# 更換安全防火牆中的故障裝置高可用性威脅防禦

目錄

<u>簡介</u>
<u>必要條件</u>
採用元件
<u>背景資訊</u>
開始之前
確定故障裝置
用備用裝置替換故障裝置
<u>在不備份的情況下更換故障裝置</u>
相關資訊

簡介

本文說明如何更換高可用性(HA)設定中的故障Secure Firewall威脅防禦模組。

必要條件

需求

思科建議您瞭解以下主題:

- 思科安全防火牆管理中心(FMC)
- Cisco Firepower可擴充作業系統(FXOS)
- 思科安全防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Firepower 4110運行FXOS v2.12(0.498)
- 邏輯裝置運行Cisco安全防火牆7.2.5版

- Secure Firewall Management Center 2600運行v7.4
- 安全複製協定(SCP)知識

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。

### 背景資訊

裝置支援以下過程:

- Cisco Secure Firewall 1000系列裝置
- Cisco Secure Firewall 2100系列裝置
- Cisco Secure Firewall 3100系列裝置
- Cisco Secure Firewall 4100系列裝置
- Cisco Secure Firewall 4200系列裝置
- 思科安全防火牆9300裝置
- 適用於VMWare的思科安全防火牆威脅防禦

## 開始之前

本文檔要求您使用相同的FXOS和FTD版本配置新裝置。

# 確定故障裝置

FTD-HA High Availability						1:
FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD 7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	¢Þ	:
FTD-02(Secondary, Failed) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD 7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«P	:

在此案例中,輔助裝置(FTD-02)處於故障狀態。

# 用備用裝置替換故障裝置

#### 您可以使用此過程替換主要或輔助裝置。本指南假定您有要更換的故障裝置的備份。

步驟1.從FMC下載備份檔案。導覽至System > Tools > Restore > Device Backups,然後選擇正確 的備份。按一下「Download」:

Firewall Management Center System / Tools / Backup/Restore / Backup Manageme	nt Overview A	analysis Policies	Devices Obj	ects Integration	Deploy	Q 🔮 -	🗘 🕜 admin 🗸	cisco S	ECURE			
								Remote	Storage			
Backup Management Backup Profiles												
				Firewall Manag	ement Backup	Managed	Device Backup	Upload Ba	ckup			
Firewall Management Backups												
System Information Date Created	File Name	VDB Versi	ion Locatio	on Size (MB)	Config	gurations	Events	TID	>			
Restore Download Delete Move Storage Location: /var/sf/backup/ (Disk Usage: 8%)												
System Information	Date Created	File Name		VDB Version	Location	Size (MB)	Configurations	Events	TID			
Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:48:04	FTD-02_Seconda	ary_20230926234646.tar	build 365	Local	53	Yes	No	No			
Cisco Firepower 4110 Threat Defense v7.2.5	2023-09-26 23:47:57	FTD-01_Primary_	20230926234637.tar	build 365	Local	52	Yes	No	No			
Ļ												
Download												

步驟2.將FTD備份上傳到新FTD的/var/sf/backup/目錄:

2.1從test-pc(SCP客戶端)將備份檔案上傳到/var/tmp/目錄下的FTD:

@test-pc ~ % scp FTD-02\_Secondary\_20230926234646.tar cisco@10.88.243.90:/var/tmp/

2.2在FTD CLI專家模式下,將備份檔案從/var/tmp/移動到/var/sf/backup/:

root@firepower:/var/tmp# mv FTD-02\_Secondary\_20230926234646.tar /var/sf/backup/

步驟3.從清潔模式應用下一個命令,以還原FTD-02備份:

>restore remote-manager-backup FTD-02\_Secondary\_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense This Device Model :: Cisco Firepower 4110 Threat Defense

