在FP9300(机箱内)上配置FTD集群

目录

简介 先决条件 要求 使用的组件 背景信息 配置 网络图 任务1.为FTD集群创建必要接口 任务2.创建FTD集群 任务3.将FTD集群注册到FMC 任务4.在FMC上配置端口通道子接口 任务5.检验基本连通性 从机箱管理器UI捕获集群 任务6.从集群中删除从设备 验证 故障排除 相关信息

简介

本文档介绍如何在FPR9300设备上配置和验证集群功能。

警告:本文档中提供的信息包括集群的初始安装/配置。本文档不适用于设备更换(退货授权 — RMA)流程

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 运行1.1(4.95)的思科Firepower 9300安全设备
- •运行6.0.1的Firepower威胁防御(FTD)(内部版本1213)
- •运行6.0.1.1的FireSIGHT管理中心(FMC)(内部版本1023)

实验完成时间:1小时.

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。

背景信息

- •在带FTD设备的FPR9300上,您可以在所有受支持版本上配置机箱内集群。
- 机箱间集群在6.2中引入。
- ・端口通道48创建为集群控制链路。对于机箱内集群,此链路使用Firepower 9300背板进行集群 通信。
- 不支持单个数据接口,管理接口除外。
- •管理接口分配给集群中的所有设备。

配置

网络图



任务1.为FTD集群创建必要接口

任务要求:

创建集群、管理接口和端口通道数据接口。

解决方案:

步骤1.创建端口通道数据接口。

要创建新接口,您必须登录FPR9300机箱管理器并导航至接口选项卡。

选择Add Port Channel并使用以下参数创建新的端口通道接口:

端口通道ID	5
类型	数据
enable	Yes
成员ID	Ethernet1/3、Ethernet 1/4

选择OK以保存配置,如图所示。

Add Port Cha	nnel				?×
Port Channel ID:	5	🗹 Enable			
Туре:	Data				
Speed:	1gbps 👻	•			
Interfaces					
Ava	ilable Interface		Member ID		
	Search]	Ethernet	1/3	
	Ethernet1/2		III Ethernet	1/4	
	Ethernet1/3				1
	Ethernet1/4				
	Ethernet1/5				
	Ethernet1/6	Add Telesford			
	Ethernet1/7	Add Interrace			
	Ethernet1/8				
11	Ethernet2/1				
	Ethernet2/2				
	Ethernet2/3				
	Ethernet2/4				
	Ethernet3/1				
	Ethernet3/2				
				ОК	Cancel

步骤2.创建管理接口。

在Interfaces选**项**卡上,选择该接口,单击**Edit**并配置Management Type接口。

单击OK保存配置,如图所示。

Edit Inte	rface - Ethernet1/1	? X
Name:	Ethernet1/1 🗹 Enal	ble
Type:	mgmt	*
Speed:	1gbps	*
	ок	Cancel

步骤3.创建集群控制链路接口。

单击"添**加端口通道**"按钮,然后使用这些参数创建一个新的端口通道接口,如图所示。

端口通道ID	48
类型	集群
enable	Yes
成员ID	-

Add Port Cha	annel				?×			
Port Channel ID:	48	🗹 Enable						
Type:	Cluster]						
Speed:	1gbps 👻]	· •					
Interfaces	Interfaces							
Av	ailable Interface		Member ID					
	Search							
	Ethernet1/2							
	Ethernet1/5							
	Ethernet1/6							
	Ethernet1/7							
	Ethernet1/8							
	Ethernet2/1	Add Interface						
	Ethernet2/2							
	Ethernet2/3							
	Ethernet2/4							
	Ethernet3/1							
	Ethernet3/2							
	Ethernet3/3							
	Ethernet3/4							
				ок	Cancel			

任务2.创建FTD集群

任务要求:

创建FTD集群设备。

解决方案:

步骤1.导航至Logical Devices,然后单击Add Device按钮。

创建FTD集群,如下所示:

设备名	FTD_cluster
模板	思科Firepower威胁防御
映像版本	6.0.1.1213
设备模式	集群

要添加设备,请单击OK,如图所示。

Add Device			?×
Device Name:	FTD_cluster		
Template:	Cisco Firepower Threat Defense	~	
Image Version:	6.0.1.1213	~	
Device Mode:	🔵 Standalone 💿 Cluster		
		_	
	ОК		Cancel

