# 在Firepower 4100上配置FTD多例項高可用性

目錄 簡介 必要條件 需求 採用元件 <u>背景資訊</u> 網路圖表 組態 步驟 1.預配置介面 步驟 2.為容器例項增加2個資源配置檔案。 步驟3. (可選)為容器例項介面增加虛擬MAC地址的MAC池字首。 步驟 4.新增獨立執行處理。 步驟 5.配置介面 步驟 6.為每個例項增加高可用性對。 驗證 疑難排解 參考

## 簡介

本檔案介紹如何在FTD容器執行處理(多重執行處理)中設定容錯移轉。

## 必要條件

需求

思科建議您瞭解Firepower管理中心和防火牆威脅防禦。

採用元件

Cisco Firepower管理中心虛擬7.2.5 思科Firepower 4145 NGFW裝置(FTD) 7.2.5 Firepower可擴展作業系統(FXOS) 2.12 (0.498) Windows 10

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。

在部署FTD多重執行處理之前,請務必瞭解它如何影響您的系統效能,並據此進行規劃。請務必參 閱Cisco官方文檔或諮詢Cisco技術代表,以確保實現最佳部署和配置。

## 背景資訊

多例項是Firepower威脅防禦(FTD)的一項功能,它類似於ASA多情景模式。此功能可讓您在單一硬 體上執行多個不同的FTD容器執行個體。每個容器例項允許硬資源分離、單獨的組態管理、單獨的 重新載入、單獨的軟體更新和全面的威脅防禦功能支援。這對於需要不同部門或專案採用不同安全 策略,但又不想投資於多個獨立硬體裝置的組織特別有用。多例項功能當前在運行FTD 6.4及更高 版本的Firepower 4100和9300系列安全裝置上受支援。

本文檔使用支援最多14個容器例項的Firepower4145。有關Firepower裝置支援的最大例項數,請參 閱<u>每個型號的最大容器例項和資源數</u>。

## 網路圖表

本檔案介紹此圖表上多執行處理中HA的組態和驗證。



邏輯配置圖



物理配置圖

## 組態

## 步驟 1.預配置介面

a.導航到FCM上的介面。設定2個管理介面。在本例中, Ethernet1/3和Ethernet1/7。

Overview Interface	Logical Devices	Security Engine	Platform Settings						System	ı Tools Help	admin
			Network Module 1 1 3 1 USB 2 4 0	5 7 5 8	Network Module 2 :	Empty	Network Module 3 : Em	pty			
All Interfaces Hardware	Bypass								Add New	• Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	X	J 🗟	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up	$\frown$	ø	
Ethernet1/5	data	1gbps	lgbps			Full Duplex	yes	up	$\frown$	ø	
Ethernet1/6	data	1gbps	lgbps			Full Duplex	yes	up	$\frown$	0	
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up	$\overline{}$	0	
Ethernet1/8	data	1gbps	lgbps			Full Duplex	yes	up		0	

預配置介面

步驟 2.為容器例項增加2個資源配置檔案。

a.導航到平台設定 > 資源配置檔案 > 增加。設定第一個資源設定檔。

在本示例中: ·名稱:Instance01 ·核心數:10個



註:對於容器例項對的HA,它們必須使用相同的資源配置檔案屬性。

將設定檔的名稱設定在1到64個字元之間。請注意,新增此設定檔後,您就無法變更其名稱 。

設定設定檔的核心數量,介於6和最大值之間。

Overview Interfaces Logica	al Devices Security Engine Pla	atform Settings			System Tools Help admir
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS AAA	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 0	
Syslog					
FIPS and Common Criteria					
Access List MAC Pool		Add Resource Profile			
Resource Profiles		Name:" Instance01			
Network Control Policy		Description:			
Chassis URL		Number of Cores:* 10 Range: 6 to 86			
		Specify even value for number of cores.			
		OK Cancel			

