間 : 70293 ( 秒 ) NET202介面(172.16.202.1) : 正常 ( 受監控 ) NET203介面(172.16.203.1) : 正常 ( 受監控 ) 介面診斷(0.0.0.0) : 正常 ( 等待 ) NET204介面(172.16.204.1) : 正常 ( 受監控 ) 插槽1 : snort rev (1.0)狀態(up) 插槽2 : diskstatus rev (1.0)狀態(up)  <省略部分輸出>	插槽1 : snort rev (1.0)狀態(up) 插槽2 : diskstatus rev (1.0)狀態(up) 其他主機 : 主要-待命就緒 活動時間 : 0 ( 秒 ) 插槽0 : UCSB-B200-M3-U硬體/軟體版本 (0.0/9.18(4)210)狀態 ( 啟動系統 ) NET202介面(172.16.202.2) : 正常 ( 受監控 ) NET203介面(172.16.203.2) : 正常 ( 受監控 ) 介面診斷(0.0.0.0) : 正常 ( 等待 ) NET204介面(172.16.204.2) : 正常 ( 受監控 ) 插槽1 : snort rev (1.0)狀態(up) 插槽2 : diskstatus rev (1.0)狀態(up)  <省略部分輸出>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

步驟 4.兩台FTD裝置皆已從FMC中取消註冊 :

```
<#root>
> show managers
No managers configured.
```

FMC 中「停用 HA 」選項的主要注意事項 :

