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

Inhalt

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.

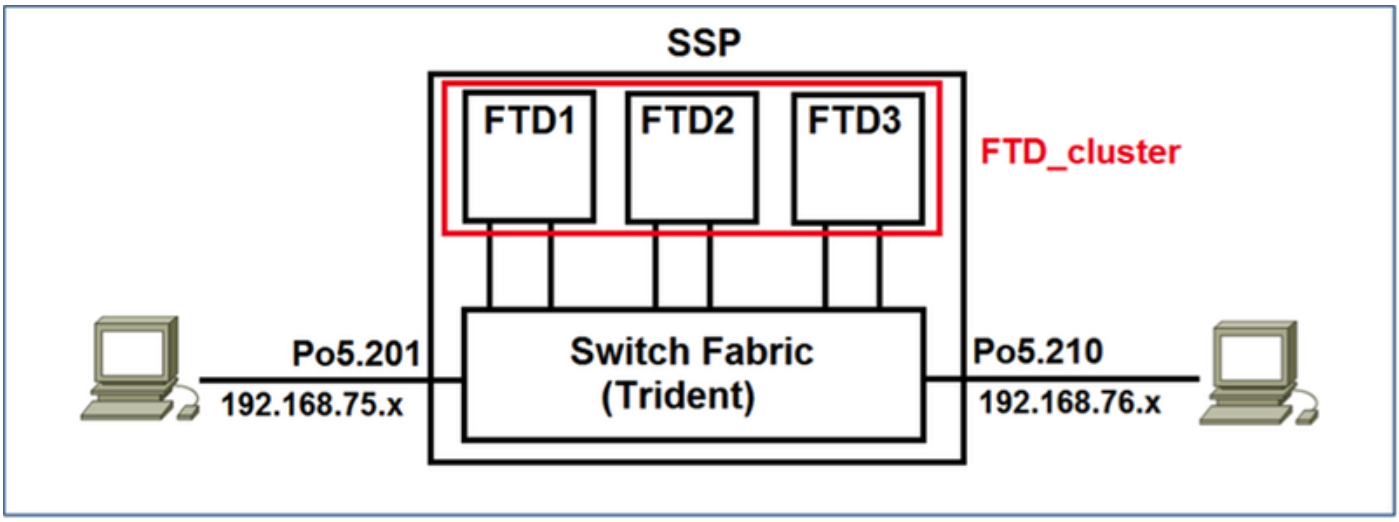
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

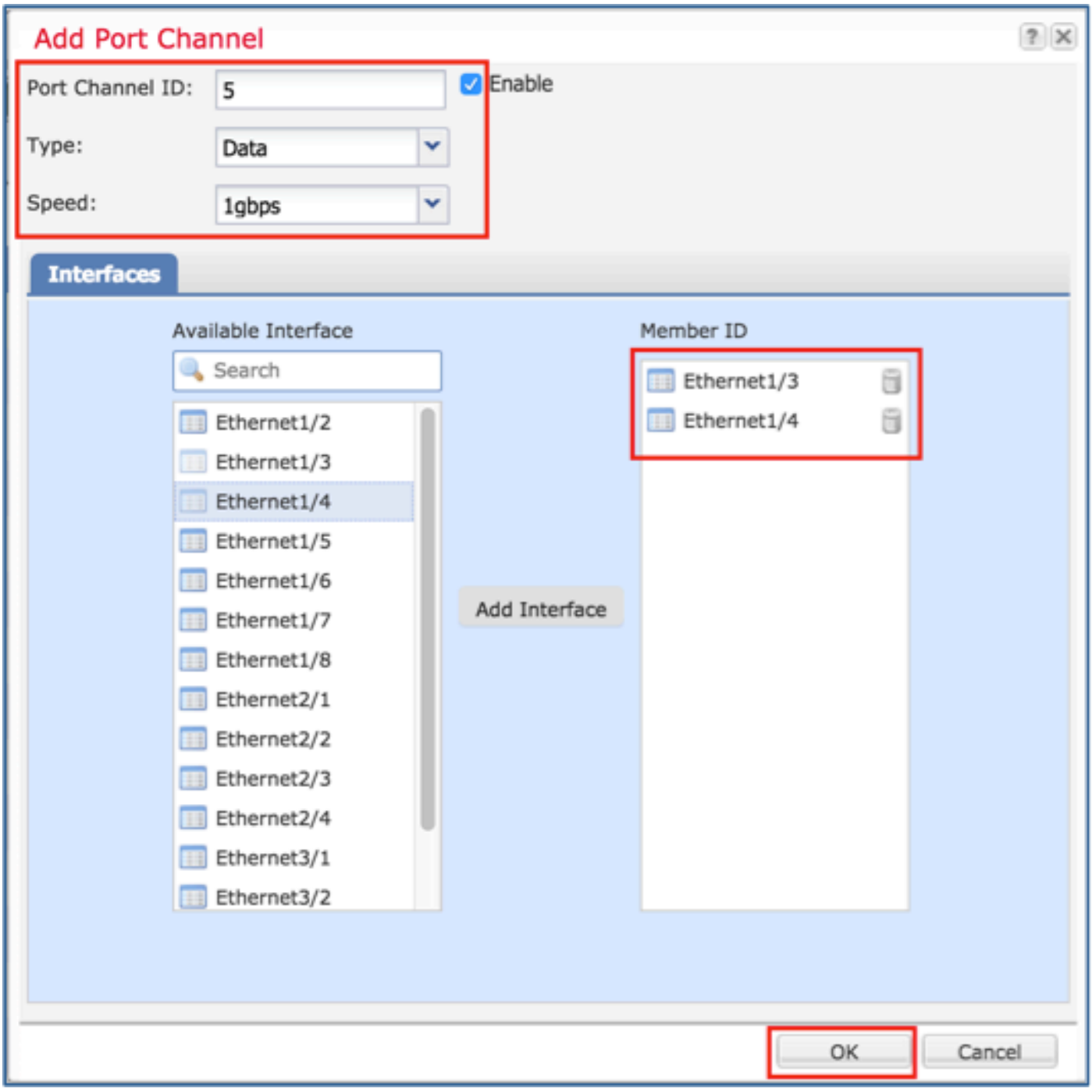
Schritt 1: Erstellen einer Port-Channel-Datenschnittstelle.

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
Typ	Daten
Aktivieren	Ja
Mitglied-ID	Ethernet1/3, Ethernet 1/4

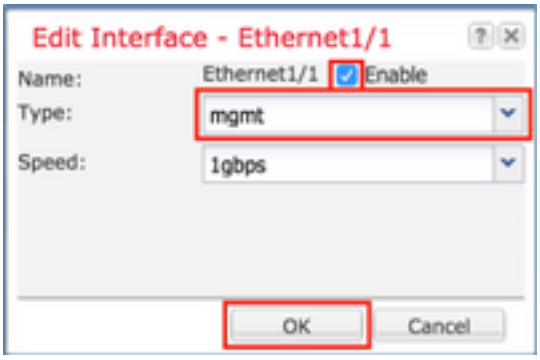
Wählen Sie **OK**, um die Konfiguration wie im Bild gezeigt zu speichern.



