

Configuración del agrupamiento de FTD en FP9300 (dentro del chasis)

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Tarea 1. Crear las interfaces necesarias para el clúster de FTD](#)

[Tarea 2. Crear clúster FTD](#)

[Tarea 3. Registrar clúster de FTD en FMC](#)

[Tarea 4. Configuración de las subinterfaces de canal de puerto en FMC](#)

[Tarea 5. Verificar conectividad básica](#)

[Captura de clúster desde la interfaz de usuario del administrador de chasis](#)

[Tarea 6. Eliminar un dispositivo esclavo del clúster](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar y verificar la función de clúster en el dispositivo FPR9300.

Precaución: La información proporcionada en este documento abarca la instalación/configuración inicial del clúster. Este documento no es aplicable a un procedimiento de reemplazo de unidades (Autorización de devolución de mercancía - RMA)

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad Cisco Firepower 9300 que ejecuta 1.1(4.95)
- Firepower Threat Defense (FTD) que ejecuta 6.0.1 (compilación 1213)
- FireSIGHT Management Center (FMC) que ejecuta 6.0.1.1 (compilación 1023)

Tiempo de finalización del laboratorio: 1 hora.

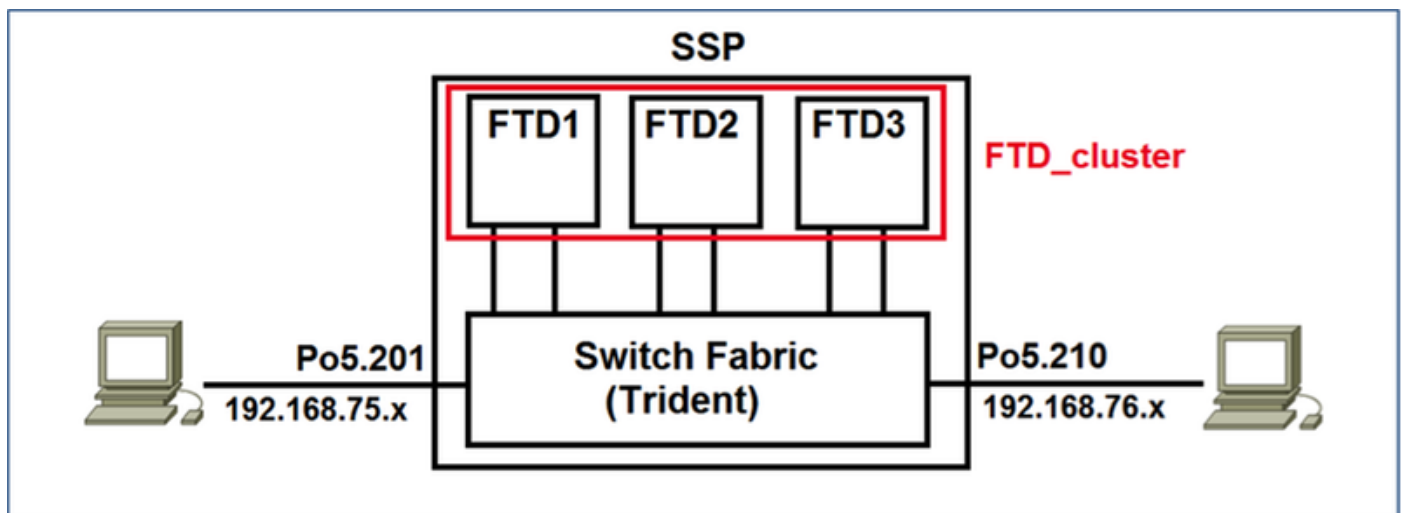
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

- En el FPR9300 con el dispositivo FTD, puede configurar la agrupación en clústeres dentro del chasis en todas las versiones compatibles.
- La agrupación en clúster entre chasis se introdujo en la versión 6.2.
- El canal de puerto 48 se crea como un link de control de clúster. Para la agrupación en clúster dentro del chasis, este enlace utiliza la placa de interconexiones Firepower 9300 para las comunicaciones en clúster.
- No se soportan interfaces de datos individuales, con la excepción de una interfaz de administración.
- La interfaz de administración se asigna a todas las unidades del clúster.

Configurar

Diagrama de la red



Tarea 1. Crear las interfaces necesarias para el clúster de FTD

Requisito de tarea:

Cree un clúster, una interfaz de administración y una interfaz de datos de canal de puerto.

Solución:

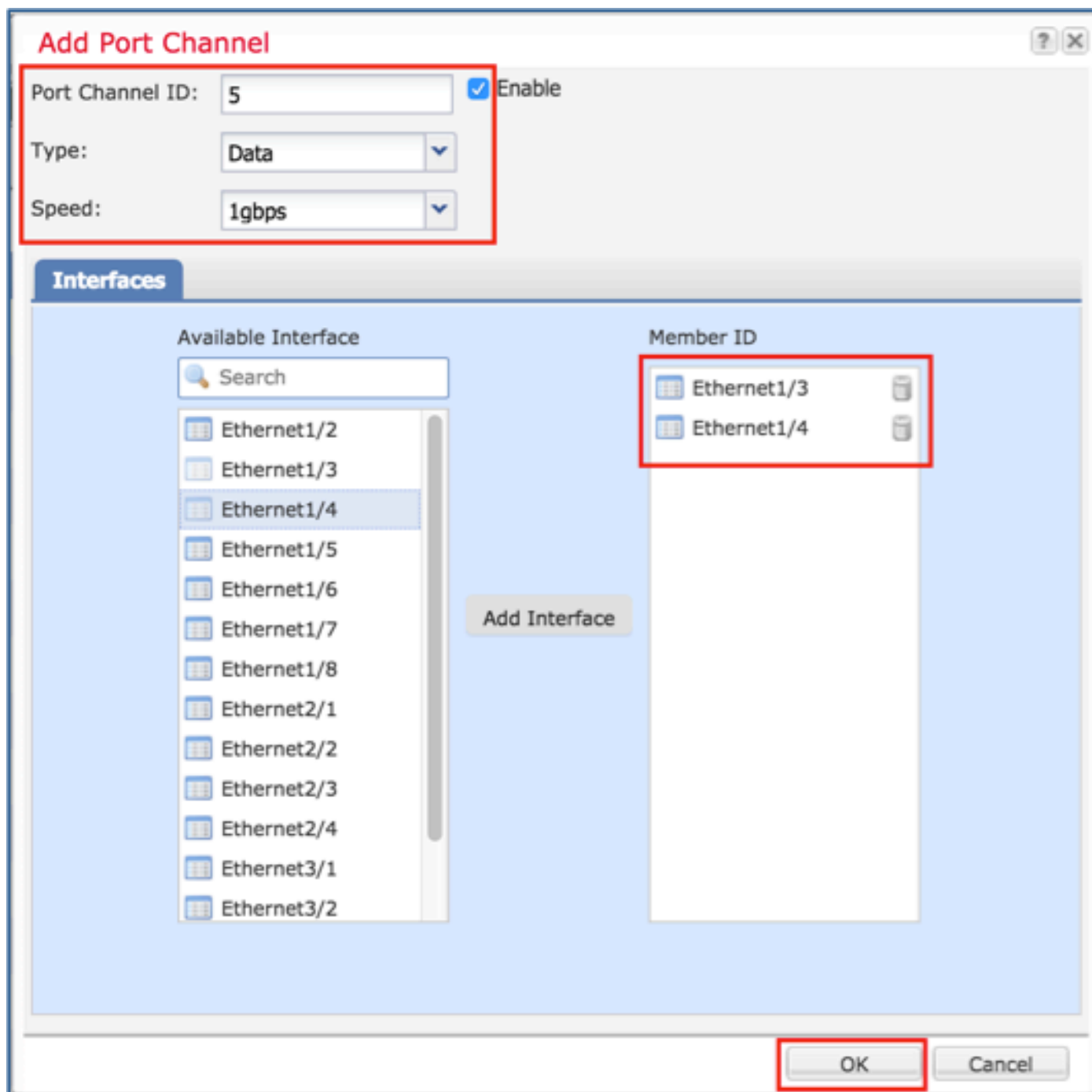
Paso 1. Cree una interfaz de datos de canal de puerto.

