

Configurazione del clustering FTD su FP9300 (all'interno dello chassis)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Task 1. Creazione delle interfacce necessarie per il cluster FTD](#)

[Attività 2. Creazione del cluster FTD](#)

[Attività 3. Registra cluster FTD in FMC](#)

[Attività 4. Configurazione delle sottointerfacce porta-canale su FMC](#)

[Attività 5. Verifica della connettività di base](#)

[Acquisizione cluster dall'interfaccia utente di Gestione chassis](#)

[Attività 6. Eliminare un dispositivo slave dal cluster](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare la funzionalità cluster sul dispositivo FPR9300.

Attenzione: Le informazioni fornite in questo documento riguardano l'installazione/configurazione iniziale del cluster. Questo documento non è applicabile alla procedura di sostituzione di un'unità (autorizzazione restituzione materiale - RMA)

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Appliance di sicurezza Cisco Firepower 9300 con 1.1(4.95)
- Firepower Threat Defense (FTD) con versione 6.0.1 (build 1213)
- FireSIGHT Management Center (FMC) con versione 6.0.1.1 (build 1023)

Ora di completamento del laboratorio: 1 ora.

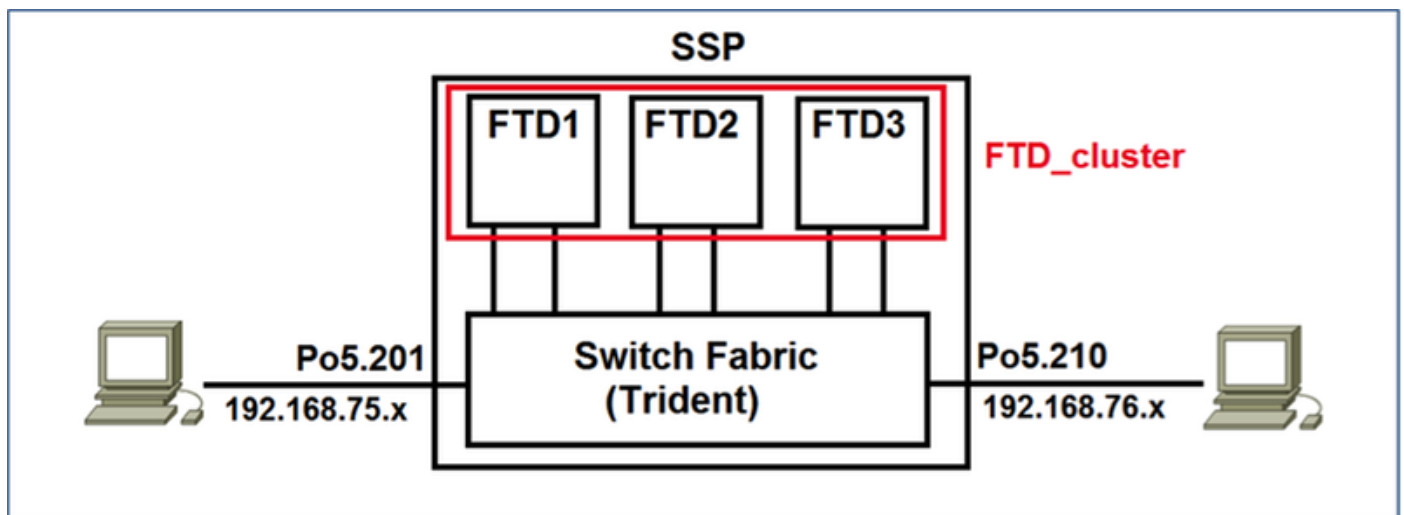
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

- Sull'accessorio FPR9300 con FTD è possibile configurare il clustering all'interno dello chassis su tutte le versioni supportate.
- Il clustering tra chassis è stato introdotto nella versione 6.2.
- Port-channel 48 viene creato come collegamento di controllo del cluster. Per il clustering all'interno dello chassis, questo collegamento utilizza il backplane Firepower 9300 per le comunicazioni cluster.
- Le singole interfacce dati non sono supportate, ad eccezione dell'interfaccia di gestione.
- L'interfaccia di gestione è assegnata a tutte le unità nel cluster.

Configurazione

Esempio di rete



Task 1. Creazione delle interfacce necessarie per il cluster FTD

Attività richiesta:

Creare un cluster, un'interfaccia di gestione e un'interfaccia dati del canale della porta.

Soluzione:

Passaggio 1. Creare un'interfaccia dati del canale della porta.

Per creare una nuova interfaccia, è necessario accedere a FPR9300 Chassis Manager e passare alla scheda **Interfacce**.

Selezionare **Add Port Channel** e creare una nuova interfaccia Port Channel con questi parametri:

ID canale porta	5
Tipo	Dati
Attiva	Sì
ID membro	Ethernet 1/3, Ethernet 1/4

Selezionare **OK** per salvare la configurazione come mostrato nell'immagine.

Add Port Channel

Port Channel ID: 5 Enable

Type: Data

Speed: 1gbps

Interfaces

Available Interface

- Ethernet1/2
- Ethernet1/3
- Ethernet1/4**
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet3/1
- Ethernet3/2

Member ID

- Ethernet1/3**
- Ethernet1/4**

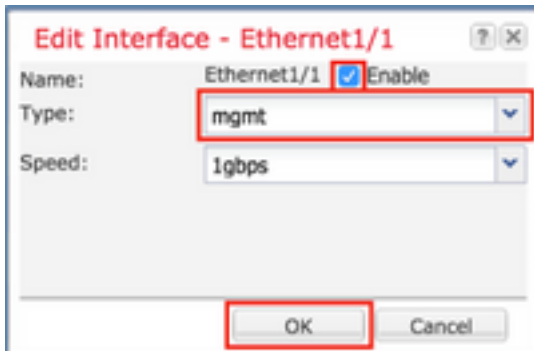
Add Interface

OK Cancel

Passaggio 2. Creare un'interfaccia di gestione.

Nella scheda **Interfacce**, scegliere l'interfaccia, fare clic su **Modifica** e configurare l'interfaccia del tipo di gestione.

