FP9300(シャーシ内)でのFTDクラスタリング の設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 設定 ネット<u>ワーク図</u> 作業1:FTDクラスタに必要なインターフェイスの作成 作業2:FTDクラスタの作成 作業3:FTDクラスタのFMCへの登録 作業4:FMCでのポートチャネルサブインターフェイスの設定 作業5.基本接続の確認 Chassis Manager UIからのクラスタキャプチャ 作業6:クラスタからのスレーブデバイスの削除 確認 トラブルシュート 関連情報

概要

このドキュメントでは、FPR9300デバイスでクラスタ機能を設定および確認する方法について説 明します。

注意:このドキュメントの情報は、クラスタの初期インストール/設定について説明してい ます。このドキュメントは、ユニット交換(Return Material Authorization - RMA)手順には適 用されません

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

• 1.1(4.95)が稼働するCisco Firepower 9300セキュリティアプライアンス

• 6.0.1 (ビルド1213)を実行するFirepower Threat Defense(FTD)

• 6.0.1.1(ビルド 1023)を実行している FireSIGHT Management Center 構成(FMC) ラボの完了時間:1時間.

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

- FTDアプライアンスを搭載したFPR9300では、サポートされているすべてのバージョンでシャーシ内クラスタリングを設定できます。
- ・シャーシ間クラスタリングは6.2で導入されました。
- ポートチャネル48は、クラスタ制御リンクとして作成されます。シャーシ内クラスタリングの場合、このリンクはクラスタ通信にFirepower 9300バックプレーンを使用します。
- •管理インターフェイスを除き、個々のデータインターフェイスはサポートされません。
- 管理インターフェイスは、クラスタ内のすべてのユニットに割り当てられます。

設定

ネットワーク図



作業1:FTDクラスタに必要なインターフェイスの作成

タスク要件:

クラスタ、管理インターフェイス、およびポートチャネルデータインターフェイスを作成します。

ソリューション:

ステップ1:ポートチャネルデータインターフェイスを作成します。

新しいインターフェイスを作成するには、FPR9300 Chassis Managerにログインし、 [Interfaces]タブに移動する必要**があ**ります。

[ポートチャネ**ルの追加]を選択**し、次のパラメータを使用して新しいポートチャネルインターフェ イスを作成します。

Port Channel ID	5
Туре	Data
Enable	Yes
Member ID	Ethernet1/3、Ethernet 1/4

[OK]を選択し、図に示すように設定を保存します。

Add Port Channel				? ×		
Port Channel ID: 5	🗹 Enable					
Type: Data	~					
Speed: 1gbps	*					
Interfaces						
Available Interfa	ice	Member ID				
🔍 Search		Ethernet1/3	6			
Ethernet1/2	2	Ethernet1/4	8			
Ethernet1/3	3		_	1		
Ethernet1/4	\$					
Ethernet1/5	5					
Ethernet1/6	;					
Ethernet1/7	Add Interface					
Ethernet1/8	3					
Ethernet2/1	L I					
Ethernet2/2	2					
Ethernet2/3	3					
Ethernet2/4						
Ethernet3/1						
Ethernet3/2	2					
		L	ОК	Cancel		

ステップ2:管理インターフェイスを作成します。

[Interfaces]タブ**でイ**ンターフェイスを選択し、[Edit]をクリックして[Management Type]インター

フェイスを設定します。

[OK]をクリックし、図に示すように設定を保存します。

Edit Inte	rface - Ethernet1/1	? X	
Name:	Ethernet1/1 Cable		
Type:	mgmt	*	
Speed:	1gbps	*	
	OK Can	wel .	

