在 Firepower 設備上設定 FTD 高可用性

目錄

 簡介

 必要條件

 憲求

 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-FI	PR9K-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-FP	R9K-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 Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	<q+< th=""><th>1</th></q+<>	1
FTD4100-6 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	¢۶	1

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。





Add High Availability Pair Name:* FTD4100-HA Device Type: Firewall Threat Defense	nt (2
Name:* FTD4100-HA Device Type: Firewall Threat Defense	rt (;
FTD4100-HA Device Type: Firewall Threat Defense	rt (: rt (:
Device Type: Firewall Threat Defense	rt (;
Firewall Threat Defense 🔻	a ()
Primary Peer:	
FTD4100-5	
Secondary Peer:	
FTD4100-6 v	
Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.	
Cancel Continue	

▲ 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。

Interface:* Port-channel3 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 Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 IPsec Encryption Enabled Key Generation: Auto	ligh Availability Link	State Link		
Logical Name:* FOVER Logical Name:* FOVER Primary IP:* 172.16.51.1 Primary IP:* 172.16.51.1 Use IPv6 Address Use IPv6 Address Use IPv6 Address Secondary IP:* 172.16.51.2 Secondary IP:* 172.16.51.2 Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 Psec Encryption Image: Secondary IP:* Image: Secondary IP:* Image: Secondary IP:*	Interface:* Port-channel3	▼ Interface:*	Same as LAN Failover Link	٣
Primary IP:* 172.16.51.1 Primary IP:* 172.16.51.1 Use IPv6 Address Use IPv6 Address Secondary IP:* 172.16.51.2 Secondary IP:* 172.16.51.2 Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 Psec Encryption Image: Conservation: Auto Image: Conservation:	ogical Name:* FOVER	Logical Name:*	FOVER	
Use IPv6 Address Use IPv6 Address Secondary IP:* 172.16.51.2 Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 Psec Encryption Enabled	Primary IP:* 172.16.51.1	Primary IP:*	172.16.51.1	
Secondary IP:* 172.16.51.2 Secondary IP:* 172.16.51.2 Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 Psec Encryption Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2 Image: Conservation in the secondary IP:* 172.16.51.2	Use IPv6 Address		Use IPv6 Address	
Subnet Mask:* 255.255.255.0 Subnet Mask:* 255.255.255.0 Psec Encryption Enabled Cert Generation: Auto	Secondary IP:* 172.16.51.2	Secondary IP:*	172.16.51.2	
Psec Encryption Enabled	Subnet Mask:* 255.255.255.0	Subnet Mask:*	255.255.255.0	
Veu Ceneration: Auto	Enabled			
Vey deneration. Auto				

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。

V FTD4120-HA High Availability							1
FTD4100-5(Primary, Active) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	¢9	:
FTD4100-6(Secondary, Standby) Short 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EII Security Module - 1	Base, Threat (2 more)	acp_simple	¢Þ	:

步驟 5.配置介面設定:

General IPv6 Path Monitoring Advanced Name:	Edit Physi	cal Inter	face				0
Name: Inside Ensided Management Only Description: Mode: None None Security Zene: Imagement 1/4 Mtl: 1500 (# - 9184) Prioring: (# - 65325) Propagate Security Group Tag: NE Only:	General	IPv4	IPv6	Path Monitoring	Advanced		
Inside Ensided Management Only Description: Mode: None None Security Zone: v Interface ID: Ethernet1/4 MTU: 1500 (d - 9184) Priority: 0 (v) - 65535) Propagate Security Group Tag: NVE Only:	Namec						
Enabled Management Only Description: Mode: Mode: None Scurity Zone: Tetrface ID: Ethemet1/4 MTU: 1500 (0 - 65525) Propagate Security Group Tag: (0 - 65525) Propagate Security Group Tag: (0 - 65525)	Inside						
Management: Only Description: Mode: Mone Nome Security Zone: Interface ID: Ethermet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65525) Propagate Security Group Tag: NKE Only:	Enabled						
Description: Mode: None Security Zone: v Interface ID: Ethernet1/4 MO0 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NKE Only:	Manager	nent Only					
Mode: None Security Zone: v Interface ID: Ethemet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only:	Description:						
Mode: None Security Zone: Security Zone: Tetraface ID: Ethernet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: OCCOND: OCCOND: OCCOND: Cancel OCC							
None • Security Zone: • Interface ID: • Ethemet1/4 • MTU: • 1500 • (#4 - 9184) • Priority: • 0 • NVE Only: • • •	Mode:						
Security Zone:	None			*			
w Interface ID: Ethernet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only:	Security Zon	e:					
Interface ID: Ethernet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: .				*			
Etternet1/4 MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: Cancel CK	Interface ID:						
MTU: 1500 (64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: Cancel CK	Ethernet1/-	4					
1500 (%4 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: Cancel OK	MTU:						
(64 - 9184) Priority: 0 (0 - 65535) Propagate Security Group Tag: NVE Only: Cancel OK	1500						
Priority:	(64 - 9184)						
0 (0 - 63535) Propagate Security Group Tag: NVE Only: Cancel OK	Priority:						
Propagate Security Group Tag:	0			(0 - 65535)			
NVE Only: Cancel OK	Propagate Se	ecurity Gr	oup Tag:				
Cancel OK	NVE Only:						
Cancel OK							
							Cancel OK

