Konfigurieren von FTD-Clustering auf dem FP9300 (Intra-Chassis)

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm Aufgabe 1: Erstellung der erforderlichen Schnittstellen für FTD-Cluster Aufgabe 2: FTD-Cluster erstellen Aufgabe 3: FTD-Cluster auf FMC registrieren Aufgabe 4: Konfigurieren von Port-Channel-Subschnittstellen auf FMC Aufgabe 5: Grundlegende Konnektivität überprüfen Cluster-Erfassung über Chassis Manager-Benutzeroberfläche Aufgabe 6: Löschen eines Slave-Geräts aus dem Cluster Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument wird beschrieben, wie die Clusterfunktion auf dem FPR9300-Gerät konfiguriert und verifiziert wird.

Vorsicht: Die in diesem Dokument enthaltenen Informationen beziehen sich auf die Erstinstallation/Konfiguration des Clusters. Dieses Dokument gilt nicht für ein Austauschverfahren (Retourengenehmigung - RMA).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Firepower 9300 Security Appliance mit 1.1(4.95)
- Firepower Threat Defense (FTD) mit 6.0.1 (Build 1213)
- FireSIGHT Management Center (FMC) mit 6.0.1.1 (Build 1023)

Laborabschlusszeit: 1 Stunde.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

- Auf dem FPR9300 mit FTD-Appliance können Sie Chassis-interne Clustering-Funktionen für alle unterstützten Versionen konfigurieren.
- Chassisübergreifendes Clustering wurde in 6.2 eingeführt.
- Port-Channel 48 wird als Cluster-Steuerungsverbindung erstellt. Bei Chassis-internen Clustering verwendet diese Verbindung die FirePOWER 9300-Backplane für die Cluster-Kommunikation.
- Einzelne Datenschnittstellen werden mit Ausnahme einer Verwaltungsschnittstelle nicht unterstützt.
- Die Management-Schnittstelle wird allen Einheiten im Cluster zugewiesen.

Konfigurieren

Netzwerkdiagramm



Aufgabe 1: Erstellung der erforderlichen Schnittstellen für FTD-Cluster

Aufgabenanforderung:

Erstellen Sie einen Cluster, eine Management-Schnittstelle und eine Port-Channel-Datenschnittstelle. Lösung:

Schritt 1: Erstellen einer Port-Channel-Datenschnittstelle.

Um eine neue Schnittstelle zu erstellen, müssen Sie sich beim FPR9300 Chassis Manager anmelden und zur Registerkarte **Schnittstellen** navigieren.

Wählen Sie **Port-Channel hinzufügen aus**, und erstellen Sie eine neue Port-Channel-Schnittstelle mit den folgenden Parametern:

Port-Channel-ID	5
Тур	Daten
Aktivieren	Ja
Mitglied-ID	Ethernet1/3, Ethernet 1/4

Wählen Sie **OK**, um die Konfiguration wie im Bild gezeigt zu speichern.

Add Port Cha	nnel			? ×
Port Channel ID:	5	🗹 Enable		
Туре:	Data]		
Speed:	1gbps 🗸			
Interfaces		_		
Ava	ilable Interface		Member ID	
	Search]	Ethernet1/3	
	Ethernet1/2		🔲 Ethernet1/4 🛛 🗍	
	Ethernet1/3			
	Ethernet1/4			
	Ethernet1/5			
	Ethernet1/6	Add Interface		
	Ethernet1/7	Add Interface		
	Ethernet1/8			
	Ethernet2/1			
	Ethernet2/2			
	Ethernet2/3			
	Ethernet2/4			
	Ethernet3/1			
	Ethernet3/2			
			ок	Cancel

Schritt 2: Erstellen einer Verwaltungsschnittstelle

Wählen Sie auf der Registerkarte **Schnittstellen** die Schnittstelle aus, klicken Sie auf **Bearbeiten**, und konfigurieren Sie die Schnittstelle Verwaltungstyp.

Klicken Sie auf OK, um die Konfiguration wie im Bild gezeigt zu speichern.

Edit Inte	rface - Ethernet1/1	? X
Name:	Ethernet1/1 ZEnabl	e
Туре:	mgmt	*
Speed:	1gbps	*
	ОК	Cancel

Schritt 3: Erstellen Sie eine Cluster-Control-Verbindungsschnittstelle.