Backup Details

Model = Cisco Firepower 4110 Threat Defense

Software Version = 7.2.5

Serial = FLM22500791Hostname = firepower Device Name = FTD-02\_Secondary IP Address = 10.88.171.89 Role = SECONDARYVDB Version = 365SRU Version = FXOS Version = 2.12(0.498)Manager IP(s) = 10.88.243.90Backup Date = 2023-09-26 23:46:46 Backup Filename = FTD-02\_Secondary\_20230926234646.tar \*\*\*\*\*\*\* Verify that you are restoring a valid backup file. Make sure that FTD is installed with same software version and matches versions from backup manifest be Restore operation will overwrite all configurations on this device with configurations in backup. If this restoration is being performed on an RMA device then ensure old device is removed from network \*\*\*\*\*\*\* Are you sure you want to continue (Y/N)Y Added table audit\_log with table\_id 1 Added table health\_alarm\_syslog with table\_id 2 Added table dce\_event with table\_id 3 Added table application with table\_id 4 Added table rna\_scan\_results\_tableview with table\_id 5 Added table rna\_event with table\_id 6 Added table ioc\_state with table\_id 7 Added table third\_party\_vulns with table\_id 8 Added table user\_ioc\_state with table\_id 9 Added table rna\_client\_app with table\_id 10 Added table rna\_attribute with table\_id 11 Added table captured\_file with table\_id 12 Added table rna\_ip\_host with table\_id 13 Added table flow\_chunk with table\_id 14 Added table rua\_event with table\_id 15 Added table wl\_dce\_event with table\_id 16 Added table user\_identities with table\_id 17 Added table whitelist\_violations with table\_id 18 Added table remediation\_status with table\_id 19 Added table syslog\_event with table\_id 20 Added table rna\_service with table\_id 21 Added table rna\_vuln with table\_id 22 Added table SRU\_import\_log with table\_id 23 Added table current\_users with table\_id 24 Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023): The system is going down for reboot NOW!



附註:恢復完成後,裝置將您從CLI註銷、重新啟動並自動連線到FMC。此時,裝置似乎已 過時。

步驟 4. 恢復HA同步。在FTD CLI中,輸入configure high-availability resume:

>configure high-availability resume

#### FTD高可用性配置現在已完成:

FTD-HA High Availability 11 FTD-01(Primary, Active) Snort 3 Firepower 4110 with FTD 7.2.5 FPR4110-02:443 Security Module - 1 Base-ACP ÷ Essentials ¢P 10.88.171.87 - Routed FTD-02(Secondary, Standby) Snort 3 FPR4110-02:443 Security Module - 1 Firepower 4110 with FTD 7.2.5 Base-ACP ¢P ÷ Essentials 10.88.171.89 - Routed

# 在不備份的情況下更換故障裝置

如果沒有故障裝置的備份,可以繼續本指南。您可以替換主裝置或輔助裝置,此過程因裝置是主裝 置還是輔助裝置而異。本指南中介紹的所有步驟都是要恢復有故障的輔助裝置。如果要恢復有故障 的主裝置,請在步驟5中配置高可用性,即在註冊期間將現有輔助/主用裝置用作主裝置,將替換裝 置用作輔助/備用裝置。

步驟1.導航到Device > Device Management,獲取高可用性配置的螢幕截圖(備份)。 編輯正確 的FTD HA配對(按一下鉛筆圖示),然後按一下High Availability選項:

FTD-HA							Cancel
Cisco Firepower 4110 Threat Defense							_
Summary High Availability Device Routing Interfaces Inline Sets	DHCP VTEP						
High Availability Configuration							
High Availability Link		State Link					
Interface	Ethernet1/5	Interface				Ether	net1/5
Logical Name	FA-LINK	Logical Name				F/	A-LINK
Primary IP	10.10.10.1	Primary IP				10.1	0.10.1
Secondary IP	10.10.10.2	Secondary IP				10.1	0.10.2
Subnet Mask	255.255.255.252	Subnet Mask				255.255.25	55.252
IPsec Encryption	Disabled	Statistics					۹
Monitored Interfaces							
Interface Name Active IPv4 Standby IPv4 Ac	ctive IPv6 - Standby IPv6		Active Link-Local IPv6	Standby Link-Loca	l IPv6	Monitoring	
Inside 192.168.30.1						•	1
diagnostic						0	1
Outside 192.168.16.1						•	1
501500 192.100.10.1						•	-
Failover Trigger Criteria	1	Interface MAC Addres	sses				+
Failure Limit	Failure of 1 Interfaces	Physical Interface	Active Mac	ddress	Standby Mac Ad	idress	
Peer Poll Time	1 sec	No records to display					
Peer Hold Time	15 sec						
Interface Poll Time	5 sec						
Interface Hold Time	25 sec						