Edit Physical Interface			Θ
General IPv4 IPv6	Path Monitoring	Advanced	
IP Type:			
Use Static IP	Ŧ		
IP Address:			
192.168.75.10/24			
eg. 192.0.2.1/255.255.255.128 or 1	192.0.2.1/25		
			Cancel OK

在子介面的情況下,需要首先啟用父介面:

Edit Ether	Channe	el Interfa	ace		0
General	IPv4	IPv6	Path Monitoring	Advanced	
Name:	nent Only				
Description:	ion only				

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。

Firewall Management Cer Devices / High Availability	overview	Analysis Policies	Devices Objects Integra	tion			Deploy Q 🚱 🔅	mzafeiro •	cite SECURE
FTD4120-HA Cisco Firepower 4120 Threat Defense Summary High Availability Devi	ce Routing Interfa	ces Inline Sets DI	ICP VTEP					Sav	Cancel
High Availability Configuration									
High Availability Link					State Link				
Interface			Port-channel3		Interface			Port-o	channel3
Logical Name			FOVER		Logical Name				FOVER
Primary IP			172.16.51.1		Primary IP			172	.16.51.1
Secondary IP			172.16.51.2		Secondary IP			172	.16.51.2
Subnet Mask			255.255.255.0		Subnet Mask			255.2	55.255.0
IPsec Encryption			Disabled		Statistics				Q,
Monitored Interfaces									
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6			Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	_
🗃 Inside	192.168.75.10							•	1
diagnostic								•	1
Cutside	192.168.76.10							٠	1

步驟 7.用於Inside介面,如圖所示。

Edit Inside	0
Monitor this interface for failures IPv4 IPv6	
Interface Name: Inside Active IP Address: 192.168.75.10 Mask: 24 Standby IP Address: 192.168.75.11	
Cancel	ж

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						•	/
Cutside	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	/1
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	1

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。

Firewall Manag Devices / High Availa	ement Center Overview Analysis	Policies Devices Objects Inte	ration		Deploy Q	e	° 0
FTD4120-HA Cisco Firepower 4120 Three Summary High Avail	t Defense ability Device Routing Interfaces in	ine Sets DHCP VTEP					
	General	/ ±	+	License			1
	Name:	FTD4120-F	A	Base:		[Yes
	Transfer Packets:	Y	5	Export-Controlled Features:			No
	Status:		b	Malware:			Yes
	Primary Peer:	FTD4100-5(Activ	:)	Threat:			Yes
	Secondary Peer:	FTD4100-6(Standb	i)	URL Filtering:			Yes
	Failover History:	0	2	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-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 2 of 1291 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(4)210, Mate 9.18(4)210 Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG Last Failover at: 08:46:30 UTC Jul 18 2024 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

This host -	State Primary	Last Failure Reason	Date/Time
Other host -	Active Secondary	None	
	Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016
====Configurat Sync Done ====Communicat Mac set	ion State=== ion State===		
firepower#			

步驟 5.從主要單元(LINA CLI)驗證設定:

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 Т interface Port-channel2 no nameif no security-level no ip address 1 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 I interface Port-channel3 description LAN/STATE Failover Interface interface Ethernet1/1 management-only nameif diagnostic security-level 0 no ip address Т 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)。

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

步驟 2.確認操作。

可以使用show failover history命令輸出:

在新的使用中		在新待
> show failover history		
		=
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)	> show ====== 從狀態 ======
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 Active
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 m	ne 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)	

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)。

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

步驟 2.請檢查圖中所示的通知。

Confirm Break
Breaking the High Availability pair "FTD4120-HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair? Force break, if standby peer does not respond
No Yes

步驟 3.請注意如下圖所示的消息。

Deploymen	ts Upgrad	des 🏮	Health	Tasks		C Sho	ow Notifica	ations	
20+ total	0 waiting	0 running	0 retrying	20+ success	1 failure	Q. Filter			J
Policy Depl Policy Dep	oyment ployment to F1	TD4100-5.	Applied succe	essfully			<u>47s</u>	×	Î
Policy Pre-I Pre-deplo success	Deployment by Device Cont	figuration fo	or FTD4100-	-5			<u>3s</u>	×	
Policy Pre-I Pre-deplo success	Deployment ny Global Conf	Iguration G	eneration				4s	×	
 High Availat HA pair has peer FTD41 complete or 	bility been broken su 00-5 policies ar n FTD4100-5 be	ccessfully an re being delet fore configur	d all policies I ted by an auto ing its policie:	have been retained triggered deployn 5.	l on active peer F nent. Please allow	TD4100-6. Standby w this deployment to	<u>1m 59s</u>	×	
			Remo	ve completed ta	isks				

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
> show running-config :已儲存	>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。
: : 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	> 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 !