Klicken Sie auf die Schaltfläche **Port-Channel hinzufügen**, und erstellen Sie eine neue Port-Channel-Schnittstelle mit diesen Parametern, wie im Bild gezeigt.

Port-Channel-ID	48
Тур	Cluster
Aktivieren	Ja
Mitglied-ID	-

Add Port Cha	annel			?×
Port Channel ID:	48	Enable		
Type:	Cluster	•		
Speed:	1gbps 💌	•	· •	
Interfaces		_		_
Ava	ailable Interface		Member ID	
	Search]		1
	Ethernet1/2			
	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

Aufgabe 2: FTD-Cluster erstellen

Aufgabenanforderung:

Erstellen Sie eine FTD-Cluster-Einheit.

Lösung:

Schritt 1: Navigieren Sie zu Logical Devices (Logische Geräte), und klicken Sie auf die Schaltfläche Gerät hinzufügen.

Erstellen Sie das FTD-Clustering wie folgt:

FTD-Cluster
Cisco FirePOWER Threat
Defense
6,0 1,1213
Cluster

Um das Gerät hinzuzufügen, klicken Sie auf OK, wie im Bild gezeigt.

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

Schritt 2: Konfigurieren und Bereitstellen des FTD-Clusters

Nachdem Sie ein FTD-Gerät erstellt haben, werden Sie zum Fenster Provisioning- device_name umgeleitet.

Klicken Sie auf das Gerätesymbol, um die Konfiguration wie im Bild gezeigt zu starten.

Overview Interfaces Logical Devices Security N	odules Platform Settings			System Tools Help admin
Provisioning - FTD_cluster Clustered Cisco Firepower Threat Defense 6.0.1.1213]			Save Canosi
Data Ports				
Ethernet1/2				
Ethernet1/5				
Ethernet1/6				
Ethernet1/7				
Ethernet1/8				
Ethernet2/1				
Ethernet2/2			FTD - 6.0.1.1213	
Ethernet2/3			Security Module 1,2,3	
Ethernet2/4				
Ethernet3/1				
Ethernet3/2				
Ethernet3/3				
Ethernet3/4				
Pert-channels				
Security Module Application Version	Management IP	Gateway	Management Port Status	
Security Module 1 PTD 6.0.1.1213				
Geouvity Module 2 PTD 6.0.1.1213				
al Security Module 3 PTD 6.0.1.1213				

Konfigurieren Sie die Registerkarte "FTD-**Cluster-Informationen**" mit diesen Einstellungen und wie im Bild gezeigt.

Cluster-SchlüsselCisCluster-GruppennameFTVerwaltungsschnittstelleEth

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	Iodule-2,Security Module-3			
Interface Information				
Cluster Key:				
Cluster Group Name:	FTD_cluster			
Management Interface:	Ethernet1/1			
	OK Cancel			

Konfigurieren Sie die Registerkarte FTD-Einstellungen mit diesen Einstellungen, wie im Bild gezeigt.

Registrierungsschlüssel	Cisco
Kennwort	Administrator123
FirePOWER Management	10 62 148 73
Center IP	10.02.140.70
Domänen durchsuchen	Cisco.com
Firewall-Modus	Geroutet
DNS-Server	173.38.200.100
Vollqualifizierter Hostname	ksec-fpr9k-1-1-3.cisco.com
Ereignisschnittstelle	Keine

Cisco Firepower Three Cluster Information Settings	at Defense - Configu Interface Information A	greement
Registration Key:		
Firepower Management	10.62.148.73	
Center IP: Search domains:	cisco.com	
Firewall Mode: DNS Servers:	Routed 173.38.200.100	
Fully Qualified Hostname:	ksec-fpr9k-1-1-3.cisco.com	n
Eventing Interface:	None	
	OK	Cancel

Konfigurieren Sie die Registerkarte "Informationen zur FTD-Schnittstelle" mit diesen Einstellungen und wie im Bild gezeigt.

Adresstyp	Nur IPv4
Sicherheitsmodul 1	
Management-IP	10.62.148.67
Netzwerkmaske	255 255 255 128
Gateway	10.62.148.1
Sicherheitsmodul 2	
Management-IP	10.62.148.68
Netzwerkmaske	255 255 255 128
Gateway	10.62.148.1
Sicherheitsmodul 3	
Management-IP	10.62.148.69
Netzwerkmaske	255 255 255 128
Gateway	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		

Akzeptieren Sie die Vereinbarung auf der Registerkarte "Vereinbarung", und klicken Sie wie im Bild gezeigt auf OK.