Schritt 2: Erstellen einer Verwaltungsschnittstelle

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

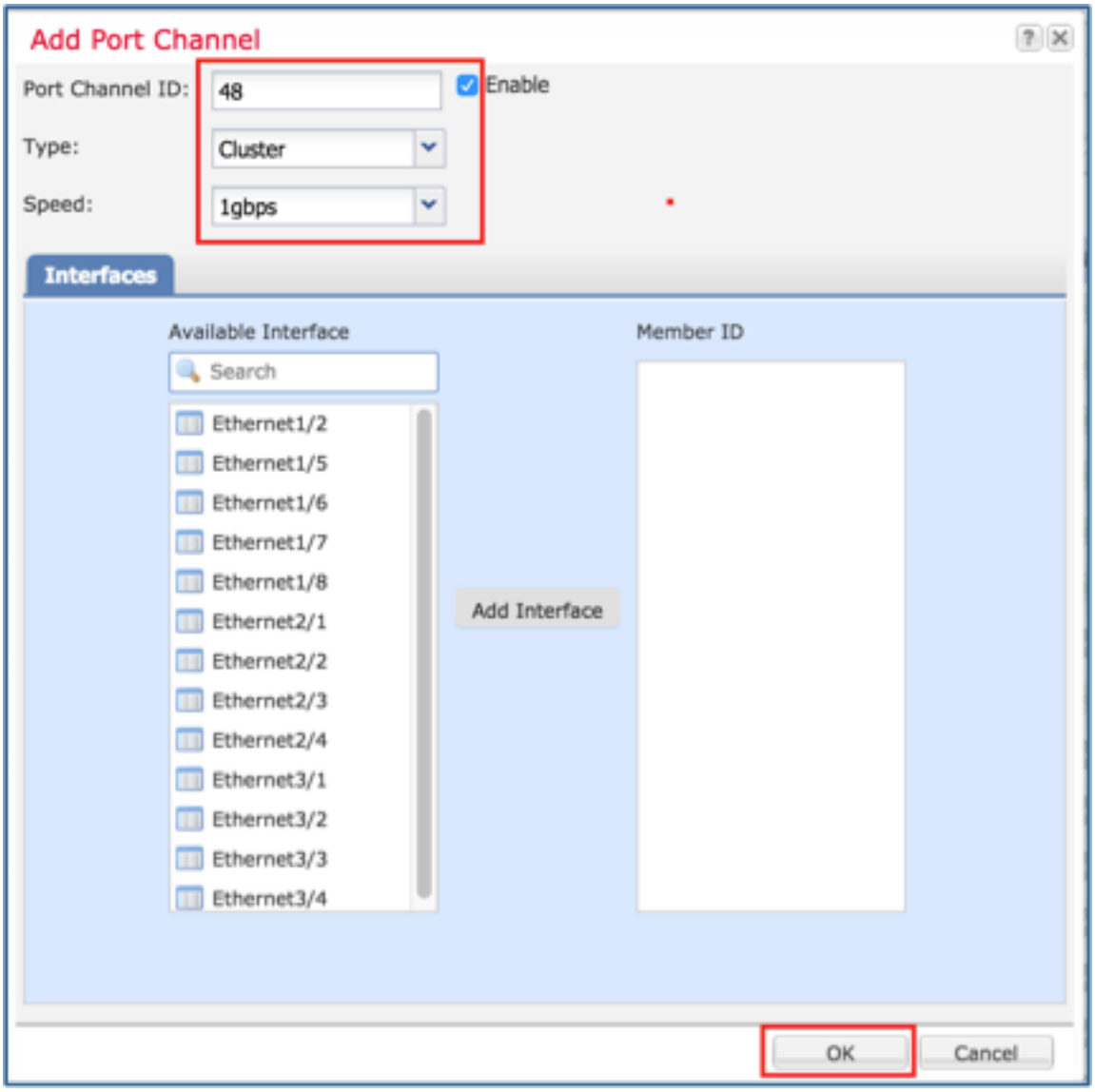
Klicken Sie auf **OK**, um die Konfiguration wie im Bild gezeigt zu speichern.



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
Typ	Cluster
Aktivieren	Ja
Mitglied-ID	-



Aufgabe 2: FTD-Cluster erstellen

Aufgabenanforderung:

Erstellen Sie eine FTD-Cluster-Einheit.

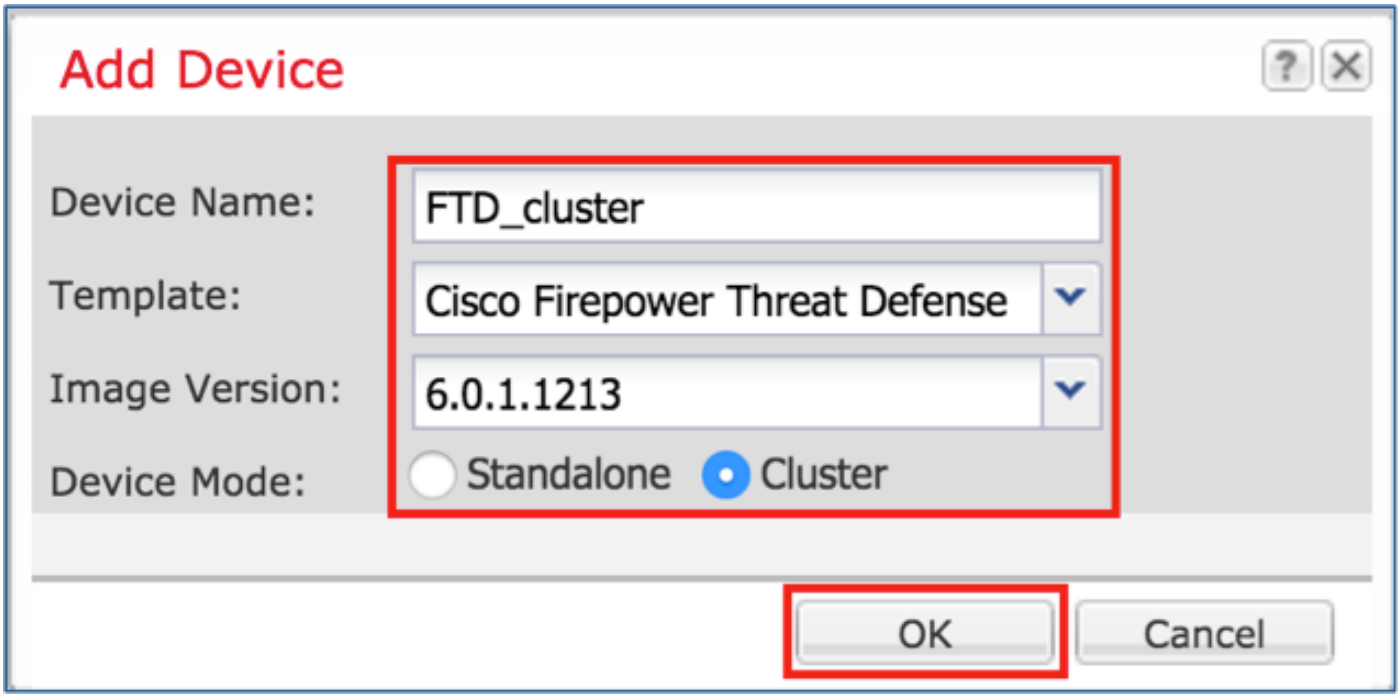
Lösung:

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

Erstellen Sie das FTD-Clustering wie folgt:

Gerätename	FTD-Cluster
Vorlage	Cisco FirePOWER Threat Defense
Image-Version	6,0 1,1213
Gerätemodus	Cluster

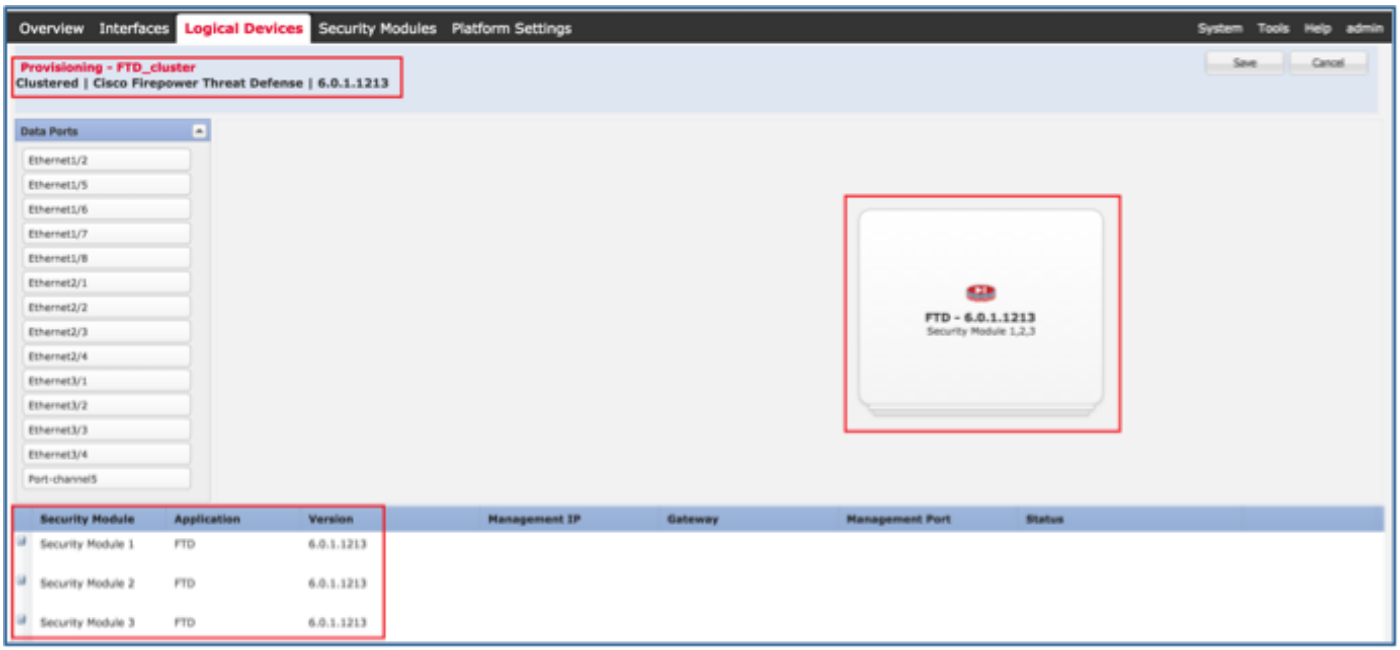
Um das Gerät hinzuzufügen, klicken Sie auf **OK**, wie im Bild gezeigt.