ステップ3:クラスタ制御リンクインターフェイスを作成します。

図に示すように、[Add Port Channel]ボタンをクリックし、これらのパラメータを使用して新しい ポートチャネルインターフェイスを作成します。

Port Channel ID	48
Туре	クラスタ
Enable	Yes
Member ID	-

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

作業2:FTDクラスタの作成

タスク要件:

FTDクラスタユニットを作成します。

ソリューション:

ステップ1:[Logical Devices]に移動し、[Add Device]ボタンをクリックします。

次のようにFTDクラスタリングを作成します。

Device Name	FTD_cluster
Tomplete	Cisco Firepower Threat
rempiate	Defense
Image Version	6.0.1.1213
デバイスモード	クラスタ

デバイスを追加するには、図に示すように[OK]をクリックします。

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

ステップ2:FTDクラスタを設定および導入します。

FTDデバイスを作成すると、[Provisioning- device_name]ウィンドウにリダイレクトされます。

図に示すように、デバイスアイコンをクリックして設定を開始します。

•	verview Interfac	es Logical Devic	Security N	odules Platform Settings			System Tools	Help admin
-	vovisioning - FTD_ ustered Cisco Fire	cluster epower Threat Defe	nse 6.0.1.1213]			Seve	Cancel
0	ata Ports	-						
ľ	Ethernet1/2							
R	Ethernet1/S							
	Ethernet1/6							
	Ethernet1/7							
	Ethernet1/8							
	Ethernet2/1							
	Ethernet2/2					FTD - 6.0.1.1213		
Ы	Ethernet2/3					Security Module 1,2,3		
Ы	Ethernet2/4							
	Ethernet3/1							
	Ethernet3/2							
	Ethernet3/3							
	Ethernet3/4							
Ľ	Port-Unerriels							
	Security Module	Application	Version	Management IP	Gateway	Management Port Status		
9	Security Module 1	FTD	6.0.1.1213					
a	Security Module 2	FTD	6.0.1.1213					
	Security Module 3	FTD	6.0.1.1213					

図に示すように、FTDクラスタ情報タブを次の設定で構成します。

クラスタキー クラスタグループ名 Management Interface

cisco FTD_cluster Ethernet1/1

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

図に示すように、FTDの**[Settings]**タブを設定します。

登録キー	cisco
Password	Admin123
Firepower Management	10 62 148 73
Center の IP	10.02.140.70
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	なし

Cisco Firepower Three Cluster Information Settings	at Defense - Configuration 2 ×
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
	OK Cancel

図に示すように、これらの設**定を使用**して[FTDインターフェイス情報]タブを設定します。

Address Type	IPv4のみ
セキュリティモジュール1	
Management IP	10.62.148.67
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1
セキュリティモジュール2	
Management IP	10.62.148.68
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1
セキュリティモジュール3	
Management IP	10.62.148.69
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1

Cisco Firepower Thre	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					

[Agreement]タブの[Agreement]に同意し、図に示すように[**OK**]をクリックします。

Cisco Firepower Threat Defense - Configuration								
Cluster Information Settings Interface Information								
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 ACCEPTANCE OF THIS AGREEMENT.								
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								

ステップ3:FTDへのデータインターフェイスの割り当て

[Data Ports] 領域を展開し、FTD に割り当てる各インターフェイスをクリックします。完了した ら、[**Save**]を選択して、図に示すようにFTDクラスタを作成します。

0	verview Interface:	Logical Device	Security Modules Pla	tform Settings				System Tools	Help admin
P	rovisioning - FTD_clu lustered Cisco Firep	aster power Threat Defens	e 6.0.1.1213					Save	Cancel
D	ata Ports								
ļ	Ethernet1/7								
l l	Ethernet1/8								
	Ethernet2/1	- 1							
1	Ethernet2/2	_							
U.	[thernet2/3	_		Port- channel5		_			
15	Ethernet2/4	_							
	[thernet3/1	- 1				FTD - 6	.0.1.1213		
	Ethernet3/2	- 1		Burt.		Security	Module 1,2,3		
	Ethernet3/3			channel48					
	Rut-rhanneld8								
	Port-channel5								
2									_
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status		
1	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							