Cisco Firepower Threat Defense - Configuration (2) Cluster Information Settings Interface Information Agreement					
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					

Schritt 3: Zuweisen von Datenschnittstellen zu FTD

Erweitern Sie den Bereich Datenports, und klicken Sie auf die einzelnen Schnittstellen, die Sie FTD zuweisen möchten. Wählen Sie nach Abschluss die Option **Speichern**, um einen FTD-Cluster zu erstellen, wie im Bild gezeigt.

0	verview Interfaces	Logical Device	Security Modules Pla	tform Settings				System Tools	Help admin
P	rovisioning - FTD_clu lustered Cisco Firej	uster power Threat Defen	se 6.0.1.1213					Save	Cancel
D	ata Ports								1
	Ethernet1/7								
L.	Ethernet1/8								
IJ	Ethernet2/1	_							
ų	Ethernet2/2								
ų	Ethernet2/3	_1		Port- channel5		_			
ų	Ethernet2/4								
	Ethernet3/1	-1				FTD - 6.0.1	.1213		
	Ethernet3/2			Ports		Security Modu	ie 1,2,3		
	Ethernet 3/4			channel48					
	Port-channel48								
	Port-channel5								1
1					-				
	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							
	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							

Warten Sie einige Minuten, bis der Cluster bereitgestellt wird, nach dem die Haupteinheit gewählt wird.

Überprüfung:

• Aus der grafischen Benutzeroberfläche FPR9300 wie im Bild gezeigt.

0	erview Interface	s Logical Dev	ices Security Modu	les Platform Settings				System Tools Help admin
								C Refresh Q Add Device
۲	FTD_cluster	Clustered	Status: ok					F. 🥒 B 💌
	Security Module	Application	Version	Management IP	Gateway	Management Port	Status	
	Security Module 1	FTD	6.0.1.1213	10.62.148.67	10.62.148.1	Ethernet1/1	online	(trained 🕲 🍌
	Ports: Data Interfaces Cluster Interfac	Port-channel	5	Attributes: Cluster Operational St Firepower Managemen Cluster Role Management URL UUID	atus : in-cluster t IP : 10.62.148.67 ; primary : https://10.62.148.73/ : b2a42bba-5da0-11e6-a	f1e-efdb62f3eeb1		
	Security Module 2	FTD	6.0.1.1213	10.62.148.68	10.62.148.1	Ethernet1/1	online	(trained 🔘 🥠
	Ports: Data Interfaces Cluster Interfac	Port-channel es: Port-channel	5	Attributes: Cluster Operational Sti Frepower Managemen Cluster Role Management URL UUID	atus : in-cluster t IP : 10.62.148.68 : secondary : https://10.62.148.73/ : b2c13764-5da0-11e6-8	795- 048a09566 c19		
	Security Module 3	FTD	6.0.1.1213	10.62.148.69	10.62.148.1	Ethernet1/1	online	(tested 🕲 🍌
	Ports: Data Interfaces Cluster Interfac	: Port-channel es: Port-channel	5 18	Attributes: Cluster Operational St. Firepower Managemen Cluster Role Management URL UUED	atus : in-cluster t IP : 10.82.148.69 : eecondary : https://10.82.148.73/ : beb5ca68-5da0-11e6-b	846-450516114340		

• Von der CLI FPR9300

CCL IP : 127.2.1.3 CCL MAC : 0015.c500.018f

FPR9K-1-A#						
FPR9K-1-A# scope ssa						
FPR9K-1-A /ssa # sh o	ow app-insta	nce				
Application Name	Slot ID	Admin State	Operational State	Running Version	Startup	
Version Cluster Open	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						
• Über die LINA (ASA)-CLI					
	- / -					
firepower# show clus	ter info					
Cluster FTD cluster:	0n					
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.c500.0	16f				
Last join :	Last join : 21:51:03 CEST Aug 8 2016					
Last leave:	Last leave: N/A					
Other members in the cluster:						
Unit "unit-1-3"	in state SL	AVE				
ID :	1					
Version :	9.6(1)					
Serial No.:	FLM19206H7T					