步骤2.配置和部署FTD集群。

创建FTD设备后,系统会将您重定向到Provisioning- device_name窗口。

点击设备图标以启动配置,如图所示。

0	verview	Interfaces	ogical Devices	Security M	odules Platform Settin	gs					System	Tools	Help	admin
e l	rovisionin ustered (g - FTD_cluster Cisco Firepower	Threat Defense	6.0.1.1213]						Se	-	Canoti	
D	ata Ports		-											
1	Ethernet1/2													
10	Ethernet1/S													
10	Ethernet1/6							C		5				
0	Ethernet1/7													
	Ethernet1/8													
	Ethernet2/1													
	Ethernet2/2							FTD - 6.0.	1.1213					
	(thernet2/3							Security Mod	tule 1,2,3					
	Ethernet2/4													
	Ethernet3/2													
	Ethernet3/3									r				
	Ethernet3/4													
10	Port-channel5													
	Security 1	todule Ace	lication	Version	Management	4 10	Esteway	Nanapagent Port	Status					-
a	Security M	odule 1 FTD		6.0.1.1213			outer of							_
4	Security M	odule 2 FTD		6.0.1.1213										
a	Security M	odule 3 PTD		6.0.1.1213										

使用这些设**置配置**FTD集群信息选项卡,如图所示。

群集密钥	思科
群集组名称	FTD_cluster
管理接口	以太网接口1/1

Cisco Firepower Thre	eat Defense - Configuration					
Cluster Information Setti	ngs Interface Information Agreement					
Security Module(SM)						
Security Module-1,Security M	Iodule-2,Security Module-3					
Interface Information						
Cluster Key:	•••••					
Cluster Group Name:	FTD_cluster					
Management Interface:	Ethernet1/1					
1						
	OK Cancel					

使用这些设置**配**置FTD设置选项卡,如图所示。

注册密钥	思科
密码	管理123
Firepower管理中心IP	10.62.148.73
搜索域	cisco.com
防火墙模式	路由
DNS Servers	173.38.200.100
完全限定主机名	ksec-fpr9k-1-1-3.cisco.com
事件接口	无

Cisco Firepower Thre	at Defense - Confi	guration
Cluster Information Settings	Interface Information	Agreement
Registration Key:	••••	
Password:	•••••	
Firepower Management Center IP:	10.62.148.73	
Search domains:	cisco.com	
Firewall Mode:	Routed	~
DNS Servers:	173.38.200.100	
Fully Qualified Hostname:	ksec-fpr9k-1-1-3.cisco.	com
Eventing Interface:	None	•
	ОК	Cancel

使用这些设**置配置**FTD接口信息选项卡,如图所示。

地址类型	仅IPv4
安全模块1	
管理IP	10.62.148.67
网络掩码	255.255.255.128
网关	10.62.148.1
安全模块2	
管理IP	10.62.148.68
网络掩码	255.255.255.128
网关	10.62.148.1
安全模块3	
管理IP	10.62.148.69
网络掩码	255.255.255.128
网关	10.62.148.1

Cisco Firepower Threat Defense - Configuration						
Cluster Information Settings	Interface Information Agreement					
Address Type:	IPv4 only					
Security Module 1						
Management IP:	10.62.148.67					
Network Mask:	255.255.255.128					
Gateway:	10.62.148.1					
Security Module 2						
Management IP:	10.62.148.68					
Network Mask:	255.255.255.128					
Gateway:	10.62.148.1					
Security Module 3						
Management IP:	10.62.148.69					
Network Mask:	255.255.255.128					
Gateway:	10.62.148.1					
	OK Cancel					

接受"协议"选**项卡**上的协议,**然后**单击"确定",如图所示。

Cisco Firepower Threat Defense - Configuration							
End User License Agreement							
IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT FROM AN APPROVED SOURCE AND THAT YOU, OR THE ENTITY YOU REPRESENT (COLLECTIVELY, THE "CUSTOMER") HAVE BEEN REGISTERED AS THE END USER FOR THE PURPOSES OF THIS CISCO END USER LICENSE AGREEMENT. IF YOU ARE NOT REGISTERED AS THE END USER YOU HAVE NO LICENSE TO USE THE SOFTWARE AND THE LIMITED WARRANTY IN THIS END USER LICENSE AGREEMENT DOES NOT APPLY. ASSUMING YOU HAVE PURCHASED FROM AN APPROVED SOURCE, DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES							
CISCO SYSTEMS, INC. OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF CISCO SYSTEMS, INC. ("CISCO") IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU PURCHASED THE SOFTWARE							
 I understand and accept the agreement 							
OK Cancel							