クラスタが展開されるまで数分間待機し、その後にマスターユニットの選択が行われます。

• 図に示すように、FPR9300 GUIから。

٥v	erview Interface	s Logical Devic	ces Security Modul	es Platform Settings				System Tools Help admin
	FTD_cluster	Clustered	Status: ok					C Refresh Add Device
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
3	Security Module 1	FTD	6.0.1.1213	10.62.148.67	10.62.148.1	Ethernet1/1	Online	Ensteil 🖨 A
	Ports: Data Interfaces: Cluster Interface	Port-channel5 es: Port-channel48	3	Attributes: Cluster Operational St Firepower Managemer Cluster Role Management URL UUID	atus : in-cluster it IP : 10.62.148.67 ; primary : https://10.62.148.73/ ; b2a42bba-5da0-11e6-	f1e-efdb62t3eeb1		
	Security Module 2	FTD	6.0.1.1213	10.62.148.68	10.62.148.1	Ethernet1/1	Online	Ender 🖨 A
	Ports: Data Interfaces: Cluster Interface	Port-channel5 es: Port-channel48	3	Attributes: Cluster Operational St Firepower Managemer Cluster Role Management URL UUID	atus : In-cluster It IP : 10.62.148.68 : secondary : https://10.62.148.73/ : b2c13764-5da0-11e6-	1795-e46a89566c19		
۲	Security Module 3	FTD	6.0.1.1213	10.62.148.69	10.62.148.1	Ethernet1/1	Online	(tradinal 🕒 🥠
	Ports: Data Interfaces: Cluster Interface	Port-channel5 es: Port-channel48	1	Attributes: Cluster Operational St Firepower Managemer Cluster Role Management URL UUID	atus : In-Cluster It IP : 10.62.148.69 : secondary : https://10.62.148.73/ : beb5ca08-5da0-11e6-	846-450516116340		

・FPR9300 CLIから

FPR9K-1-A#					
FPR9K-1-A# scope	ssa				
FPR9K-1-A /ssa #	show app-inst	ance			
Application Name	Slot ID	Admin State	Operational State	Running Version	n Startup
Version Cluster O	per 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					

・LINA(ASA)CLIから

firepower# show clus	ster 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 Received cluster control message ELECTION 21:51:27 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:51:30 CEST Aug 8 2016 Received cluster control message ONCALL SLAVE_COLD 21:51:30 CEST Aug 8 2016 SLAVE_COLD SLAVE_APP_SYNC Client progression done 21:51:31 CEST Aug 8 2016 Slave application configuration sync done SLAVE_APP_SYNC SLAVE_CONFIG 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#

作業3:FTDクラスタのFMCへの登録

タスク要件:

論理デバイスをFMCに追加し、クラスタにグループ化します。

ソリューション:

ステップ1:論理デバイスをFMCに追加します。FMCバージョン6.3と同様に、1つのFTDデバイ スだけを登録する必要があります(マスターとして推奨)。 残りのFTDはFMCによって自動検出 されます。

FMCにログインし、[Devices] > [**Device Management**]タブに**移動し、[Add Device**]をクリックし ます。

図に示されている設定で、最初の論理デバイスを追加します。

登録を開始するには登録をクリックしてください。

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:						
URL Filtering: Advanced On version 5.4 devices or earlier, the licensing options will need to be specified from licensing page. Register Cancel						

図に確認を示します。

Cisco Firepower 9000 Series SM-36 Threat Defense Cluster			/ 5
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	
PTD2 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	8
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

作業4:FMCでのポートチャネルサブインターフェイスの設定

タスク要件:

ポートチャネルデータインターフェイスのサブインターフェイスを設定します。

ソリューション:

ステップ1:FMCのGUIで、[**FTD**_cluster **Edit]ボタンを選択し**ます。

[Interfaces]タブに移動し、図に示すように[Add Interfaces] > [Sub Interface]をクリックします。

Overview Analysis Policies Dev	ices Objects AMP				Deploy 🧕	System Help v olga v
Device Management NAT VPN	Platform Settings					
FTD_cluster						Save Cancel
Cisco Firepower 9000 Series SM-36 Threat Def	ense					
Cluster Devices Routing N	T Interfaces Inline Sets	DHCP				
2						Add Interfaces •
Interface	Logical Name	Type S	Security Zone	Mac Address(Active/Standby)	IP Address	Sub Interface
17 Port-channel5		EtherChannel				/
Port-channel48		EtherChannel				۹.
Ethernet1/1	diagnostic	Physical				1