新增第一個資源設定檔

b.在步驟2中重複a.來配置第二個資源配置檔案。

在本示例中: ·名稱:Instance02 ·核心數:20

Overview Interfaces Logi	cal Devices Security Engine Platfor	m Settings			System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
HTTPS	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 8	
Syslog	Instance01		10	Ø 6	
DNS					
FIPS and Common Criteria		Add Pasauraa Brafila			
Access List					
MAC Pool		Name:* Instance02			
Resource Profiles		Description			
Network Control Policy		Description.			
Chassis URL		Number of Cores:* 20 Range: 6 to 86			
		Specify even value for number of cores.			
		OK Cancel			

新增第二個資源設定檔

c.檢查2個資源配置檔案已成功增加。

Overview Int	terfaces	Logica	al Devices	Security Engine	Platform Settings						System	Tools	Help	admin
NTP														
SSH									0	Add				
SNMP			Name			Description		Cores						
HTTPS			Default	-Small		Auto-created application resource-profile with 6 cpu-co	ores	6		28				
AAA														
Syslog			Instanc	e01				10		a 🖉				
DNS			Instance	*02				20		20				
FIPS and Comm	mon Criteria		instants	4V4				**		ø 🗉				
Access List														
MAC Pool														
Resource Prof	ofiles													
Network Contro	rol Policy													
Chassis URL														

確認資源配置檔案

## 步驟3. (可選)為容器例項介面增加虛擬MAC地址的MAC池字首。

您可以手動設定主用/備用介面的虛擬MAC地址。如果未設定虛擬MAC地址,對於多例項功能,機 箱會自動為例項介面生成MAC地址,並確保每個例項中的共用介面使用唯一的MAC地址。

有關MAC地址的詳細資訊,請檢查<u>為容器例項介面增加MAC池字首和檢視MAC地址</u>。

步驟 4.新增獨立執行處理。

a.導航到邏輯裝置 > 增加獨立。設定第一個例項。

在本示例中: ·裝置名稱:FTD01 ·例項型別:容器



注意:部署容器應用程式的唯一方法是預部署例項型別設定為容器的應用例項。 確保選擇 Container。

增加邏輯裝置後,無法更改此名稱。

Overview Interfaces Logical Devices Security Engine	Platform Settings	System Tools Help admin
Logical Device List	(O instances) 100% (86 of 86) Cores Available	C Refresh Add •
No logical devices available. Click on Add Device to add a new logical device.		
	Add Standalone	
	Device Name: FTD01	
	Template: Cisco Secure Firewall Threat Defense 💙	
	Image Version: 7.2.5.208	
	Instance Type: Container	
	Before you add the first container instance, you must reinitialize the security modulerging on so that the talk has the correct formatting. You only need to perform this action once.	
	OKCancel	

增加例項

## 步驟 5.配置介面

a.為Instance01設定Resource Profile、Management Interface和Management IP。

在本示例中: ·資源配置檔案:Instance01 ·管理介面:Ethernet1/3 ·管理IP:x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform S	Settings	System Tools Help admin
Provisioning - FTD01 Standalone   Cisco Secure Firewall Threat Defense   7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 💽 🗵	Save Cancel
Data Ports	General Information Settings Agreement	
Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/5 Ethernet1/6 Ethernet1/8	SM 1 - 86 Cores Available Resource Profile: Instance01  Hanagement Interface: Ethernet1/3  Address Type: IPv4 only  IPv4 Hanagement IP: 1:2:::11 Network Mask: 255.0.0 Network Gateway: 1.^	
Application Version Resource Profile	irt Status	
FTD 7.2.5.208		
	OK Cancel	
4		•

配置配置檔案/管理介面/管理IP

b.設定資料介面。

在本示例中:

·Ethernet1/1(用於內部)

·Ethernet1/2(用於外部)

·Ethernet1/4(用於HA鏈路)

c	overview Interfaces	Logical Devices Secu	rity Engine Platform Set	tings				System Tools Help admin
P S	rovisioning - FTD01 itandalone   Cisco Sec	ure Firewall Threat Defense	2   7.2.5.208					Save Cancel
	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/6			Ethernet	1/1 1/2 1/2	FID - 7.2.5.20 Ethernet1/3 Click to configure	8	
	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
	FTD Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/2	7.2.5.208	Instance01	11 Type data data data	1.0 *****	Ethernet1/3		

