# 在Firepower 4100上配置FTD多实例高可用性

目录 简介 先决条件 要求 使用的组件 背景信息 网络图 配置 步骤1:预配置接口 <u> 第二步:为容器实例添加2个资源配置文件。</u> <u>第3步:(可选)为容器实例接口添加虚拟MAC地址的MAC池前缀。</u> <u>第四步:添加独立实例。</u> <u>第五步:配置接口</u> <u> 第六步:为每个实例添加高可用性对。</u> 验证 故障排除 参考

# 简介

本文档介绍如何在FTD容器实例(多实例)中配置故障切换。

# 先决条件

# 要求

思科建议您具备Firepower管理中心和防火墙威胁防御知识。

# 使用的组件

思科Firepower管理中心虚拟7.2.5 思科Firepower 4145 NGFW设备(FTD) 7.2.5 Firepower可扩展操作系统(FXOS) 2.12 (0.498) Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

在部署FTD多实例之前,必须了解它如何影响您的系统性能并做出相应的规划。务必参考思科官方 文档或咨询思科技术代表,以确保实现最佳部署和配置。

# 背景信息

多实例是Firepower威胁防御(FTD)的一项功能,类似于ASA多情景模式。它允许您在单个硬件上运 行FTD的多个独立容器实例。每个容器实例允许硬资源分离、独立的配置管理、独立的重新加载、 独立的软件更新和全面的威胁防御功能支持。这对于需要针对不同部门或项目实施不同安全策略 ,但又不想投资于多个独立硬件设备的组织特别有用。运行FTD 6.4及更高版本的Firepower 4100和 9300系列安全设备当前支持多实例功能。

本文档使用最多支持14个容器实例的Firepower4145。有关Firepower设备支持的最大实例数,请参 阅<u>每个型号的最大容器实例和资源数。</u>

# 网络图

本文档介绍此图上多实例中的HA配置和验证。



逻辑配置图



物理配置图

# 配置

# 步骤1:预配置接口

# a.导航到FCM上的接口。设置2个管理接口。在本示例中,Ethernet1/3和Ethernet1/7。

Overview Interfaces	Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	admin
All Interfaces Hardware	Benars		Network Module 1	5 7 5 8	Network Module 2 :	Empty	Network Module 3 : Em	pty			
An Incentaces Horomore	ulhass								Add Ne	w • 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)	a 🖉	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/2	data	lgbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/5	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up		0	
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up		ø	
Ethernet1/8	data	lgbps	1gbps			Full Duplex	yes	up		0	

预配置接口

# 第二步:为容器实例添加2个资源配置文件。

a.导航到平台设置 > 资源配置文件 > 在FCM上添加。设置第一个资源配置文件。

在本例中: ·名称:Instance01 ·核心数:10



注意:对于容器实例对的高可用性,必须使用相同的资源配置文件属性。 将配置文件的名称设置为1到64个字符。请注意,添加此配置文件后,无法更改其名称。 设置配置文件的核心数量,在6和最大数量之间。

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

添加第一个资源配置文件

b.在第2步中重复a.以配置第2个资源配置文件。

在本例中: ·名称:Instance02 ·核心数:20

Overview Interfaces Log	ical Devices Security Engine	Platform Settings	l i		System Tools Help admin
NTP SSH				Add	
SNMP	Name	Description	Cores		
AAA	Default-Small	Auto-created application resource-profile with 6 cpu-cores	6	/ 8	
Syslog	Instance01		10	/ 8	
DNS FIPS and Common Criteria		Add Resource Profile			
MAC Pool		Name:* Instance02			
Resource Profiles		Description			
Network Control Policy Chassis URL		Vumber of Cores:* 20 Range: 6 to 86 Specify even value for number of cores.			
		OK Cancel			

添加第2个资源配置文件

# c.检查2个资源配置文件已成功添加。

(	Overview Interfaces	Logica	I Devices	Security Engine	Platform Settings						System	Tools	Help	admin
	NTP													
	SSH								0	Add				
	SNMP		Name			Description	Core							
	HTTPS		Default-	Small		Auto-created application resource-profile with 6 cpu-cores	6			28				
	AAA							_						
	Syslog		Instance	01			10			a 🖉				
	DNS		Instance	02			20							
	FIPS and Common Criteria		instance	V4			20			6				
	Access List													
	MAC Pool													
	Resource Profiles													
	Network Control Policy													
	Chassis URL													