Last join : 21:51:05 CEST Aug 8 2016 Last leave: N/A Unit "unit-1-2" in state SLAVE : 2 ID 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 DISABLED Enabled from CLI 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 Master post config done and waiting for ntfy _____ _____ From State To State Reason _____ 21:49:44 CEST Aug 8 2016 DISABLED DISABLED Disabled at startup 21:50:37 CEST Aug 8 2016 Enabled from CLI DISABLED ELECTION 21:50:37 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 ONCALL Received cluster control message 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 ONCALL ELECTION 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 ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 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 Enabled from CLI ELECTION 21:50:17 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 21:50:21 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:21 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:50:26 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 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 Received cluster control message ONCALL 21:50:36 CEST Aug 8 2016 ONCALL Received cluster control message ELECTION 21:50:36 CEST Aug 8 2016 ELECTION ONCALL Received cluster control message 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 Received cluster control message ELECTION 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 ONCALL Received cluster control message 21:50:56 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:50:56 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:51:01 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:01 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 21:51:06 CEST Aug 8 2016 ONCALL ELECTION Received cluster control message 21:51:06 CEST Aug 8 2016 ELECTION Received cluster control message ONCALL 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 Received cluster control message ELECTION 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
               SLAVE_COLD Received cluster control message
ONCALL
21:51:30 CEST Aug 8 2016
               SLAVE_APP_SYNC Client progression done
SLAVE_COLD
21:51:31 CEST Aug 8 2016
SLAVE_APP_SYNC SLAVE_CONFIG Slave application configuration sync done
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#

Aufgabe 3: FTD-Cluster auf FMC registrieren

Aufgabenanforderung:

Fügen Sie die logischen Geräte dem FMC hinzu, und gruppieren Sie sie dann in einem Cluster.

Lösung:

Schritt 1: Fügen Sie dem FMC logische Geräte hinzu. Ab FMC Version 6.3 müssen Sie nur ein FTD-Gerät registrieren (empfohlen, der Master zu sein). Die übrigen FTDs werden vom FMC automatisch erkannt.

Melden Sie sich beim FMC an, navigieren Sie zur Registerkarte **Devices >Device Management** (Gerätemanagement), und klicken Sie auf Add Device (Gerät hinzufügen).

Fügen Sie das erste logische Gerät mit den Einstellungen hinzu, wie im Bild erwähnt.

Klicken Sie auf Registrieren, um die Registrierung zu starten.

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 Cano	:el		

Die überprüfung erfolgt wie im Bild gezeigt.

Cisco Firepower 9000 Series SM-36 Threat Defense Cluster			28
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	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

Aufgabe 4: Konfigurieren von Port-Channel-Subschnittstellen auf FMC

Aufgabenanforderung:

Konfigurieren Sie Subschnittstellen für die Port-Channel-Datenschnittstelle.

Lösung:

Schritt 1: Wählen Sie in der FMC-GUI die Schaltfläche FTD_Cluster Bearbeiten aus.

Navigieren Sie zur Registerkarte Interfaces (Schnittstellen), und klicken Sie auf **Add Interfaces**> Sub Interface (Schnittstellen **hinzufügen**> Subschnittstelle), wie im Bild gezeigt.

Overview Analysis Policies Devices Objects AMP		Deploy \varTheta System Help 🕶 olga 🕶
Device Management NAT VPN Platform Settings		
FTD_cluster		Save Save
Cisco Firepower 9000 Series SM-36 Threat Defense		
Cluster Devices Devices NAT Totalans Talias Cat	DUCD	
a lancer bevices Routing RAT Interfaces Inline set	UNCP	Add Interfaces
~		
Interface Logical Name	Type Security Zone Mac Address(Active/Standby) IP	Address Sub Interface
1 Port-channel5	EtherChannel	/
m Port-channel48	EtherChannel	9
Ethernet1/1 diagnostic	Physical	1

Konfigurieren Sie die erste Subschnittstelle mit diesen Details. Wählen Sie **OK**, um die Änderungen zu übernehmen und wie in den Bildern gezeigt.