service-module 0 keepalive-counter 6	主機名firepower
名稱	enable password ***** encrypted
no mac-address auto	strong-cryption-disable
	service-module 0 keepalive-timeout 4
	service-module 0 keepalive-counter 6
interface Port-channel2	名稱
	no mac-address auto
cts手冊	
propagate sgt preserve-untag	!
策略靜態sgt已停用受信任	interface Port-channel2
無安全等級	關機
無ip地址	
!	無安全等級
interface Port-channel2.202	mip地址
vlan 202	!
nameif Outside	interface Port-channel3
cts手冊	關機
propagate sgt preserve-untag	無名稱
策略靜態sgt已停用受信任	無安全等級
安全性層級0	無ip地址
ip address 192.168.76.10 255.255.255.0 standby	!
192.168.76.11	interface Ethernet1/1
!	僅管理
interface Port-channel3	關機
說明LAN/狀態故障切換介面	無名稱
!	無安全等級
interface Ethernet1/1	無ip地址
僅管理	
nameif diagnostic	interface Ethernet1/4
cts手冊	關機
propagate sqt preserve-untag	無名稱
策略靜態sat已停用受信任	無安全等級
安全性層級0	無ip地址
() 無ip地址	
	r. Iftp mode passive
interface Ethernet1/4	ngips conn-match ylan-id
nameif Inside	object-group-search access-control
rts王冊	access-group CSM FW ACL global
propagate sat preserve-untag	access-group COM_I W_ACL_ grobal
的pagale sgl pleselve-ullag 学軟藝能ad日位田孚信任	0008 · DEELI TED DOLLOV · Dofault Tuppol
灾啦呼您Sylup可又后亡 空全性菌级0	and Priority Policy
女主に肩載り in address 102 168 75 10 255 255 255 0 standby	and Filolity Folicy
100 468 75 14	
	19990 . RULE . DEFAULT TUNNEL ACTION
the mode possive	RULE
nip mode passive	access-list CSIVI_FW_ACL_ advanced permit
ngips conn-match vian-io	וויזין מחא מחא נחופ-ום אאאא ו

object-group-search access-control	access-list CSM_FW_ACL_ advanced permit
access-group CSM_FW_ACL_ global	udp any eq 3544 any range 1025 65535 rule-id
access-list CSM_FW_ACL_ remark rule-id	9998
9998 : PREFILTER POLICY : Default Tunnel	access-list CSM_FW_ACL_ advanced permit
and Priority Policy	udp any range 1025 65535 any eq 3544 rule-id
access-list CSM_FW_ACL_ remark rule-id	9998
9998 : RULE : DEFAULT TUNNEL ACTION	access-list CSM_FW_ACL_ advanced permit 41
RULE	any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
ipinip any any rule-id 9998	gre any rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp	access-list CSM_FW_ACL_ remark rule-id
any eq 3544 any range 1025 65535 rule-id 9998	268439552 : ACCESS POLICY : acp_simple -
access-list CSM_FW_ACL_ advanced permit udp	必備
any range 1025 65535 any eq 3544 rule-id 9998	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ advanced permit 41	268439552: L7規則: rule1
any any rule-id 9998	access-list CSM_FW_ACL_ advanced permit ip
access-list CSM_FW_ACL_ advanced permit gre	any any rule-id 268439552
any rule-id 9998	!
access-list CSM_FW_ACL_ remark rule-id	tcp-map UM_STATIC_TCP_MAP
268434433 : ACCESS POLICY : acp_simple -	tcp選項範圍67允許
預設	tcp-options範圍9 18 allow
access-list CSM_FW_ACL_ remark rule-id	tcp-options range 20 255 allow
268434433: L4 RULE:預設操作規則	urgent-flag allow
access-list CSM_FW_ACL_ advanced permit ip	!
any any rule-id 268434433	無尋呼機
!	no logging message 106015 -無記錄訊息
tcp-map UM_STATIC_TCP_MAP	no logging message 313001 -無記錄訊息
tcp選項範圍6 7允許	no logging message 313008 -無記錄訊息
tcp-options範圍9 18 allow	no logging message 106023 -無記錄訊息
tcp-options range 20 255 allow	no logging message 710003 -無記錄訊息
urgent-flag allow	no logging message 106100 -無記錄訊息
!	no logging message 302015 -無記錄訊息
無尋呼機	no logging message 302014 -無記錄訊息
no logging message 106015 -無記錄訊息	no logging message 302013 -無記錄訊息
no logging message 313001 -無記錄訊息	no logging message 302018 -無記錄訊息
no logging message 313008 -無記錄訊息	no logging message 302017 -無記錄訊息
no logging message 106023 -無記錄訊息	no logging message 302016 -無記錄訊息
no logging message 710003 -無記錄訊息	no logging message 302021 -無記錄訊息
no logging message 106100 -無記錄訊息	no logging message 302020 -無記錄訊息
no logging message 302015 -無記錄訊息	無故障轉移
no logging message 302014 -無記錄訊息	<省略部分輸出>
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	
ho logging moscogo 202021 毎囙 段団 自	
IIO IOgging message 302021 -無記錄訊怎	