設定資料介面

## c.導航至邏輯裝置。正在等待執行個體啟動。

(	overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
L	gical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Core	s Available			C Refresh O Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	tion	Version	Resource F	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1.11113	1.0-0-000	Ethernet1/3	🐝 Installing	0180 🎋 c 🕍

確認Instance01的狀態

## d.在步驟4.a和步驟5.a到c中重複a.以增加第二個例項並為其設定詳細資訊。

在本示例中:

- ·裝置名稱:FTD11
- ·例項型別:容器
- ·資源配置檔案:Instance02
- ·管理介面:Ethernet1/7
- ·管理IP : x.x.10.1
- ·乙太網1/5 =內部
- ·乙太網1/6 =外部
- ·Ethernet1/8 = HA鏈路
- e.確認FCM上的2個執行處理為「線上」狀態。

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devic	ce List		0	2 Container instand	ces) 66% (56 of 86) Co	res Available			C Refresh 🕥 Add •
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource #	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02	]	10.1	1.0.0.000	Ethernet1/7	Online	🕶 🕅 c 🖄
FTD01	]		Standalone	Status:ok					01
Applica	tion	Version	Resource #	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01	]	C al.1	1.0	Ethernet1/3	Online	💌 🕅 🖘

確認主裝置中的例項狀態

f. (可選)在Firepower CLI中運行 scope ssa、 scope slot 1 和 show app-Instance 命令,確認2個例項處於聯機狀態。

## <#root>

FPR4145-ASA-K9#

scope ssa

FPR4145-ASA-K9 /ssa #

scope slot 1

FPR4145-ASA-K9 /ssa/slot #

show app-Instance

Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo Online

7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11 Online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

## g.在輔助裝置上執行相同的操作。 確認2個執行處理為線上狀態。

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
L	ogical Devic	e List			(2 Container instand	xes) 66% (56 of 86) Co	res Available			C Refresh 🕥 Add •
	FTD12			Standalone	Status:ok					
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
	# FTD		7.2.5.208	Instance02	]	10.2	1.*	Ethernet1/7	Online	💌 🌾 c 🚈
	FTD02			Standalone	Status:ok					<b>/</b> :
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01			1.6	Ethernet1/3	Online	💌 🎋 c 🔤

確認輔助裝置中的例項狀態

#### 步驟 6.為每個例項增加高可用性對。

a.導航到裝置 > 增加裝置(在FMC上)。將所有例項增加到FMC。

## 在本示例中:

·FTD1之Instance01的顯示名稱:FTD1\_FTD01 ·FTD1之Instance02的顯示名稱:FTD1\_FTD11 ·FTD2的Instance01的顯示名稱:FTD2\_FTD02 ·FTD2的Instance02的顯示名稱:FTD2\_FTD12

## 下圖顯示了FTD1\_FTD01的設定。

Firewall Management Center Overview Analyst Devices / Device Management	Add Device		Deploy Q 🥩 🐼 🔕 admin 🕶 👶 SECURE
View By:         Group         •           All (0)         • Error (0)         • Warning (0)         • Offline (0)         • Normal (0)	CDO Managed Device		Q, Search Device Add •
Collacse All	Display Name:		
Name	FTD1_FTD01	Licenses	Access Control Policy Auto RollBeck
Ungrouped (0)	Registration Key:*		
	None v		
	Access Control Policy:*		
	scp-rule     v      Smart Licensing Note: All virtual formed Threat Defense devices require a performance for license.     Note: All virtual formed Licensing account occlasies be variable licensing you need.     This imported to choose the fire that matches the license you have in your account.     Click have for information about the Firewall Threat Defense virtual and performance-tiered licensing.     Until you choose a tier, your Firewall Threat Defense virtual 2.0 and above):     Prove account     Threat     Threat     URL; Fittering     Advanced     Unique NAT EX:		
	Transfer Packets		
	Cancel Register		