主要單位	輔助裝置
會從 FMC 中移除裝置。	會從 FMC 中移除裝置。
不會從 FTD 裝置移除任何組態。	不會從 FTD 裝置移除任何組態。

案例 1

運行「configure high-availability disable」命令以從活動FTD裝置刪除故障切換配置 :

```
<#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.

結果：

主裝置 ( 非備用 )	輔助裝置 ( 非活動 )
<pre> &gt; INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state.  &gt; 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 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  &gt; 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 </pre>	<pre> &gt; 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  &gt; 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 </pre>

主要 ( 非待命 )	輔助 ( 非活動 )
<pre> &gt; show running-config : 已儲存  : : 序列號 : FLM1949C5RR : 硬體 : FPR4K-SM-24 , 73853 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名Firepower-module1 enable password ***** encrypted strong-cryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 關機 無名稱 無安全等級 no ip address &lt;-刪除IP ! interface Port-channel3 說明LAN/狀態故障切換介面 ! interface Ethernet1/1 僅管理 關機 無名稱 無安全等級 無ip地址 ! interface Ethernet1/4 關機 無名稱 無安全等級 無ip地址 ! ftp mode passive </pre>	<pre> &gt; show running-config : 已儲存  : : 序列號 : FLM2108V9YG : 硬體 : FPR4K-SM-24 , 73853 MB RAM , CPU Xeon E5系列2200 MHz , 2個 CPU ( 48核 ) : NGFW版本7.2.8 ! 主機名Firepower-module1 enable password ***** encrypted strong-cryption-disable no asp inspect-dp ack-passthrough service-module 0 keepalive-timeout 4 service-module 0 keepalive-counter 6 名稱 no mac-address auto  ! interface Port-channel2 無名稱 無安全等級 無ip地址 ! interface Port-channel2.202 vlan 202 nameif NET202 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 ip address 172.16.202.1 255.255.255.0 standby 172.16.202.2 ! interface Port-channel2.203 vlan 203 nameif NET203 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級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 : 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 rule-id 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : ACCESS POLICY : acp_simple - 預設 access-list CSM_FW_ACL_ remark rule-id 268434433 : L4 RULE : 預設操作規則 access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433 ! tcp-map UM_STATIC_TCP_MAP tcp選項範圍6 7允許 tcp-options範圍9 18 allow tcp-options range 20 255 allow tcp-options md5 clear urgent-flag allow ! 無尋呼機 no logging message 106015 -無記錄訊息 no logging message 313001 -無記錄訊息 no logging message 313008 -無記錄訊息 no logging message 106023 -無記錄訊息 no logging message 710003 -無記錄訊息 no logging message 106100 -無記錄訊息 no logging message 302015 -無記錄訊息 no logging message 302014 -無記錄訊息 no logging message 302013 -無記錄訊息 </pre>	<pre> 172.16.203.2 ! interface Port-channel3 無名稱 無安全等級 無ip地址 ! interface Ethernet1/1 僅管理 nameif diagnostic cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級0 無ip地址 ! interface Ethernet1/4 nameif NET204 cts手冊 propagate sgt preserve-untag 策略靜態sgt已停用受信任 安全性層級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 : 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 </pre>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>no logging message 302018 -無記錄訊息  no logging message 302017 -無記錄訊息  no logging message 302016 -無記錄訊息  no logging message 302021 -無記錄訊息  no logging message 302020 -無記錄訊息  無故障轉移  主要容錯移轉lan裝置  failover lan interface FOVER Port-channel3  故障切換複製http  故障切換鏈路FOVER Port-channel3  故障切換介面IP FOVER 172.16.51.1  255.255.255.0 standby 172.16.51.2  no monitor-interface service-module</p> <p>&lt;省略部分輸出&gt;</p>	<p>any rule-id 9998  access-list CSM_FW_ACL_ remark rule-id  268434433 : ACCESS POLICY : acp_simple -  預設  access-list CSM_FW_ACL_ remark rule-id  268434433 : L4 RULE : 預設操作規則  access-list CSM_FW_ACL_ advanced permit ip  any any rule-id 268434433  !  tcp-map UM_STATIC_TCP_MAP  tcp選項範圍6 7允許  tcp-options範圍9 18 allow  tcp-options range 20 255 allow  tcp-options md5 clear  urgent-flag allow  !  無尋呼機  no logging message 106015 -無記錄訊息  no logging message 313001 -無記錄訊息  no logging message 313008 -無記錄訊息  no logging message 106023 -無記錄訊息  no logging message 710003 -無記錄訊息  no logging message 106100 -無記錄訊息  no logging message 302015 -無記錄訊息  no logging message 302014 -無記錄訊息  no logging message 302013 -無記錄訊息  no logging message 302018 -無記錄訊息  no logging message 302017 -無記錄訊息  no logging message 302016 -無記錄訊息  no logging message 302021 -無記錄訊息  no logging message 302020 -無記錄訊息  mtu NET202 1500  mtu NET203 1500  mtu diagnostic 1500  mtu NET204 1500  無故障轉移  監控介面NET202  監控介面NET203  no monitor-interface service-module</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

從作用中FTD CLI停用HA的注意事項：


使用中單位	備用裝置
-------	------



<ul style="list-style-type: none"> <li>• 已移除容錯移轉設定</li> <li>• 未移除待命IP</li> </ul>	<ul style="list-style-type: none"> <li>• 會移除介面組態.</li> <li>• 未移除容錯移轉組態，但已停用容錯移轉（虛擬待命）</li> </ul>
----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------

此時，您也可以在前備用裝置上停用HA。

案例2 (不建議)

 警告：此案例會導致「活動/活動」情況，因此不建議使用。僅用於感知。

運行「configure high-availability disable」命令以從備用FTD裝置刪除故障切換配置：