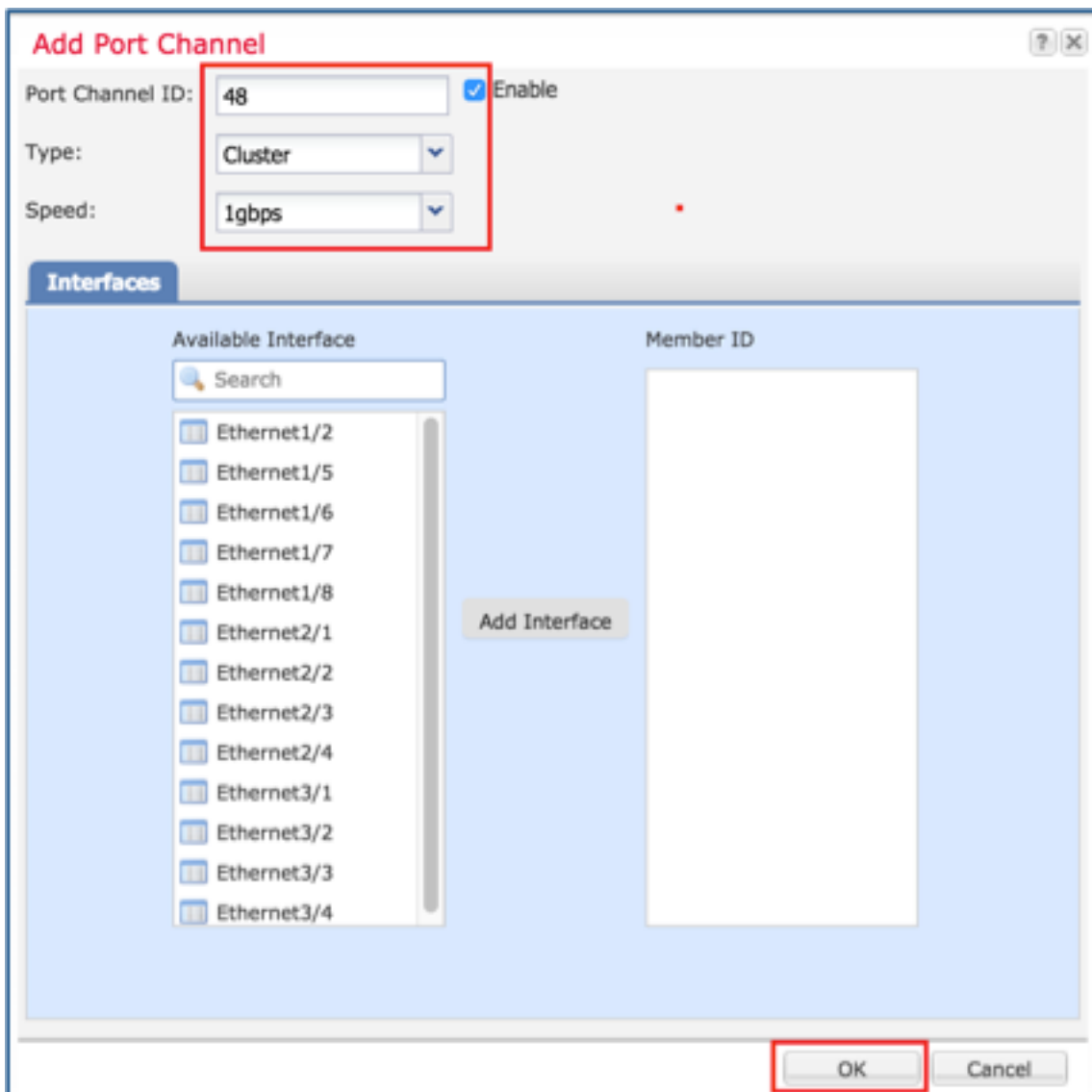
Fare clic su **OK** per salvare la configurazione come mostrato nell'immagine.



Passaggio 3. Creare un'interfaccia di collegamento di controllo del cluster.

Fare clic sul pulsante **Add Port Channel** e creare una nuova Port Channel Interface con questi parametri e come mostrato nell'immagine.

ID canale porta	48
Tipo	Cluster
Attiva	Sì
ID membro	-



Attività 2. Creazione del cluster FTD

Attività richiesta:

Creare un'unità cluster FTD.

Soluzione:

Passaggio 1. Passare a **Logical Devices** e fare clic sul pulsante **Add Device**.

Creare il clustering FTD nel modo seguente:

Nome dispositivo	FTD_cluster
Modello	Cisco Firepower Threat Defense
Versione immagine	6.0.1.1213
Modalità periferica	Cluster

Per aggiungere la periferica, fare clic su **OK**, come mostrato nell'immagine.

Add Device

Device Name: FTD_cluster

Template: Cisco Firepower Threat Defense

Image Version: 6.0.1.1213

Device Mode: Standalone Cluster

OK Cancel

Passaggio 2. Configurare e distribuire il cluster FTD.

Dopo aver creato un dispositivo FTD, si viene reindirizzati alla finestra Provisioning-nome_dispositivo.


Fare clic sull'icona del dispositivo per avviare la configurazione come mostrato nell'immagine.