Schritt 2: Konfigurieren und Bereitstellen des FTD-Clusters

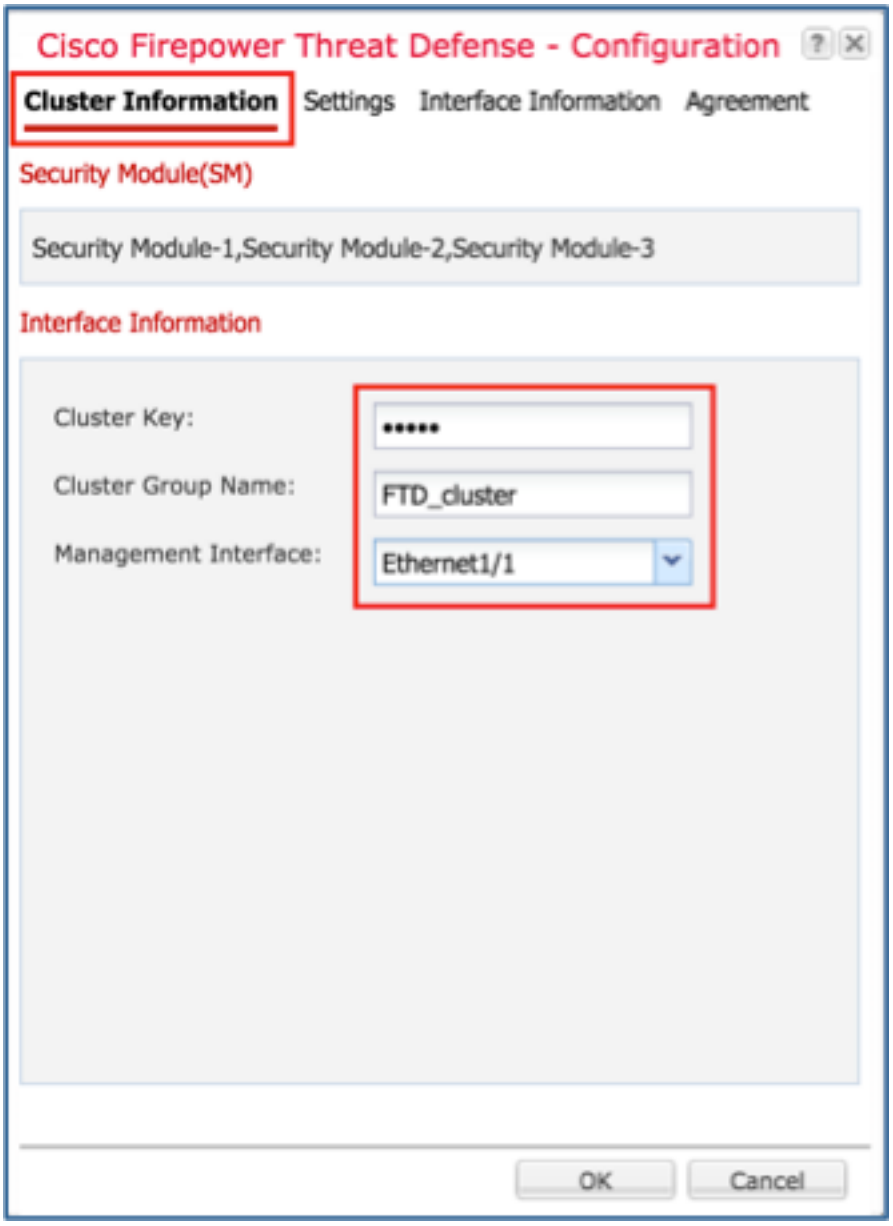
Nachdem Sie ein FTD-Gerät erstellt haben, werden Sie zum Fenster Provisioning- device_name umgeleitet.

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



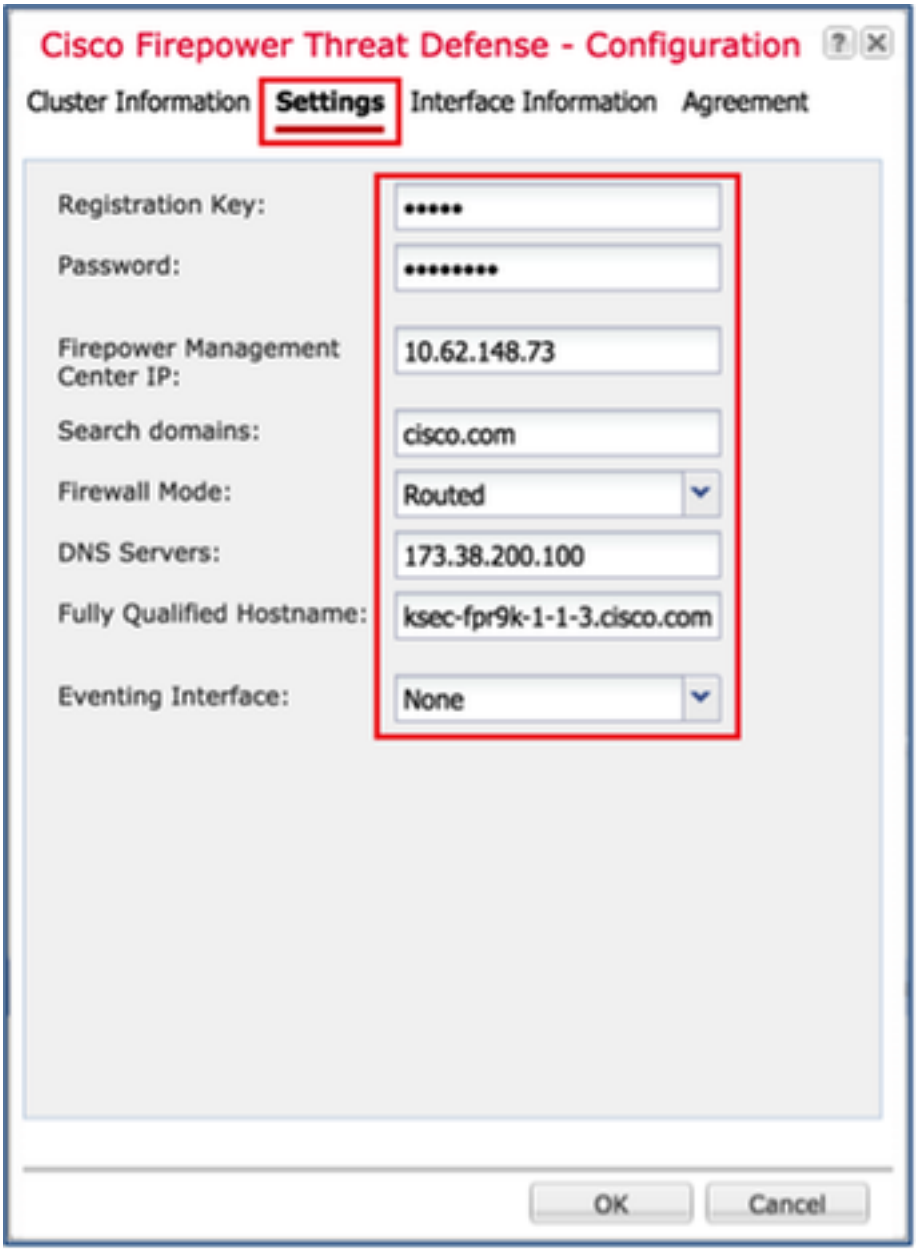
Konfigurieren Sie die Registerkarte "FTD-**Cluster-Informationen**" mit diesen Einstellungen und wie im Bild gezeigt.