Para crear una nueva interfaz, debe iniciar sesión en FPR9300 Chassis Manager y navegar a la pestaña **Interfaces**.

Seleccione **Add Port Channel** y cree una nueva interfaz de canal de puerto con estos parámetros:

ID de canal de puerto	5
Tipo	Datos
Habilitar	Yes
ID de miembro	Ethernet1/3, Ethernet 1/4

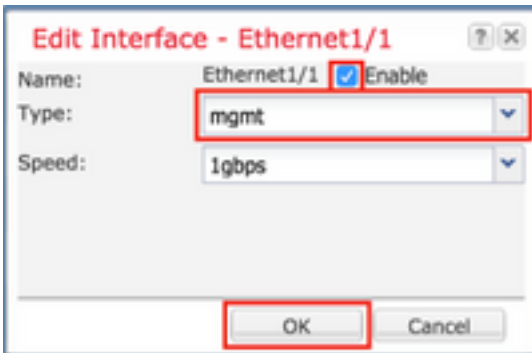
Seleccione **OK** para guardar la configuración como se muestra en la imagen.



Paso 2. Cree una interfaz de administración.

En la pestaña **Interfaces**, elija la interfaz, haga clic en **Edit** y configure la interfaz Management Type.

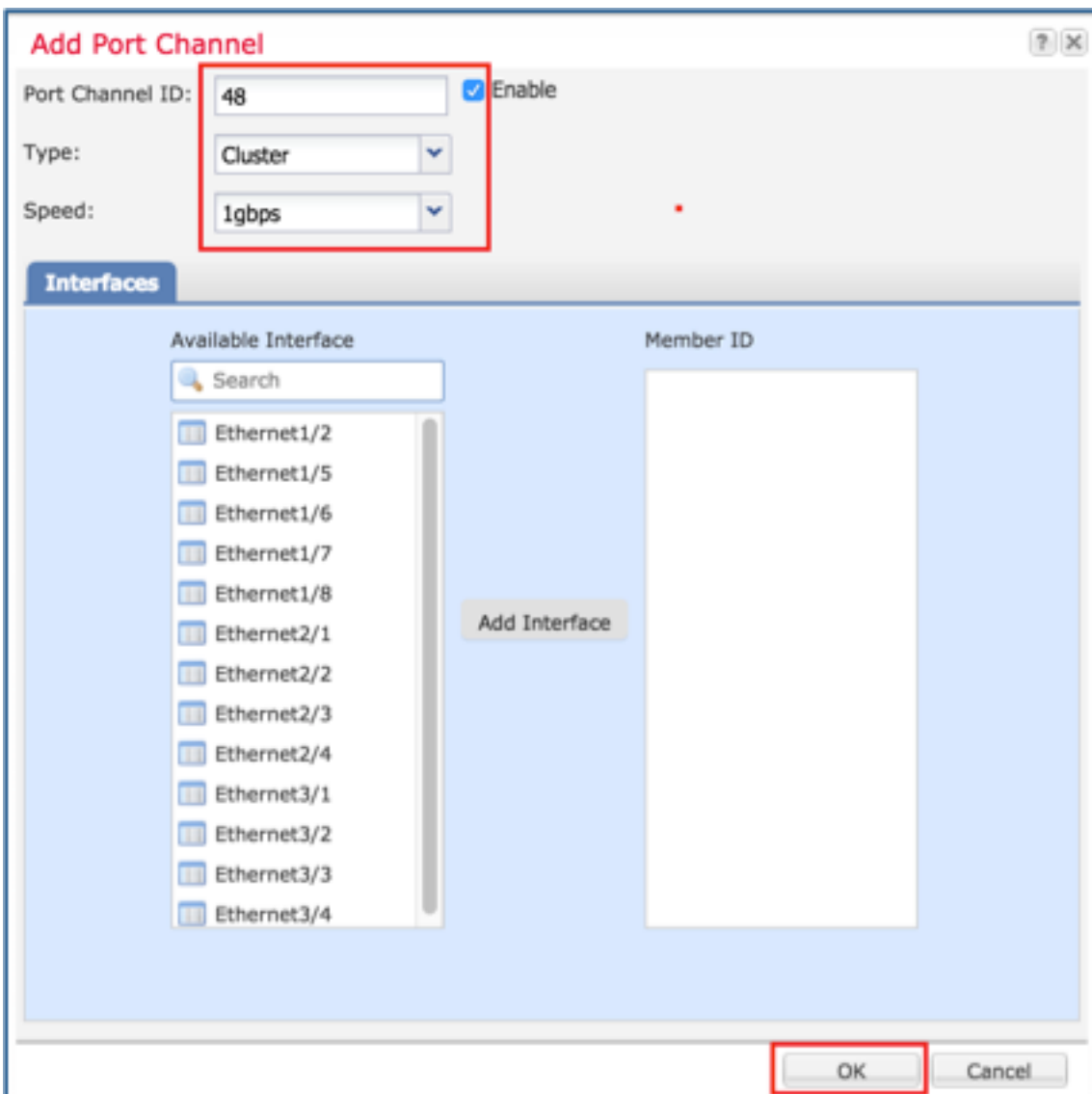
Haga clic en **Aceptar** para guardar la configuración como se muestra en la imagen.