确认资源配置文件

# 第3步:(可选)为容器实例接口添加虚拟MAC地址的MAC池前缀。

您可以手动设置主用/备用接口的虚拟MAC地址。如果未设置虚拟MAC地址,对于多实例功能,机 箱会自动为实例接口生成MAC地址,并确保每个实例中的共享接口使用唯一的MAC地址。

有关MAC地址的详细信息,请选中<u>添加一个MAC池前缀和查看容器实例接口的MAC地址</u>。

第四步:添加独立实例。

a.导航到逻辑设备 > 添加独立。设置第一个实例。

在本例中:

·设备名称:FTD01

·实例类型:容器



注意:部署容器应用的唯一方法是预部署实例类型设置为容器的应用实例。 确保选择 Container。

添加逻辑设备后,无法更改此名称。

Overview Interfaces Logical Devices Security Engine	Platform Settings	System Tools Help admin
Logical Device List	(0 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	
	Towelstan Court Formul Threat Defense A	
	Templace: Usco secure rirevali inreat Defense V	
	Image version: 7.4.3.4.08	
	Instance Type: Container	
	Before you add the first container instance, you must reinitialize the security module(engine so that the disk has the correct formatting. You only need to perform this action once.	
	OK Cancel	

添加实例

# 第五步:配置接口

a.为Instance01设置Resource Profile、Management Interface和Management IP。

在本例中: ·资源配置文件:Instance01 ·管理接口: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	SM 1 - 86 Cores Available  Resource Profile: Instance01  Interface Information  Hanagement Interface: Ethernet1/3  Address Type: IPv4 only  IPv4  Hanagement IP: 1: Network Mask: 255.0.0.0 Network Gateway: 1.^^	
Application Version Resource Profile	rt Status	
FTD 7.2.5.208		
	OK Cancel	

配置配置文件/管理接口/管理IP

b.设置数据接口。

在本例中:

·Ethernet1/1(用于内部)

·Ethernet1/2(用于外部)

·Ethernet1/4(用于高可用性链路)

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 Ethernet1/4	7.2.5.208	Instance01	11 Type data data data	1.0 *****	Ethernet1/3		

设置数据接口

# c.导航到逻辑设备。正在等待实例启动。

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	s				System Tools Help admin
L	ogical Devic	e List			1 Container instance	e] 100% (86 of 86) Cores Avai	lable			C Refresh O Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0.0.000	Ethernet1/3	* Installing	000 🎋 c 🖄

确认Instance01的状态

# d.在步骤4.a和步骤5.a至c中重复a.以添加第二个实例并设置其详细信息。

在本例中:

- ·设备名称:FTD11
- ·实例类型:容器
- ·资源配置文件:Instance02
- ·管理接口:Ethernet1/7
- ·管理IP:x.x.10.1
- ·以太网接口1/5 =内部
- ·以太网接口1/6=外部
- ·以太网接口1/8 =高可用性链路

e.确认2个实例在FCM上处于在线状态。

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 I	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					<b>/</b> I
Applicat	tion	Version	Resource #	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01	]	C: a1.1	1.0	Ethernet1/3	Online	💌 🏹 C 🕍

确认主设备中的实例状态

f.(可选)在Firepower CLI上运行 scope ssa、scope slot 1 和 show app-Instance 命令以确认2个实例处于联机状态。

<**#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.在辅助设备上执行相同的操作。确认2个实例处于联机状态。

Ov	erview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logi	al Devio	e List			(2 Container instan	ces) 66% (56 of 86) Co	res Available			C Refresh 🕥 Add •
C	FTD12			Standalone	Status:ok					
	Applicat	lon	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance02	]		1.	Ethernet1/7	Online	💌 🎋 c 🚈
E	FTD02			Standalone	Status:ok					/:
	Applicat	ion	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
۲	FTD		7.2.5.208	Instance01			1.0	Ethernet1/3	nline 🕜	💌 🕅 c 🔙

确认辅助设备中的实例状态

#### 第六步:为每个实例添加高可用性对。

a.导航到设备 > 在FMC上添加设备。将所有实例添加到FMC。

在本例中:

·FTD1的实例01的显示名称:FTD1\_FTD01 ·FTD1的实例02的显示名称:FTD1\_FTD11 ·FTD2的实例01的显示名称:FTD2\_FTD02 ·FTD2的实例02的显示名称:FTD2\_FTD12