將FTD執行處理新增至FMC

## b.確認所有例項均為正常。

Firewall Management Center Overview Analysis Pole Devices / Device Management	cies Devices Objects &	ntegration			Deploy	Q 📀 🔅 🚱 admin •	dade SECURE
View By:         Group           All (4)         € Error (0)         € Warning (0)         © Offline (0)         ● Normal (4)         ● De	ployment Pending (0) • Upgrade	(0) • Snort 3	(4)			Q, Search Device	Ment History
Collapse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)							
FTD1_FTD01 Snort 3     1_453.1.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	( <sup>0</sup>	1
OFTD1_FTD11 Snort 3     Snort 3     Snort 3     FtD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	45	11
FTD2_FTD02 Snort 3	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	11
FTD2_FTD12_Short 3     Loc 2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	11

確認FMC中的例項狀態

c.導航到裝置 > 增加高可用性。設定第一個故障轉移對。

在本示例中:

·名稱:FTD01\_FTD02\_HA

·主要對等體:FTD1\_FTD01



**註**:確保選擇正確的裝置作為主要裝置。

Firewall Management Center Overview Analysis Pol	icies Devices Objects I	integration		Deploy	Q 😂 🌣 🔞 admin 🔻	tiste SECURE
View By: Group					Deploy	ment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4) • De	eployment Pending (0)	(0) Snort 3 (4)			Q, Search Device	Add 🔻
Collarse Al						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (&)		Add High Availability Pair				
FTD1_FTD01_Snort3	Firepower 4145 with FTD	Name:* FTD01_FTD02_HA	Base, Threat (2 more)	acp-rule	49	1
C FTD1_FTD11 Soort.3     Ito 1 - Routed	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-rule	*9	1
FTD2_FTD2_Stort 3     1 2 - Routed	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01	Base, Threat (2 more)	acp-rule	*9	1
FID2_FID12_Sourt.3	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 v	Base, Threat (2 more)	acp-rule	«Ø	1
		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				

增加第一個故障轉移對

## d.為第1個故障轉移對中的故障轉移鏈路設定IP。

在本示例中:

·高可用性鏈路:Ethernet1/4

## ·狀態鏈路:Ethernet1/4

·主IP:192.168.90.1/24

## ·輔助IP:192.168.90.2/24

Firewall Management Center Overview Analysis Devices / Device Management	Policies	Devices Objects Integration		Deploy	् 🥥 🌣 😧 admin •	disds SECURE
Mew Br. Group					Depl	oyment History
All (4) • Error (0) • Warning (0) = Offline (0) • Normal (4)	Deploymen	Pending (0)   Upgrade (0)   Snort 3 (4)			Q, Search Device	Add 🔻
Collacse Al						
Name	Model	Add High Availability Dair		Access Control Policy	Auto RollBack	
Ungrouped (4)		And Figh Atomasing Full	Ű			
		High Availability Link	State Link			
FTD1_FTD01 Snort 3	Firepow	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	4Q	11
- HOURD		Logical Name:* ha_link	Logical Name:*			
O FTD1_FTD11 Snort 3	Firepow	Primary IP:* 192.168.90.1	Primary IP;*	acp-rule	40	11
E10.1 - Mouted		Use IPv6 Address	Use IPv6 Address			
FTD2_FTD02 Snort 3	Firepow	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	+©	1:
1.2 - Routed		Subnet Mask:* 255.255.255.0	Subnet Mask:*			
FTD2_FTD12 Snort 3	Firepow	IPsec Encryption			40	1:
		Enabled			18	
		Key Generation: Auto v				
		LAN failover link is used to sync configuration, statef between peers. Selected interface links and encryption	ul failover link is used to sync application content settings cannot be changed later.			
			Cancel Add			

為第一個故障轉移對設定HA介面和IP

## e.確認故障切換狀態

·FTD1\_FTD01:主用,活動

·FTD2\_FTD02:輔助、備用

Fire Devi	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n:			Deploy Q 🧲	🔅 🔞 admin 🗸	cinco SECURE
View By:	Group +							Dep	loyment History
All (4)	• Error (0) • Warning (0) • Offline (0) • Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Ipgrade (0)	Snort 3 (4)				Q, Search Device	Add 💌
Collapse All									
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack		
	V Ungrouped (3)								
	FTD01_FTD02_HA High Availability								/1
	FTD1_FTD01(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ф		:
	FTD2_FTD02(Secondary, Standby) Short 3 FTD1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4XHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q		1
	C FTD1_FTD11 Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q		11
	C FTD2_FTD12 Snort 3 (	Firepower 4145 with FTD	7.2.5	Firepower4XHG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	(Q)		1