```
<#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.
```

結果：

主要（非待命）	輔助（活動）
<pre>&gt; show failover 故障切換關閉 故障轉移裝置輔助 容錯移轉LAN介面：未設定 重新連線超時0:00:00 單位輪詢頻率1秒，保持時間15秒 介面輪詢頻率5秒，保持時間25秒 介面策略1 受監控的介面4（最多1291個） 未設定MAC地址移動通知間隔  &gt; show ip 系統IP位址： 介面名稱IP地址子網掩碼方法</pre>	<pre>&gt; show failover 故障切換於&lt;-未停用故障切換 故障轉移裝置輔助 容錯移轉LAN介面：FOVER Port-channel3 (up) 重新連線超時0:00:00 單位輪詢頻率1秒，保持時間15秒 介面輪詢頻率5秒，保持時間25秒 介面策略1 受監控的介面4（最多1291個） 未設定MAC地址移動通知間隔 故障切換複製http 版本：Ours 9.18(4)210、Mate 9.18(4)210 序號：我們的FLM2108V9YG、配對 FLM1949C5RR 上次故障切換時間：UTC 2024年7月17日</pre>

<p>Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊&lt;-裝置使用與ex-Active相同的 IP !</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊</p> <p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊</p> <p>當前IP地址： 介面名稱IP地址子網掩碼方法</p> <p>Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊</p> <p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊</p>	<p>12:44:06</p> <p>此主機：次要-活動</p> <p>活動時間：632 ( 秒 )</p> <p>插槽0：UCSB-B200-M3-U硬體/軟體版本 (0.0/9.18(4)210)狀態 ( 啟動系統 )</p> <p>介面診斷(0.0.0.0)：正常 ( 等待 )</p> <p>NET204介面(172.16.204.1)：正常 ( 受監控 )</p> <p>NET203介面(172.16.203.1)：正常 ( 受監控 )</p> <p>NET202介面(172.16.202.1)：正常 ( 受監控 )</p> <p>插槽1：snort rev (1.0)狀態(up)</p> <p>插槽2：diskstatus rev (1.0)狀態(up)</p> <p>其他主機：主要-已停用</p> <p>活動時間：932 ( 秒 )</p> <p>插槽0：UCSB-B200-M3-U硬體/軟體版本 (0.0/9.18(4)210)狀態 ( 啟動系統 )</p> <p>介面診斷(0.0.0.0)：未知 ( 等待 )</p> <p>NET204介面(172.16.204.2)：未知 ( 受監控 )</p> <p>Interface NET203 (172.16.203.2)：未知 ( 受監 控 )</p> <p>Interface NET202 (172.16.202.2)：未知 ( 受監 控 )</p> <p>插槽1：snort rev (1.0)狀態(up)</p> <p>插槽2：diskstatus rev (1.0)狀態(up)</p> <p>&gt; show ip</p> <p>系統IP位址：</p> <p>介面名稱IP地址子網掩碼方法</p> <p>Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊&lt;-裝置使用與ex-Standby相同的 IP !</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊</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手冊</p> <p>當前IP地址： 介面名稱IP地址子網掩碼方法</p> <p>Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊</p> <p>Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊</p> <p>Port-channel3 FOVER 172.16.51.2 255.255.255.0 ( 未設定 )</p> <p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

從作用中FTD CLI停用HA的注意事項：

使用中單位	備用裝置
<ul style="list-style-type: none"> <li>故障切換配置未刪除，仍保持啟用狀態</li> <li>裝置使用與ex-Standby裝置相同的IP</li> </ul>	<ul style="list-style-type: none"> <li>已移除容錯移轉設定</li> <li>裝置使用與主用裝置相同的IP</li> </ul>

### 案例 3

運行configure high-availability disable clear-interfaces命令以從活動FTD裝置刪除故障切換配置：