## 下图显示FTD1\_FTD01的设置。



将FTD实例添加到FMC

#### b.确认所有实例都是正常的。

Firewall Management Center Overview Analysis Polic	cies Devices Objects I	ntegration			Deploy	Q 🥝 🗭 🚱 admin 🔹	dede SECURE
View By:         Group         View By:         Office (0)         Office (0)         Office (0)         One         Operating (0)         Office (0)         Operating (0) <td>ployment Pending (0)</td> <td>(0) • Snort 3</td> <td>(4)</td> <td></td> <td></td> <td>Deploy Q, Search Device</td> <td>Ment History</td>	ployment Pending (0)	(0) • Snort 3	(4)			Deploy Q, Search Device	Ment History
Collecte All Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4) FTD1_FTD01 Sect 3	Economic (145 mill) ETD	796		Base Thread (2 more 3			
1.051.01 - Routed      FTD1_FTD11 Scort 3     Vices 10.1 - Routed	Firepower 4145 with FTD	7.2.5	Security Module - 1 (Container)      FPR4145-ASA-K9.443      Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	10 10	/1
FTD2_FTD02 Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1
FTD2_FTD12 Short 3     Log - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	11

确认FMC中的实例状态

c.导航到设备 > 添加高可用性。设置第1个故障转移对。

在本例中:

·名称:FTD01\_FTD02\_HA

·主对等体:FTD1\_FTD01



**注意**:请确保选择正确的设备作为主设备。

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				

添加第1个故障转移对

# d.为第1个故障转移对中的故障转移链路设置IP。

在本例中:

# ·高可用性链路:Ethernet1/4

·状态链路:Ethernet1/4

# ·主IP:192.168.90.1/24

# ·辅助IP:192.168.90.2/24

Firewall Management Center Overview Analysis	Policies	Devices Objects Integration		Deploy	옥 💈 🌣 📵 admin 🕶	disco SECURE
Mew Br. Group					Depk	yment History
All (4)	Deploymen	t Pending (0)   Upgrade (0)  Snort 3 (4)			Q, Search Device	Add •
Collapse Al						
Name	Model	Add Link Availability Date		Access Control Policy	Auto RollBack	
Ungrouped (4)		Add high Availability Pail				
		High Availability Link	State Link			
O FTD1_FTD01 Snort 3	Firepow	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +	acp-rule	49	1:
The second		Logical Name:* ha_link	Logical Name:*			
FTD1_FTD11 Snort 3	Firepow	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	4 <b>9</b>	1:
L.10.1 - Moused		Use IPv6 Address	Use IPv6 Address			
© FTD2_FTD02 Snort 3	Firepow	Secondary IP:* 192.168.90.2	Secondary IP:*	acp-rule	«©	11
II.2 - Houted		Subnet Mask:* 255.255.255.0	Subnet Mask:*			
FTD2_FTD12 Snort 3	Firepow	IPsec Encryption		acp-rule	4Q	1:
- III.2 - Routed		Enabled				
		Key Generation: Auto +				
		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			

为第1个故障转移对设置HA接口和IP

# e.确认故障切换状态

·FTD1\_FTD01:主,活动

·FTD2\_FTD02:备用

Fir Dov	rewall Management Center Overview Analysis	Policies Devices Obje	cts Integratio	n:			Deploy Q 😋	admin      dealers SECURE				
View By:	Group							Deployment History				
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Upgrade (0)	Snort 3 (4)				Q, Search Device Add •				
College AT												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack					
	<ul> <li>Ungrouped (3)</li> </ul>											
	FTD01_FTD02_HA High Availability							1				
	FTD1_FTD01(Primary, Active) Snort 3     CAMD 1.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	I				
	FTD2_FTD02(Secondary, Standby) Snort 3     Clini 1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Frepower4KHG cisco com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۹	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	4D	11				
	C FID2_FID12 Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۶	11				