Paso 3. Cree la interfaz de link de control de clúster.

Haga clic en el botón **Add Port Channel** y cree una nueva interfaz de canal de puerto con estos parámetros y como se muestra en la imagen.

ID de canal de puerto	48
Tipo	Clúster
Habilitar	Yes
ID de miembro	-



Tarea 2. Crear clúster FTD

Requisito de tarea:

Cree una unidad de clúster de FTD.

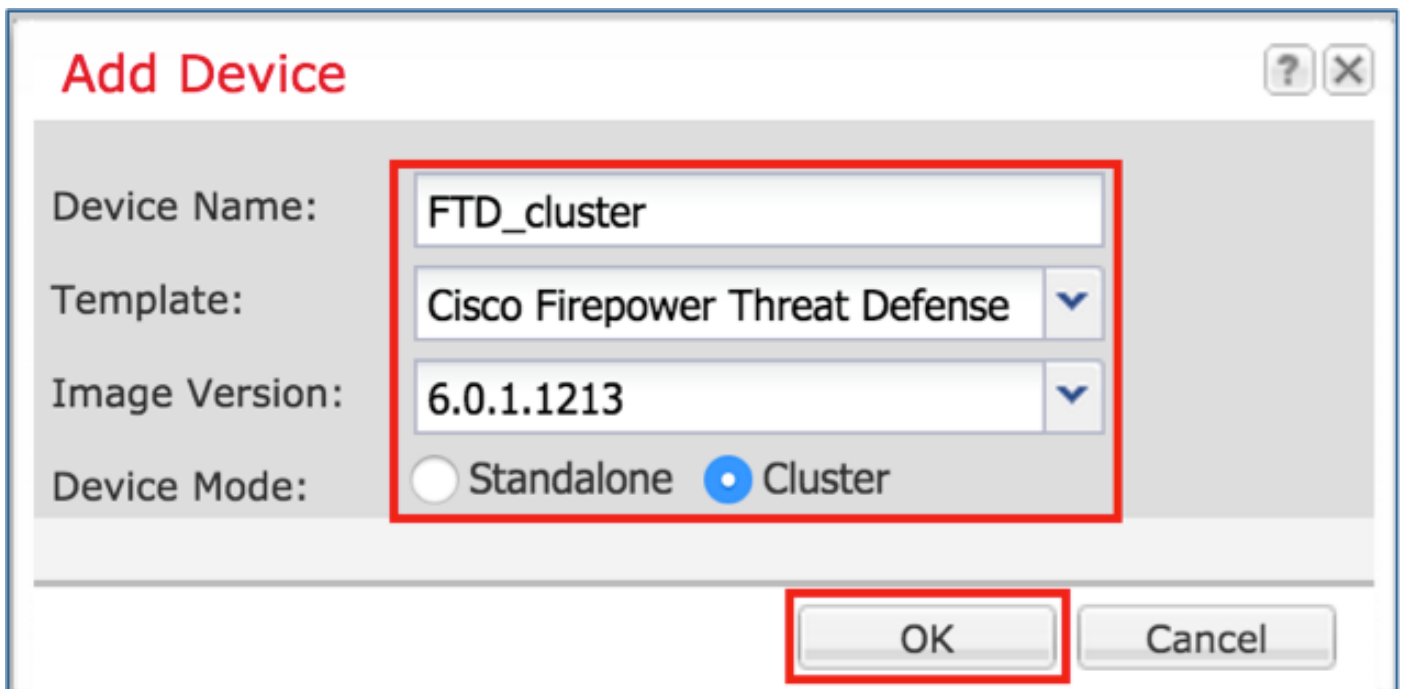
Solución:

Paso 1. Navegue hasta **Dispositivos lógicos** y haga clic en el **botón Agregar dispositivo**.

Cree el agrupamiento FTD de la siguiente manera:

Nombre del dispositivo	FTD_cluster
Plantilla	Defensa frente a amenazas Cisco Firepower
Versión de imagen	6.0.1.1213
Modo de dispositivo	Clúster

Para agregar el dispositivo, haga clic en **Aceptar** como se muestra en la imagen.



Add Device

Device Name: FTD_cluster

Template: Cisco Firepower Threat Defense

Image Version: 6.0.1.1213

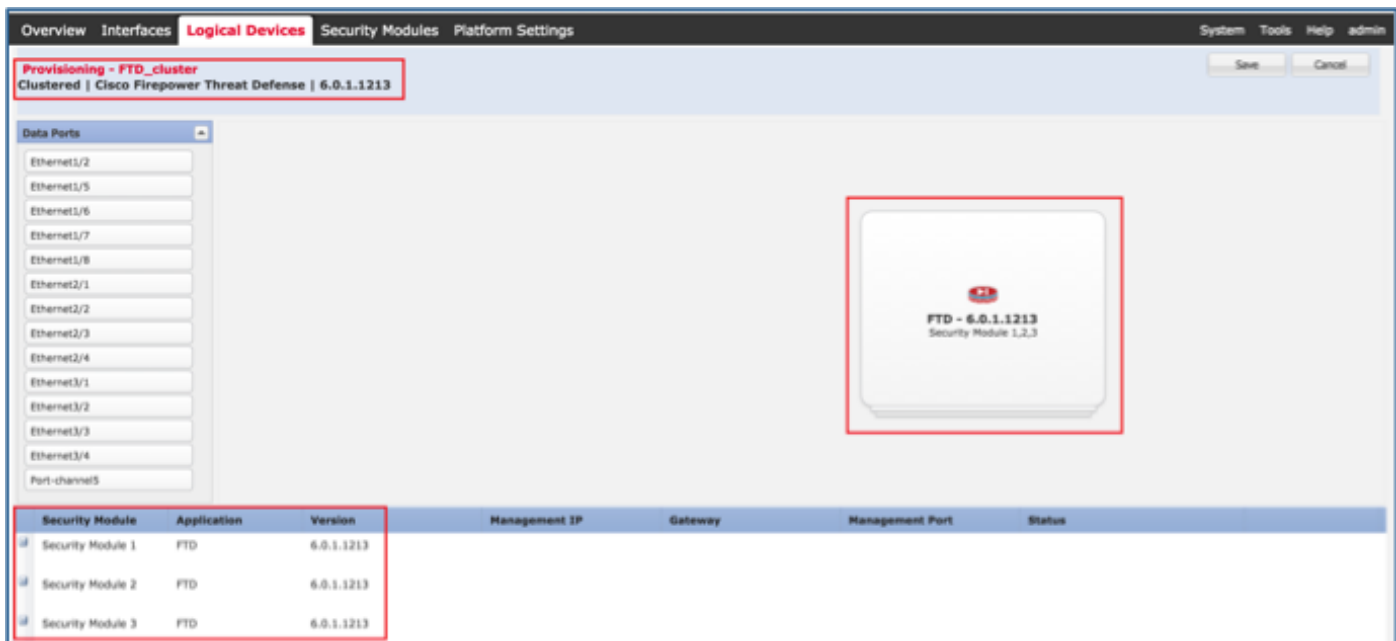
Device Mode: Standalone Cluster

OK Cancel

Paso 2. Configure e implemente el clúster de FTD.

