

Configurer la mise en grappe FTD sur FP9300 (intra-châssis)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Tâche 1. Créer les interfaces nécessaires pour le cluster FTD](#)

[Tâche 2. Créer un cluster FTD](#)

[Tâche 3. Enregistrer le cluster FTD sur FMC](#)

[Tâche 4. Configuration des sous-interfaces Port-Channel sur FMC](#)

[Tâche 5. Vérification de la connectivité de base](#)

[Capture de cluster à partir de l'interface utilisateur du Gestionnaire de châssis](#)

[Tâche 6. Supprimer un périphérique esclave du cluster](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer et vérifier la fonctionnalité de cluster sur le périphérique FPR9300.

Attention : Les informations fournies dans ce document couvrent l'installation/configuration initiale du cluster. Ce document ne s'applique pas à une procédure de remplacement d'unité (autorisation de retour de matériel - RMA)

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité Cisco Firepower 9300 exécutant 1.1(4.95)
- Firepower Threat Defense (FTD) exécutant la version 6.0.1 (build 1213)
- FireSIGHT Management Center (FMC) exécutant 6.0.1.1 (build 1023)

Durée de fin des travaux pratiques : 1 heure.

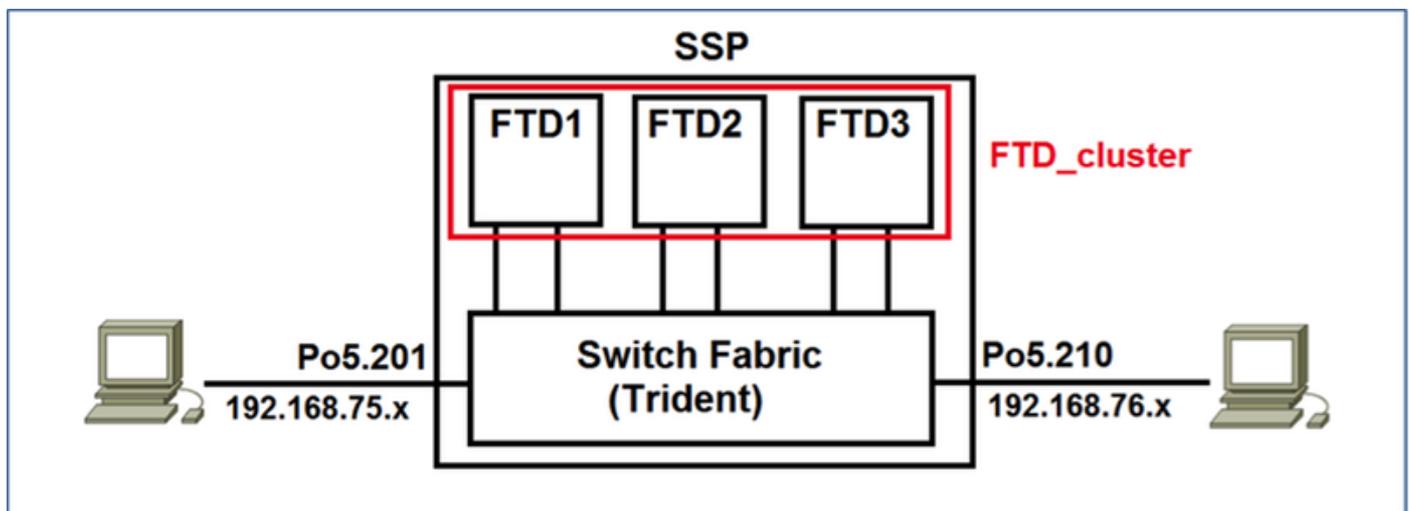
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

- Sur le FPR9300 avec le dispositif FTD, vous pouvez configurer la mise en grappe intra-châssis sur toutes les versions prises en charge.
- La mise en grappe inter-châssis a été introduite dans la version 6.2.
- Port-channel 48 est créé en tant que liaison de contrôle de cluster. Pour la mise en grappe intra-châssis, cette liaison utilise le fond de panier Firepower 9300 pour les communications en grappe.
- Les interfaces de données individuelles ne sont pas prises en charge, à l'exception d'une interface de gestion.
- L'interface de gestion est affectée à toutes les unités du cluster.

Configuration

Diagramme du réseau



Tâche 1. Créer les interfaces nécessaires pour le cluster FTD

Exigence de la tâche :

Créez un cluster, une interface de gestion et une interface de données de canal de port.

Solution :

Étape 1. Créez une interface de données de canal de port.

Pour créer une nouvelle interface, vous devez vous connecter à FPR9300 Chassis Manager et accéder à l'onglet **Interfaces**.

Sélectionnez **Ajouter un canal de port** et créez une interface de canal de port avec les paramètres suivants :

ID de canal de port	5
Type	Données
Activer	Oui
ID membre	Ethernet1/3, Ethernet 1/4

Sélectionnez **OK** pour enregistrer la configuration comme indiqué dans l'image.

Add Port Channel

Port Channel ID: 5 Enable

Type: Data

Speed: 1gbps

Interfaces

Available Interface

Search

- 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

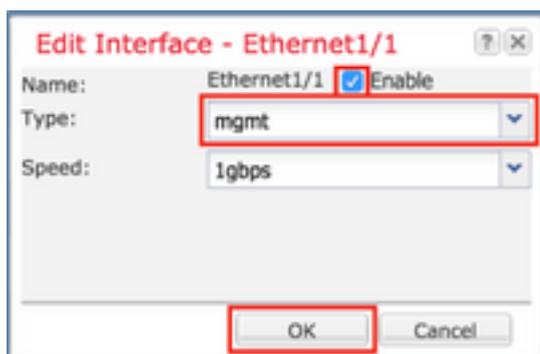
OK Cancel

Étape 2. Créez une interface de gestion.