步骤3.为FTD分配数据接口。

展开Data Ports区域,然后点击要分配给FTD的每个接口。完成后,选择**Save**以创建FTD集群,如 图所示。

0	verview Interfaces	Logical Device	Security Modules Pla	tform Settings				System Tools	Help admin
P	rovisioning - FTD_clu lustered Cisco Firej	uster power Threat Defens	e 6.0.1.1213					Save	Cancel
D	ata Ports								1
	Ethernet1/7								
ļ	Ethernet1/8								
IJ	Ethernet2/1	_							
IJ	Ethernet2/2								
ļ	Ethernet2/3			Port- channel5		_			
IJ	Ethernet2/4	_							
U.	Ethernet3/1					FTD - 6.0.1	.1213		
I.	Ethernet3/2	_				Security Modu	//1 /e 1,2,3		
l,	Ethernet3/3	-1		channel48		_			
	Ethernet3/4	_							
	Port-channel48								
Ľ	Port-channels								_
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status		
9	Security Module 1	FTD	6.0.1.1213	10.62.148.67	10.62.148.1	Ethernet1/1			
	Cluster Interfaces:	Port-channel48							
9	Security Module 2	FTD	6.0.1.1213	10.62.148.68	10.62.148.1	Ethernet1/1			
	Cluster Interfaces:	Port-channel48							
۲	Security Module 3	FTD	6.0.1.1213	10.62.148.69	10.62.148.1	Ethernet1/1			
	Cluster Interfaces:	Port-channel48							

验证:

•从FPR9300 GUI,如图所示。

0	erview Interface	s Logical Devi	Security Module	es Platform Settings				System Tools Help admin
	FTD_cluster	Clustered	Status: ok					C Refresh O Add Device
	-							
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
9	Security Module 1	FTD	6.0.1.1213	10.62.148.67	10.62.148.1	Ethernet1/1	Online	Ended 🕒 A
	Ports: Data Interfaces: Cluster Interfac	Port-channel5 es: Port-channel4	8	Attributes: Cluster Operational St Firepower Managemen Cluster Role Management URL UUID	atus : in-cluster it IP : 10.62.148.67 ; primary : https://10.62.148.73/ : b2a42bba-5da0-11e6-a	1e-efdb62f3eab1		
	Security Module 2	FTD	6.0.1.1213	10.62.148.68	10.62.148.1	Ethernet1/1	Online	Ended 🕒 🥕
	Ports: Data Interfaces: Cluster Interfac	Port-channel5 es: Port-channel4	8	Attributes: Cluster Operational St Frepower Managemen Cluster Role Management URL UUID	atus : In-cluster it IP : 10.82.148.68 : secondary : https://10.82.148.73/ : b2c13764-5da0-11e6-8	795-e46a69566c19		
	Security Module 3	FTD	6.0.1.1213	10.62.148.69	10.62.148.1	Ethernet1/1	Online	(trainer 🖨 🥕
	Ports: Data Interfaces: Cluster Interfac	: Port-channel5 es: Port-channel4	8	Attributes: Cluster Operational 5t Firepower Managemen Cluster Role Management URL UUID	atus : in-cluster it IP : 10.62.148.69 : secondary : https://10.62.148.73/ : beb5ca08-5da0-11e6-b	846-450546116340		

•从FPR9300 CLI

FPR9K-1-A#									
FPR9K-1-A# scope ssa									
FPR9K-1-A /ssa # s	how app-inst	ance							
Application Name	Slot ID	Admin State	Operational State	Running Versio	n Startup				
Version Cluster Op	er State								
ftd	1	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									
ftd	2	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									
ftd	3	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									