确认第1个故障转移对的状态

# f.导航到设备>单击FTD01\_FTD02\_HA(在本例中)>接口。为数据接口设置活动IP。

### 在本例中:

·以太网接口1/1(内部):192.168.10.254/24

·以太网接口1/2(外部):192.168.20.254/24

·以太网接口1/3(诊断):192.168.80.1/24

### 下图显示了Ethernet1/1的"Active IP"设置。

Firewall Management Center Devices / Secure Frewall Interfaces	Dverview Analysis I	Policies Devices Objects Integration		Deploy Q 🚱 🌣 🕲 admin 🔹 🕬 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Summary High Availability Device Routin	ng Interfaces Inline S	Edit Physical Interface	Edit Physical Interface	ealiable for use. X
		General IPv4 IPv6 Path Monitoring Advanced	General IPv4 IPv6 Path Monitoring Advanced	Add Interfaces *
Interface	Logi	inside	er sype: Use Static IP v	
Ethernet1/1	inside	Management Only	192.168.10.254/24	
© Ethernet1/2	outside	Description:	192 THE W. LIED CONTINUE WILLIGHT CONTINUE (120	
© Ethernet1/3	ciagnostic	Mode:		
		Security Zone:		
		Inside_zone   Interface ID:		Cancel
		Ethernet1/1 MTU:		
		1500		
		Priority: 0 (0 - 65535)		
		Propagate Security Group Tag:		
			Cancel	

设置数据接口的活动IP

g.导航到设备>点击FTD01\_FTD02\_HA(在本例中)>高可用性。设置数据接口的备用IP。

#### 在本例中:

- ·以太网接口1/1(内部):192.168.10.253/24
- ·以太网接口1/2(外部):192.168.20.253/24
- ·以太网接口1/3(诊断):192.168.80.2/24

下图显示Ethernet1/1的备用IP设置。

Devices / High Availability	Center Overview Analysis Policies Device	s Objects Inte	gration		Deploy	९ 🗳 🌣	👩 admin 🔻 🖓	SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defensi Summary High Availability	e Device Routing Interfaces Inline Sets DHCP y	VTEP						Cancel
IPsec Encryption	Edit inside	0	itics					٩
Monitored Interfaces	Monitor this interface for failures							
Interface Name	IPv4 IPv6			Active Link-Local IPv6	Standby Link-	-Local IPv6	Monitoring	
outside	Interface Name:						0	1
diagnostic	inside Active IP Address:						0	1
inside	192.168.10.254						0	1
	24							
	Standby IP Address:							
Failover Trigger Criteria	192.108.10.253		face MAC Add	resses				+
Failure Limit			cal Interface	Active Mac Ad	dress	Standby Mac	Address	
Peer Poll Time			et1/1	1234.1234.00	01	1234.1234.0	002	11
Peer Hold Time		Cancel						

设置数据接口的备用IP

### h.重复步骤6.c至g,添加第2个故障转移对。

在本例中:

· 名称:FTD11\_FTD12\_HA

·主要对等体:FTD1\_FTD11

·次要对等体:FTD2\_FTD12

·高可用性链路:Ethernet1/8

·状态链路:Ethernet1/8

·以太网接口1/8 (ha\_link处于活动状态): 192.168.91.1/24

·以太网接口1/5(内部主用):192.168.30.254/24

- ·以太网接口1/6(外部主用接口):192.168.40.254/24
- ·以太网接口1/7(诊断活动接口):192.168.81.1/24

·以太网接口1/8 (ha\_link备用): 192.168.91.2/24

- ·以太网接口1/5(内部备用):192.168.30.253/24
- ·以太网接口1/6(外部备用):192.168.40.253/24
- ·以太网接口1/7(诊断待机):192.168.81.2/24

i.导航到逻辑设备 > 添加独立。设置ACP规则以允许从内部到外部的流量。

þ	Firewall Ma Policies / Acces	anagement C is Control / Policy I	enter Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	Q 🔮 🌣	🛛 admi	in •	diste SI	ÉCURE
∎ a Er	Acadyze Hit Counts     Sove     Cancel     Enter Description																		
Rule	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy: Default Prefilter Policy: None Identity Policy: None																		
Filter b	v Device	Search Rules											×	Show Rule Con	ficts 🛛 + /	idd Categ	ory	+ Add	d Rule
= N	lame	Source Zones	Dest Zones	Source Networks	De	est Networks	VLAN Tags	Usors	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O I	1. A I		•
~ Mand	latory - acp-rule	(1-1)		_															
1 f	td_ha_acp	inside_zone	outside_zone	Any	An		Any	Any	Any	Any	Any	Any	Any	Any	Allow	15 O D	1.0.1	ā 🚺	0/1
✓ Defau	V Default - acp-rule (-)																		
There a	re no rules in thi	s section. Add Ru	le or Add Categ	ory															