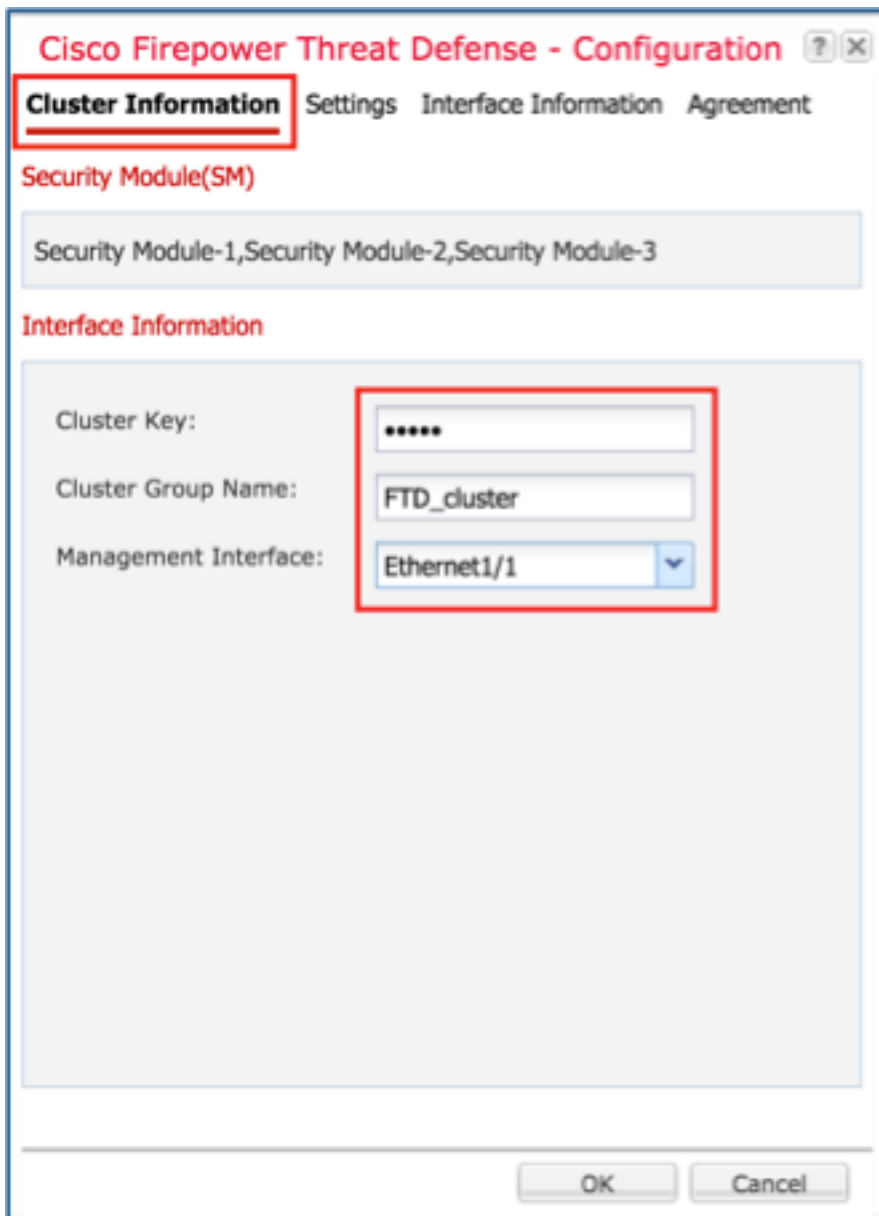
Después de crear un dispositivo FTD, se le redirige a la ventana Provisioning- device_name.

Haga clic en el icono del dispositivo para iniciar la configuración como se muestra en la imagen.



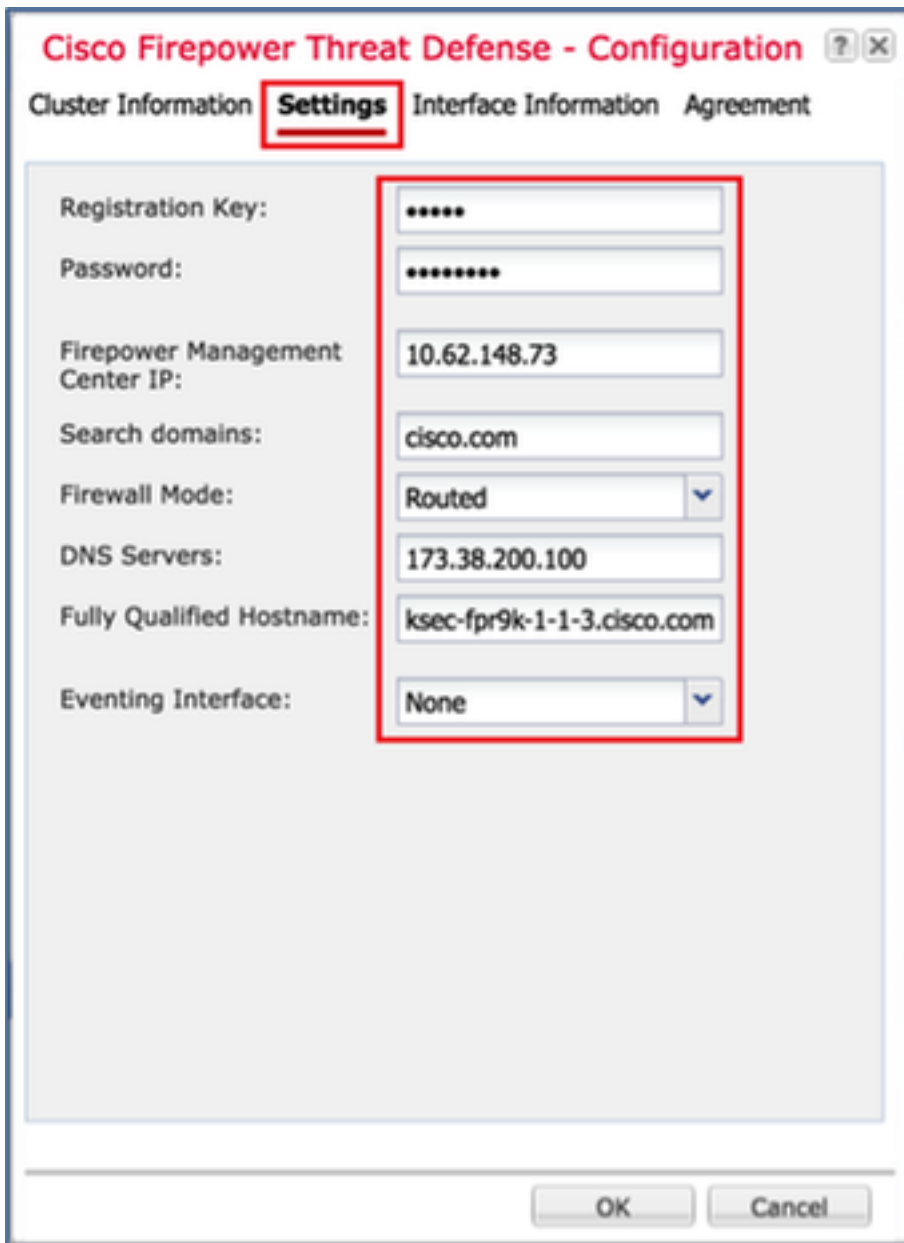
Configure la ficha **Información del clúster** FTD con estos parámetros y como se muestra en la imagen.