ſ

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Ian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 <省略部分輸出>	
高可用性中斷前的輔助/主用裝置	HA中斷之後的輔助裝置
> show running-config :已儲存 :	> show running-config :已儲存
:序列號:FLM2108V9YG	:
:硬體:FPR4K-SM-24,73850 MB	:序列號:FLM2108V9YG
RAM,CPU Xeon E5系列2200 MHz,2個	:硬體:FPR4K-SM-24,73850 MB
CPU(48核)	RAM,CPU Xeon E5系列2200 MHz,2個
:	CPU(48核)
NGFW版本7.2.8	:
!	NGFW版本7.2.8
主機名firepower	!
enable password ***** encrypted	土 (成石TIFepower
strong-cryption-disable	enable password ***** encrypted
service-module 0 keepalive-timeout 4	strong-cryption-disable
service-module 0 keepalive-counter 6	service-module 0 keepalive-timeout 4
名稱	service-module 0 keepalive-counter 6
no mac-address auto	名稱
!	no mac-address auto
interface Port-channel2	!
無名稱	interface Port-channel2
無安全等級	無名稱
無ip地址	無安全等級
!	無ip地址

Interface Port-channel2.202	
vlan 202	Interface Port-channel2.202
	vian 202
cts手册	
propagate sgt preserve-untag	cts手册
策略靜態sgt已停用受信仕	propagate sgt preserve-untag
安全性層級0	策略靜態sgt已停用受信仕
ip address 192.168.76.10 255.255.255.0	
standby 192.168.76.11	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 Port-channel3
!	
interface Ethernet1/1	無安全等級
	無ip地址
nameif diagnostic	!
安全性層級0	interface Ethernet1/1
無ip地址	
1	nameif diagnostic
interface Ethernet1/4	安全性層級0
nameif Inside	無ip地址
安全性層級0	!
ip address 192.168.75.10 255.255.255.0	interface Ethernet1/4
standby 192.168.75.11	nameif Inside
!	安全性層級0
ftp mode passive	ip address 192.168.75.10 255.255.255.0
ngips conn-match vlan-id	standby 192.168.75.11
object-group-search access-control	!
access-group CSM_FW_ACL_ global	ftp mode passive
access-list CSM_FW_ACL_ remark rule-id	ngips conn-match vlan-id
9998 : PREFILTER POLICY : Default Tunnel	object-group-search access-control
and Priority Policy	access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
9998 : RULE : DEFAULT TUNNEL ACTION	9998 : PREFILTER POLICY : Default Tunnel
RULE	and Priority Policy
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ remark rule-id
ipinip any any rule-id 9998	9998 : RULE : DEFAULT TUNNEL ACTION
access-list CSM_FW_ACL_ advanced permit	RULE
udp any eq 3544 any range 1025 65535 rule-id	access-list CSM_FW_ACL_ advanced permit
9998	ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544 rule-id 9998	udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41	access-list CSM_FW_ACL_ advanced permit
any any rule-id 9998	udp any range 1025 65535 any eq 3544 rule-id
access-list CSM_FW_ACL_ advanced permit gre	9998
	1

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

HA 分割的主要注意事項:

主/備用裝置	輔助/主用裝置
・ 會移除所有容錯移轉組態 ・ 刪除所有IP配置	• 會移除所有容錯移轉組態 • 備用IP將保留,但在下次部署時刪除

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:

FTD4120-HA High Availability							Switch Active Peer
FTD4100-5(Primary, Standby) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	III FP4100-5;443 IIII Security Module - 1	Base, Threat (2 more)	acp_simple	45	Break Force refresh node status Delete Report Lingurade
FTD4100-6(Secondary, Active) Short 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Health Monitor Troubleshoot Files

步驟 2.檢查通知並進行確認,如下圖所示:

Confirm Delete
Are you sure you want to delete the high availability, "FTD4120-HA"? Deleting the pair from the Firewall Management Center does not disable high availability at the device level. The devices will continue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: "configure high-availability disable"
No Yes

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)
> show running-config	> show running-config
:已儲存	:已儲存
:	:
:序列號:FLM1949C5RR	:序列號:FLM2108V9YG
:硬體:FPR4K-SM-24,73853 MB	:硬體:FPR4K-SM-24,73853 MB
RAM,CPU Xeon E5系列2200 MHz,2個	RAM,CPU Xeon E5系列2200 MHz,2個
CPU(48核)	CPU(48核)
.	.
NGFW版本7.2.8	NGFW版本7.2.8
!	!
± 機名Firepower-module1	主機名Firepower-module1
enable password ***** encrypted	enable password ***** encrypted
strong-cryption-disable	strong-cryption-disable
no asp inspect-dp ack-passthrough	no asp inspect-dp ack-passthrough
service-module 0 keepalive-timeout 4	service-module 0 keepalive-timeout 4
service-module 0 keepalive-counter 6	service-module 0 keepalive-counter 6
名稱	名稱
no mac-address auto	no mac-address auto
!	!
interface Port-channel2	interface Port-channel2
無名稱	無名稱
無安全等級	無安全等級
無ip地址	無ip地址
!	!
interface Port-channel2.202	interface Port-channel2.202
vlan 202	vlan 202
nameif NET202	nameif NET202
cts手冊	cts手冊
propagate sgt preserve-untag	propagate sgt preserve-untag
策略靜態sgt已停用受信任	策略靜態sgt已停用受信任
安全性層級0	安全性層級0
ip address 172.16.202.1 255.255.255.0 standby	ip address 172.16.202.1 255.255.255.0 standby
172.16.202.2	172.16.202.2
!	!
interface Port-channel2.203	interface Port-channel2.203
vlan 203	vlan 203
nameif NET203	nameif NET203
cts手冊	cts手冊
propagate sgt preserve-untag	propagate sgt preserve-untag
策略靜態sgt已停用受信任	策略靜態sgt已停用受信任
安全性層級0	安全性層級0
1 audress 172.10.203.1 203.203.205.205.0 Standby	μραυμεςς 172.10.203.1 203.203.205.205.0 Stanuby