Overview Interfaces **Logical Devices** Security Modules Platform Settings System Tools Help admin

Provisioning - FTD_cluster
Clustered | Cisco Firepower Threat Defense | 6.0.1.1213

Data Ports

- Ethernet1/2
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet3/1
- Ethernet3/2
- Ethernet3/3
- Ethernet3/4
- Port-channel5

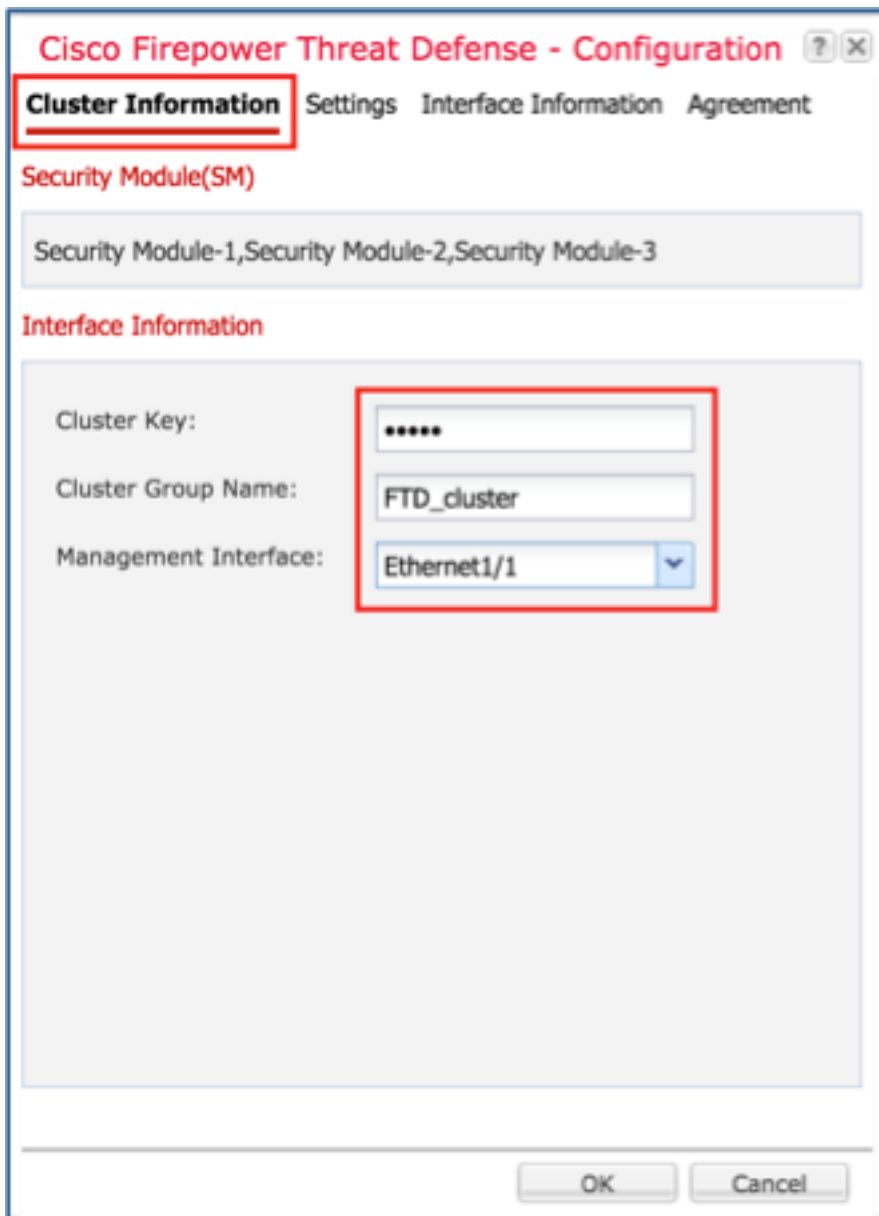


FTD - 6.0.1.1213
Security Module 1,2,3

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	FTD	6.0.1.1213				
Security Module 2	FTD	6.0.1.1213				
Security Module 3	FTD	6.0.1.1213				

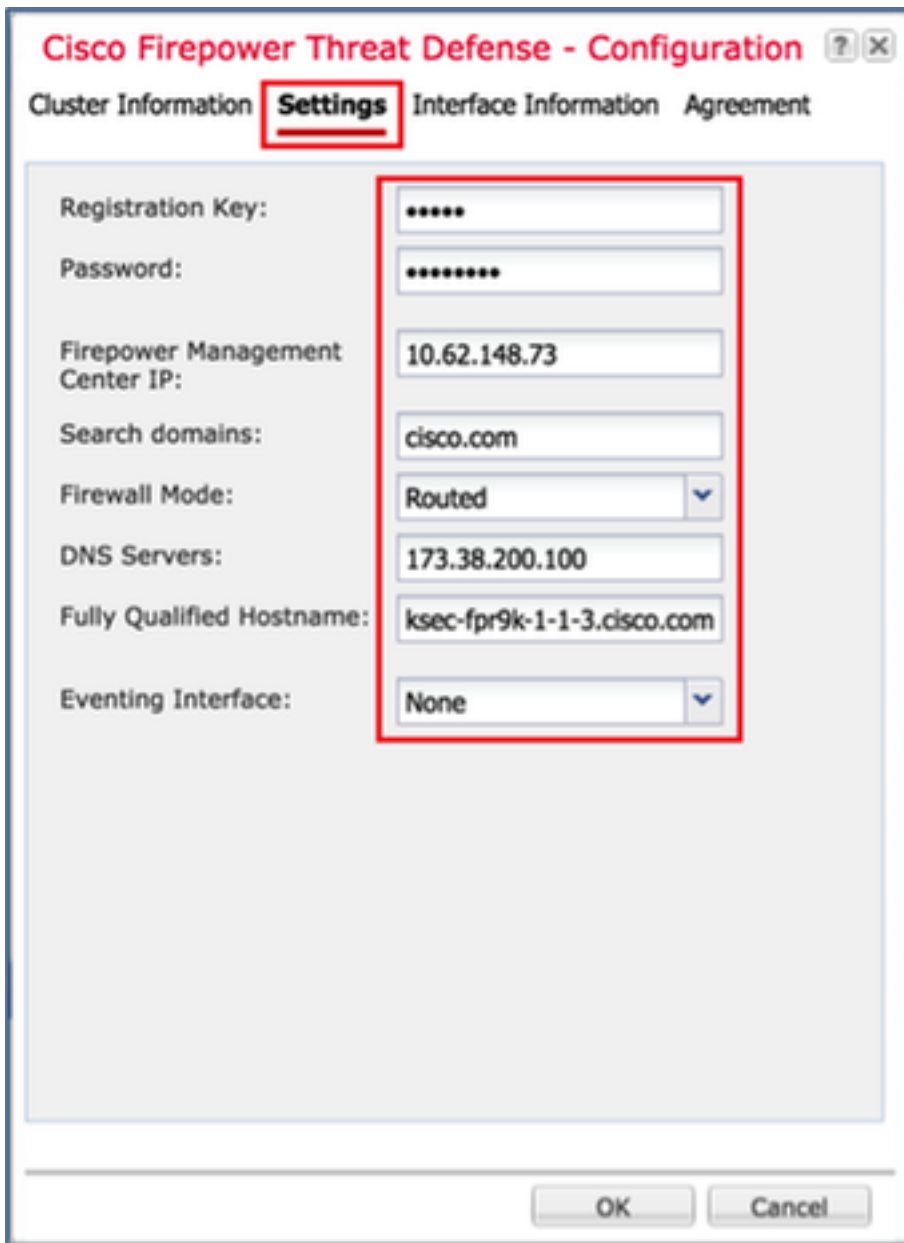
Configurare la scheda **Informazioni cluster** FTD con queste impostazioni e come mostrato nell'immagine.