Clave de clúster	Cisco
Nombre del grupo de clústeres	FTD_cluster
Interfaz de administración	Ethernet1/1



Configure la ficha **Configuración de FTD** con estos parámetros y como se muestra en la imagen.

Clave de registro	Cisco
Contraseña	Admin123
IP del centro de administración de Firepower	10.62.148.73
Buscar dominios	cisco.com
Modo Firewall	Enrutado
Servidores DNS	173.38.200.100
Nombre de host completamente calificado	ksec-fpr9k-1-1-3.cisco.com
Interfaz de eventos	Ninguno



Configure la ficha **Información de interfaz** FTD con estos parámetros y como se muestra en la imagen.

Tipo de dirección	Sólo IPv4
Módulo de seguridad 1	
IP de administración	10.62.148.67
Máscara de red	255.255.255.128
Gateway	10.62.148.1
Módulo de seguridad 2	
IP de administración	10.62.148.68
Máscara de red	255.255.255.128
Gateway	10.62.148.1
Módulo de seguridad 3	
IP de administración	10.62.148.69
Máscara de red	255.255.255.128
Gateway	10.62.148.1

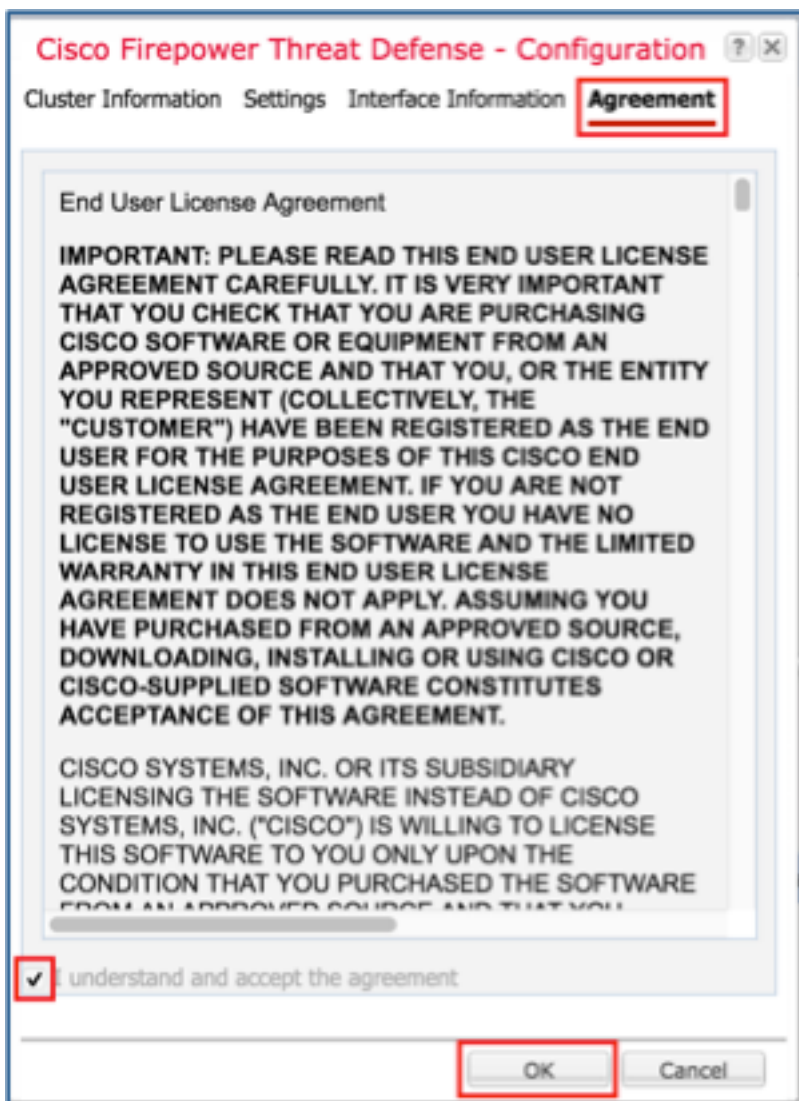
Cisco Firepower Threat Defense - Configuration ? ×