次の詳細を使用して、最初のサブインターフェイスを設定します。[**OK**]を**選択**して、変更を適用 します(図を参照)。

[名前(Name)]	INSIDE
[General] タブ	
インターフェイス	ポートチャネル5
サブインターフェイスID	201
VLAN ID	201
[IPv4]タブ	
- IPタイプ	スタティックIPの使用
iSCSIポータルの	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	? ×	2
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	

次の詳細を使用して、2番目のサブインターフェイスを設定します。

OUTSIDE
ポートチャネル5
210
210
スタティックIPの使用
192.168.76.10/24

[**OK**]をク**リック**して、サブインターフェイスを作成します。[**Save**]をクリックし**て、**図に示すように[Deploy changes to the FTD_cluster]をクリックします。

検証:

Overview Analysis Policies Devices Objects AMP		Deploy 0, System Help + olga +				
Device Management NAT VPN Platform Settings						
FTD_cluster						
Lisco nirepower 5000 denes den-30 mirest belense						
Cluster Devices Routing NAT Interfaces Inline Set	B DHCP					
2		Add Interfaces •				
Interface Logical Name	Type Security Zone Mac Address(Active/Standby)	IP Address				
Port-channel5	EtherChannel	1				
Port-channel48	EtherChannel	٩,				
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)				

作業5.基本接続の確認

タスク要件:

キャプチャを作成し、2つのVM間の接続を確認します。

ソリューション:

ステップ1:すべてのクラスタユニットでキャプチャを作成します。

マスターユニットのLINA(ASA)CLIに移動し、内部インターフェイスと外部インターフェイスのキャプチャを作成します。

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# 検証: 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

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

4パケットでテストを実行します。テスト後のキャプチャ出力を確認します。

特定のユニットのキャプチャ出力を確認するには、次のコマンドを実行します。

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

8 packets captured

1: 12:58:36.162253 802.1Q vlan#201 P0 192.168.75.100 > 192.168.76.100: icmp: echo request 2: 12:58:36.162955 802.10 vlan#201 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 802.10 vlan#201 P0 192.168.75.100 > 192.168.76.100: icmp: echo 3: 12:58:37.173834 request 802.1Q vlan#201 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 4: 12:58:37.174368 5: 12:58:38.187642 802.1Q vlan#201 P0 192.168.75.100 > 192.168.76.100: icmp: echo request 802.1Q vlan#201 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 6: 12:58:38.188115 7: 12:58:39.201832 802.1Q vlan#201 P0 192.168.75.100 > 192.168.76.100: icmp: echo request 8: 12:58:39.202321 802.1Q vlan#201 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 8 packets 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: 12:58:36.162894 802.1Q vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo 3: 12:58:37.174002 request 4: 12:58:37.174307 802.10 vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 5: 12:58:38.187764 802.10 vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo request 802.1Q vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 6: 12:58:38,188085 7: 12:58:39.201954 802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo request 8: 12:58:39.202290 802.1Q vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply 8 packets shown firepower# この作業が完了したら、次のコマンドでキャプチャを削除します。

firepower# cluster exec no capture capi firepower# cluster exec no capture capo ステップ3:VM2からVM1にファイルをダウンロードします。 VM1はFTPサーバとして事前設定され、VM2はFTPクライアントとして事前設定されました。 次の内容で新しいキャプチャを作成します。 firepower# cluster exec capture capi interface inside match ip host 192.168.75.100 host 192.168.76.100 firepower# cluster exec capture capo interface outside match ip host 192.168.775.100 host 192.168.76.100 FTPクライアントを使用して、VM2からVM1にファイルをダウンロードします。

show connの出力をチェックします。

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 Show captureの出力:

Chassis Manager UIからのクラスタキャプチャ

次の図では、2つのポートチャネル(8および48)を備えたFPR9300上の3ユニットクラスタを確認できます。 論理デバイスはASAですが、FTDの場合は同じ概念になります。重要な点は、クラスタユニットは**3つあり**ますが、キャプチャの観点から見ると、論理デバイスは1つしかありません。