Chiave cluster	cisco
Nome gruppo cluster	FTD_cluster
Interfaccia di gestione	Ethernet 1/1



Configurare la scheda **Impostazioni** FTD con queste impostazioni e come mostrato nell'immagine.

Chiave di registrazione	cisco
Password	Admin123
IP di Firepower Management Center	10.62.148.73
Cerca domini	cisco.com
Modalità firewall	Stesura
Server DNS	173.38.200.100
Nome host completo	ksec-fpr9k-1-1-3.cisco.com
Interfaccia eventi	Nessuna



Configurare la scheda **Informazioni interfaccia** FTD con queste impostazioni e come mostrato nell'immagine.

Tipo di indirizzo	Solo IPv4
Modulo di sicurezza 1	
IP di gestione	10.62.148.67
Network mask	255.255.255.128
Gateway	10.62.148.1
Modulo di sicurezza 2	
IP di gestione	10.62.148.68
Network mask	255.255.255.128
Gateway	10.62.148.1
Modulo di sicurezza 3	
IP di gestione	10.62.148.69
Network mask	255.255.255.128
Gateway	10.62.148.1

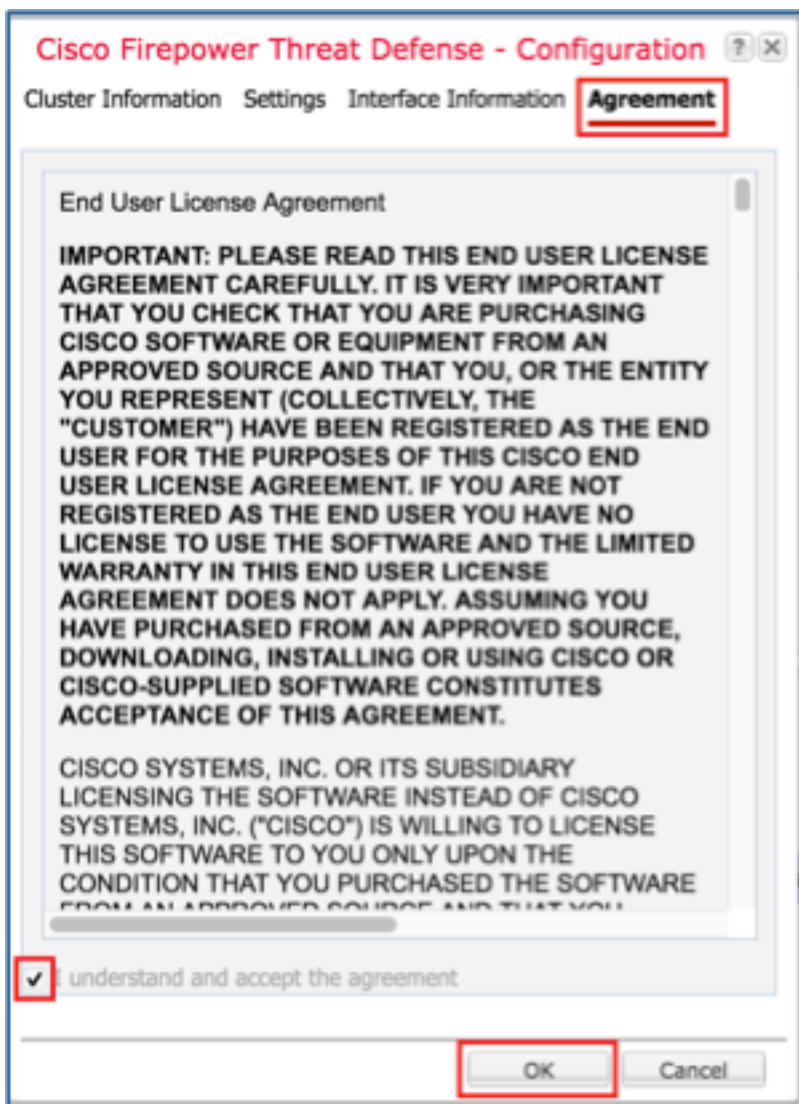
Cisco Firepower Threat Defense - Configuration ? ×

Cluster Information Settings **Interface Information** Agreement

Address Type:	IPv4 only ▼
Security Module 1 IPv4	
Management IP:	10.62.148.67
Network Mask:	255.255.255.128
Gateway:	10.62.148.1
Security Module 2 IPv4	
Management IP:	10.62.148.68
Network Mask:	255.255.255.128
Gateway:	10.62.148.1
Security Module 3 IPv4	
Management IP:	10.62.148.69
Network Mask:	255.255.255.128
Gateway:	10.62.148.1