Cluster-Schlüssel	Cisco
Cluster-Gruppenname	FTD-Cluster
Verwaltungsschnittstelle	Ethernet1/1



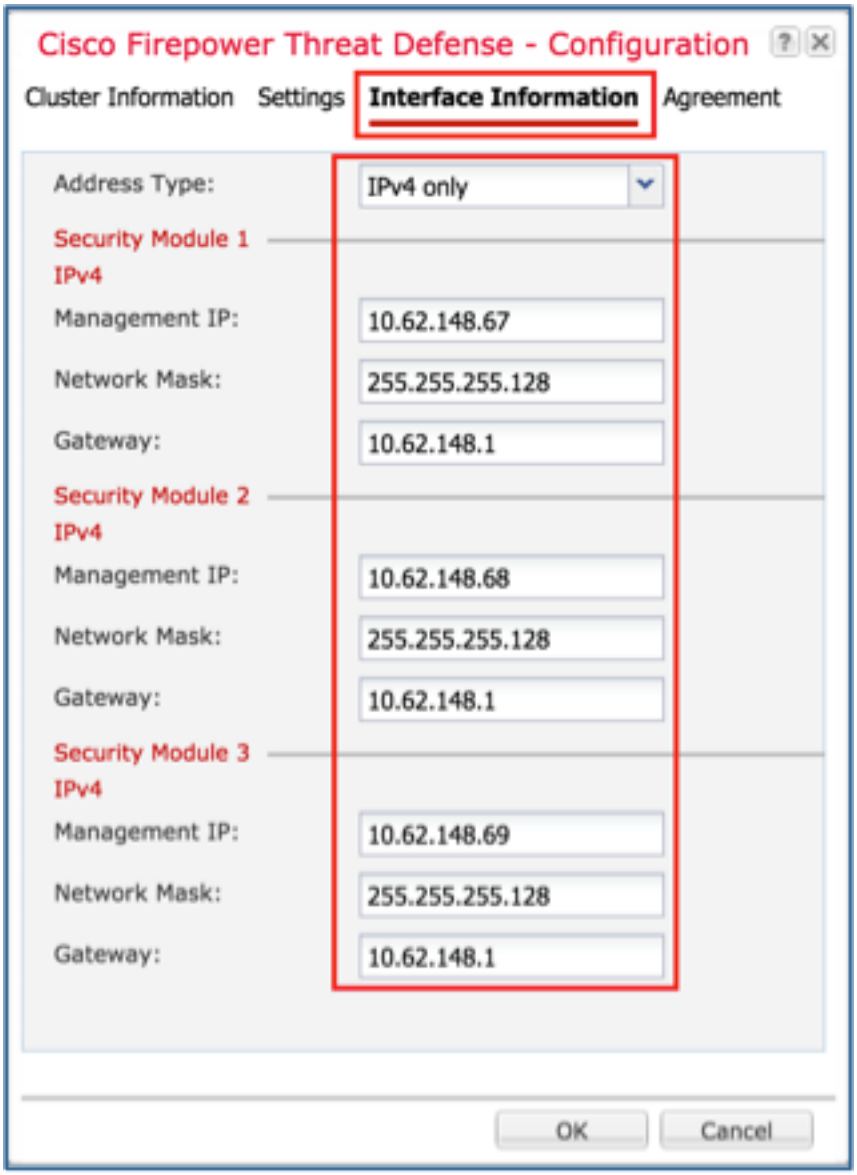
Konfigurieren Sie die Registerkarte FTD-Einstellungen mit diesen Einstellungen, wie im Bild gezeigt.

Registrierungsschlüssel	Cisco
Kennwort	Administrator123
FirePOWER Management Center IP	10.62.148.73
Domänen durchsuchen	Cisco.com
Firewall-Modus	Geroutet
DNS-Server	173.38.200.100
Vollqualifizierter Hostname	ksec-fpr9k-1-1-3.cisco.com
Ereignisschnittstelle	Keine

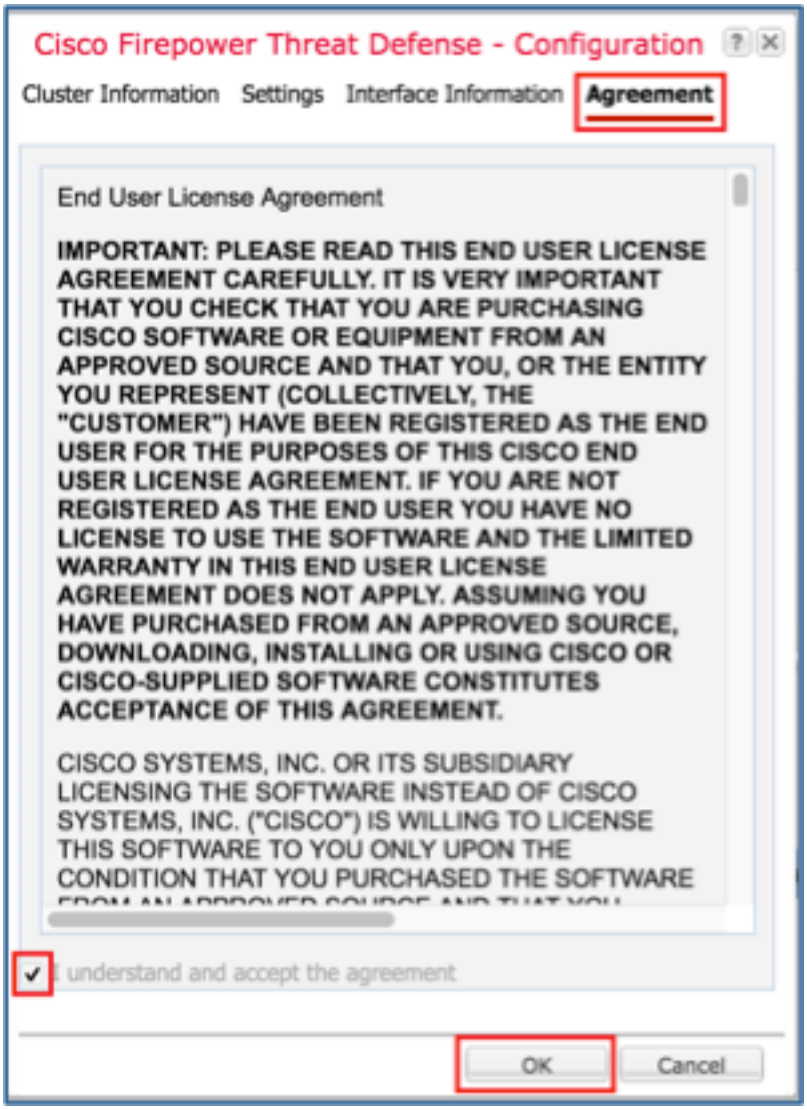


Konfigurieren Sie die Registerkarte "**Informationen zur** FTD-**Schnittstelle**" mit diesen Einstellungen und wie im Bild gezeigt.