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

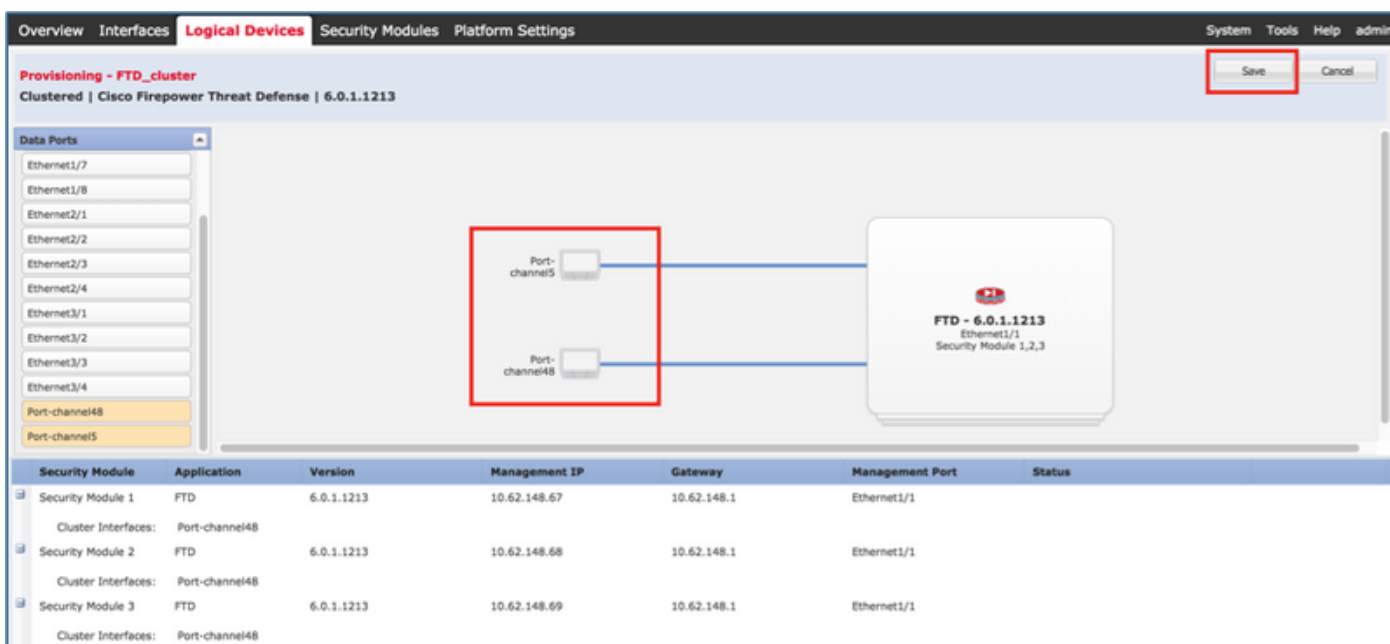
OK Cancel

Acepte el Acuerdo en la pestaña **Acuerdo** y haga clic en **Aceptar** como se muestra en la imagen.



Paso 3. Asignar interfaces de datos a FTD.

Expanda el área Puertos de datos y haga clic en cada interfaz que desee asignar a FTD. Después de finalizar, seleccione **Guardar** para crear un clúster FTD como se muestra en la imagen.



Espere unos minutos hasta que se implemente el clúster, después de lo cual se produce la

elección de la unidad maestra.

Verificación:

- Desde la GUI de FPR9300 como se muestra en la imagen.



- Desde la 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
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					