Dans l'onglet **Interfaces**, sélectionnez l'interface, cliquez sur **Modifier** et configurez l'interface Type

de gestion.

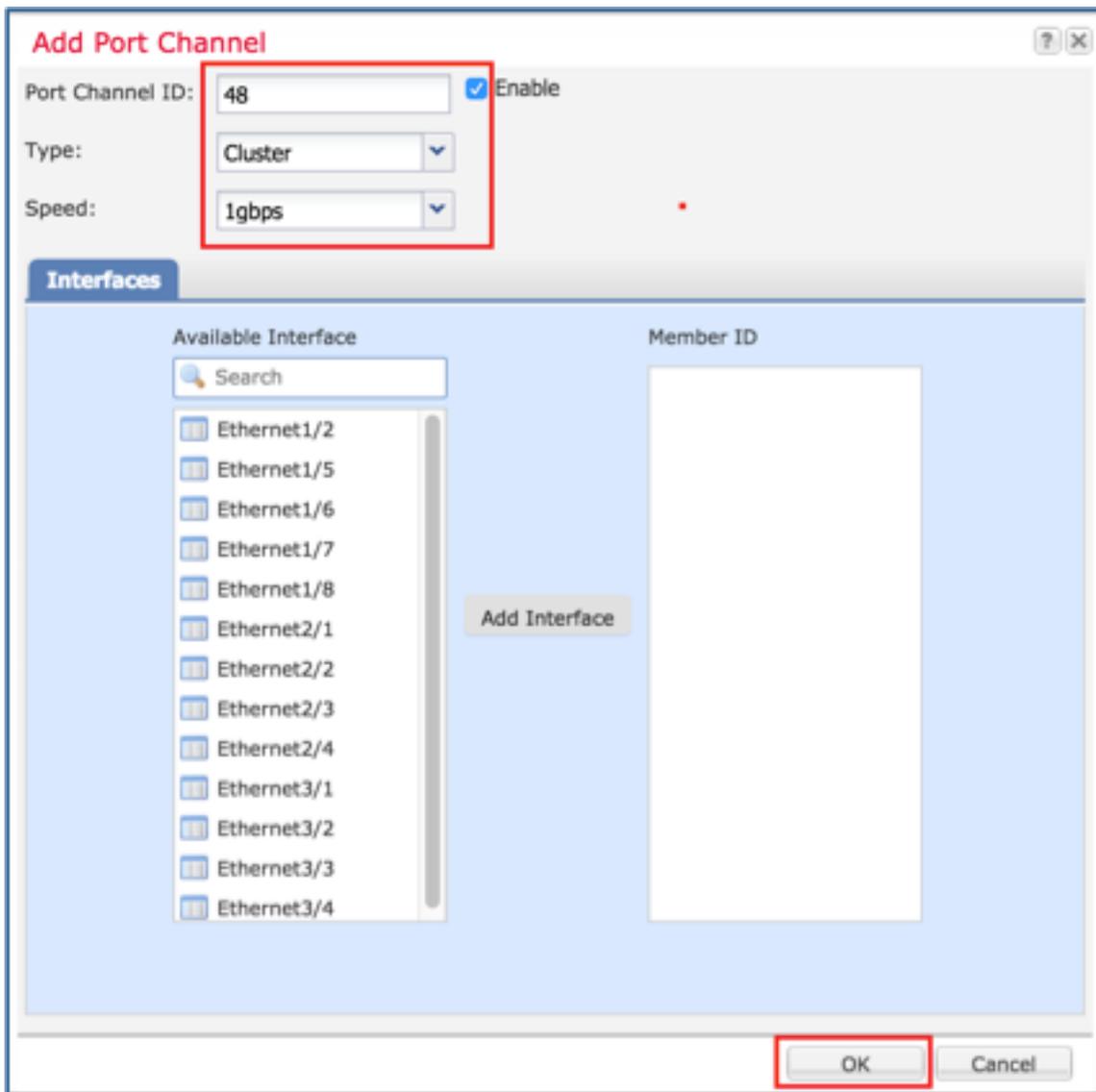
Cliquez sur **OK** pour enregistrer la configuration comme indiqué dans l'image.



Étape 3. Créer une interface de liaison de contrôle de cluster.

Cliquez sur le bouton **Ajouter un canal de port** et créez une nouvelle interface de canal de port avec ces paramètres et comme indiqué dans l'image.

ID de canal de port	48
Type	Grappe
Activer	Oui
ID membre	-



Tâche 2. Créer un cluster FTD

Exigence de la tâche :

Créez une unité de cluster FTD.

Solution :

Étape 1. Accédez à **Périphériques logiques** et cliquez sur le bouton **Ajouter un périphérique**.

Créez la mise en grappe FTD comme suit :

Nom du périphérique	FTD_cluster
Modèle	Cisco Firepower Threat Defense
Version de l'image	6.0.1.1213
Mode Périphérique	Grappe

Pour ajouter le périphérique, cliquez sur **OK** comme indiqué dans l'image.

Add Device

Device Name:

Template:

Image Version:

Device Mode: Standalone Cluster

Étape 2. Configurer et déployer le cluster FTD.

Après avoir créé un périphérique FTD, vous êtes redirigé vers la fenêtre Provisioning-device_name.

Cliquez sur l'icône du périphérique pour démarrer la configuration comme indiqué dans l'image.