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

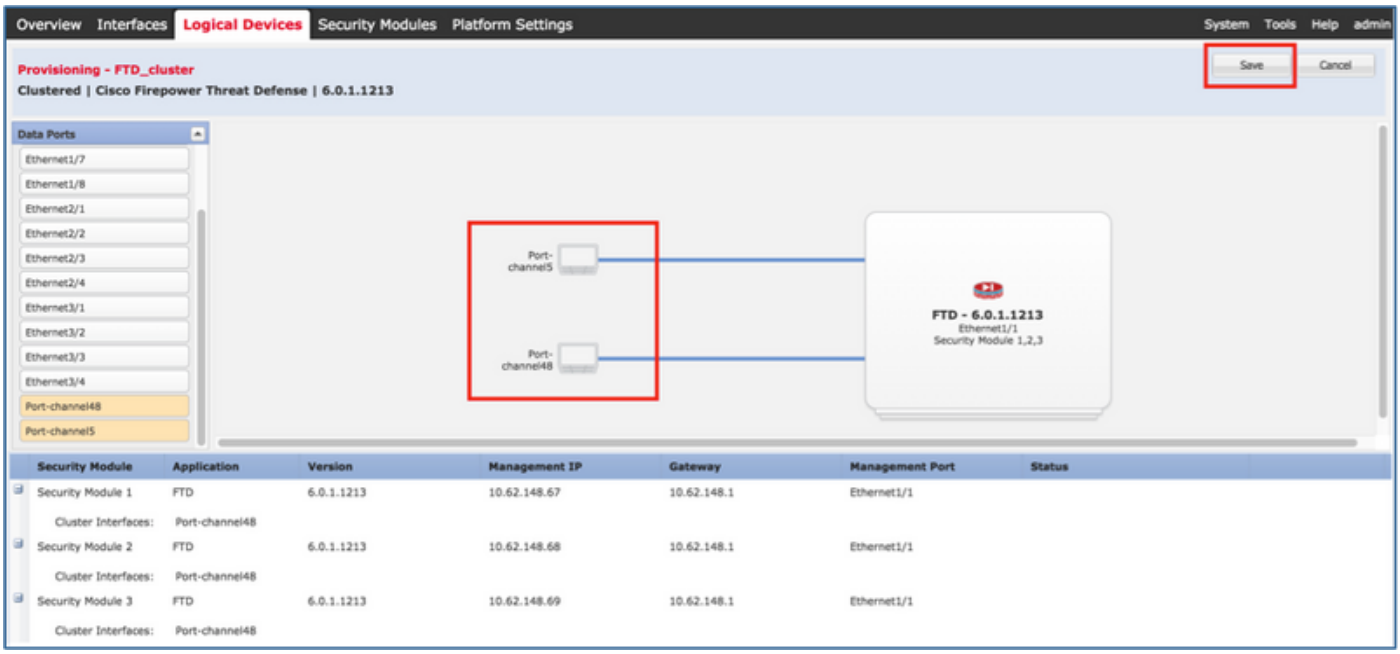


Akzeptieren Sie die Vereinbarung auf der Registerkarte "**Vereinbarung**", und klicken Sie wie im Bild gezeigt auf **OK**.



Schritt 3: Zuweisen von Datenschnittstellen zu FTD

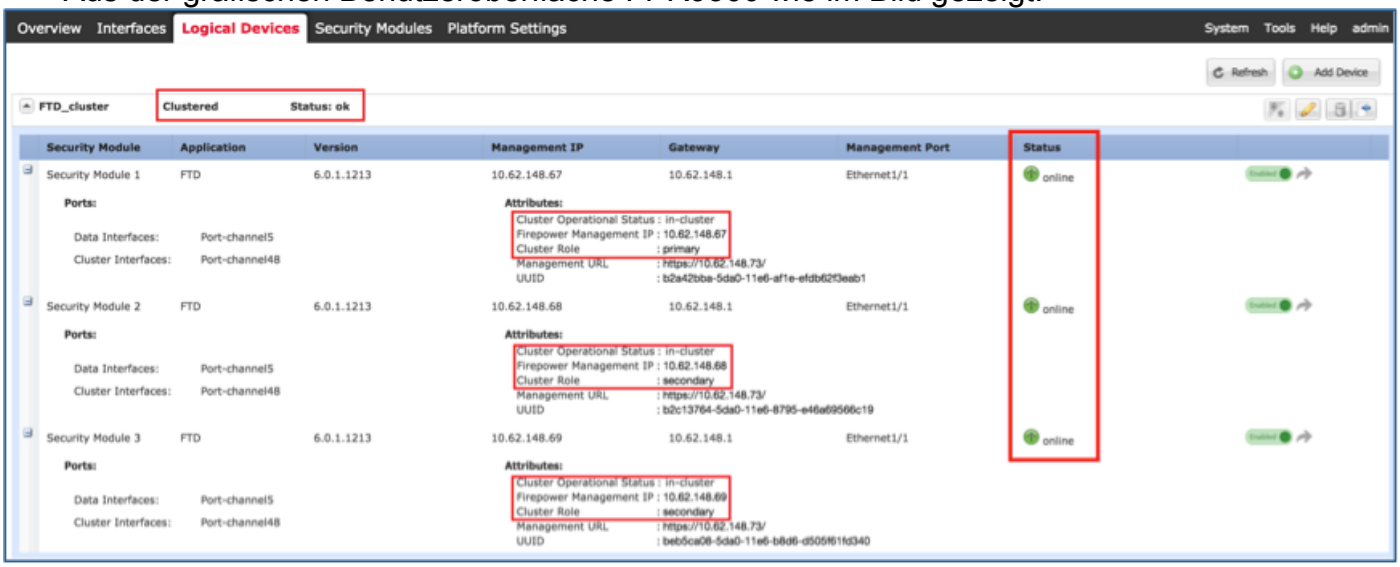
Erweitern Sie den Bereich Datenports, und klicken Sie auf die einzelnen Schnittstellen, die Sie FTD zuweisen möchten. Wählen Sie nach Abschluss die Option **Speichern**, um einen FTD-Cluster zu erstellen, wie im Bild gezeigt.



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.



- Von der CLI FPR9300

```
FPR9K-1-A#
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
```

- Über die 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
        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# cluster exec show cluster interface-mode
cluster interface-mode spanned


unit-1-3:**********************************************************
cluster interface-mode spanned


unit-1-2:**********************************************************
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             ELECTION             Enabled from CLI

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

================================================================================


unit-1-3:**********************************************************
================================================================================
From State           To 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               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               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             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

==============================================================================


unit-1-2:************************************************************
==============================================================================
From State           To 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              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             ONCALL               Received cluster control message

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            ONCALL              Received cluster control message

21:50:36 CEST Aug 8 2016
ONCALL              ELECTION            Received cluster control message

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              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            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            ONCALL              Received cluster control message

21:51:06 CEST Aug 8 2016
ONCALL              ELECTION            Received cluster control message

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            ONCALL              Received cluster control message

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_COLD           SLAVE_APP_SYNC       Client progression done

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.

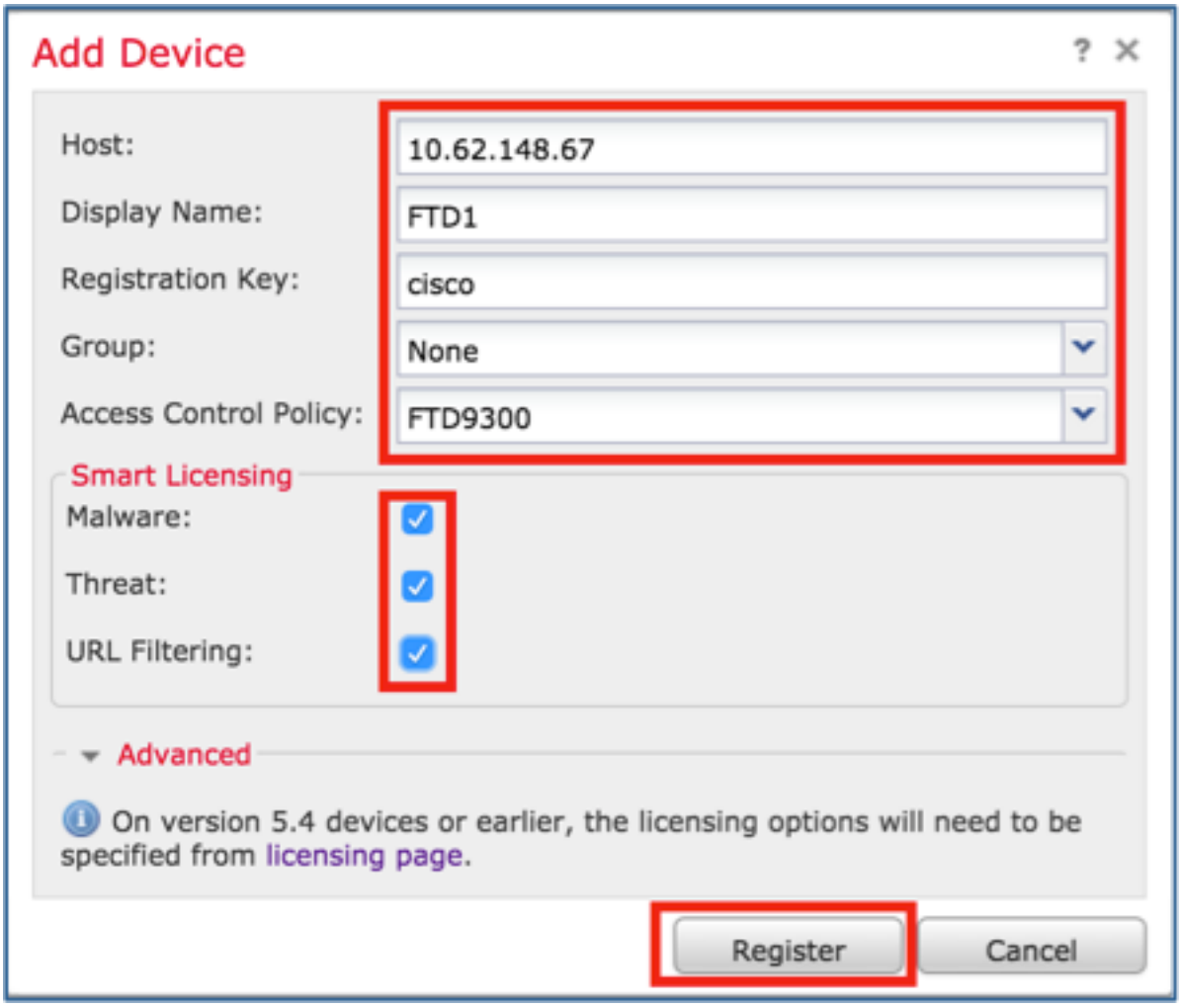
Lösung:

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.