•从LINA(ASA)CLI

firepower# show cluster info					
Cluster FTD_cluster	: On				
Interface mode:	spanned				
This is "unit-1-	-1" in state MASTER				
ID :	0				
Version :	9.6(1)				
Serial No.:	FLM19216KK6				
CCL IP :	127.2.1.1				
CCL MAC :	0015.c500.016f				
Last join :	21:51:03 CEST Aug 8 2016				
Last leave:	N/A				
Other members in the	e cluster:				
Unit "unit-1-3"	in state SLAVE				
ID :	1				
Version :	9.6(1)				
Serial No.:	FLM19206H7T				
CCL IP :	127.2.1.3				
CCL MAC :	0015.c500.018f				
Last join :	21:51:05 CEST Aug 8 2016				
Last leave:	N/A				
Unit "unit-1-2"	in state SLAVE				

TD : 2 Version : 9.6(1) Serial No.: FLM19206H71 CCL IP : 127.2.1.2 CCL MAC : 0015.c500.019f Last join : 21:51:30 CEST Aug 8 2016 Last leave: N/A firepower# cluster exec show cluster interface-mode cluster interface-mode spanned cluster interface-mode spanned cluster interface-mode spanned firepower# firepower# cluster exec show cluster history _____ From State To State Reason _____ 21:49:25 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:18 CEST Aug 8 2016 Enabled from CLI DISABLED ELECTION 21:51:03 CEST Aug 8 2016 ELECTION MASTER_POST_CONFIG Enabled from CLI 21:51:03 CEST Aug 8 2016 MASTER_POST_CONFIG Master post config done and waiting for ntfy MASTER _____ To State From State Reason _____ 21:49:44 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:37 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:37 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:41 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:41 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:46 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:46 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message

21:50:51 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:51 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:56 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:56 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:01 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:04 CEST Aug 8 2016 ONCALL SLAVE_COLD Received cluster control message 21:51:04 CEST Aug 8 2016 SLAVE_COLD SLAVE_APP_SYNC Client progression done 21:51:05 CEST Aug 8 2016 SLAVE_APP_SYNC SLAVE_CONFIG Slave application configuration sync done 21:51:17 CEST Aug 8 2016 SLAVE_CONFIG SLAVE_BULK_SYNC Configuration replication finished 21:51:29 CEST Aug 8 2016 SLAVE_BULK_SYNC SLAVE Configuration replication finished _____ _____ To State From State Reason _____ 21:49:24 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:16 CEST Aug 8 2016 DISABLED ELECTION Enabled from CLI 21:50:17 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:21 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:21 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:26 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:26 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:31 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message

21:50:31 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:36 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:36 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:41 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:41 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:46 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:46 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:51 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:51 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:56 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:56 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:01 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:51:01 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:06 CEST Aug 8 2016 Received cluster control message ONCALL ELECTION 21:51:06 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:12 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:12 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:17 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:17 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:51:22 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:22 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message

21:51:27 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:27 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:30 CEST Aug 8 2016 ONCALL SLAVE_COLD Received cluster control message 21:51:30 CEST Aug 8 2016 SLAVE_APP_SYNC SLAVE_COLD Client progression done 21:51:31 CEST Aug 8 2016 SLAVE_CONFIG Slave application configuration sync done SLAVE_APP_SYNC 21:51:43 CEST Aug 8 2016 SLAVE_CONFIG SLAVE_BULK_SYNC Configuration replication finished 21:51:55 CEST Aug 8 2016 SLAVE_BULK_SYNC SLAVE Configuration replication finished _____

firepower#

任务3.将FTD集群注册到FMC

任务要求:

将逻辑设备添加到FMC,然后将其分组到集群。

解决方案:

步骤1.将逻辑设备添加到FMC。与FMC版本6.3一样,您必须仅注册一个FTD设备(建议成为主设备)。 其余FTD由FMC自动发现。

登录FMC并导航至"设备">"设备管理"选项卡,然后单击"添加设备"。

使用映像中所述的设置添加第一个逻辑设备。

单击"Register(注册)"开始注册。

Add Device		?	×				
Host:	10.62.148.67						
Display Name:	FTD1						
Registration Key:	cisco						
Group:	None	~					
Access Control Policy:	FTD9300	~					
Smart Licensing Malware:							
Threat: URL Filtering:							
- • Advanced							
On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page.							
	Register Canc	el					

验证如图所示。

FTD_cluster Cisco Firepower 9000 Series SM-36 Threat Defense Cluster			/ 0
PTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	
FTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	6
FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	8

任务4.在FMC上配置端口通道子接口

任务要求:

为端口通道数据接口配置子接口。

解决方案:

步骤1.从FMC GUI中,选择"FTD_cluster编辑"按钮。

导航至接口选项卡,然后单击**添加接口>子接**口,如图所示。

Overview Analysis	Policies	Devices	Objects	AMP				Deploy 🍳	System Help 🛪 olga 🛪
Device Management	NAT	VPN PI	latform Setting	s					
FTD_cluster									Save Cancel
Cisco Firepower 9000 Serie	is SM-36 Thre	at Defense							
Cluster Devices	Routing	NAT	Interfaces	Inline Sets	DHCP				
2									Add Interfaces •
Interface			Logical Nam	e	Туре	Security Zone	Mac Address(Active/Standby)	IP Address	Sub Interface
Port-channel5					EtherChannel				1
Port-channel48					EtherChannel				4
Ethernet1/1			diagnostic		Physical				1

使用这些详细信息配置第一个子接口。选择OK以应用更改,如图所示。

名称	内部
General 选项卡	
接口	端口通道5
子接口ID	201
VLAN ID	201
IPv4选项卡	
IP类型	使用静态IP
IP Address	192.168.75.10/24

Add Sub Interface			? ×
Name: Inside	🗹 Enabled	Management Only	
Security Zone:	~	-	
Description:			
General IPv4 IPv6	Advanced		
MTU:	1500	(64 - 9000)	
Interface *:	Port-channel5	🗹 Enabled	
Sub-Interface ID *:	201	(1 - 4294967295)	
VLAN ID:	201	(1 - 4094)	
			OK Cancel

Add Sub Interface	?	×
Name: Inside	C Enabled Management Only	
Security Zone:	~	
Description:		
General IPv4 IPv6	Advanced	
IP Type:	Use Static IP	
IP Address:	eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25	
	OK Cancel)

使用这些详细信息配置第二个子接口。

外部
端口通道5
210
210
使用静态IP
192.168.76.10/24

单击OK以创建子接口。单击Save,然后Deploy changes to the FTD_cluster,如图所示。

验证:

Overview Analysis Policies Devices Objects AMP		Deploy 🍳 System Help 🔹 olga 🔹							
Device Management NAT VPN Platform Settings									
FTD_cluster									
Cisco Firepower 9000 Series SM-36 Threat Defense	Cisco Firepower 9000 Series SM-36 Threat Defense								
Cluster Devices Routing NAT Interfaces Inline Sets	DHCP								
2		Add Interfaces •							
Interface Logical Name	Type Security Zone Mac Address(Active/Standby)	IP Address							
Port-channel5	EtherChannel	1							
Port-channel48	EtherChannel	9							
Ethernet1/1 diagnostic	Physical	1							
Port-channel5.201 Inside	SubInterface	192.168.75.10/24(Static)							
Port-channel5.210 Outside	SubInterface	192.168.76.10/24(Static)							

任务5.检验基本连通性

任务要求:

创建捕获并检查两台虚拟机之间的连接。

解决方案:

步骤1.在所有集群设备上创建捕获。

导航至主设备的LINA(ASA)CLI,并为内部和外部接口创建捕获。

firepower# firepower# cluster exec capture capi interface inside match icmp any any firepower# firepower# cluster exec capture capo interface outside match icmp any any firepower# 验证: firepower# cluster exec show capture capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any capture capo type raw-data interface Outside [Capturing - 0 bytes] match icmp any any capture capi type raw-data interface Inside [Capturing - 0 bytes] match icmp any any

capture capo type raw-data interface Outside [Capturing - 0 bytes]
match icmp any any

步骤2.从VM1对VM2执行ping测试。

对4个数据包进行测试。在测试后检查捕获输出:

capture capo type raw-data interface Outside [Capturing - 752 bytes]
match icmp any any

match icmp any any

firepower#

运行命令以检查特定设备上的捕获输出:

firepower# cluster exec unit unit-1-3 show capture capi

8 packets captured

1:	12:58:36.162253	802.1Q	vlan#201	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo
reques	st								
2:	12:58:36.162955	802.1Q	vlan#201	ΡO	192.168.76.100	>	192.168.75.100:	icmp:	echo reply
3:	12:58:37.173834	802.1Q	vlan#201	ΡO	192.168.75.100	>	192.168.76.100:	icmp:	echo
reques	st								
4:	12:58:37.174368	802.1Q	vlan#201	ΡO	192.168.76.100	>	192.168.75.100:	icmp:	echo reply
5:	12:58:38.187642	802.1Q	vlan#201	ΡO	192.168.75.100	>	192.168.76.100:	icmp:	echo
reques	st								
6:	12:58:38.188115	802.1Q	vlan#201	ΡO	192.168.76.100	>	192.168.75.100:	icmp:	echo reply
7:	12:58:39.201832	802.1Q	vlan#201	PO	192.168.75.100	>	192.168.76.100:	icmp:	echo
reques	st								
8:	12:58:39.202321	802.1Q	vlan#201	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo reply
8 pacl	kets shown								