Name	Innen
Registerkarte Allgemein	
Schnittstelle	Port-Channel5
Subschnittstelle-ID	201
VLAN-ID	201
Registerkarte "IPv4"	
ІР-Тур	Statische IP verwenden
IP-Adresse	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 Interfac	e ? ×	
Name: Insid	de Catalog Management Only	
Security Zone:	~	
Description:		
General IPv4 I	Pv6 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	

Konfigurieren Sie die zweite Subschnittstelle mit diesen Details.

Name	Außen
Registerkarte Allgemein	
Schnittstelle	Port-Channel5
Subschnittstelle-ID	210
VLAN-ID	210
Registerkarte "IPv4"	
IP-Typ	Statische IP verwenden
IP-Adresse	192.168.76.10/24

Klicken Sie auf **OK**, um die Subschnittstelle zu erstellen. Klicken Sie auf **Speichern** und dann auf **Bereitstellen** von Änderungen am FTD_Cluster, wie im Bild gezeigt.

Überprüfung:

Overview Analysis Policies Devices Objects AMP		Deploy 🔍 System Help v olga v						
Device Management NAT VPN Platform Settings								
FTD_cluster Cisco Firepower 9000 Series SM-36 Threet Defense								
Cluster Devices Routing NAT Interfaces Inline S	ts DHCP							
2		Add Interfaces •						
Interface Logical Name	Type Security Zone Mac Address(Active/Standby)	IP Address						
Port-channel5	EtherChannel	/						
Port-channel48	EtherChannel	۹,						
Ethernet1/1 diagnostic	Physical	1						
Port-channel5.201 Inside	SubInterface	192.168.75.10/24(Støtic) 🥜 🗑						
Port-channel5.210 Outside	SubInterface	192.168.76.10/24(Static) 🥜 🗒						

Aufgabe 5: Grundlegende Konnektivität überprüfen

Aufgabenanforderung:

Erstellen Sie eine Erfassung, und überprüfen Sie die Verbindung zwischen zwei VMs.

Lösung:

Schritt 1: Erstellen Sie auf allen Cluster-Einheiten Erfassungen.