172.16.203.2	172.16.203.2
interface Port-channel3	interface Port-channel3
說明LAN/狀態故障切換介面	說明LAN/狀態故障切換介面
!	!
interface Ethernet1/1	interface Ethernet1/1
僅管理	僅管理
nameif diagnostic	nameif diagnostic
cts手冊	cts手冊
propagate sgt preserve-untag	propagate sgt preserve-untag
策略靜態sgt已停用受信任	策略靜態sgt已停用受信任
安全性層級0	安全性層級0
無ip地址	無ip地址
!	!
interface Ethernet1/4	interface Ethernet1/4
nameif NET204	nameif NET204
cts手冊	cts手冊
propagate sgt preserve-untag	propagate sgt preserve-untag
策略靜態sgt已停用受信任	策略靜態sgt已停用受信任
安全性層級0	安全性層級0
ip address 172.16.204.1 255.255.255.0 standby	ip address 172.16.204.1 255.255.255.0 standby
172.16.204.2	172.16.204.2
!	!
ftp mode passive	ftp mode passive
ngips conn-match vlan-id	ngips conn-match vlan-id
no object-group-search access-control	no object-group-search access-control
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
9998 : PREFILTER POLICY : Default Tunnel	9998 : PREFILTER POLICY : Default Tunnel
and Priority Policy	and Priority Policy
9998 : RULE : DEFAULT TUNNEL ACTION	9998 : RULE : DEFAULT TUNNEL ACTION
RULE	RULE
lininin any any rule id 0008	access-list CSM_FW_ACL_ advanced permit
access list CSM EW ACL advanced permit	access list CSM EW ACL advanced permit
udp any eq 3544 any range 1025 65535 rule id	udn anv eg 3514 anv range 1025 65535 rule-id
access-list CSM_EW_ACL_advanced permit	access-list CSM_EW_ACL_advanced permit
udp any range 1025 65535 any eq 3544 rule-id	udp any range 1025 65535 any eq 3544 rule-id
9998	9998
access-list CSM FW ACL advanced permit 41	access-list CSM FW ACL advanced permit 41
any any rule-id 9998	any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit are	access-list CSM_FW_ACL_ advanced permit are
any rule-id 9998	any rule-id 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id

268434433 : ACCESS POLICY : acp_simple -	268434433 : ACCESS POLICY : acp_simple - 표한
268434433: L4 RULE:	268434433: L4 RULE:
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ advanced permit ip
any any rule-id 268434433	any any rule-id 268434433
!	!
tcp-map UM_STATIC_TCP_MAP	tcp-map UM_STATIC_TCP_MAP
tcp選項範圍6 7允許	tcp選項範圍6 7允許
tcp-options範圍9 18 allow	tcp-options範圍9 18 allow
tcp-options range 20 255 allow	tcp-options range 20 255 allow
tcp-options md5 clear	tcp-options md5 clear
urgent-flag allow	urgent-flag allow
!	
無尋呼機	無尋呼機
no logging message 106015 -無記錄訊息	no logging message 106015 -無記錄訊息
no logging message 313001 -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 313008 -無記錄訊息
no logging message 106023 -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 710003 - 無記錄訊息
no logging message 106100 - 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 302015 - 無記錄訊息
no logging message 302013 - 黑記錄記念	no logging message 302013 - 黑記錄記念
no logging message 302017 - 黑記錄記念	no logging message 302017 - 黑記或記念
no logging message 302013 - 黑記錄記念	no logging message 302013 - 黑記歐記念
no logging message 302017 無記錄記念	no logging message 302017 無記錄記念
Ind logging message 302017 - 無記嫁記念	Ind logging message 302017 - 無記嫁記念
no logging message 302010 - 無記錄訊总	IND IOgging message 302010 - 無記錄訊总
no logging message 302021 - 無記嫁訊忌	IND IOgging message 302021 - 無記錄訊息
no logging message 302020 - 無記録訊息	IND IOgging message 302020 - 無記録訊息
mtu NET202 1500	
mtu diagnostic 1500	mtu diagnostic 1500
mtu NE I 204 1500	mtu NE I 204 1500
谷銷移轉	谷鉗移轉
王要谷錯移轉lan裝直	 故障轉移lan車元軸切
failover lan interface FOVER Port-channel3	failover lan interface FOVER Port-channel3
故障切換複製http	故障切換複製http
故障切換鏈路FOVER Port-channel3	故障切換鏈路FOVER Port-channel3
故障切換介面IP FOVER 172.16.51.1	故障切換介面IP FOVER 172.16.51.1
255.255.255.0 standby 172.16.51.2	255.255.255.0 standby 172.16.51.2
監控介面NET202	監控介面NET202
監控介面NET203	監控介面NET203
icmp unreachable rate-limit 1 burst-size 1	icmp unreachable rate-limit 1 burst-size 1
<1 略部分輸出>	<1 略部分1113