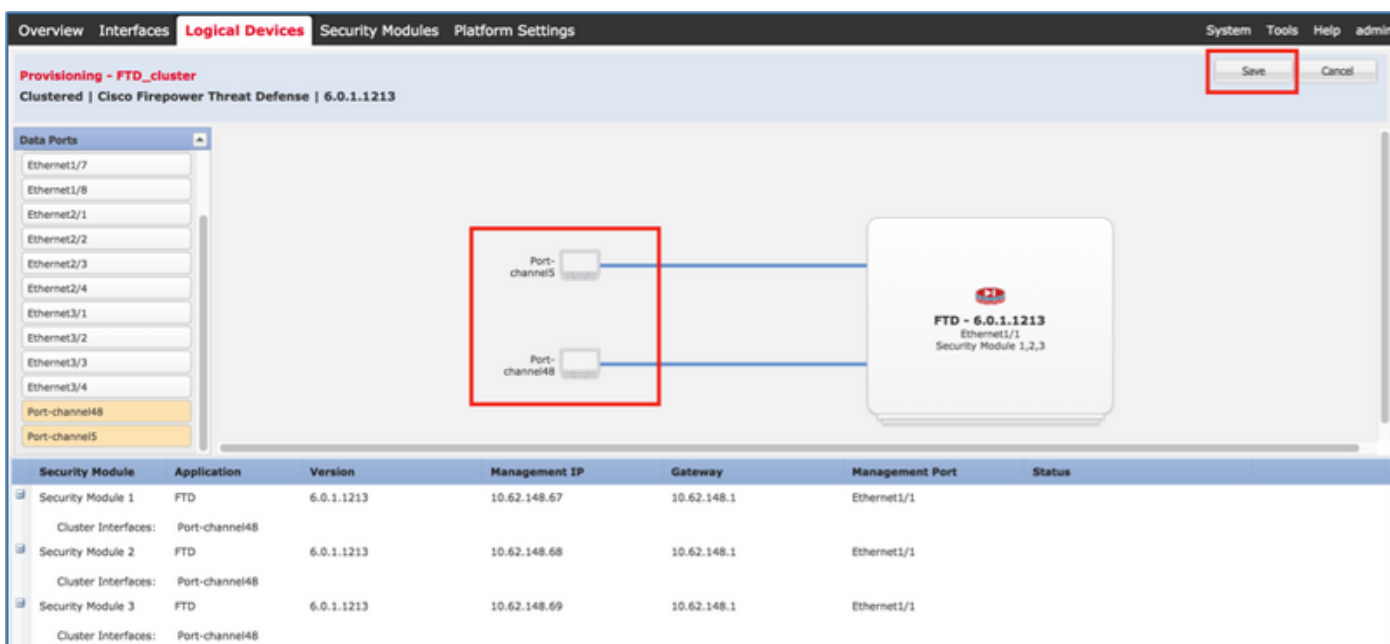
OK Cancel

Accettare il contratto nella scheda **Contratto** e fare clic su **OK**, come illustrato nell'immagine.



Passaggio 3. Assegnare le interfacce dati a FTD.

Espandere l'area Porte dati e fare clic su ciascuna interfaccia che si desidera assegnare a FTD. Al termine, selezionare **Salva** per creare un cluster FTD come mostrato nell'immagine.

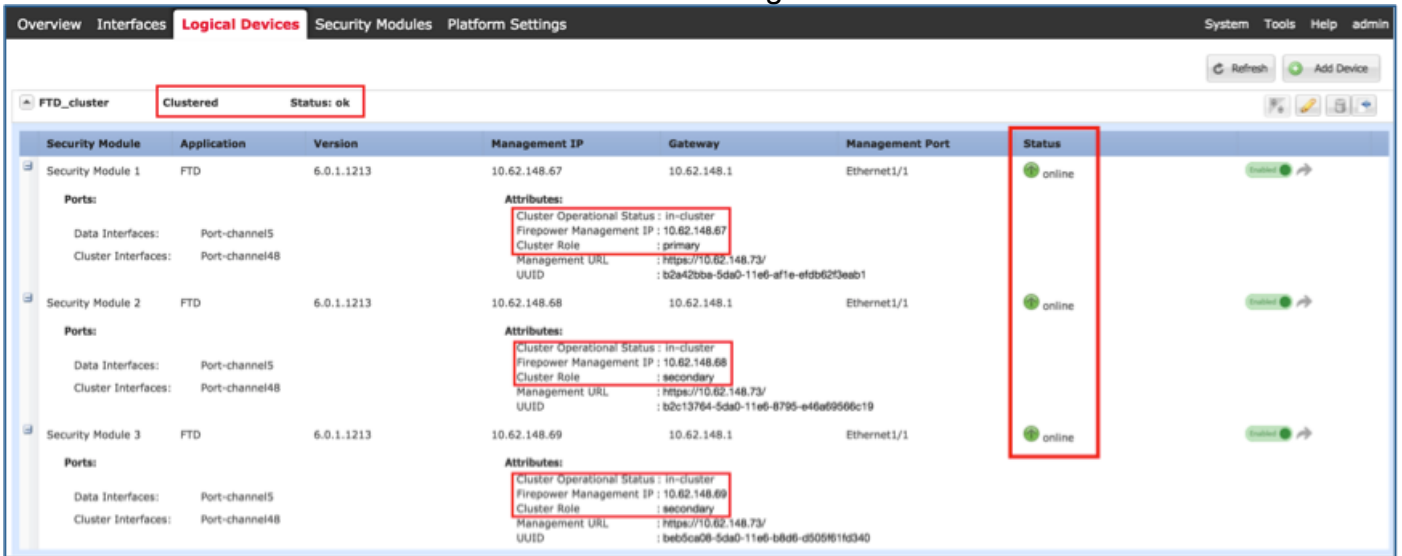


Attendere alcuni minuti prima di distribuire il cluster, dopodiché verrà eseguita la scelta dell'unità

master.

Verifica:

- Dalla GUI dell'FPR9300 come mostrato nell'immagine.