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

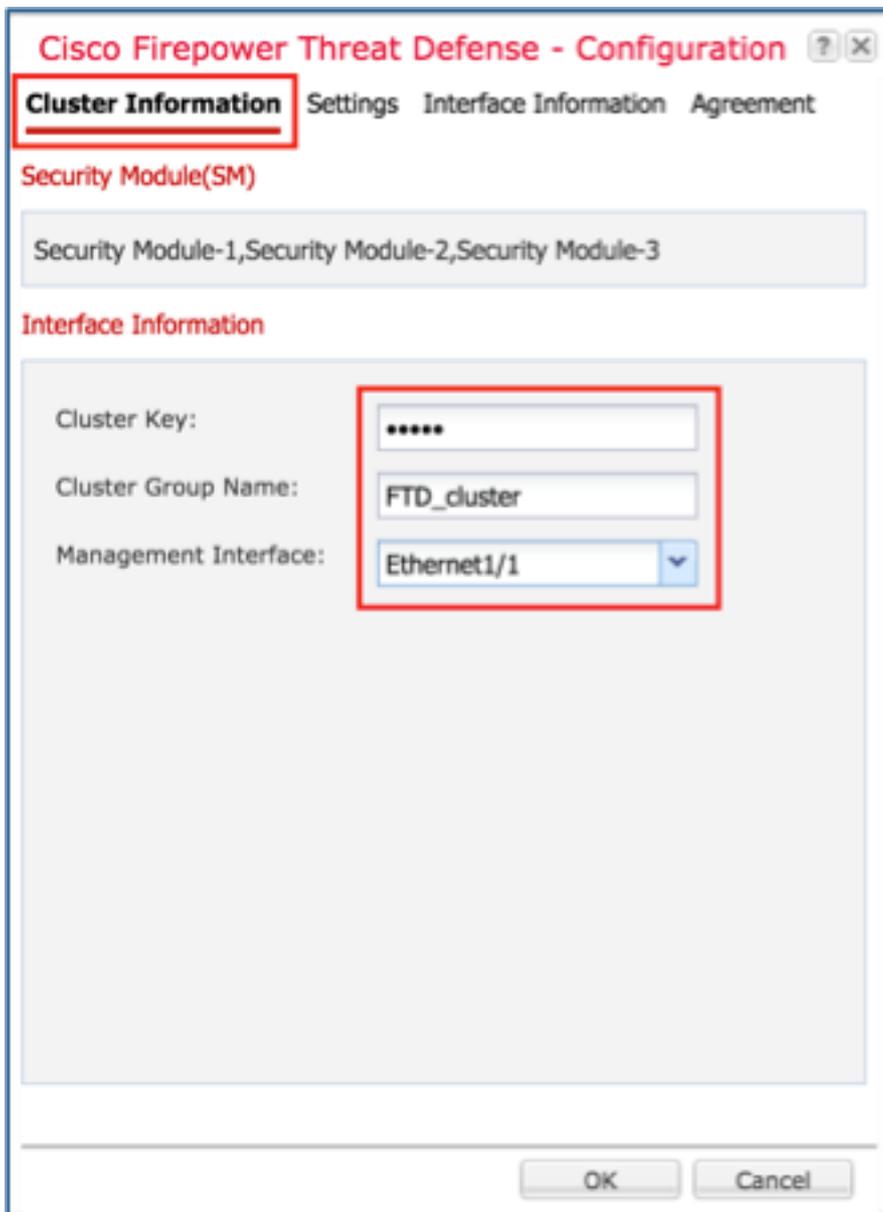
- Ethernet1/2
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet3/1
- Ethernet3/2
- Ethernet3/3
- Ethernet3/4
- Port-channel5



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				

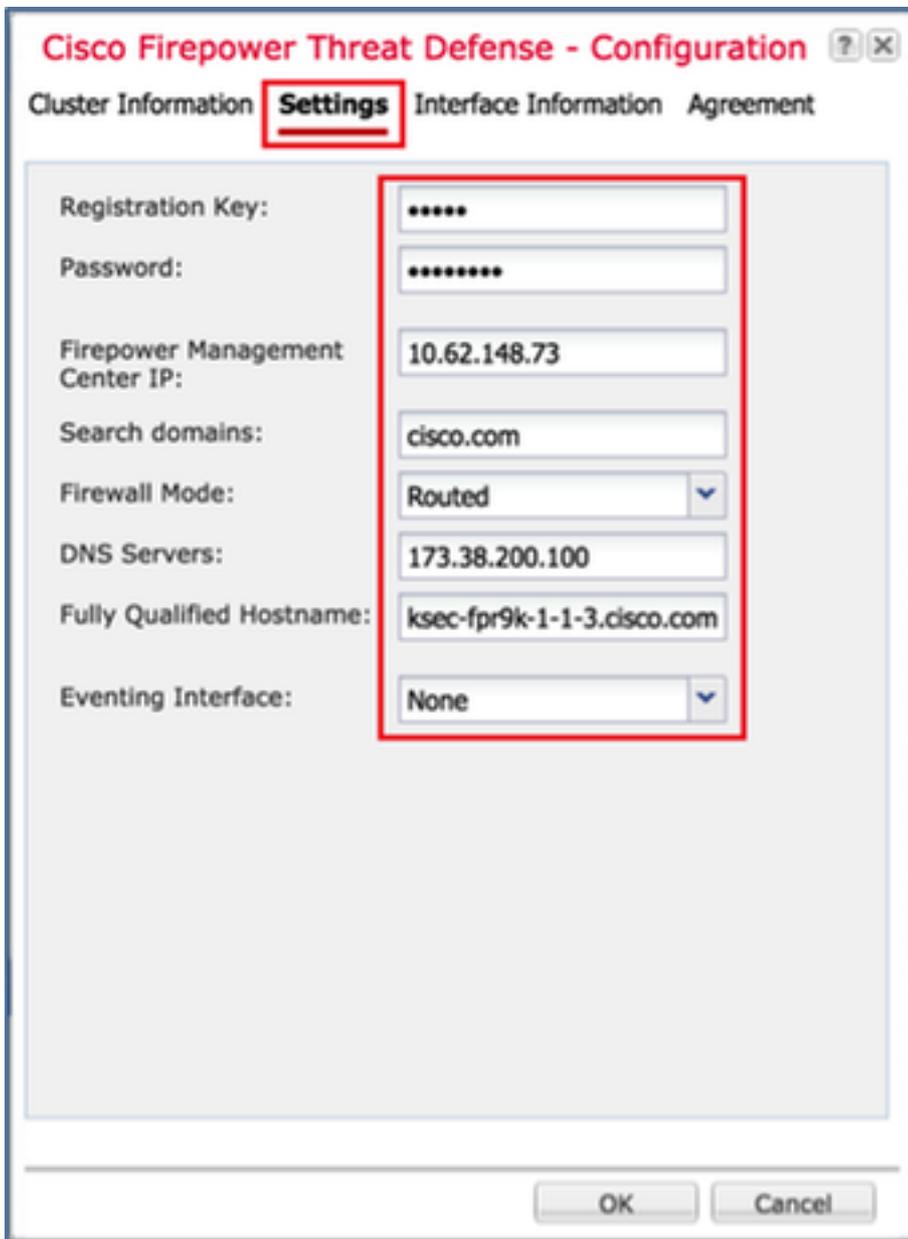
Configurez l'onglet **Informations sur le cluster** FTD avec ces paramètres et comme indiqué dans l'image.