> show ip	> show ip
系統IP位址:	系統IP位址:
介面名稱IP地址子網掩碼方法	介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.1	Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置	255.255.255.0配置
Port-channel2.203 NET203 172.16.203.1	Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置	255.255.255.0配置
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.1
255.255.255.0 unset	255.255.255.0 unset
Ethernet1/4 NET204 172.16.204.1	Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置	255.255.255.0配置
當前IP地址:	當前IP地址:
介面名稱IP地址子網掩碼方法	介面名稱IP地址子網掩碼方法
Port-channel2.202 NET202 172.16.202.2	Port-channel2.202 NET202 172.16.202.1
255.255.255.0配置	255.255.255.0配置
Port-channel2.203 NET203 172.16.203.2	Port-channel2.203 NET203 172.16.203.1
255.255.255.0配置	255.255.255.0配置
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.2
255.255.255.0 unset	255.255.255.0(未設定)
Ethernet1/4 NET204 172.16.204.2	Ethernet1/4 NET204 172.16.204.1
255.255.255.0配置	255.255.255.0配置
> show failover	> show failover
容錯移轉開啟	容錯移轉開啟
主要容錯移轉單元	故障轉移裝置輔助
	一家供移植LAN公面,FOMED Deat shows all (up)
	谷蛨侈鸭LAN介面:FOVER Port-channels (up)
重新連線超時0:00:00	香頭移轉LANJ面:FOVER Pon-channels (up) 重新連線超時0:00:00
重新連線超時0:00:00 單位輪詢頻率1秒,保持時間15秒	容弱後時LANJT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
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	革動移轉LANJT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
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	革頭移轉LANJT面: FOVER Port-channels (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
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)	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)
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	革頭後轉LANJT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
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	全頭移轉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
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	 本
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	 本頭疹轉LAN介面: FOVER Port-channels (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
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	各頭移轉LANJI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
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	 各頭疹轉LANJI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
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	各頭移轉LANJI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
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	各頭移轉LANJI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
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)	各頭移轉LANJI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)
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	 本頭疹轉LANJI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
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)	各頭移轉LANJI面: FOVER Port-channels (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)
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)	各頭移轉LANJI面: FOVER Port-channels (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)
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)	各頭移轉LANJI面: FOVER Port-channels (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)
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(172.16.203.2):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)	本頭移轉LANJT面: FOVER Port-channels (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):正常(等待)
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):正常(等待) NET204介面(172.16.204.2):正常(受監控)	各頭移轉LANJT值: FOVER Port-channels (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)