- Dalla CLI di 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
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					

- Dalla CLI di LINA (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# **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#
```

Attività 3. Registra cluster FTD in FMC

Attività richiesta:

Aggiungere le periferiche logiche al FMC e quindi raggrupparle in un cluster.

Soluzione:

Passaggio 1. Aggiungere dispositivi logici al CCP. A partire dalla versione 6.3 di FMC, è necessario registrare un solo dispositivo FTD (si consiglia di utilizzarlo come dispositivo master). Gli altri FTD vengono rilevati automaticamente dal FMC.

Accedere al FMC e selezionare **Devices > Device Management**, quindi fare clic su **Add Device** (Aggiungi dispositivo).

Aggiungere la prima periferica logica con le impostazioni indicate nell'immagine.

Fare clic su **Register** (Registrali) per avviare la registrazione.

Add Device ? X

Host: 10.62.148.67

Display Name: FTD1

Registration Key: cisco

Group: None

Access Control Policy: FTD9300

Smart Licensing

Malware:

Threat:

URL Filtering:

Advanced

i On version 5.4 devices or earlier, the licensing options will need to be specified from [licensing page](#).

Register Cancel

La verifica è come mostrato nell'immagine.

FTD_cluster		Cisco Firepower 9000 Series SM-36 Threat Defense Cluster		
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	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

Attività 4. Configurazione delle sottointerfacce porta-canale su FMC