Clé de cluster	cisco
Nom du groupe de clusters	FTD_cluster
Interface de gestion	Ethernet1/1



Configurez l'onglet **Paramètres** FTD avec ces paramètres et comme indiqué dans l'image.

Clé d'enregistrement	cisco
Mot de passe	Admin123
IP Firepower Management Center	10.62.148.73
Domaines de recherche	cisco.com
Mode pare-feu	Routé
Serveurs DNS	173.38.200.100
Nom d'hôte complet	ksec-fpr9k-1-1-3.cisco.com
Interface de modification	Aucune



Configurez l'onglet **Informations sur l'interface** FTD avec ces paramètres et comme indiqué dans l'image.

Type d'adresse	IPv4 uniquement
Module de sécurité 1	
IP de gestion	10.62.148.67
Masque de réseau	255.255.255.128
Passerelle	10.62.148.1
Module de sécurité 2	
IP de gestion	10.62.148.68
Masque de réseau	255.255.255.128
Passerelle	10.62.148.1
Module de sécurité 3	
IP de gestion	10.62.148.69
Masque de réseau	255.255.255.128
Passerelle	10.62.148.1

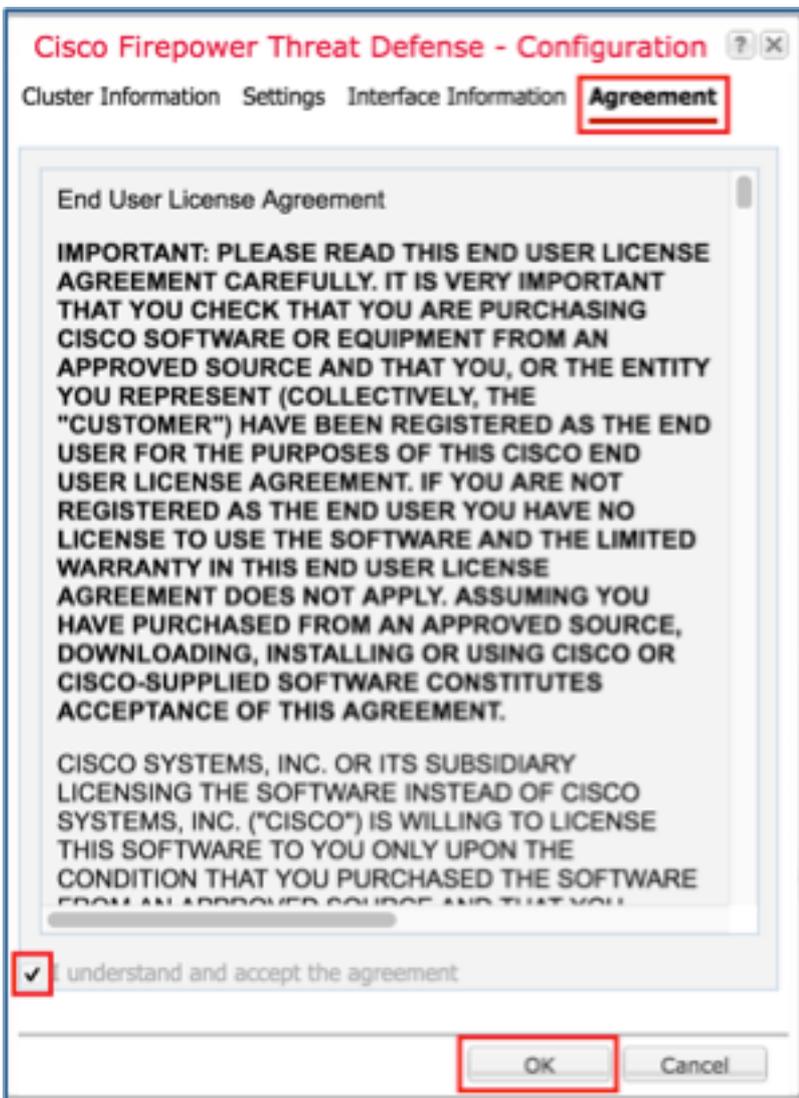
Cisco Firepower Threat Defense - Configuration ? X