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	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
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)
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>	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 <<r>

```
<#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)
> INFO: This unit is currently in standby state. By	> show failover
disabling failover, this unit will remain in standby	Failover Off
state.	Failover unit Secondary
	Failover LAN Interface: not Configured
	Reconnect timeout 0:00:00
	Unit Poll frequency 1 seconds, holdtime 15
> snow fallover	seconds
Fallover Off (pseudo-Standby)	Interface Poll frequency 5 seconds, holdtime 25
Fallover unit Primary	seconds
ranover LAN Interface: FOVER Port-channels	Interface Policy I
(up) Reconnect timeout 0.00.00	Monitored Interfaces 4 of 1291 maximum
Unit Poll frequency 1 seconds, holdtime 15	MAC Address Move Notification Interval not set
Interface Poll frequency 5 seconds holdtime 25	
seconds	> show ip
Interface Policy 1	System IP Addresses:
Monitored Interfaces 0 of 1291 maximum	Interface Name IP address Subnet mask Method
MAC Address Move Notification Interval not set	Port-channel2.202 NET202 172.16.202.1
failover replication http	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
> show ip	CONFIG
System IP Addresses:	Current IP Addresses:
Interface Name IP address Subnet mask Method	Interface Name IP address Subnet mask Method
Port-channel3 FOVER 1/2.16.51.1 255.255.255.0	Port-channel2.202 NET202 172.16.202.1
Unset Current ID Addresses	255.255.255.0 CONFIG
United IF Addresses: Interface Name ID address Subnet mask Method	Port-channel2.203 NET203 172.16.203.1
Port-channel3 FOVER 172 16 51 1 255 255 0	233.233.233.UUNFIG Ethomat 1/4 NET 204 172 16 204 1 255 255 255 0
unset	CONFIG

主要(非待命)	輔助(非活動)
> show running-config	> show running-config
:已儲存	:已儲存
:	:
:序列號:FLM1949C5RR	:序列號:FLM2108V9YG
:硬體:FPR4K-SM-24,73853 MB	:硬體:FPR4K-SM-24,73853 MB
RAM,CPU Xeon E5系列2200 MHz,2個	RAM,CPU Xeon E5系列2200 MHz,2個
CPU(48核)	CPU(48核)
.	.
NGFW版本7.2.8	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 	 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
腳機	無名稱
無名稱	無安全等級
無安全等級	無ip地址
no ip address <-刪陈IP	!
!	interface Port-channel2.202
interface Port-channel3	vlan 202
說明LAN/狀態故障切換介面	nameif NET202
!	cts手冊
· interface Ethernet1/1 僅管理 關機 無名稱 無安全等級 舞inth th	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
「「P454」 ! interface Ethernet1/4 關機 無名稱 毎安全等級	interface Port-channel2.203 vlan 203 nameif NET203 cts手冊
mip地址	策略靜態sgt已停用受信任
!	安全性層級0
ftp mode passive	ip address 172.16.203.1 255.255.255.0 standby

ngips conn-match vlan-id	172.16.203.2	
no object-group-search access-control	!	
access-group CSM FW ACL global	interface Port-channel3	
access-list CSM FW ACL remark rule-id	無名稱	
9998 : PREFILTER POLICY : Default Tunnel	無安全等級	
and Priority Policy	無ip地址	
access-list CSM_FW_ACL_ remark rule-id		
9998: RULE: DEFAULT TUNNEL ACTION	interface Ethernet1/1	
RULE	僅管理	
access-list CSM_FW_ACL_ advanced permit	nameif diagnostic	
ipinip any any rule-id 9998	cts手冊	
access-list CSM_FW_ACL_ advanced permit	propagate sgt preserve-untag	
udp any eq 3544 any range 1025 65535 rule-id	策略靜態sgt已停用受信任	
9998	安全性層級0	
access-list CSM_FW_ACL_ advanced permit	無ip地址	
udp any range 1025 65535 any eq 3544 rule-id	!	
9998	interface Ethernet1/4	
access-list CSM_FW_ACL_ advanced permit 41	nameif NET204	
any any rule-id 9998	cts手冊	
access-list CSM_FW_ACL_ advanced permit gre	propagate sgt preserve-untag	
any rule-id 9998	策略靜態sgt已停用受信任	
access-list CSM_FW_ACL_ remark rule-id	安全性層級0	
268434433 : ACCESS POLICY : acp_simple -	ip address 172.16.204.1 255.255.255.0 standby	
預設	172.16.204.2	
access-list CSM_FW_ACL_ remark rule-id		
268434433: L4 RULE: 預設操作規則	ftp mode passive	
access-list CSM_FW_ACL_ advanced permit ip	ngips conn-match vlan-id	
any any rule-id 268434433	no object-group-search access-control	
	access-group CSM_FVV_ACL_ global	
tcp-map UM_STATIC_TCP_MAP		
ICP进垻軋剧0 / 儿計 ten entigeng符图0.10 elleur	9998 PREFILTER POLICY : Default Tunnel	
ICP-Options 輕星9 18 allow	and Phonty Policy	
top options range 20 255 allow		
urgent flag allow	BUILE	
	access_list CSM_EW_ACL_advanced permit	
金融资格	ininin any any rule-id 9998	
no logging message 106015 - 無記錄訊息	access-list CSM_EW_ACL_advanced permit	
no logging message 313001 - 無記錄訊息	udp any eq 3544 any range 1025 65535 rule-id	
no logging message 313008 - 無記錄訊息	9998	
no logging message 106023 -無記錄訊息	access-list CSM FW ACL advanced permit	
no logging message 710003 -無記錄訊息	udp any range 1025 65535 any eq 3544 rule-id	
no logging message 106100 -無記錄訊息	9998	
no logging message 302015 -無記錄訊息	access-list CSM_FW_ACL_ advanced permit 41	
no logging message 302014 -無記錄訊息	any any rule-id 9998	
no logging message 302013 -無記錄訊息	access-list CSM_FW_ACL_ advanced permit gre	

no logging message 302018 -無記錄訊息	any rule-id 9998