Die überprüfung erfolgt wie im Bild gezeigt.

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

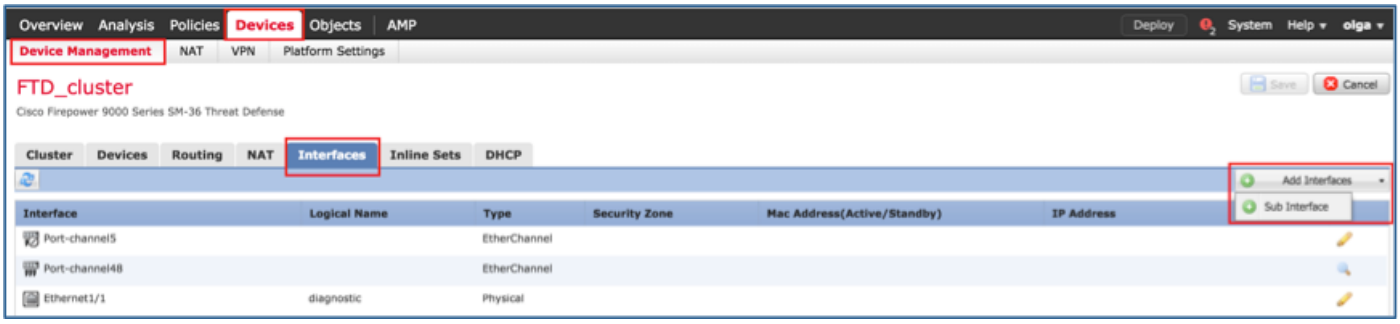
Aufgabenanforderung:

Konfigurieren Sie Subschnittstellen für die Port-Channel-Datenschnittstelle.

Lösung:

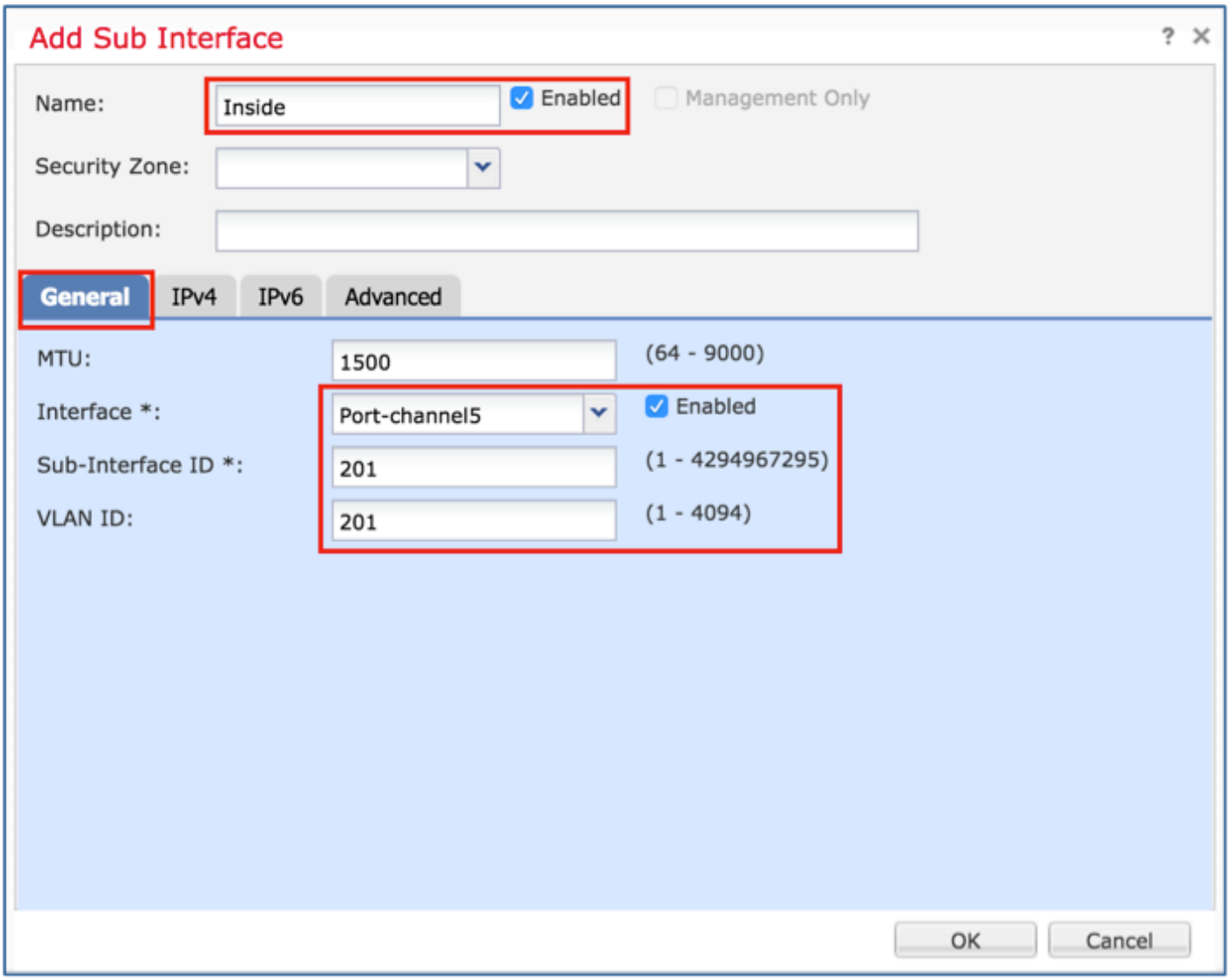
Schritt 1: Wählen Sie in der FMC-GUI die Schaltfläche **FTD_Cluster Bearbeiten** aus.

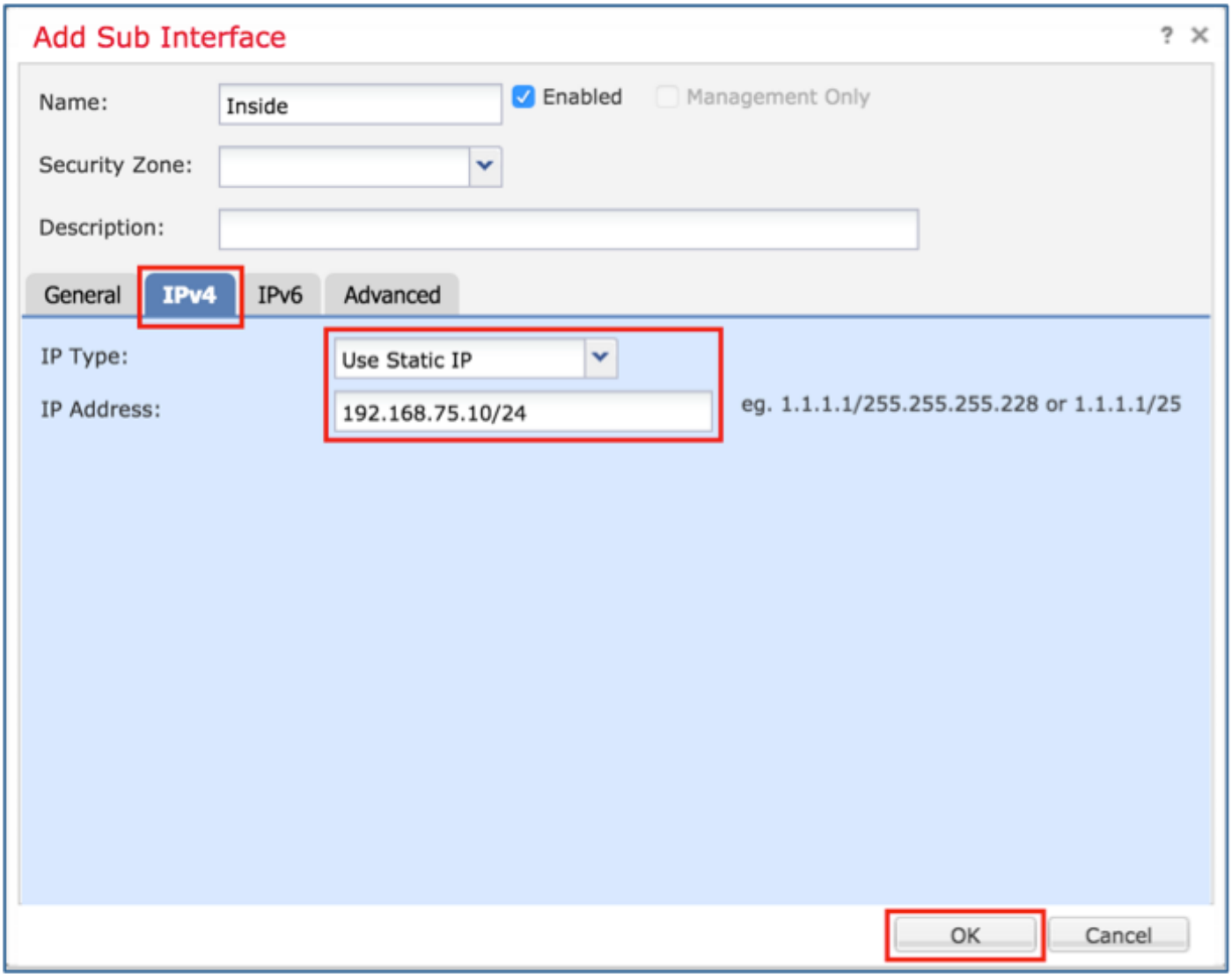
Navigieren Sie zur Registerkarte Interfaces (Schnittstellen), und klicken Sie auf **Add Interfaces>** Sub Interface (Schnittstellen **hinzufügen>** Subschnittstelle), wie im Bild gezeigt.