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

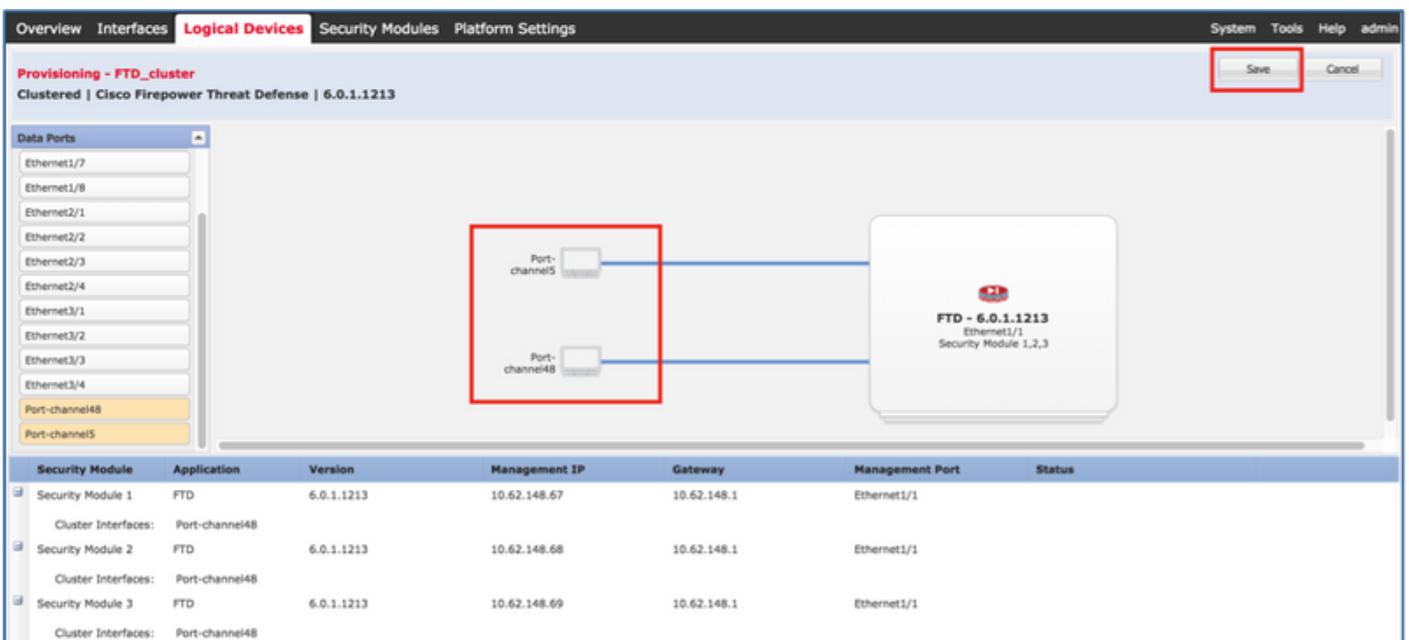
OK Cancel

Acceptez le Contrat dans l'onglet **Contrat** et cliquez sur **OK** comme indiqué dans l'image.



Étape 3. Attribuez des interfaces de données à FTD.

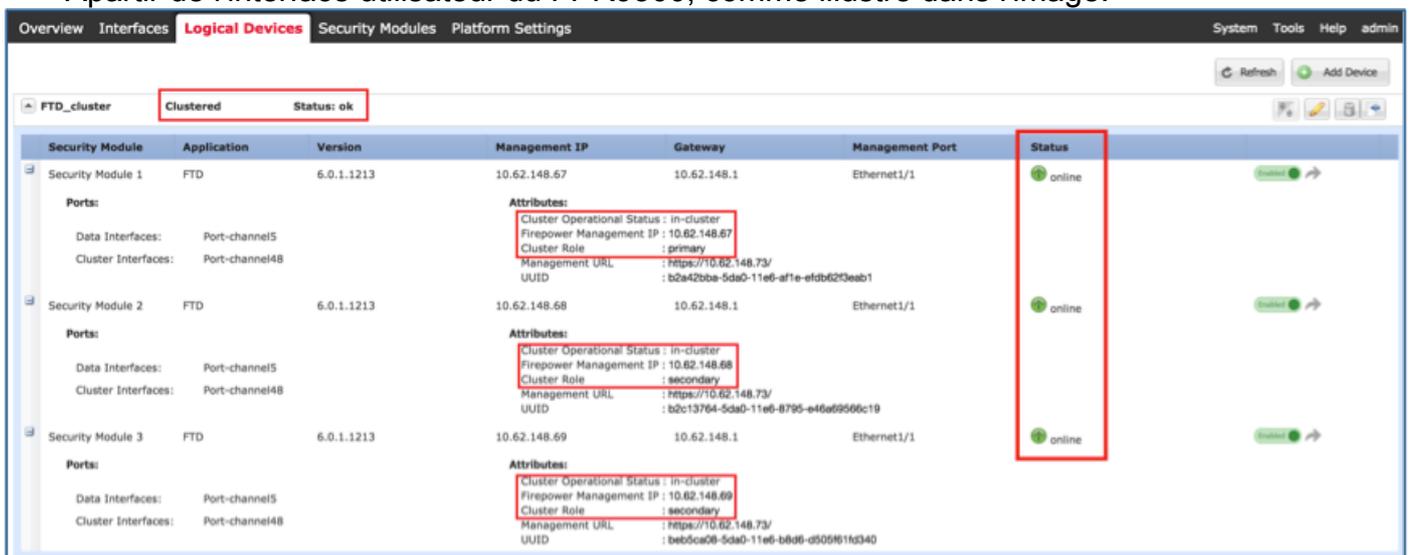
Développez la zone Ports de données et cliquez sur chaque interface que vous souhaitez affecter à FTD. Une fois terminé, sélectionnez **Enregistrer** pour créer un cluster FTD comme indiqué dans l'image.



Patientez quelques minutes avant que le cluster ne soit déployé, après quoi se produit le choix de l'unité maître.

Vérification :

- À partir de l'interface utilisateur du FPR9300, comme illustré dans l'image.