- Desde la CLI de 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#

```

Tarea 3. Registrar clúster de FTD en FMC

Requisito de tarea:

Agregue los dispositivos lógicos al FMC y, a continuación, agruparlos en un clúster.

Solución:

Paso 1. Agregue dispositivos lógicos al FMC. A partir de la versión 6.3 de FMC, sólo debe registrar un dispositivo FTD (recomendado para ser el maestro). El FMC detecta automáticamente el resto de los FTD.

Inicie sesión en el FMC y navegue hasta la pestaña **Devices > Device Management** y haga clic en **Add Device**.

Agregue el primer dispositivo lógico con la configuración mencionada en la imagen.

Haga clic en **Registrarse** para iniciar el registro.

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 verificación es como se muestra en la imagen.

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

Tarea 4. Configuración de las subinterfaces de canal de puerto en FMC

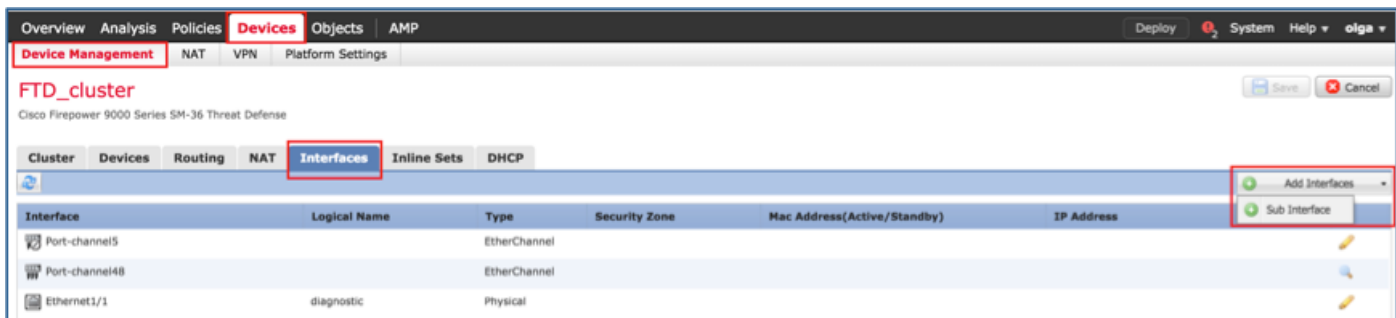
Requisito de tarea:

Configure las subinterfaces para la interfaz de datos de canal de puerto.

Solución:

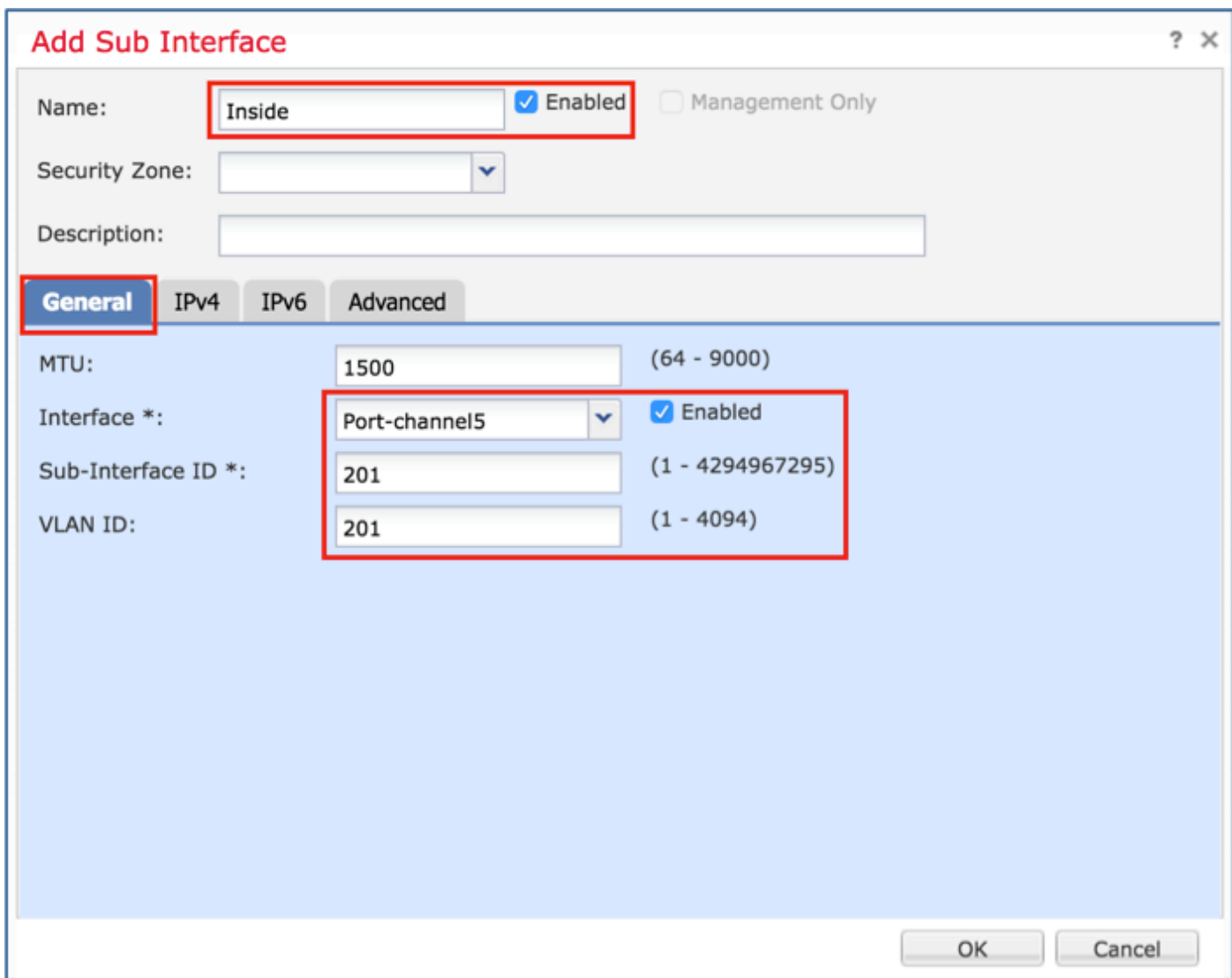
Paso 1. Desde la GUI de FMC, seleccione el botón **FTD_cluster Edit**.

Navegue hasta la pestaña Interfaces y haga clic en la **Subinterfaz Add Interfaces >** como se muestra en la imagen.



Configure la primera subinterfaz con estos detalles. Seleccione **Aceptar** para aplicar los cambios y como se muestra en las imágenes.

Nombre	Dentro
Ficha General	
Interfaz	Port-channel5
ID de subinterfaz	201
ID DE VLAN	201
ficha IPv4	
Tipo de IP	Utilizar IP estática
IP Address	192.168.75.10/24

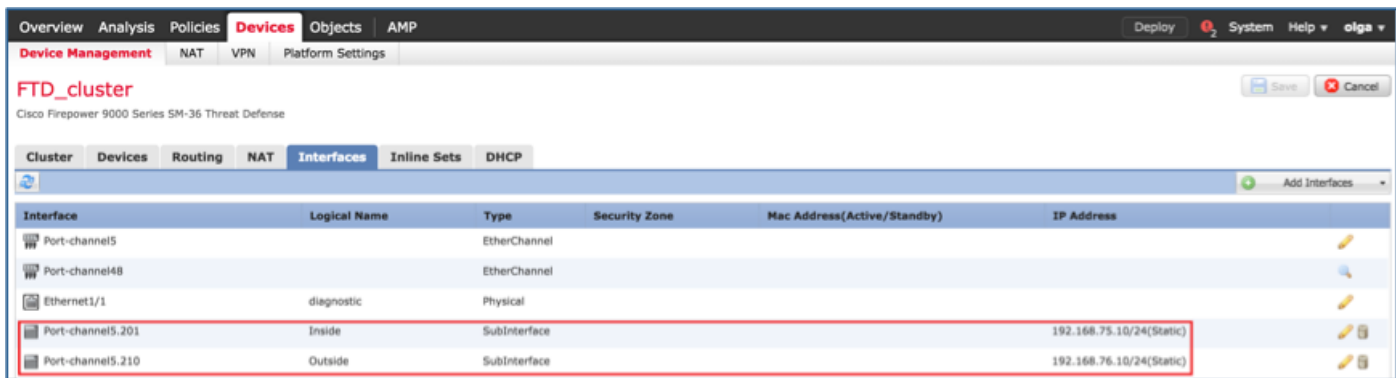


Configure la segunda subinterfaz con estos detalles.

Nombre	Fuera
Ficha General	
Interfaz	Port-channel5
ID de subinterfaz	210
ID DE VLAN	210
ficha IPv4	
Tipo de IP	Utilizar IP estática
IP Address	192.168.76.10/24

Haga clic en **Aceptar** para crear la subinterfaz. Haga clic en **Guardar** y, a continuación, **Implementar** cambios en FTD_cluster como se muestra en la imagen.

Verificación:



Tarea 5. Verificar conectividad básica

Requisito de tarea:

Cree una captura y verifique la conectividad entre dos VM.

Solución:

Paso 1. Cree capturas en todas las unidades de clúster.

Navegue hasta la CLI de LINA (ASA) de la unidad principal y cree capturas para las interfaces interna y externa.

```
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#
```

Verificación:

```
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#
```

Paso 2. Realice la prueba de ping de VM1 a VM2.

Realice la prueba con 4 paquetes. Verifique el resultado de la captura después de la prueba:

```
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#
```

Ejecute el comando para verificar la salida de captura en la unidad específica:

```
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#

```

Después de finalizar esta tarea, elimine las capturas con el siguiente comando:

```

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: *****

```

Paso 3. Descargue un archivo de VM2 a VM1.

VM1 se preconfiguró como servidor FTP, VM2 como cliente FTP.

Cree nuevas capturas con lo siguiente:

```

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: *****

```

Descargue el archivo de VM2 a VM1, con el uso del cliente FTP.

Verifique el resultado 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
```