步驟2.中斷HA。

2.1導航到Devices > Device Management,然後按一下右上角的三點選單。然後按一下Break選項 :

<ul> <li>✓ FTD-HA High Availability</li> </ul>							Switch Active Peer
<ul> <li>FTD-01(Primary, Active) Snort 3</li> <li>10.88.171.87 - Routed</li> </ul>	Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	4	Force refresh node status Delete Revert Upgrade
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	~5	Health Monitor Troubleshoot Files

2.2.選擇Force break, if standby peer does not response選項:

Collapse All Download Device List Report										
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack				
Ungrouped (1)	Confirm Break									
High Availability	Breaking the except the poperation m	e High Availa Access Contr ight also res	bility pair "FTD-HA" will erase all rol and Flex Config policy from st tart Snort processes of primary a	I configuration tandby peer. This and secondary			×1			
• FTD-01(Primary, Active) Snort 3 10.88.171.87 - Routed	File Force break, if	nporarily cau air? f standby pee	sing traffic interruption. Are you a	sure you want to	Base-ACP	«P	:			
FTD-02(Secondary, Standby) Snort 3     10.88.171.89 - Routed	Fit			Base-ACP	«9	:				



附註:由於裝置無響應,您需要強制中斷HA。當您中斷高可用性對時,活動裝置將保留完 全部署的功能。備用裝置丟失其故障切換和介面配置,成為獨立裝置。

步驟3.刪除有故障的FTD。確定要替換的FTD,然後按一下三點式選單。按一下「Delete」:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Roll	Back	
✓ Ungrouped (2)								
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«D		1:
FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«9	Delete	1
							Packet Trac Packet Cap Revert Upg Health Mon Troubleshoo	er iture rade itor ot Files

步驟4.新增新的FTD。

### 4.1.導航到Devices > Device Management > Add,然後按一下Device:

View By:	Group	*							Migrate	Deployment History
All (1)	• Error (0)	<ul> <li>Warning (1)</li> </ul>	Offline (0)	Normal (0)	ployment Pe	nding (1) • Upgrade (0)	<ul> <li>Snort 3 (1)</li> </ul>		Q Search Dev	ice Add 🔻
Collapse All									Do	Device High Availability
Na	me			Model	Version	Chassis	Licenses	Access Control Policy	Auto Rolli	Chassis
	Ungrouped (1)									Group
	FTD-01 Snort 3	Routed		Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	49	11

4.2.選擇預配方法,在本例中為Registration Key,配置Host、Display Name和Registration Key。 配置Access Control Policy,然後按一下Register。

### Add Device

Select the Provisioning Method:

Registration Key
 Serial Number

CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:\*

.....

Group:

None

Access Control Policy:\*

Base-ACP	•
----------	---

#### Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click here for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

w

Select a recommended Tier	•
Carrier	
Malware Defense	
IPS IPS	
URL	
Advanced	
Unique NAT ID:†	
Transfer Packets	

Cancel

8

步驟5.建立HA。

5.1導航到Devices > Device Management > Add, 然後點選High Availability選項。

View By	c Group •						Migrate   [	Deployment History
All (2	Error (0)      Warning (0)      Offline (0)      Normal (2)	<ul> <li>Deployment Pending (0)</li> </ul>	<ul> <li>Upgrade (0)</li> </ul>	<ul> <li>Snort 3 (2)</li> </ul>			Q. Search Devic	ce Add • Device
Collapse							200 E	High Availability Cluster
	Ame	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rolli	Group
	<ul> <li>Origrouped (2)</li> </ul>							
	FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	«P	11
	FTD-02 Snort 3     10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02;443 Security Module - 1	Essentials	Base-ACP	¢9	×:

5.2.配置新增高可用性對。配置名稱、裝置類型,選擇FTD-01作為主對等方,選擇FTD-02作為輔助 對等,然後按一下Continue。

View By: Group *						Migrate   Deployme	ent History
All (2) • Error (0) • Warning (0) • Offline (0) • Normal (2)	Deployment Pending (0)	) • Upgrade (0)	• Snort 3 (2)			Q, Search Device	Add 🔻
Collacse All						Download Devi	ice List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (2)		Add High Availa	ability Pair				
FTD-01 Snort 3 10.88.171.87 - Routed	Firepower 4110 with FTD	Name:* FTD-HA		Essentials	Base-ACP	e?>	1
FTD-02 Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	Device Type: Firewall Threat De	fense •	Essentials	Base-ACP	\$%	1
		Primary Peer: FTD-01 Secondary Peer: FTD-02 Threat Defense F configuration. Lic converted to thei on both peers.	Figh Availability pair will have primary consess from primary peer will be r high availability versions and applied				



附註:請記得選擇主裝置作為仍具有配置的裝置,在本例中為FTD-01。

5.3.確認建立HA,然後按一下Yes。

	Add High Availability Pair	
FTD	Name:* FTD-HA	Essenti
FTD	Warning	Essenti
	This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption. Do you want to continue?	
	Do not display this message again No Yes	
	converted to their high availability versions and applied on both peers.	
	Cancel Continue	



附註:配置高可用性會重新啟動兩台裝置的snort引擎,這可能會導致流量中斷。

5.4.配置步驟2中介紹的高可用性引數,然後按一下Add選項:

Firewall Management Center Overview Analysis Devices / Device Management	Policies Devices Objects Integration		Deploy Q 💞 🌣	admin ~ admin SECURE
View By:         Group         •           All (2)         • Error (0)         • Warning (0)         • Offline (0)         • Normal (2)	Deployment Pending (0)     Upgrade (0)     Sn	ort 3 (2)		Migrate   Deployment History Q. Search Device Add •
Collaçue All				Download Device List Report
Name	Add High Availability Pair	ø	Access Control Policy	Auto RollBack
□	High Availability Link	State Link		
FTD-01 Snort 3 10.88.171.87 - Routed	Interface: Ethernet1/5   Logical Name: FA-LINK	Interface: Same as LAN Failover Link	Base-ACP	«» 🖌 :
FTD-92 Snort 3 10.88.171.89 - Routed	Primary IP: 10.10.10.1	Primary IP:* 10.10.10.1	Base-ACP	«p 🖌 :
	Secondary IP: 10.10.10.2	Secondary IP:* 10.10.10.2		
	Subnet Mask: 255.255.255.252	Subnet Mask:* 255.255.255.252		
	IPsec Encryption			
	Enabled			
	Key Generation: Auto v			
	<ul> <li>LAN failover link is used to sync configuration, stateful between peers. Selected interface links and encryption se</li> </ul>	failover link is used to sync application content titings cannot be changed later.		
		Cancel		

### 6. FTD高可用性配置現在已完成:

FTD-HA High Availability							1:
<ul> <li>FTD-01(Primary, Active) Snort 3</li> <li>10.88.171.87 - Routed</li> </ul>	Firepower 4110 with FTD	7.2.5	EPR4110-02:443 Security Module - 1	Essentials	Base-ACP	49	:
FTD-02(Secondary, Standby) Snort 3 10.88.171.89 - Routed	Firepower 4110 with FTD	7.2.5	FPR4110-02:443 Security Module - 1	Essentials	Base-ACP	4D	:



附註:如果不配置虛擬MAC地址,您需要清除相連路由器上的ARP表,以便在主裝置更換 時恢復流量。有關詳細資訊,請參閱<u>高可用性中的MAC地址和IP地址</u>。

相關資訊

• 思科技術支援與下載

#### 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)。