- À partir de l'interface de ligne de commande 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					

- À partir de l'interface de ligne de commande 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#
```

Tâche 3. Enregistrer le cluster FTD sur FMC

Exigence de la tâche :

Ajoutez les périphériques logiques au FMC, puis regroupez-les dans un cluster.

Solution :

Étape 1. Ajoutez des périphériques logiques au FMC. À partir de la version 6.3 de FMC, vous ne devez enregistrer qu'un seul périphérique FTD (recommandé pour être le maître). Les autres FTD sont détectés automatiquement par le FMC.

Connectez-vous à FMC et accédez à l'onglet **Devices > Device Management** et cliquez sur **Add Device**.

Ajoutez le premier périphérique logique avec les paramètres mentionnés dans l'image.

Cliquez sur **Register** pour commencer l'enregistrement.

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 vérification est illustrée dans l'image.

FTD_cluster		Cisco Firepower 9000 Series SM-36 Threat Defense Cluster		
FTD1(primary)	10.62.148.67 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300
FTD2	10.62.148.68 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300
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

Tâche 4. Configuration des sous-interfaces Port-Channel sur FMC

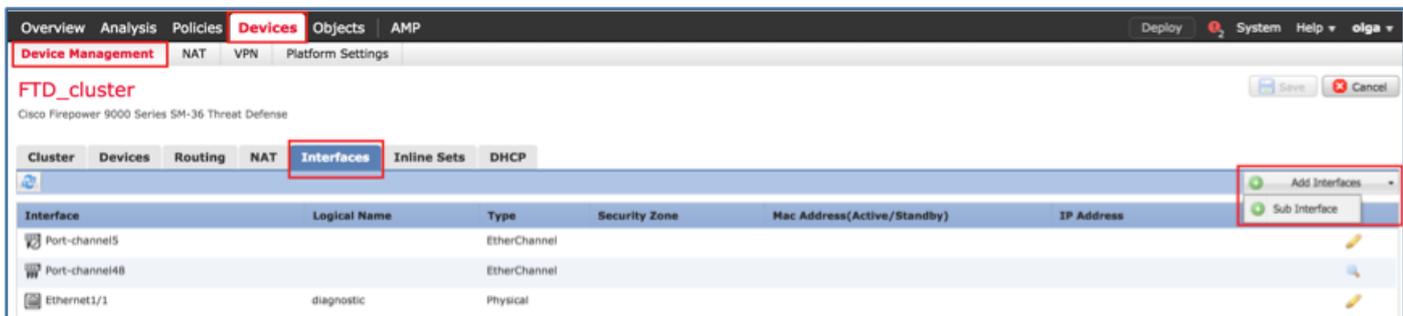
Exigence de la tâche :

Configurez des sous-interfaces pour l'interface de données Port-Channel.

Solution :

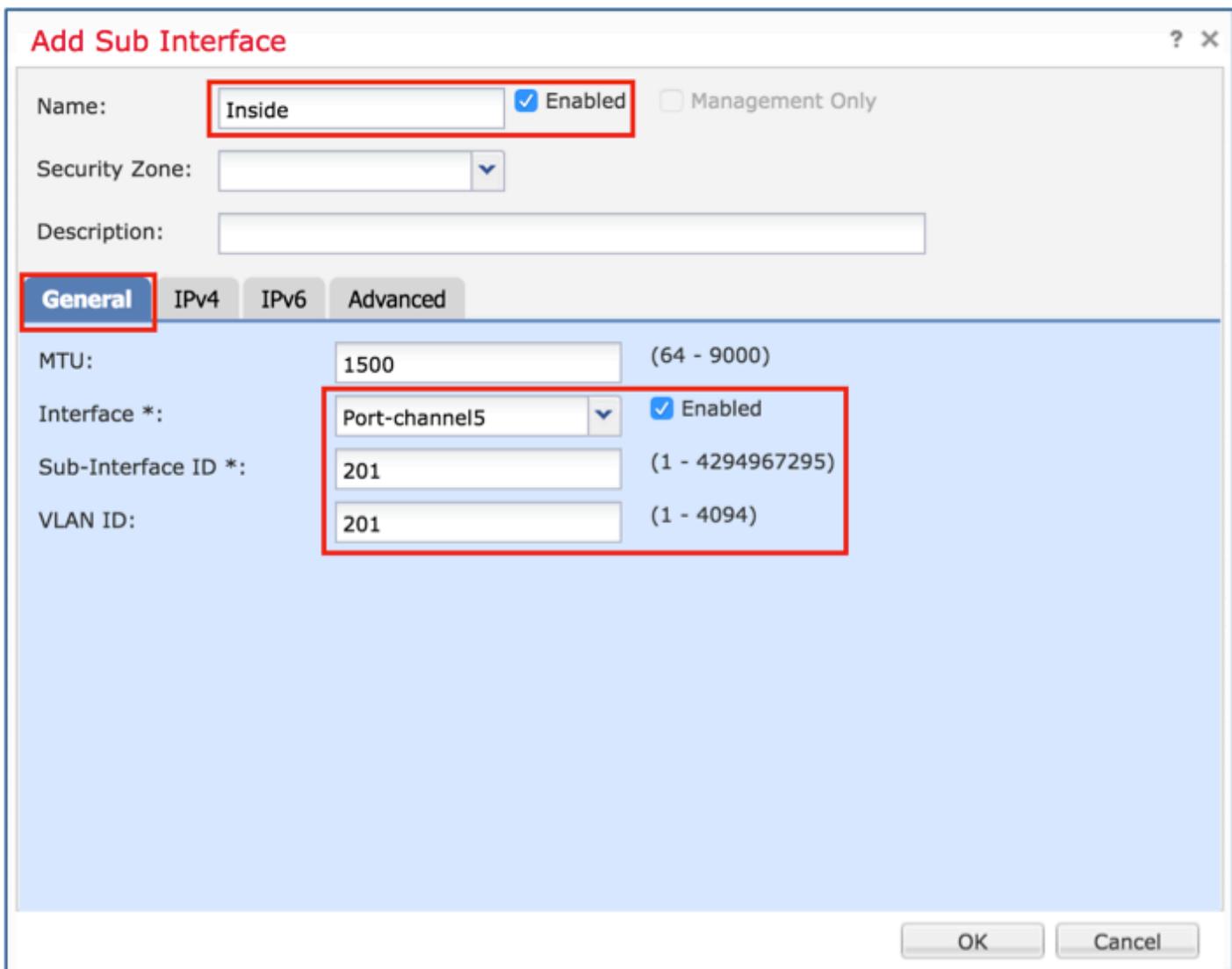