```
<#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.
```

```
>
```

結果：

主要（非待命）	輔助（非活動）
<pre>&gt; show failover 故障切換關閉（虛擬備用） 主要容錯移轉單元 容錯移轉LAN介面：FOVER Port-channel3 (up) 重新連線超時0:00:00 單位輪詢頻率1秒，保持時間15秒 介面輪詢頻率5秒，保持時間25秒 介面策略1 受監控介面0的最大值為1291 未設定MAC地址移動通知間隔 故障切換複製http</pre>	<pre>&gt; show failover 故障切換關閉 故障轉移裝置輔助 容錯移轉LAN介面：未設定 重新連線超時0:00:00 單位輪詢頻率1秒，保持時間15秒 介面輪詢頻率5秒，保持時間25秒 介面策略1 受監控介面0的最大值為1291 未設定MAC地址移動通知間隔</pre>

<pre>&gt; show ip 系統IP位址： 介面名稱IP地址子網掩碼方法 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset 當前IP地址： 介面名稱IP地址子網掩碼方法 Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset &gt;</pre>	<pre>&gt; show ip 系統IP位址： 介面名稱IP地址子網掩碼方法 當前IP地址： 介面名稱IP地址子網掩碼方法 &gt;</pre>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------

自活動FTD CLI停用HA以及「clear-interfaces」的注意事項：

使用中單位	備用裝置
<ul style="list-style-type: none"> <li>• 已移除容錯移轉設定</li> <li>• IP將被刪除</li> </ul>	<ul style="list-style-type: none"> <li>• 未移除容錯移轉組態，但已停用容錯移轉（虛擬待命）</li> <li>• IP將被刪除</li> </ul>

#### 案例 4

運行configure high-availability disable clear-interfaces命令，從備用FTD裝置刪除故障切換配置：

```
<#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.
```

```
>
```

結果：

主要（非待命）	輔助（活動）
---------	--------

```
> show failover
故障切換關閉
故障轉移裝置輔助
容錯移轉LAN介面：未設定
重新連線超時0:00:00
單位輪詢頻率1秒，保持時間15秒
介面輪詢頻率5秒，保持時間25秒
介面策略1
受監控介面0的最大值為1291
未設定MAC地址移動通知間隔
```

```
> show ip
系統IP位址：
介面名稱IP地址子網掩碼方法
當前IP地址：
介面名稱IP地址子網掩碼方法
>
```

```
> show failover
容錯移轉開啟
故障轉移裝置輔助
容錯移轉LAN介面：FOVER Port-channel3 (up)
重新連線超時0:00:00
單位輪詢頻率1秒，保持時間15秒
介面輪詢頻率5秒，保持時間25秒
介面策略1
受監控的介面4 (最多1291個)
未設定MAC地址移動通知間隔
故障切換複製http
版本：Ours 9.18(4)210、Mate 9.18(4)210
序號：我們的FLM2108V9YG、配對
FLM1949C5RR
上次故障切換時間：07:06:56 UTC 2024年7月
18日
此主機：次要-活動
活動時間：1194 (秒)
插槽0：UCSB-B200-M3-U硬體/軟體版本
(0.0/9.18(4)210)狀態 (啟動系統)
介面診斷(0.0.0.0)：正常 (等待)
NET204介面(172.16.204.1)：正常 (受監控)
NET202介面(172.16.202.1)：正常 (受監控)
NET203介面(172.16.203.1)：正常 (受監控)
插槽1：snort rev (1.0)狀態(up)
插槽2：diskstatus rev (1.0)狀態(up)
其他主機：主要-已停用
活動時間：846 (秒)
插槽0：UCSB-B200-M3-U硬體/軟體版本
(0.0/9.18(4)210)狀態 (啟動系統)
介面診斷(0.0.0.0)：未知 (等待)
NET204介面(172.16.204.2)：未知 (受監控)
Interface NET202 (172.16.202.2)：未知 (受監
控)
Interface NET203 (172.16.203.2)：未知 (受監
控)
插槽1：snort rev (1.0)狀態(up)
插槽2：diskstatus rev (1.0)狀態(up)

> show ip
系統IP位址：
介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.1
255.255.255.0手冊
Port-channel2.203 NET203 172.16.203.1
255.255.255.0手冊
```

	Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊 當前IP地址： 介面名稱IP地址子網掩碼方法 Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊 Port-channel3 FOVER 172.16.51.2 255.255.255.0 ( 未設定 ) Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

自活動FTD CLI停用HA以及「clear-interfaces」的注意事項：

使用中單位	備用裝置
<ul style="list-style-type: none"> <li>• 未移除容錯移轉設定</li> <li>• 未刪除IP</li> </ul>	<ul style="list-style-type: none"> <li>• 已移除容錯移轉設定</li> <li>• IP將被刪除</li> </ul>

步驟 6.完成任務後，將裝置註冊到FMC並啟用HA對。

## 任務7.暫停HA

工作需求：

透過 FTD CLISH CLI 暫停 HA

解決方案：

步驟 1.在主FTD上，執行指令並確認(鍵入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.
```