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"	
IP-Typ	Statische IP verwenden
IP-Adresse	192.168.75.10/24



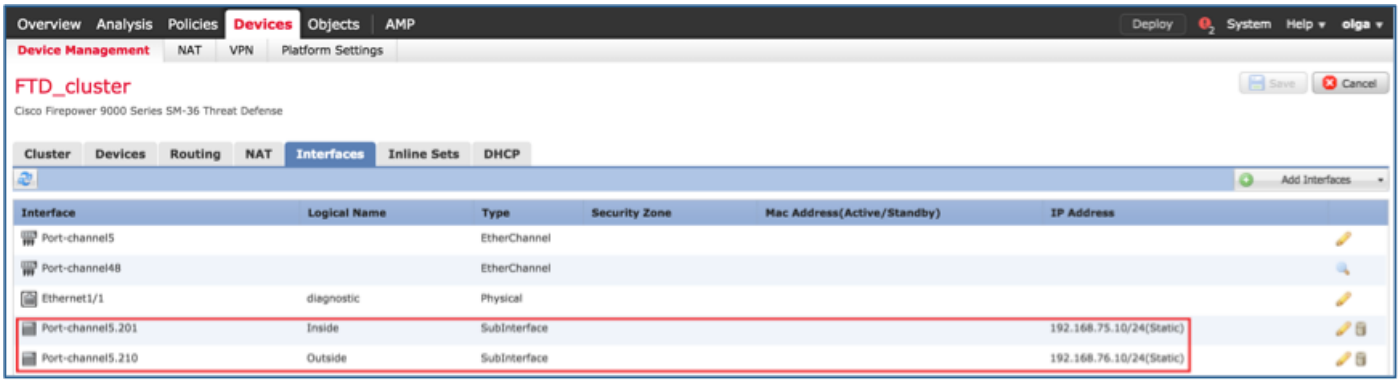


Konfigurieren Sie die zweite Subschnittstelle mit diesen Details.

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:



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 Inside- und Outside-Schnittstellen.

```
firepower#
firepower# cluster exec capture capi interface inside match icmp any any
unit-1-1(LOCAL):*******************************************************


unit-1-3:*************************************************************


unit-1-2:*************************************************************
firepower#
firepower# cluster exec capture capo interface outside match icmp any any
unit-1-1(LOCAL):*******************************************************


unit-1-3:*************************************************************


unit-1-2:*************************************************************
firepower#
```

Überprüfung:

```
firepower# cluster exec show capture
unit-1-1(LOCAL):*******************************************************
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


unit-1-3:*************************************************************
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


unit-1-2:**********************************************************
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#
```

Schritt 2: Führen Sie den Ping-Test von VM1 zu VM2 aus.

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

```
firepower# cluster exec show capture
unit-1-1(LOCAL):******************************************************
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


unit-1-3:**********************************************************
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


unit-1-2:**********************************************************
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 P0 192.168.75.100 > 192.168.76.100: icmp: echo
request
   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 P0 192.168.75.100 > 192.168.76.100: icmp: echo
request
   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 P0 192.168.75.100 > 192.168.76.100: icmp: echo
request
   6: 12:58:38.188115       802.1Q vlan#201 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply
   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
   3: 12:58:37.174002       802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo
request
   4: 12:58:37.174307       802.1Q vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply
   5: 12:58:38.187764       802.1Q vlan#210 P0 192.168.75.100 > 192.168.76.100: icmp: echo
request
   6: 12:58:38.188085       802.1Q vlan#210 P0 192.168.76.100 > 192.168.75.100: icmp: echo reply
   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#
```

Löschen Sie nach Abschluss dieser Aufgabe die Aufnahmen mit dem folgenden Befehl:

```
firepower# cluster exec no capture capi
unit-1-1(LOCAL):*******************************************************


unit-1-3:*******************************************************


unit-1-2:*******************************************************

firepower# cluster exec no capture capo
unit-1-1(LOCAL):*******************************************************


unit-1-3:*******************************************************


unit-1-2:*******************************************************
```

Schritt 3: Laden Sie eine Datei von VM2 auf VM1 herunter.

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

Erstellen Sie neue Erfassungen mit den folgenden Elementen:

```
firepower# cluster exec capture capi interface inside match ip host 192.168.75.100 host
192.168.76.100
unit-1-1(LOCAL):*******************************************************


unit-1-3:*******************************************************


unit-1-2:*******************************************************

firepower# cluster exec capture capo interface outside match ip host 192.168.775.100 host
192.168.76.100
unit-1-1(LOCAL):*******************************************************


unit-1-3:*******************************************************


unit-1-2:*******************************************************
```

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

Überprüfen Sie die Ausgabe **show conn**:

```
firepower# cluster exec show conn all
unit-1-1(LOCAL):*******************************************************
20 in use, 21 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 52 most used
centralized connections: 0 in use, 6 most used

TCP Outside  192.168.76.100:49175 Inside  192.168.75.100:21, idle 0:00:32, bytes 665, flags
UIOeN
UDP cluster  255.255.255.255:49495 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


unit-1-3:*******************************************************************
12 in use, 16 most used
Cluster:
fwd connections: 0 in use, 4 most used
dir connections: 1 in use, 10 most used
centralized connections: 0 in use, 0 most used

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


unit-1-2:*******************************************************************
12 in use, 15 most used
Cluster:
fwd connections: 0 in use, 2 most used
dir connections: 0 in use, 3 most used
centralized connections: 0 in use, 0 most used

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
```