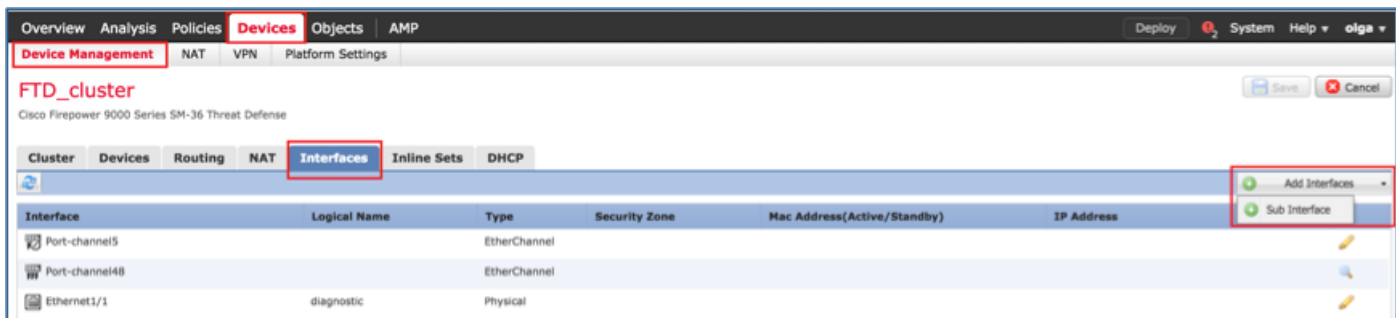
Attività richiesta:

Configurare le sottointerfacce per l'interfaccia dati del canale porta.

Soluzione:

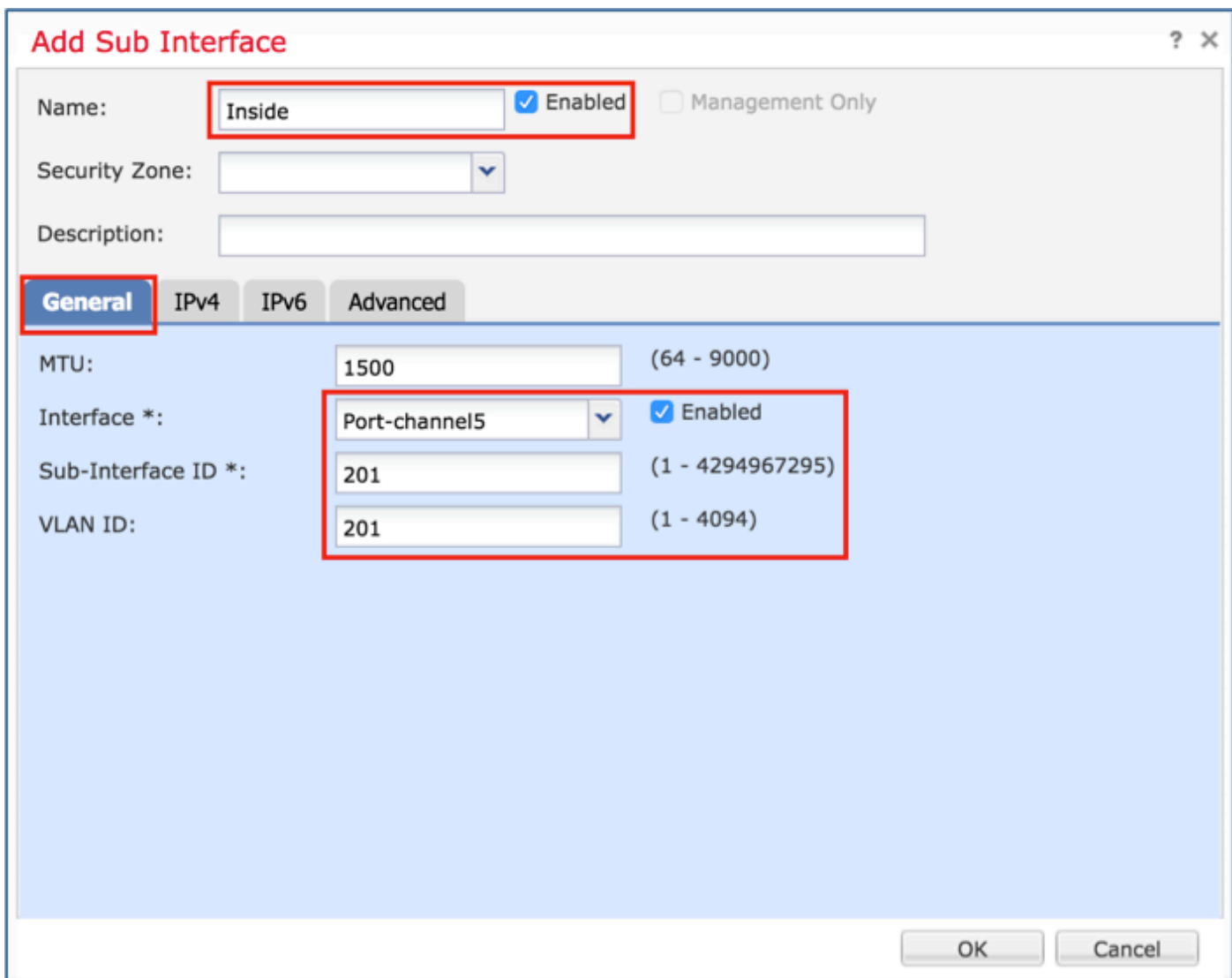
Passaggio 1. Dall'interfaccia utente di FMC, selezionare il pulsante **FTD_cluster Edit**.

Passare alla scheda Interfacce e fare clic su **Add Interfaces > Sub Interface** come mostrato nell'immagine.



Configurare la prima sottointerfaccia con questi dettagli. Selezionate OK per applicare le modifiche e come mostrato nelle immagini.

Nome Interno
Scheda Generale
 Interfaccia Port-channel5
 ID sottointerfaccia 201
 ID VLAN 201
Scheda IPv4
 Tipo IP Usa IP statico
 Indirizzo IP 192.168.75.10/24



Add Sub Interface ? X

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

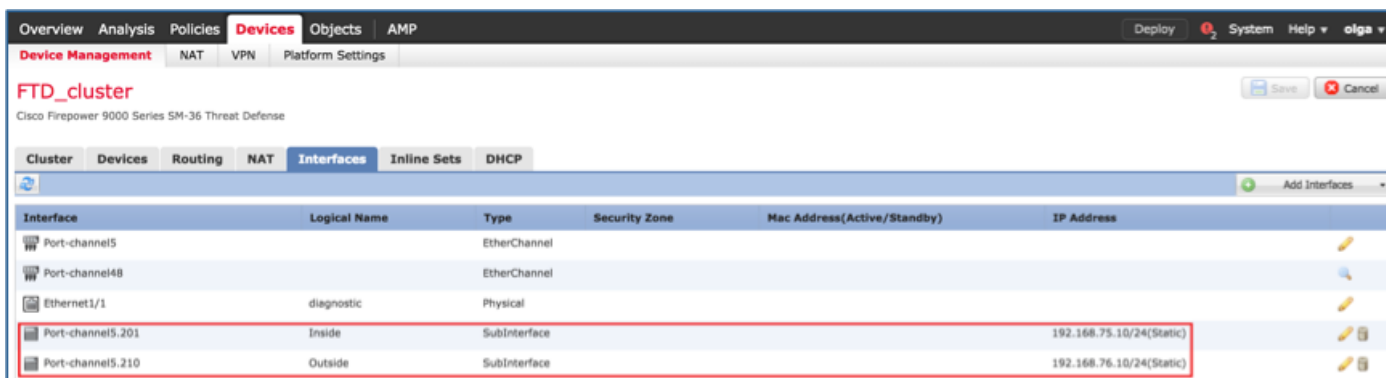
OK Cancel

Configurare la seconda sottointerfaccia con questi dettagli.

Nome	Esterno
Scheda Generale	
Interfaccia	Port-channel5
ID sottointerfaccia	210
ID VLAN	210
Scheda IPv4	
Tipo IP	Usa IP statico
Indirizzo IP	192.168.76.10/24

Fare clic su **OK** per creare l'interfaccia secondaria. Fare clic su **Save**, quindi su **Deploy changes to the FTD_cluster**, come mostrato nell'immagine.

Verifica:



Attività 5. Verifica della connettività di base

Attività richiesta:

Creare un'acquisizione e controllare la connettività tra due VM.

Soluzione:

Passaggio 1. Creare acquisizioni in tutte le unità cluster.

Passare alla CLI LINA (ASA) dell'unità master e creare clip per le interfacce interna ed esterna.