步驟 2. 驗證主裝置上的更改：

```

<#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

```

步驟 3. 輔助裝置上的結果：

```

<#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

```

步驟 4. 恢復主裝置上的HA：

```

<#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

步驟 5. 恢復HA後輔助裝置上的結果：

<#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
>
```

## 常見問題 (FAQ)

複製配置時，是立即（逐行）儲存配置，還是在複製結束時儲存配置？

在複製結束時。證據就是在 debug fover sync 命令輸出的結尾，會顯示組態/命令複製：

```
<#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 <--
```

如果裝置處於偽備用狀態（停用故障切換），然後在另一個裝置已啟用故障切換且處於活動狀態時重新載入該裝置，會發生什麼情況？

最終您將進入主用/主用場景（儘管技術上講是主用/故障切換關閉）。具體地說，就是裝置啟動後，容錯移轉便會停用，但裝置會使用與作用中裝置相同的 IP。因此，您實際上會有：

- Unit-1：活動
- Unit-2：故障切換關閉。裝置使用與Unit-1相同的資料IP，但使用不同的MAC地址。

如果手動停用故障切換（配置高可用性掛起），然後重新載入裝置，故障切換配置會發生什麼情況？

停用故障切換時，它不是永久更改（除非您決定明確執行此操作，否則不會儲存在啟動配置中）。您可以使用兩種不同的方式重新啟動/重新載入裝置，使用第二種方式時必須小心：

## 案例 1.從CLISH重新啟動

透過 CLISH 重新啟動不會要求確認。因此，組態變更不會儲存在啟動組態中：

```
<#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.
```

running-config已停用故障轉移。在這種情況下，裝置處於備用狀態，並如預期進入偽備用狀態，以避免主用/主用方案：

```
<#root>
```

```
firepower#
```

```
show failover | include Failover
```

```
Failover Off (
```

```
pseudo-standby
```

```
)
```

```
Failover unit Secondary
```

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

startup-config仍然啟用故障切換：

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

透過 CLISH 重新啟動裝置 ( reboot 命令 ) :

```
<#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 ...
```

裝置啟動後，容錯移轉便會啟用，因此裝置會進入容錯移轉交涉階段並嘗試偵測遠端對等：

```
<#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
```

## 案例 2. 從 LINA CLI 重新啟動

透過 LINA 重新啟動 ( reload 命令 ) 會要求確認。因此，如果選擇 Y ( 是 )，配置更改將儲存到啟動配置中：

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

裝置啟動後，容錯移轉便會停用：

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

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

---

 注意：要避免這種情況，請確保在出現提示時，不要將更改儲存到啟動配置中。

---

## 相關資訊

- 您可以在下列位置找到所有 Cisco Firepower Management Center 版本的組態設定指南：

[導航思科安全防火牆威脅防禦文檔](#)

- 您可以在下列位置找到所有 FXOS 機箱管理員版本和 CLI 的組態設定指南：

[瀏覽Cisco Firepower 4100/9300 FXOS文檔](#)

- 思科全球技術支援中心(TAC)強烈建議使用以下視覺指南，深入瞭解Cisco Firepower下一代安全技術：

[Cisco Firepower威脅防禦\(FTD\)：下一代防火牆\(NGFW\)、下一代入侵防禦系統\(NGIPS\)和高級惡意軟體防護\(AMP\)的配置和故障排除最佳實踐](#)

- 有關Firepower技術的所有配置和故障排除技術說明

[Cisco安全防火牆管理中心](#)

- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。