Mostrar salida de captura:

```
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

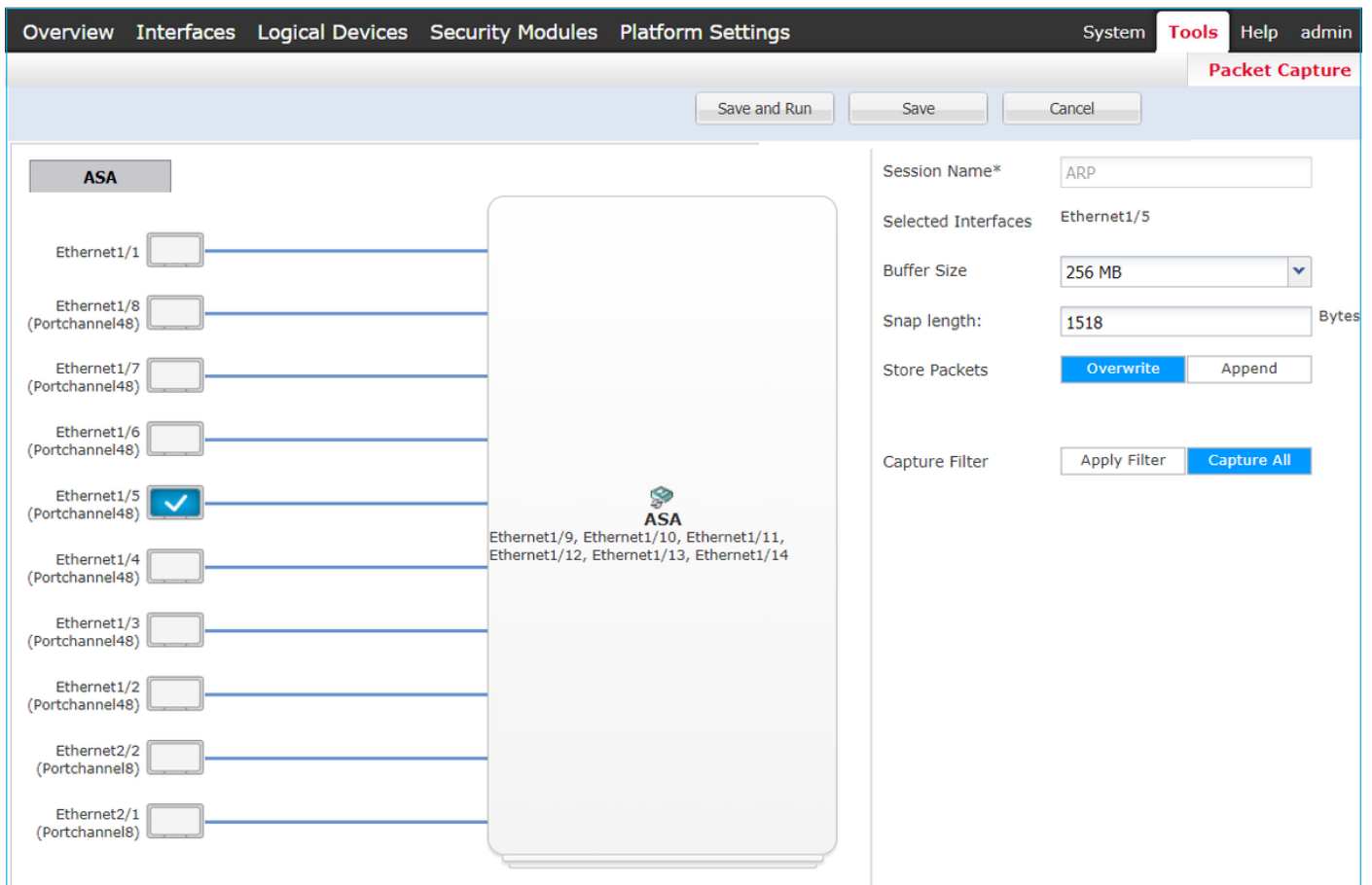
```

Captura de clúster desde la interfaz de usuario del administrador de chasis

En la siguiente imagen puede ver un clúster de 3 unidades en FPR9300 con 2 canales de puerto (8 y 48). Los dispositivos lógicos son ASA, pero en el caso de FTD será el mismo concepto. Lo importante para recordar es que aunque hay **3 unidades de clúster**, desde el punto de vista de la captura sólo hay **un dispositivo lógico**:

The screenshot shows the 'Logical Devices' tab in the chassis administrator. It displays a table of logical devices and their details.

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:		Attributes:				
Data Interfaces:	Port-channel8	Cluster Operational Status: in-cluster				
Cluster Interfaces:	Port-channel48	Management IP VIRTUAL : 10.111.8.206				
		Cluster Role : master				
		Management URL : https://10.111.8.206/				
		Management IP : 10.111.8.193				
Security Module 2	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	online
Ports:		Attributes:				
Data Interfaces:	Port-channel8	Cluster Operational Status: in-cluster				
Cluster Interfaces:	Port-channel48	Management IP VIRTUAL : 10.111.8.206				
		Cluster Role : slave				
		Management URL : https://10.111.8.206/				
		Management IP : 10.111.8.189				
Security Module 3	ASA	9.6.2.7	0.0.0.0	0.0.0.0	Ethernet1/1	online
Ports:		Attributes:				
Data Interfaces:	Port-channel8	Cluster Operational Status: in-cluster				
Cluster Interfaces:	Port-channel48	Management IP VIRTUAL : 10.111.8.206				
		Cluster Role : slave				
		Management URL : https://10.111.8.206/				
		Management IP : 10.111.8.190				



Tarea 6. Eliminar un dispositivo esclavo del clúster

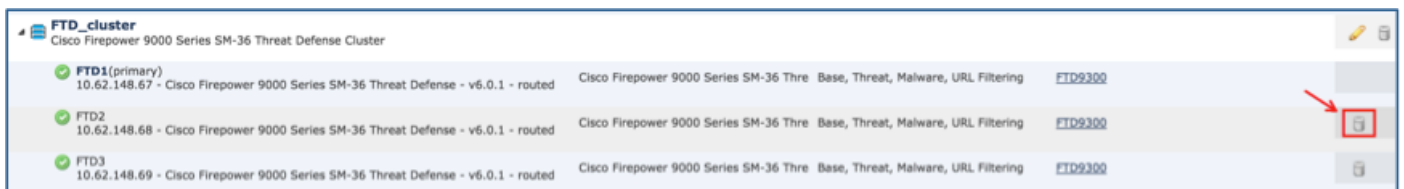
Requisito de tarea:

Inicie sesión en el FMC y elimine la unidad Slave del clúster.

Solución:

Paso 1. Inicie sesión en el FMC y navegue hasta **Device > Device Management**.

Haga clic en el icono de la papelera junto a la unidad Esclavo como se muestra en la imagen.



Aparecerá la ventana de confirmación. Seleccione **Yes** para confirmar como se muestra en la imagen.



Verificación:

- Desde el FMC como se muestra en la imagen.



- Desde la CLI de 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

- Desde la CLI de 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: El dispositivo no estaba registrado en el FMC pero sigue siendo un miembro de clúster en el FPR9300.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

La verificación se completa y abarca en tareas individuales.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Todas las versiones de la guía de configuración de Cisco Firepower Management Center se pueden encontrar aquí:

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

- Todas las versiones de las guías de configuración de la CLI y el administrador de chasis FXOS se pueden encontrar aquí:

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

- Cisco Global Technical Assistance Center (TAC) recomienda encarecidamente esta guía visual para obtener información detallada sobre las tecnologías de seguridad de última generación Cisco Firepower, incluidas las mencionadas en este artículo:

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

- Para todas las notas técnicas de configuración y resolución de problemas que pertenecen a tecnologías Firepower.

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

- [Soporte Técnico y Documentación - Cisco Systems](#)