確認第一個故障轉移對的狀態

## f.導航到裝置>點選FTD01\_FTD02\_HA(在本示例中)>介面。為資料介面設定活動IP。

#### 在本示例中:

·乙太網1/1(內部):192.168.10.254/24

- ·乙太網1/2(外部):192.168.20.254/24
- ·乙太網1/3(診斷):192.168.80.1/24

## 下圖顯示了Ethernet1/1的活動IP設定。

Firewall Management Center Devices / Secure Frewall Interfaces	view Analysis Po	licies Devices Objects Integr	ation			Deploy Q 💕 🌣 🔞 a	dmin • dede SECURE
FTD1_FTD01						You have unsaved chan	ges Save Cancel
Cisco Firepower 4145 Threat Defense Summary High Availability Device Routing	Interfaces Inline Se	Edit Physical Interface		Edit Physical Interface			e valiable for use. X
		General IPv4 IPv6 Path Mo	nitoring Advanced	General IPv4 IPv6 Path Monitoring	Advanced		Add Interfaces +
Interface	ogi	Name:		IP Type: Use Static IP v			
Ethernet1/1 in	rside	Enabled     Management Only		IP Address: 192.168.10.254/24			
© Ethernet1/2 or	utside	Description:					
© Ethernet1/3 di	lagnostic	Mode:					
		None v Security Zone:					
		inside_zone v				Course 1	-
		Ethemet1/1			_		-
		MTU:					
		(64 - 9184)					
		Priorey:	(5535)				
		Propagate Security Group Tag:					
					Cancel		

為資料介面設定活動IP

g.導航到裝置 > 點選FTD01\_FTD02\_HA(在本示例中) > 高可用性。 為資料介面設定備用IP。

在本示例中:

- ·乙太網1/1(內部):192.168.10.253/24
- ·乙太網1/2(外部):192.168.20.253/24
- ·乙太網1/3(診斷):192.168.80.2/24

## 此圖顯示Ethernet1/1的備用IP設定。

Firewall Management Devices / High Availability	Center Overview Analysis Policies Devic	es Objects Int	egration		Deploy	९ 🔮 🔅	🕜 admin 🕶 ;	SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defensi Summary High Availability	e Device Routing Interfaces Inline Sets DHCP	VTEP						Cancel
IPsec Encryption	Edit inside	Ø	itics					Q.
Monitored Interfaces	Monitor this interface for failures							
Interface Name	IPv4 IPv6			Active Link-Local IPv6	Standby Link	-Local IPv6	Monitoring	
outside	Interface Name:						٥	1
diagnostic	Active IP Address:						0	1
inside	192.168.10.254 Mask						٥	1
	24							
	Standby IP Address: 192.168.10.253							
Failover Trigger Criteria			face MAC Add	resses				+
Failure Limit			cal Interface	Active Ma	c Address	Standby Ma	c Address	
Peer Poll Time		Cancel	et1/1	1234.123	4.0001	1234.1234.	0002	1
Peer Hold Time								

設定資料介面的待命IP

## h.重複步驟6.c到g,增加第2個故障轉移對。

在本示例中:

· 名稱:FTD11\_FTD12\_HA

·主要對等點:FTD1\_FTD11

·次要同儕節點:FTD2\_FTD12

·高可用性鏈路:Ethernet1/8

·狀態鏈路: Ethernet1/8

·乙太網1/8(ha\_link活動):192.168.91.1/24

·乙太網1/5(內部活動):192.168.30.254/24

- ·乙太網1/6(外部活動):192.168.40.254/24
- ·乙太網路1/7 (診斷作用中):192.168.81.1/24

·乙太網1/8(ha\_link待機):192.168.91.2/24

- ·乙太網1/5(內部待機):192.168.30.253/24
- ·乙太網1/6(外部待機):192.168.40.253/24
- ·乙太網1/7(診斷待機):192.168.81.2/24