Étape 1. Dans l'interface graphique de FMC, sélectionnez le bouton **FTD_cluster Edit**.

Accédez à l'onglet Interfaces et cliquez sur **Add Interfaces > Sub Interface** comme indiqué dans l'image.



Configurez la première sous-interface avec ces détails. Sélectionnez **OK** pour appliquer les modifications et comme indiqué dans les images.

Name (nom)	Intérieur
Onglet Général	
Interface	Port-channel5
ID de sous-interface	201
ID de VLAN	201
Onglet IPv4	
Type IP	Utiliser une adresse IP statique
Adresse IP	192.168.75.10/24



Add Sub Interface ? X

Name: Enabled Management Only

Security Zone: ▾

Description:

General **IPv4** IPv6 Advanced

IP Type: ▾

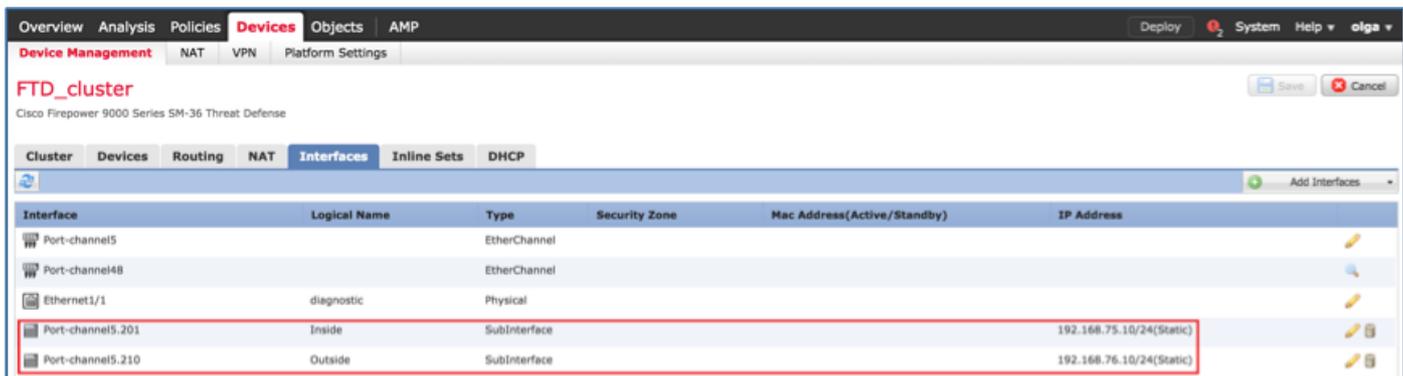
IP Address: eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

Configurez la deuxième sous-interface avec ces détails.

Name (nom)	Extérieur
Onglet Général	
Interface	Port-channel5
ID de sous-interface	210
ID de VLAN	210
Onglet IPv4	
Type IP	Utiliser une adresse IP statique
Adresse IP	192.168.76.10/24

Cliquez sur **OK** pour créer la sous-interface. Cliquez sur **Enregistrer**, puis sur **Déployer** les modifications apportées au cluster FTD_cluster comme l'illustre l'image.

Vérification :



Tâche 5. Vérification de la connectivité de base

Exigence de la tâche :

Créez une capture et vérifiez la connectivité entre deux machines virtuelles.

Solution :

Étape 1. Créer des captures sur toutes les unités de cluster.

Accédez à la CLI LINA (ASA) de l'unité maître et créez des captures pour les interfaces interne et externe.