no logging message 302017 -無記錄訊息	access-list CSM_FW_ACL_ remark rule-id
no logging message 302016 -無記錄訊息	268434433 : ACCESS POLICY : acp_simple -
no logging message 302021 -無記錄訊息	預設
no logging message 302020 -無記錄訊息	access-list CSM_FW_ACL_ remark rule-id
無故障轉移	268434433: L4 RULE:預設操作規則
主要容錯移轉lan裝置	access-list CSM_FW_ACL_ advanced permit ip
failover lan interface FOVER Port-channel3	any any rule-id 268434433
故障切換複製http	!
故障切換鏈路FOVER Port-channel3	tcp-map UM_STATIC_TCP_MAP
故障切換介面IP FOVER 172.16.51.1	tcp選項範圍6 7允許
255.255.255.0 standby 172.16.51.2	tcp-options範圍9 18 allow
no monitor-interface service-module	tcp-options range 20 255 allow
	tcp-options md5 clear
<省略部分輸出>	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

從作用中FTD CLI停用HA的注意事項:

使用中單位

備用裝置

•	已移	除容	錯移	轉設	定
---	----	----	----	----	---

• 未移除待命IP

- 會移除介面組態.
- 未移除容錯移轉組態,但已
 停用容錯移轉(虛擬待命)

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

Port-channel2.202 NET202 172.16.202.1 255.255.255.0手冊<-裝置使用與ex-Active相同的 IP ! Port-channel2.203 NET203 172.16.203.1 255.255.255.0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 Ethernet1/4 NET204 172.16.204.1 255.255.255.0手冊	12:44:06 此主機:次要-活動 活動時間:632(秒) 插槽0:UCSB-B200-M3-U硬體/軟體版本 (0.09.18(4)210)狀態(啟動系統) 介面診斷(0.0.0.0):正常(等待) NET204介面(172.16.203.1):正常(受監控) NET202介面(172.16.202.1):正常(受監控) MET202介面(172.16.202.1):正常(受監控) 插槽1:snort rev(1.0)狀態(up) 其他主機:主要-已停用 活動時間:932(秒) 插槽0:UCSB-B200-M3-U硬體/軟體版本 (0.09.18(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 NET203(172.16.203.2):未知(受監 控) Interface NET202(172.16.202.2):未知(受監 控) Interface NET202(172.16.202.2):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 NET203 172.16.203.1 255.255.255.0手冊 Port-channel3 FOVER 172.16.51.1 255.255.255.0手冊 Port-channel3 FOVER 172.16.51.1 255.255.255.0手冊 Port-channel2.202 NET203 172.16.203.1 255.255.255.0手冊 Port-channel2.203 NET203 172.16.203.1 255.255.255.0手冊
	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

ſ

從作用中FTD CLI停用HA的注意事項:

使用中單位	備用裝置
 故障切換配置未刪除,仍保持 啟用狀態 裝置使用與ex-Standby裝置相 同的IP 	・ 已移除容錯移轉設定 ・ 裝置使用與主用裝置相同的IP

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)
> 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	> 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

	> snow ip
> show ip	系統IP位址:
系統IP位址:	介面名稱IP地址子網掩碼方法
介面名稱IP地址子網掩碼方法	當前IP地址:
Port-channel3 FOVER 172.16.51.1	介面名稱IP地址子網掩碼方法
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	
>	

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
・ 已移除容錯移轉設定	 未移除容錯移轉組態,但已
・ IP將被刪除	停用容錯移轉(虛擬待命) IP將被刪除

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
	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
	// 圖水晶 受堅控的介面 <i>4</i> (最多1201個)
	00字の決徴表1110 Mata 0 18(4)210
s alagu faile ar	FLW194903KK
> SNOW fallover 北座山地間間	上次战隍切換時间:07:00:56 01C 2024年7月
战悍切揆阏闭 赴陪穂羖弉罢葀叻	18日
	此土機:
谷靖移轉LAN介面:木設定	活動時间:1194 (秒)
里新連線通時0:00:00	抽信0:UCSB-B200-M3-U硬體/軟體放平
甲位辆韵頻率1秒,保持時間15秒	((0.0/9.18(4)210)
介囬輛詢頻率5秒,保持時間25秒	介面診斷(0.0.0.0):止常(寺待)
// 面策略1 ズ町は A 〒 - // 目 - / 佐治 / /	NE1204介面(1/2.16.204.1): 止常(受監控)
受監控介面0的最大值為1291	NE1202介面(1/2.16.202.1): 止常(受監控)
未設定MAC地址移動通知間隔	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)
> Show Ip ズ体ID 体地	其他主機:主要-已停用
	活動時間:846 (秒)
川山名伸旧地址ナ網推協力法	插槽0:UCSB-B200-M3-U硬體/軟體版本
角則 1-11-11 1-12 1-12	(0.0/9.18(4)210)狀態(啟動系統)
沪囬名柟IP地址于網推噅万法 L	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
	A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
・ 未移除容錯移轉設定	• 已移除容錯移轉設定
・ 未刪除IP	• IP將被刪除

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-availablity.

> .

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

<#root>

cli_xml_server:	<pre>frep_write_cmd:</pre>	Cmd:	access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	<pre>no access-list CSM_FW_ACL_ advanced permit tcp object-group group_</pre>
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	<pre>no access-list CSM_FW_ACL_ advanced permit tcp object-group group_</pre>
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	crypto isakmp nat-traversal
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no object-group network group_311
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no object-group network group_433
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no object-group network group_6
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	Cmd:	no object-group network group_2
<pre>cli_xml_server:</pre>	<pre>frep_write_cmd:</pre>	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 192.0.2.1 255.255.0 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:

 \mathtt{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 192.0.2.1 255.255.0 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:

<u>導航思科安全防火牆威脅防禦文檔</u>

• 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:

<u>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</u> 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

<u>Cisco安全防火牆管理中心</u>

• <u>技術支援與文件 - Cisco Systems</u>

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)。