i.導航到邏輯裝置 > 增加獨立。設定ACP規則以允許從內部到外部的流量。

Ę	Policies / Acce	anagement C ss Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🔮 🕸	Ø a	dmin •	-de-de- CISCO	SECU	/RE
	acp-rule     Try New UI Layout D Analyze Hit Counts Seve Cancel     Enter Description																			
	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy: Default Prefilter Policy: None Identity Policy: None																			
Eit	ter by Device	Search Rules											×	Show Rule Con	flicts 🛛 🕂 /	Add Ca	stegory	+ /	Add Ru	le
	Name	Source Zones	Dest Zones	Source Networks	Det	st Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15	0 G	2 I I	-	¢
$\sim N$	Mandatory - acp-rule	e (1-1)		_																
1	ftd_ha_acp	inside_zone	outside_zone	Any:	Anj		Any	Any	Any	Any	Any	Any	Any	Any	C Allow	E. 1	F 15	8 🖂 🛙	10,	11
∨ D	✓ Default - acp-rule (-)																			
The	re are no rules in th	is section. Add Ru	le or Add Catego	жу																

設定ACP規則

#### j.將設定部署至FTD。

#### k.在CLI中確認高可用性狀態

每個例項的HA狀態也在Firepower CLI中確認, CLI與ASA相同。

運行 show running-config failover 和 show failover 命令以確認FTD1\_FTD01(主例項01)的HA狀態。

### <#root>

// confrim HA status of FTD1\_FTD01 (Instance01 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/4 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: P ..... Other host: Secondary - Standby Ready <---- InstanceO1 of FPRO2 is Standby Interface diagnostic

運行 show running-config failover 和 show failover 命令以確認FTD1\_FTD11(Primay Instance02)的HA狀態。

#### <#root>

// confrim HA status of FTD1\_FTD11 (Instance02 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/8 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: P Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16

運行 show running-config failover 和 show failover 命令以確認FTD2\_FTD02(輔助例項01)的HA狀態。

### <#root>

// confrim HA status of FTD2\_FTD02 (Instance01 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/4 failover replication h

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Active <---- InstanceO1 of FPRO1 is Active Active time: 31651 (sec) slot 0: UCSB- 運行 show running-config failover 和 show failover 命令以確認FTD2\_FTD12 (Seconday Instance02)的HA狀態。

## <#root>

// confrim HA status of FTD2\_FTD12 (Instance02 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/8 failover replication h Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

#### 1.確認許可證使用

所有許可證按安全引擎/機箱使用,而不是按容器例項使用。

·自動分配基准許可證:每個安全引擎/機箱一個。

·功能許可證手動分配給每個例項,但每個功能每個安全引擎/機箱僅使用一個許可證。對於特定功能許可證,無論使用的例項數量如 何,您總共只需要1個許可證。

#### 此表顯示了本文檔中許可證的使用方式。

FPR01	例項01	基礎、	URL過濾、	惡意軟體、	威脅
	例項02	基礎、	URL過濾、	惡意軟體、	威脅
FPR02	例項01	基礎、	URL過濾、	惡意軟體、	威脅
	例項02	基礎、	URL過濾、	惡意軟體、	威脅

#### 授權總數

基礎	URL篩選	惡意軟體	威脅
2	2	2	2

在FMC GUI中確認已使用的許可證數量。

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
Base (2)	<ul> <li>In-Compliance</li> </ul>					^
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	_
FTD11_FTD12_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
V Mabware (2)	In-Compliance					
FTD01_FTD02_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thre	aat Defense	Global	N/A	
FTD11_FTD12_HA (2)     Cisco Firepower 4145 Threat Defense Threat Defense High Availability	<ul> <li>In-Compliance</li> </ul>	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
V Threat (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
VIRL Filtering (2)	In-Compliance					- 1
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Frepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thre	at Defense	Global	N/A	

確認已使用的許可證

## 驗證

當FTD1\_FTD01 (主要執行處理01)發生當機時,會觸發Instance01的容錯移轉,且待命端上的資料介面會接管原始作用中介面的 IP/MAC位址,以確保Firepower能夠持續傳遞流量(本檔案中的FTP連線)。