```

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#
Verifica:

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#
```

Passaggio 2. Eseguire il ping tra VM1 e VM2.

Eseguire il test con 4 pacchetti. Controllare l'output di acquisizione dopo il 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#
```

Eseguire il comando per verificare l'output di acquisizione sull'unità specifica:

```
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#

```

Al termine dell'operazione, eliminare le clip con il comando successivo:

```

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:*****

```

Passaggio 3. Scaricare un file da VM2 a VM1.

VM1 è stato preconfigurato come server FTP, VM2 come client FTP.

Crea nuove clip con queste:

```

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:*****

```

Scaricare il file da VM2 a VM1, utilizzando il client FTP.

Controllare l'output 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
```

Mostra output acquisizione:

```
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

```

Acquisizione cluster dall'interfaccia utente di Gestione chassis

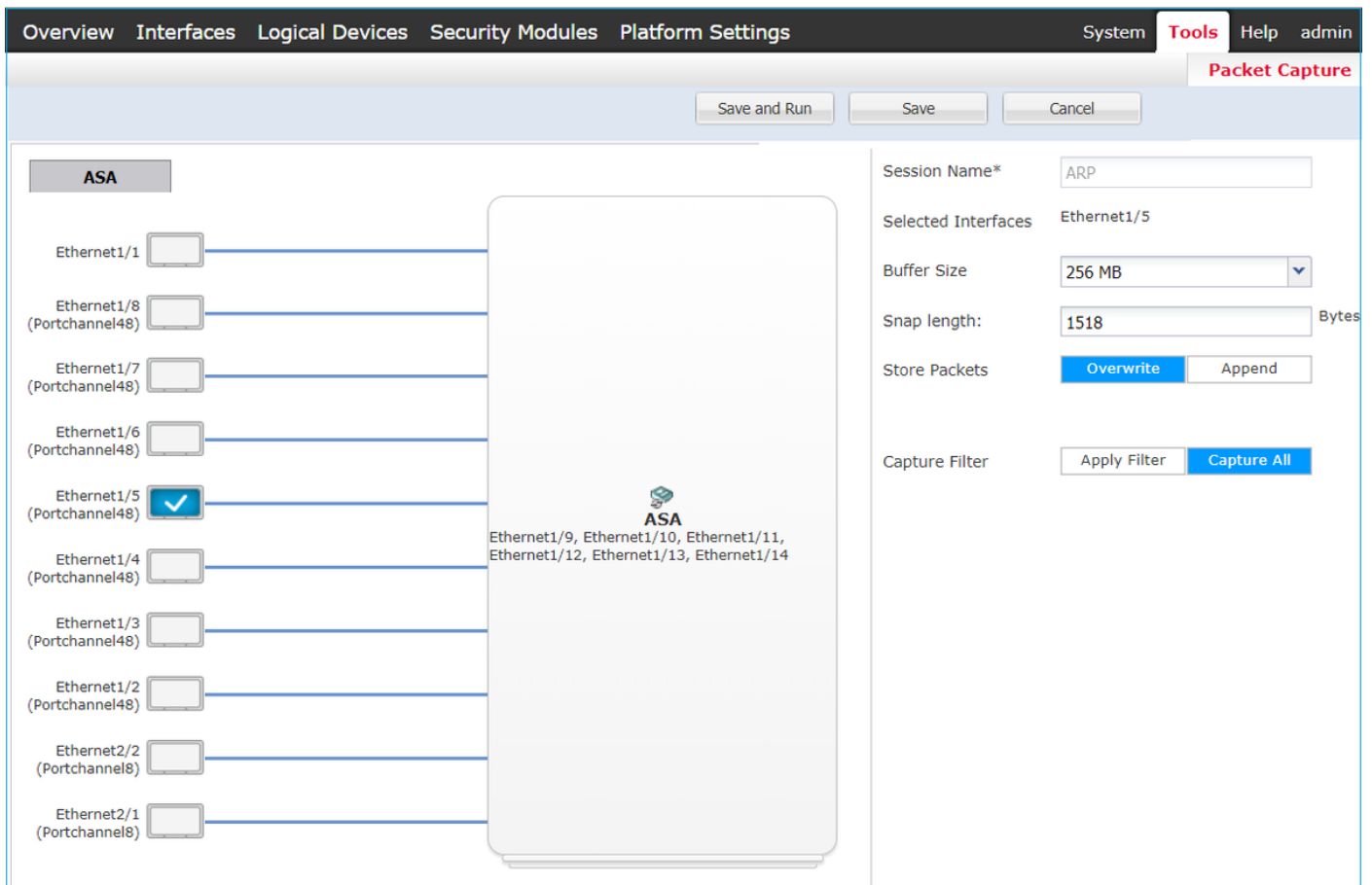
Nell'immagine seguente è illustrato un cluster di 3 unità in FPR9300 con 2 canali porta (8 e 48). Le periferiche logiche sono appliance ASA, ma nel caso di FTD si tratta dello stesso concetto. È importante ricordare che, sebbene esistano **3 unità cluster**, dal punto di vista dell'acquisizione esiste solo **una periferica logica**:

The screenshot displays the 'Logical Devices' section of the Palo Alto Networks management interface. It shows a cluster of three ASA Security Modules. The table below summarizes the key information for each module.

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
Security Module 2	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	online
Security Module 3	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	online

Additional details for each module:

- Ports:** Data Interfaces: Port-channel8; Cluster Interfaces: Port-channel48
- Attributes:** Cluster Operational Status: in-cluster; Management IP VIRTUAL: 10.111.8.206; Cluster Role: master (for SM 1), slave (for SM 2 and 3); Management URL: https://10.111.8.206/; Management IP: 10.111.8.193 (for SM 1), 10.111.8.189 (for SM 2), 10.111.8.190 (for SM 3)



Attività 6. Eliminare un dispositivo slave dal cluster

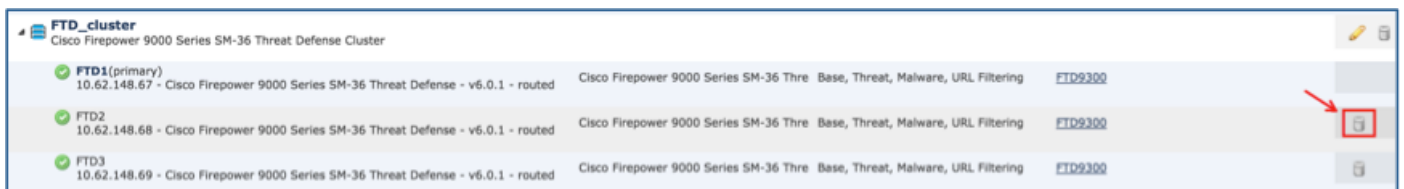
Attività richiesta:

Accedere al CCP ed eliminare l'unità slave dal cluster.

Soluzione:

Passaggio 1. Accedere al FMC e selezionare **Device > Device Management** (Gestione dispositivi).

Fare clic sull'icona del cestino accanto all'unità slave, come mostrato nell'immagine.



Viene visualizzata la finestra di conferma. Selezionare **Sì** per confermare come mostrato nell'immagine.



Verifica:

- Dal CCP come illustrato nell'immagine.



- Dalla CLI di FXOS.

```
FPR9K-1-A# scope ssa
FPR9K-1-A /ssa # show app-instance
```

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup
ftd	1	Enabled	Online	6.0.1.1213	6.0.1.1213
ftd	2	Enabled	Online	6.0.1.1213	6.0.1.1213
ftd	3	Enabled	Online	6.0.1.1213	6.0.1.1213

- Dalla CLI di LINA (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#

Nota: La registrazione del dispositivo è stata annullata dal FMC, ma il dispositivo è ancora un membro del cluster nel FPR9300.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

La verifica è completata e trattata in singoli compiti.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Tutte le versioni della guida alla configurazione di Cisco Firepower Management Center sono disponibili qui:

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

- Tutte le versioni delle guide alla configurazione di FXOS Chassis Manager e CLI sono disponibili qui:

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

- Il centro Cisco Global Technical Assistance Center (TAC) consiglia di consultare questa guida grafica per approfondire le conoscenze pratiche della tecnologia di sicurezza dei Cisco Firepower di nuova generazione, inclusi i prodotti menzionati in questo articolo:

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

- Per tutte le note tecniche sulla configurazione e la risoluzione dei problemi relative alle tecnologie Firepower.

<https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>.

- [Documentazione e supporto tecnico – Cisco Systems](#)