```
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#
```

Vérification :

```
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#

```

Étape 2. Exécutez le test ping de VM1 à VM2.

Effectuez le test avec 4 paquets. Vérifiez la sortie de capture après le 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#

```

Exécutez la commande afin de vérifier la sortie de capture sur l'unité spécifique :

```

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#

```

Après avoir terminé cette tâche, supprimez les captures à l'aide de la commande suivante :

```

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: *****

```

Étape 3. Téléchargez un fichier de VM2 vers VM1.

VM1 a été préconfiguré en tant que serveur FTP, VM2 en tant que client FTP.

Créez de nouvelles captures avec les éléments suivants :

```

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: *****

```

Téléchargez le fichier de VM2 vers VM1, à l'aide du client FTP.

Vérifiez la sortie 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
```

Afficher la sortie de capture :

```
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

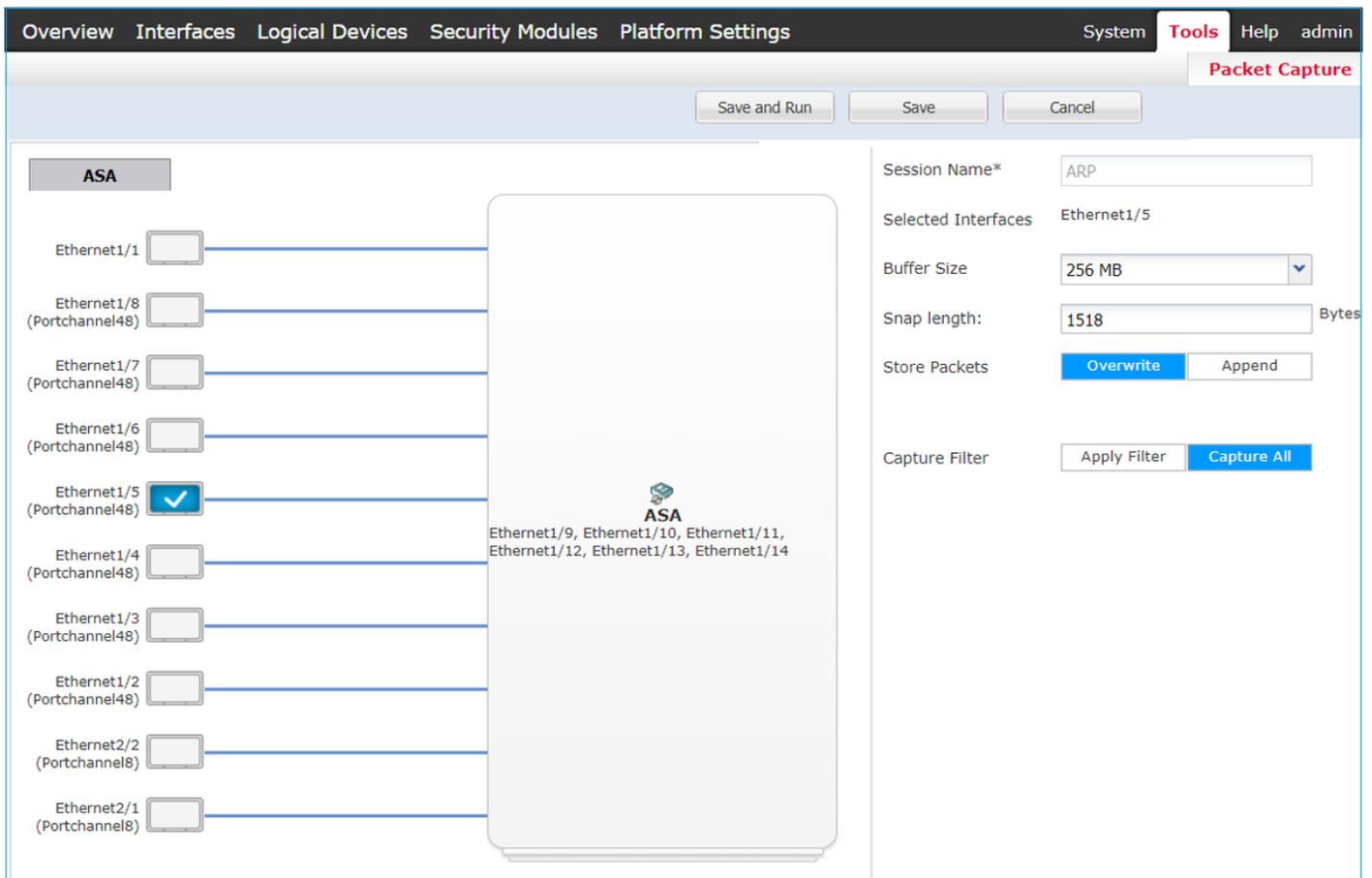
```

Capture de cluster à partir de l'interface utilisateur du Gestionnaire de châssis

Dans l'image suivante, vous pouvez voir un cluster de 3 unités sur FPR9300 avec 2 canaux de port (8 et 48). Les périphériques logiques sont des ASA, mais dans le cas de FTD sera le même concept. La chose importante à retenir est que bien qu'il y ait **3 unités de cluster**, du point de vue de la capture il n'y a qu'un **seul périphérique logique** :

The screenshot shows the Palo Alto Networks GUI for a cluster of 3 ASA security modules. The navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Modules', and 'Platform Settings'. The 'Logical Devices' section is active, showing a 'Logical Device List' with 3 entries. Each entry is a Security Module (ASA) with version 9.6.2.7, management IP 0.0.0.0, and gateway 0.0.0.0. The management port is Ethernet1/1. The status is 'online'. The ports are Port-channel8 (Data Interfaces) and Port-channel48 (Cluster Interfaces). The attributes for each module are as follows:

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				



Tâche 6. Supprimer un périphérique esclave du cluster

Exigence de la tâche :

Connectez-vous au FMC et supprimez l'unité Slave du cluster.

Solution :

Étape 1. Connectez-vous au FMC et accédez à **Device > Device Management**.

Cliquez sur l'icône de la corbeille en regard de l'unité Esclave, comme illustré dans l'image.



La fenêtre de confirmation s'affiche. Sélectionnez **Oui** pour confirmer comme indiqué dans l'image.



Vérification :

- À partir de la FMC, comme l'illustre l'image.



- À partir de l'interface de ligne de commande FXOS.

```
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
```

- À partir de l'interface de ligne de commande 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#
```

Note: Le périphérique n'a pas été enregistré à partir du FMC, mais il est toujours membre du cluster sur le FPR9300.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La vérification est terminée et couverte par des tâches individuelles.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Toutes les versions du guide de configuration de Cisco Firepower Management Center sont disponibles ici :

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

- Toutes les versions du gestionnaire de châssis FXOS et des guides de configuration CLI sont disponibles ici :

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

- Le Centre d'assistance technique mondial (TAC) de Cisco recommande vivement ce guide visuel pour des connaissances pratiques approfondies sur les technologies de sécurité de nouvelle génération Cisco Firepower, y compris celles mentionnées dans cet article :

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

- Pour toutes les notes techniques de configuration et de dépannage relatives aux technologies Firepower.

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

- [Support et documentation techniques - Cisco Systems](#)