firepower# cluster exec unit unit-1-3 show capture capo

8 packets captured

1: 12:58:36.162543 802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo

request										
2: 12:58:3	6.162894	802.1Q	vlan#210	ΡO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
3: 12:58:3	7.174002	802.1Q	vlan#210	ΡO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
request										
4: 12:58:3	7.174307	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
5: 12:58:3	8.187764	802.1Q	vlan#210	ΡO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
request										
6: 12:58:3	8.188085	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
7: 12:58:3	9.201954	802.1Q	vlan#210	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
request										
8: 12:58:3	9.202290	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
8 packets show	wn									
firepower#										

完成此任务后,使用下一个命令删除捕获:

步骤3.从VM2下载文件到VM1。

VM1预配置为FTP服务器,VM2预配置为FTP客户端。

使用以下内容创建新捕获:

使用FTP客户端将文件从VM2下载到VM1。

检查show conn输出:

TCP Outside 192.168.76.100:49175 Inside 192.168.75.100:21, idle 0:00:32, bytes 665, flags UIOeN UDP cluster 255.255.255.255.255:49495 NP Identity Ifc 127.2.1.1:49495, idle 0:00:00, bytes 17858058, flags -TCP cluster 127.2.1.3:10844 NP Identity Ifc 127.2.1.1:38296, idle 0:00:33, bytes 5496, flags UI TCP cluster 127.2.1.3:59588 NP Identity Ifc 127.2.1.1:10850, idle 0:00:33, bytes 132, flags UO

 TCP Outside
 192.168.76.100:49175 Inside
 192.168.75.100:21, idle 0:00:34, bytes 0, flags y

 TCP cluster
 127.2.1.1:10851 NP Identity Ifc
 127.2.1.3:48493, idle 0:00:52, bytes 224, flags UI

 TCP cluster
 127.2.1.1:64070 NP Identity Ifc
 127.2.1.3:10847, idle 0:00:11, bytes 806, flags UO

TCP cluster 127.2.1.1:10851 NP Identity Ifc 127.2.1.2:64136, idle 0:00:53, bytes 224, flags UI TCP cluster 127.2.1.1:15859 NP Identity Ifc 127.2.1.2:10847, idle 0:00:11, bytes 807, flags UO **显示捕获**输出:

capture capi type raw-data interface Inside [Capturing - 0 bytes]
match ip host 192.168.75.100 host 192.168.76.100
capture capo type raw-data interface Outside [Capturing - 0 bytes]
match ip host 192.168.75.100 host 192.168.76.100

从机箱管理器UI捕获集群

在下图中,您可以看到FPR9300上具有2个端口通道(8和48)的3单元集群。 逻辑设备是ASA,但 在FTD的情况下将是相同的概念。需要记住的重要一点是,尽管有**3个集群单元**,但从捕获角度看 ,只有一个**逻辑设备**:

Ov	erview	Interfaces	Logical Devices	Security Mo	odules Plat	form Settings			Syst	tem Tools Help admin
Log	ical Devi	ice List							c	Refresh 3 Add Device
	ASA	с	lustered	Status:ok						
	Securit	y Module	Application	Version	Manageme	ent IP	Gateway	Management Port	Status	
	Security Ports Da Clu	r Module 1 s: ta Interfaces: ister Interfaces:	ASA Port-channel8 Port-channel48	9.6.2.7	0.0.0.0 Attributes: Cluster Oper Management Cluster Role Management Management	ational Status: in- : IP VIRTUAL : 10. : ma : URL : http : IP : 10.	0.0.0.0 cluster .111.8.206 ister ps://10.111.8.206/ .111.8.193	Ethernet1/1	nline	C 1 2
•	Security	Module 2	ASA	9.6.2.7	0.0.0.0		0.0.0.0	Ethernet1/1	💮 online	💌 🎉 🤌
	Port: Da Clu	s: ta Interfaces: ister Interfaces:	Port-channel8 Port-channel48		Attributes: Cluster Oper Management Cluster Role Management Management	ational Status : in- : IP VIRTUAL : 10. : sla : URL : httj : IP : 10.	cluster .111.8.206 ve ps://10.111.8.206/ .111.8.189			
	Security Port Da Clu	v Module 3 s: ta Interfaces: ister Interfaces:	ASA Port-channel8 Port-channel48	9.6.2.7	0.0.0.0 Attributes: Cluster Oper Management Cluster Role Management Management	ational Status : in- : IP VIRTUAL : 10. : sla : URL : http : IP : 10.	0.0.0.0 cluster .111.8.206 ve ps://10.111.8.206/ .111.8.190	Ethernet1/1		C 🕅