崩潰前



#### 故障轉移已觸發

## 步驟 1.從Win10-01到Win10-02發起FTP連線。

步驟 2.運行 show conn 命令以確認在Instance01兩個例項中都建立了FTP連線。

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

步驟 3.從Win10-03到Win10-04發起FTP連線。

步驟 4.運行 show conn 命令以確認在Instance02兩個例項中都建立了FTP連線。

### <#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

步驟 5.運行 connect ftd FTD01和 system support diagnostic-cli命令以進入ASA CLI。 運行 enable和 crashinfo force watchdog 命令以強 制使主/主用裝置中的Instance01崩潰。

### <#root>

Firepower-module1>

connect ftd FTD01

```
>
```

```
system support diagnostic-cli
```

FTD01>

enable

Password: FTD01# FTD01#

crashinfo force watchdog

reboot. Do you wish to proceed? [confirm]:

步驟 6.故障切換發生在Instance01中, FTP連線未中斷。 運行 show failover和 show conn命令以確認Instance01在FPR02中的狀態。

### <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

步驟 7.在Instance01中發生的崩潰對Instance02沒有影響。 運行 show failover和 show conn命令以確認Instance02的狀態。

## <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (2000)

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

步驟 8.在FMC上導航到裝置 > 全部。確認HA狀態。

#### ·FTD1\_FTD01:主備模式

### ·FTD2\_FTD02:次要、活動

E Fin Dev	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n			Deploy Q	Secure admin •
View By:	Group							Deployment History
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Jpgrade (0)	<ul> <li>Snort 3 (4)</li> </ul>				Q, Search Device Add •
Collapse All								
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	Ungrouped (2)							
	V FTD01_FTD02_HA High Availability							11
	FTD1_FTD01(Primary, Standby) Snort 3     Cont_v1.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1
	FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	43	i
	✓ FTD11_FTD12_HA High Availability							11
	FTD1_FTD11(Primary, Active) Soort 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:
	FTD2_FTD12(Secondary, Standby) Short 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:

確認HA狀態

步驟9. (可選)在FPR01的Instance01恢復正常後,您可以手動切換HA的狀態。這可以透過FMC GUI或FRP CLI來實現。

在FMC上, 導航到裝置 > 全部。按一下Switch Active Peer以切換FTD01\_FTD02\_HA的HA狀態。

Fir Dev	Firewall Management Center Overview Analysis Policies Devices / De									
View By:	Group							Deployment History		
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	Deployment Pending (0)	Upgrade (0)	Snort 3 (4)				Q, Search Device Add •		
Collapse All										
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack			
	Ungrouped (2)									
	FTD01_FTD02_HA High Availability							Switch Active Peer Break		
	FTD1_FTD01(Primary, Standby) Snort 3     Control.1.1 - Routed	Firepower 4145 with FTD	7.2.5	EPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	Force refresh node status Delete Revert Upgrade		
	FTD2_FTD02(Secondary, Active) Snort 3     Control 1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	45	Health Monitor Troubleshoot Files		
	✓ FTD11_FTD12_HA High Availability							1		
	FTD1_FTD11(Primary, Active) Short 3     C.Sm1(10.1 - Routed	Firepower 4145 with FTD	7.2.5	E Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	:		
	FTD2_FTD12(Secondary, Standby) Snort 3     Actual 10.2 = Routed	Firepower 4145 with FTD	7.2.5	Erepower4KHG.cisco.com/443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1		

交換機HA狀態

在Firepower CLI上, 運行 connect ftd FTD01和 system support diagnostic-cli命令以進入ASA CLI。 運行 enable和 failover active 命令以 切換FTD01\_FTD02\_HA的HA。

## <#root>

Firepower-module1>

connect ftd FTD01

>

```
system support diagnostic-cli
```

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available

enable

firepower#

failover active

#### 疑難排解

要驗證故障切換狀態,請運行 show failover 和 show failover history 命令。

## <#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

```
>
```

show failover history

----- From State To State Reason -

運行 debug fover <option>命令以啟用故障切換的調試日誌。

## <#root>

#### >

debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution of

#### 參考

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance\_solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

## 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)。