设置ACP规则

#### j.将设置部署到FTD。

#### k.在CLI中确认高可用性状态

每个实例的HA状态也在Firepower CLI中确认,这与ASA相同。

运行 show running-config failover 和 show failover 命令以确认FTD1\_FTD01(主实例01)的高可用性状态。

#### <#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

运行 show running-config failover 和 show failover 命令以确认FTD1\_FTD11(主实例02)的高可用性状态。

#### <#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

运行 show running-config failover 和 show failover 命令以确认FTD2\_FTD02(辅助实例01)的高可用性状态。

### <#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- 运行 show running-config failover 和 show failover 命令以确认FTD2\_FTD12 (Seconday Instance02)的高可用性状态。

### <#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.确认许可证使用

所有许可证按安全引擎/机箱使用,而不是按容器实例使用。

·自动分配基本许可证:每个安全引擎/机箱一个。

·功能许可证手动分配给每个实例,但每个功能每个安全引擎/机箱仅使用一个许可证。对于特定功能许可证,无论使用的实例数量是 多少,您总共只需要1个许可证。

此表显示本文档中许可证的使用方式。

FPR01	实例01	基础、	URL过滤、	恶意软件、	威胁
	实例02	基础、	URL过滤、	恶意软件、	威胁
FPR02	实例01	基础、	URL过滤、	恶意软件、	威胁
	实例02	基础、	URL过滤、	恶意软件、	威胁

许可证总数

基础	URL 过滤	恶意软件	威胁
2	2	2	2

在FMC GUI中确认已使用的许可证数量。

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 Malware (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	at 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	
✓ 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	
✓ URL 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	

确认已使用的许可证

# 验证

当FTD1\_FTD01(主实例01)发生故障时,会触发实例01的故障切换,备用端的数据接口会接管原始主用接口的IP/MAC地址,确保 Firepower持续传递流量(本文档中的FTP连接)。



崩溃前



故障转移已触发

步骤1:启动从Win10-01到Win10-02的FTP连接。

第二步:运行 show conn 命令以确认在实例01的两个实例中均建立了FTP连接。

// 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

第三步:启动从Win10-03到Win10-04的FTP连接。

第四步:运行 show conn 命令以确认在实例02的两个实例中均建立了FTP连接。

### <#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

第五步:运行 connect ftd FTD01和 system support diagnostic-cli命令以进入ASA CLI。运行 enable和 crashinfo force watchdog 命令,强制使主/主用设备中的实例01崩溃。

### <#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]:

第六步:在Instance01中发生故障切换,且FTP连接未中断。运行 show failover和 show conn命令以确认FPR02中Instance01的状态。

### <#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

步骤 7.在Instance01中发生的崩溃对Instance02没有影响。 运行 show failover和 show conn命令以确认Instance02的状态。

### <#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 (2

#### show conn

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

步骤 8在FMC上导航到设备 > 全部。确认高可用性状态。

#### ·FTD1\_FTD01:主、备用

#### ·FTD2\_FTD02:辅助、活动

C Fin Dev	ewall Management Center Overview Analysis ices / Device Management	Policies Devices Obje	ts Integrati	on			Deploy Q	O admin     dede SECURE					
View By:	Group							Deployment History					
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Upgrade (0)	<ul> <li>Snort 3 (4)</li> </ul>				Q, Search Device Add •					
Collapse All	Colume Al												
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack						
	V Ungrouped (2)												
	V FTD01_FTD02_HA							/1					
	FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	FPR4145-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	eQ+	1					
	V FTD11_FTD12_HA High Availability							11					
	FTD1_FTD11(Primary, Active) Short 3     Short 3     10.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q	1					
	FID2_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	4 <b>9</b>	I					

确认HA状态

第9步: (可选)在FPR01的Instance01恢复正常后,您可以手动切换HA的状态。这可以通过FMC GUI或FRP CLI完成。

在FMC上,导航到设备 > 全部。单击Switch Active Peer以切换FTD01\_FTD02\_HA的HA状态。

Fir Dev	Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy									
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)									
	FID01_FID02_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	4D	1		

交换机HA状态

在Firepower CLI上,运行 connect ftd FTD01和 system support diagnostic-cli命令以进入ASA CLI。运行 enable和 failover active 命令以 切换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

#### 故障排除

要验证故障切换的状态,请运行 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

运行 debug fover <option>命令以启用故障切换调试日志。

### <#root>

#### >

debug fover

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

#### 参考

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

# 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。