D	acket Canture
Save and Run Save Cancel	
ASA Session Name* ARP	
Ethernet1/1 Buffer Size 256 MB	*
Ethernet1/8 Snap length: 1518	Bytes
Ethernet1/7 Store Packets Overwrite	Append
Ethernet1/6 Capture Filter Apply Filter Ca	pture All
Ethernet1/5 ASA	
Ethernet1/9, Ethernet1/10, Ethernet1/11, Ethernet1/14, Eth	
Ethernet1/3 (Portchannel48)	
Ethernet1/2 (Portchannel48)	
Ethernet2/2 Portchannel8	
Ethernet2/1 Portchannel8	

任务6.从集群中删除从设备

任务要求:

登录FMC并从集群中删除从属设备。

解决方案:

步骤1.登录FMC并导航至Device > Device Management。

点击从设备旁边的垃圾桶图标,如图所示。

∠			<i>s</i> 6
FTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	
FTD2 10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	6
FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre Base, Threat, Malware, URL Filtering	FTD9300	6

系统将显示确认窗口。选择是以确认,如图所示。

Confirm	Delete	
availabi Do you	Device "FTD2" will b Cluster "FTD_cluster Management Center e in Firepower Secur want to continue?	e deleted from " in Firepower r but will be rity Appliance.
	Yes	No

•从FMC,如图所示。



•从FXOS CLI。

FPR9K-1-A# scope ssa FPR9K-1-A /ssa # show app-instance									
Application Name Version Cluster Ope	Slot ID er State	Admin State	Operational State	Running Versio	n Startup				
	·								
ftd	1	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									
ftd	2	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									
ftd	3	Enabled	Online	6.0.1.1213	6.0.1.1213				
In Cluster									

•从LINA(ASA)CLI。

firepower# show cluster info Cluster FTD_cluster: On Interface mode: spanned This is "unit-1-1" in state MASTER ID : 0 Version : 9.6(1) Serial No.: FLM19216KK6 CCL IP : 127.2.1.1 CCL MAC : 0015.c500.016f Last join : 21:51:03 CEST Aug 8 2016 Last leave: N/A Other members in the cluster: Unit "unit-1-3" in state SLAVE : 1 ID Version : 9.6(1)Serial No.: FLM19206H7T CCL IP : 127.2.1.3 CCL MAC : 0015.c500.018f Last join : 21:51:05 CEST Aug 8 2016 Last leave: N/A Unit "unit-1-2" in state SLAVE ID : 2 Version : 9.6(1) Serial No.: FLM19206H71 CCL IP : 127.2.1.2 CCL MAC : 0015.c500.019f Last join : 21:51:30 CEST Aug 8 2016 Last leave: N/A firepower#

注意:设备从FMC未注册,但仍是FPR9300上的集群成员。

使用本部分可确认配置能否正常运行。

验证已完成,并涵盖在各个任务中。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

• Cisco Firepower管理中心配置指南的所有版本均位于以下位置: https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepowerroadmap.html#id_47280。

• FXOS机箱管理器和CLI配置指南的所有版本均可在以下位置找到: <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfld-</u> <u>121950。</u>

• 思科全球技术支持中心(TAC)强烈推荐此可视化指南,以深入了解思科Firepower下一代安全技术的实用知识,包括本文中提到的知识:

http://www.ciscopress.com/title/9781587144806。

• 对于与Firepower技术相关的所有配置和故障排除技术说明。

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-serieshome.html。

• <u>技术支持和文档 - Cisco Systems</u>