Navigieren Sie zur LINA (ASA)-CLI der Master-Einheit, und erstellen Sie Captures für die Insideund Outside-Schnittstellen.

```
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#
Überprüfung:
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

Führen Sie den Test mit 4 Paketen durch. Überprüfen Sie die Erfassungsausgabe nach dem Test:

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

firepower#

Führen Sie den Befehl aus, um die Erfassungsausgabe für die spezifische Einheit zu überprüfen:

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

8 packets captured

1:	12:58:36.162253	802.1Q	vlan#201	Р0	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
2:	12:58:36.162955	802.1Q	vlan#201	P0	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
3:	12:58:37.173834	802.1Q	vlan#201	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
4:	12:58:37.174368	802.1Q	vlan#201	P0	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
5:	12:58:38.187642	802.1Q	vlan#201	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
6:	12:58:38.188115	802.1Q	vlan#201	PO	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	PO	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	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
2:	12:58:36.162894	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
3:	12:58:37.174002	802.1Q	vlan#210	РO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
4:	12:58:37.174307	802.1Q	vlan#210	PO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
5:	12:58:38.187764	802.1Q	vlan#210	PO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
6:	12:58:38.188085	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
7:	12:58:39.201954	802.1Q	vlan#210	PO	192.168.75.100	>	192.168.76.100:	icmp:	echo	
reques	st									
8:	12:58:39.202290	802.1Q	vlan#210	РO	192.168.76.100	>	192.168.75.100:	icmp:	echo	reply
8 pacl	kets shown									
firepo	firepower#									
Lösch	_öschen Sie nach Abschluss dieser Aufgabe die Aufnahmen mit dem folgenden Befehl:									

VM1 wurde als FTP-Server und VM2 als FTP-Client vorkonfiguriert.

Erstellen Sie neue Erfassungen mit den folgenden Elementen:

Laden Sie die Datei mithilfe des FTP-Clients von VM2 auf VM1 herunter.

Überprüfen Sie die Ausgabe show conn:

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 U0

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

Ausgabe der Erfassung anzeigen:

Cluster-Erfassung über Chassis Manager-Benutzeroberfläche

Im folgenden Bild sehen Sie einen Cluster mit 3 Einheiten auf FPR9300 mit 2 Port-Channels (8 und 48). Die logischen Geräte sind ASAs, aber im Falle von FTD wird das gleiche Konzept.Wichtig ist, dass es, obwohl es **3 Cluster-Einheiten** gibt, aus Erfassungssicht nur **ein logisches Gerät** gibt:

Ov	erview Interfaces	Logical Devices	Security Mo	odules Platform Set	tings		Sys	tem Tools Help admin
Log	cal Device List						c	Refresh Add Device
	ASA C	lustered	Status:ok					
	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	💮 online	🕶 🎉
	Ports: Data Interfaces: Cluster Interfaces:	Port-channel8 Port-channel48		Attributes: Cluster Operational Statı Management IP VIRTUAL Cluster Role Management URL Management IP	us : 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	💌 🏂 A
	Ports: Data Interfaces: Cluster Interfaces:	Port-channel8 Port-channel48		Attributes: Cluster Operational Statı Management IP VIRTUAL Cluster Role Management URL Management IP	us : 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 Statı Management IP VIRTUAL Cluster Role Management URL Management IP	us : 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	Fools Help admin
						Packet Capture
			Save and Run	Save	Cancel	
ASA				Session Name*	ARP Ethernet1/5	
Ethernet1/1				Buffer Size	256 MB	~
Ethernet1/8 (Portchannel48)		_		Snap length:	1518	Bytes
Ethernet1/7 (Portchannel48)				Store Packets	Overwrite	Append
Ethernet1/6 (Portchannel48)				Capture Filter	Apply Filter	Capture All
Ethernet1/5 [Ethernet1/9. Eth	ASA ASA ernet1/10. Ethernet1/11.			
Ethernet1/4 (Portchannel48)		Ethernet1/12, Et	hernet1/13, Ethernet1/14			
Ethernet1/3 (Portchannel48)						
Ethernet1/2 (Portchannel48)						
Ethernet2/2 (Portchannel8)						
Ethernet2/1 (Portchannel8)						

Aufgabe 6: Löschen eines Slave-Geräts aus dem Cluster

Aufgabenanforderung:

Melden Sie sich beim FMC an, und löschen Sie die Slave-Einheit aus dem Cluster.

Lösung:

Schritt 1: Melden Sie sich beim FMC an, und navigieren Sie zu **Device > Device Management** (Gerät > Gerätemanagement).

Klicken Sie auf das Papierkorbsymbol neben der Slave-Einheit, wie im Bild gezeigt.

ETD_cluster Cisco Firepower 9000 Series SM-36 Threat Defense Cluster			J 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	Û
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

Das Bestätigungsfenster wird angezeigt. Wählen Sie zur Bestätigung Ja, wie im Bild gezeigt.



Überprüfung:

• Aus dem FMC, wie im Bild gezeigt.

- 6	FTD_cluster Cisco Firepower 9000 Series SM-36 Threat Defense Cluster	1	3
	FTD1(primary) 10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed Cisco Firepower 9000 Series SM-36 Threat, Malware, URL Filtering FID9300		
	FTD3 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed Cisco Firepower 9000 Series SM-36 Threat, Malware, URL Filtering FTD9300	8	

• Aus der FXOS-CLI.

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

• Aus der LINA-CLI (ASA).

firepower# show cluster info Cluster FTD_cluster: On Interface mode: spanned This is "unit-1-1" in state MASTER ID : 0 : 9.6(1) Version 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 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 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#
```

Hinweis: Das Gerät wurde vom FMC nicht registriert, ist jedoch weiterhin Cluster-Mitglied auf dem FPR9300.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Die Überprüfung ist abgeschlossen und wird in einzelnen Aufgaben durchgeführt.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

• Alle Versionen des Konfigurationsleitfadens für das Cisco FirePOWER Management Center finden Sie hier:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280.

 Alle Versionen der Konfigurationsleitfäden für den FXOS Chassis Manager und die CLI finden Sie hier:

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

• Das Cisco Global Technical Assistance Center (TAC) empfiehlt diesen visuellen Leitfaden dringend, um umfassende praktische Kenntnisse über die Sicherheitstechnologien der nächsten Generation von Cisco Firepower zu erwerben, einschließlich der in diesem Artikel erwähnten Technologien:

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

• Für alle Konfigurations- und Fehlerbehebungsdetails finden Sie technische Hinweise zu FirePOWER-Technologien.

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

<u>Technischer Support und Dokumentation - Cisco Systems</u>