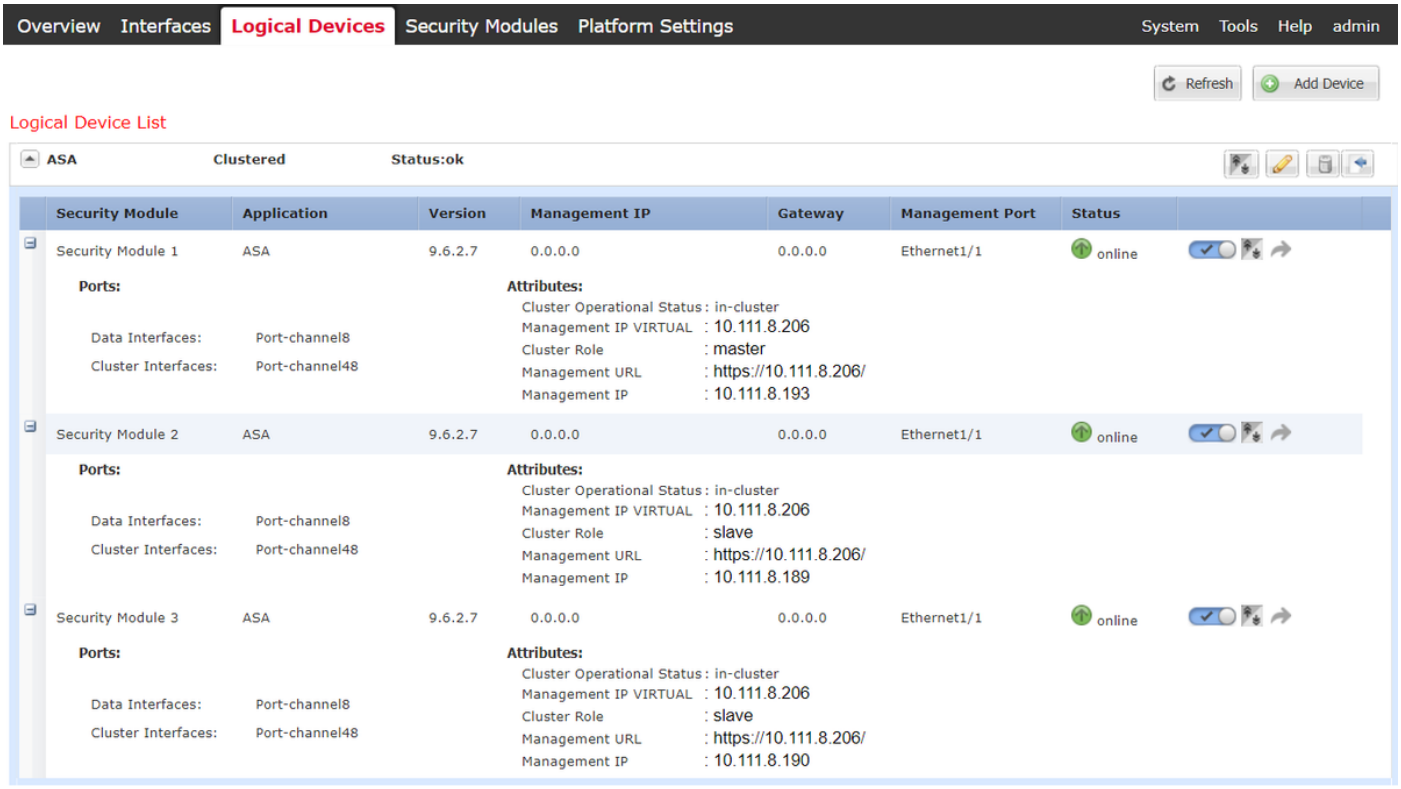
Ausgabe **der Erfassung anzeigen**:

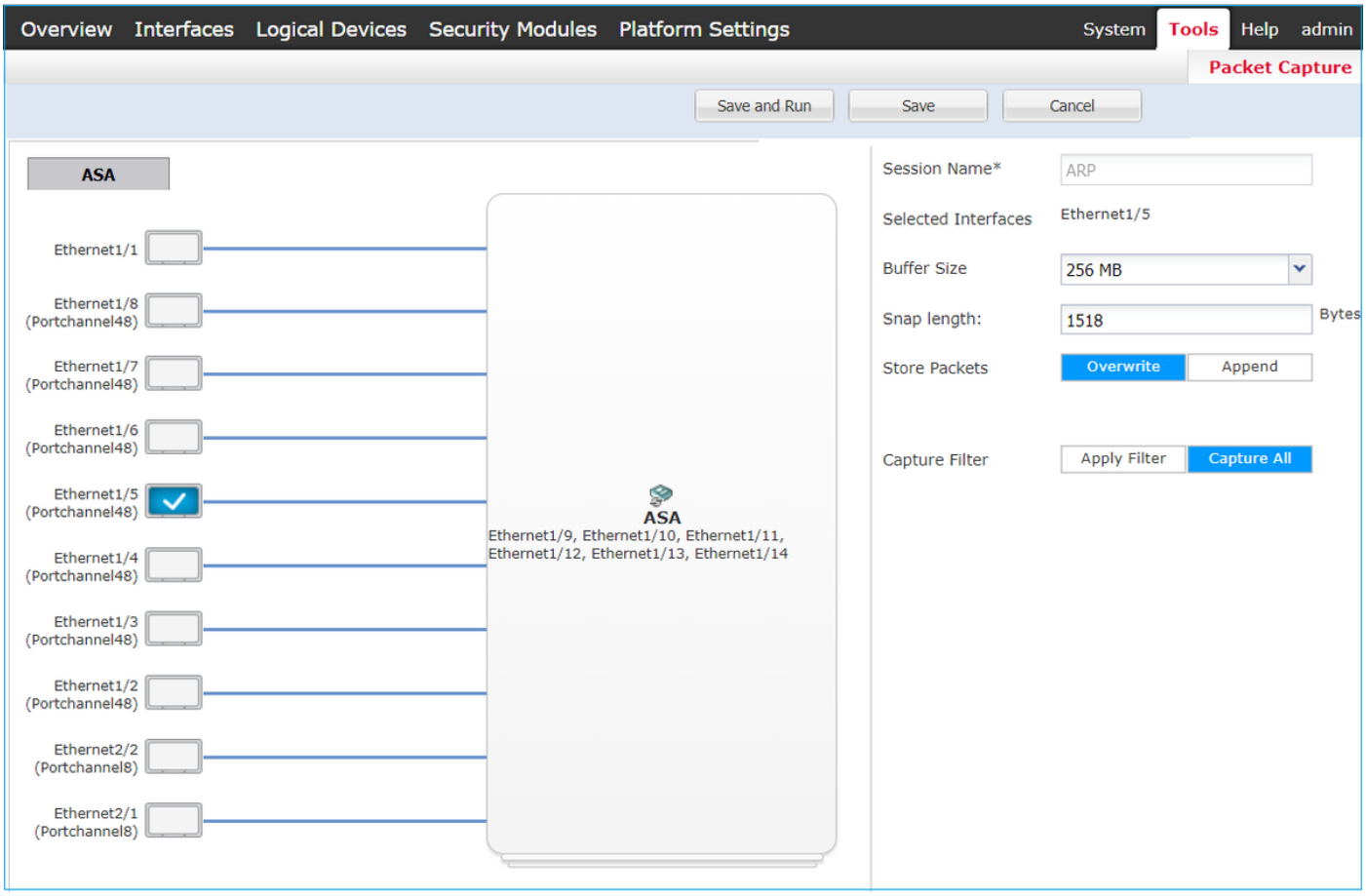
```
firepower# cluster exec show cap
unit-1-1(LOCAL):*******************************************************
capture capi type raw-data interface Inside [Buffer Full - 523954 bytes]
  match ip host 192.168.75.100 host 192.168.76.100
capture capo type raw-data interface Outside [Buffer Full - 524028 bytes]
  match ip host 192.168.75.100 host 192.168.76.100


unit-1-3:*******************************************************************
capture capi type raw-data interface Inside [Buffer Full - 524062 bytes]
  match ip host 192.168.75.100 host 192.168.76.100
capture capo type raw-data interface Outside [Buffer Full - 524228 bytes]
  match ip host 192.168.75.100 host 192.168.76.100
```

```
unit-1-2:************************************************************
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
```

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:





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:

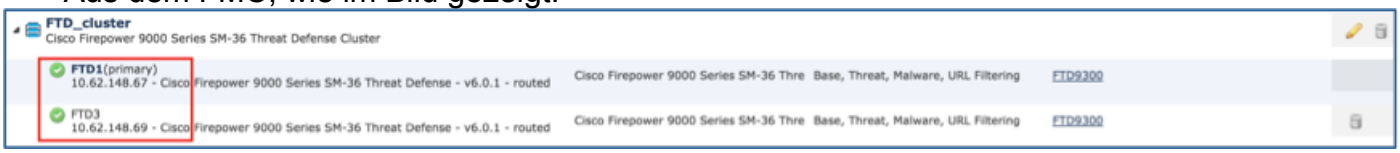
Schritt 1: Melden Sie sich beim FMC an, und navigieren Sie zu **Device > Device Management (Gerät > Gerätemanagement)**.

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

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

Überprüfung:

- Aus dem FMC, wie im Bild gezeigt.



- Aus der FXOS-CLI.

```
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
```

- 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
        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
        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#pgfId-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-series-home.html.

- Technischer Support und Dokumentation - Cisco Systems