Ov	erview Interfaces	Logical Devices	Security Mo	dules Platform Sett	ings		Sys	tem Tools Help admin
Log	cal Device List						d	Refresh OAdd Device
	ASA	Clustered	Status:ok					F. 2 E •
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
•	Security Module 1	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	nline	🕶 💱
	Ports: Data Interfaces: Cluster Interfaces:	Port-channel8 Port-channel48	,	Attributes: Cluster Operational Statu Management IP VIRTUAL Cluster Role Management URL Management IP	s: in-cluster : 10.111.8.206 : master : https://10.111.8.206/ : 10.111.8.193			
•	Security Module 2	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	🕥 online	💌 🎉 🌧
	Ports: Data Interfaces: Cluster Interfaces:	Port-channel8 Port-channel48	,	Attributes: Cluster Operational Statu Management IP VIRTUAL Cluster Role Management URL Management IP	s: in-cluster : 10.111.8.206 : slave : https://10.111.8.206/ : 10.111.8.189			
•	Security Module 3	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	💮 online	🕶 🎉
	Ports: Data Interfaces: Cluster Interfaces:	Port-channel8 Port-channel48	,	Attributes: Cluster Operational Statu Management IP VIRTUAL Cluster Role Management URL Management IP	s: in-cluster : 10.111.8.206 : slave : https://10.111.8.206/ : 10.111.8.190			

Overview Interfaces	Logical Devices	Security Modules	Platform Settings		System	Tools Help admin
						Packet Capture
			Save and Run	Save	Cancel	
ASA Ethernet1/1 Ethernet1/8 (Portchannel48) Ethernet1/6 (Portchannel48) Ethernet1/6 (Portchannel48) Ethernet1/5 Ethernet1/5 Ethernet1/4 (Portchannel48) Ethernet1/2 (Portchannel48) Ethernet1/2 (Portchannel48) Ethernet2/2 (Portchannel8) Ethernet2/1 (Portchannel8)		Ethernet1/9, Ethernet1/12, Eth	ASA ernet1/10, Ethernet1/11, hernet1/13, Ethernet1/14	Save Session Name* Selected Interfa Buffer Size Snap length: Store Packets Capture Filter	Cancel	■ Bytes Append r Capture All

作業6:クラスタからのスレーブデバイスの削除

タスク要件:

FMCにログインし、クラスタからスレーブユニットを削除します。

ソリューション:

ステップ1:FMCにログインし、[Device] > [Device Management]に移動します。

図に示すように、スレーブユニットの横にあるごみ箱アイコンをクリックします。

∠			J 🗊
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	- B
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

確認ウィンドウが表示されます。図に示すように、[Yes]を選択して確認します。

Confirm	Delete	
available Do you	Device "FTD2" will I Cluster "FTD_cluste Management Cente e in Firepower Secu want to continue?	be deleted from r" in Firepower r but will be rity Appliance.
	Yes	No

• 図に示すように、FMCから実行します。



・FXOS CLIから。

FPR9K-1-A# scope ssa FPR9K-1-A /ssa # show app-instance							
Application Name	Slot ID	Admin State	Operational State	Running Version	Startup		
Version Cluster Oper	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							

・LINA(ASA)CLIから。

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:デバイスはFMCから登録解除されましたが、FPR9300のクラスタメンバーのままです

ここでは、設定が正常に機能しているかどうかを確認します。

検証が完了し、個々のタスクでカバーされます。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

Cisco Firepower Management Centerコンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

<u>https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280</u> にアクセスしてください。

• FXOS Chassis ManagerおよびCLIコンフィギュレーションガイドのすべてのバージョンは、 次の場所にあります。

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfld-121950

 Cisco Global Technical Assistance Center(TAC)では、このビジュアルガイドを使用して、 Cisco Firepower次世代セキュリティテクノロジーに関する詳細な実務知識を得ることを強く 推奨しています。このガイドには、次の内容が含まれます。

<u>http://www.ciscopress.com/title/9781587144806</u> にアクセスしてください。

• Firepowerテクノロジーに関連するすべての設定およびトラブルシューティングのテクニカル ノート。

<u>https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html</u> にアクセスしてください。

• <u>テクニカル サポートとドキュメント – Cisco Systems</u>