

# FP9300 ( シャーシ内 ) でのFTDクラスタリング の設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[作業1:FTDクラスタに必要なインターフェイスの作成](#)

[作業2:FTDクラスタの作成](#)

[作業3:FTDクラスタのFMCへの登録](#)

[作業4:FMCでのポートチャンネルサブインターフェイスの設定](#)

[作業5.基本接続の確認](#)

[Chassis Manager UIからのクラスタキャプチャ](#)

[作業6 : クラスタからのスレーブデバイスの削除](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

## 概要

このドキュメントでは、FPR9300デバイスでクラスタ機能を設定および確認する方法について説明します。

**注意：**このドキュメントの情報は、クラスタの初期インストール/設定について説明しています。このドキュメントは、ユニット交換(Return Material Authorization - RMA)手順には適用されません

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 1.1(4.95)が稼働するCisco Firepower 9300セキュリティアプライアンス

- 6.0.1 (ビルド1213) を実行するFirepower Threat Defense(FTD)
- 6.0.1.1 (ビルド 1023) を実行している FireSIGHT Management Center 構成 ( FMC )

ラボの完了時間：1 時間。

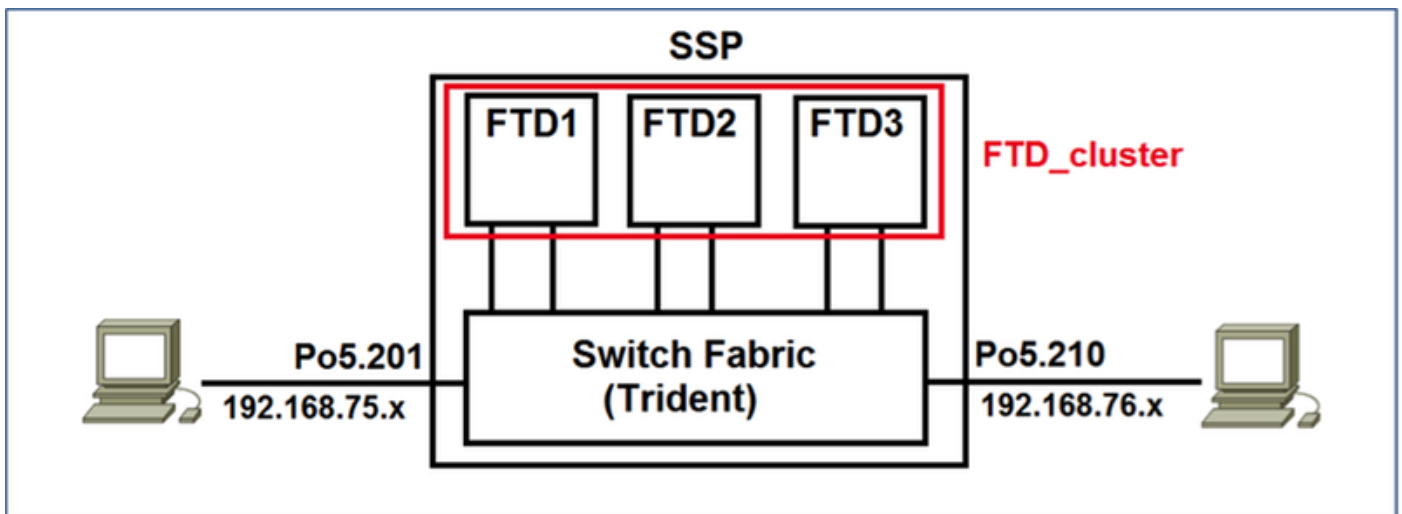
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

- FTDアプライアンスを搭載したFPR9300では、サポートされているすべてのバージョンでシャーシ内クラスタリングを設定できます。
- シャーシ間クラスタリングは6.2で導入されました。
- ポートチャンネル48は、クラスタ制御リンクとして作成されます。シャーシ内クラスタリングの場合、このリンクはクラスタ通信にFirepower 9300バックプレーンを使用します。
- 管理インターフェイスを除き、個々のデータインターフェイスはサポートされません。
- 管理インターフェイスは、クラスタ内のすべてのユニットに割り当てられます。

## 設定

### ネットワーク図



## 作業1:FTDクラスタに必要なインターフェイスの作成

タスク要件：

クラスタ、管理インターフェイス、およびポートチャンネルデータインターフェイスを作成します。

ソリューション：

ステップ1：ポートチャンネルデータインターフェイスを作成します。

新しいインターフェイスを作成するには、FPR9300 Chassis Managerにログインし、[Interfaces]タブに移動する必要があります。

[ポートチャネルの追加]を選択し、次のパラメータを使用して新しいポートチャネルインターフェイスを作成します。

Port Channel ID	5
Type	Data
Enable	Yes
Member ID	Ethernet1/3、Ethernet 1/4

[OK]を選択し、図に示すように設定を保存します。

**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

ステップ2：管理インターフェイスを作成します。

[Interfaces]タブでインターフェイスを選択し、[Edit]をクリックして[Management Type]インター

フェイスを設定します。

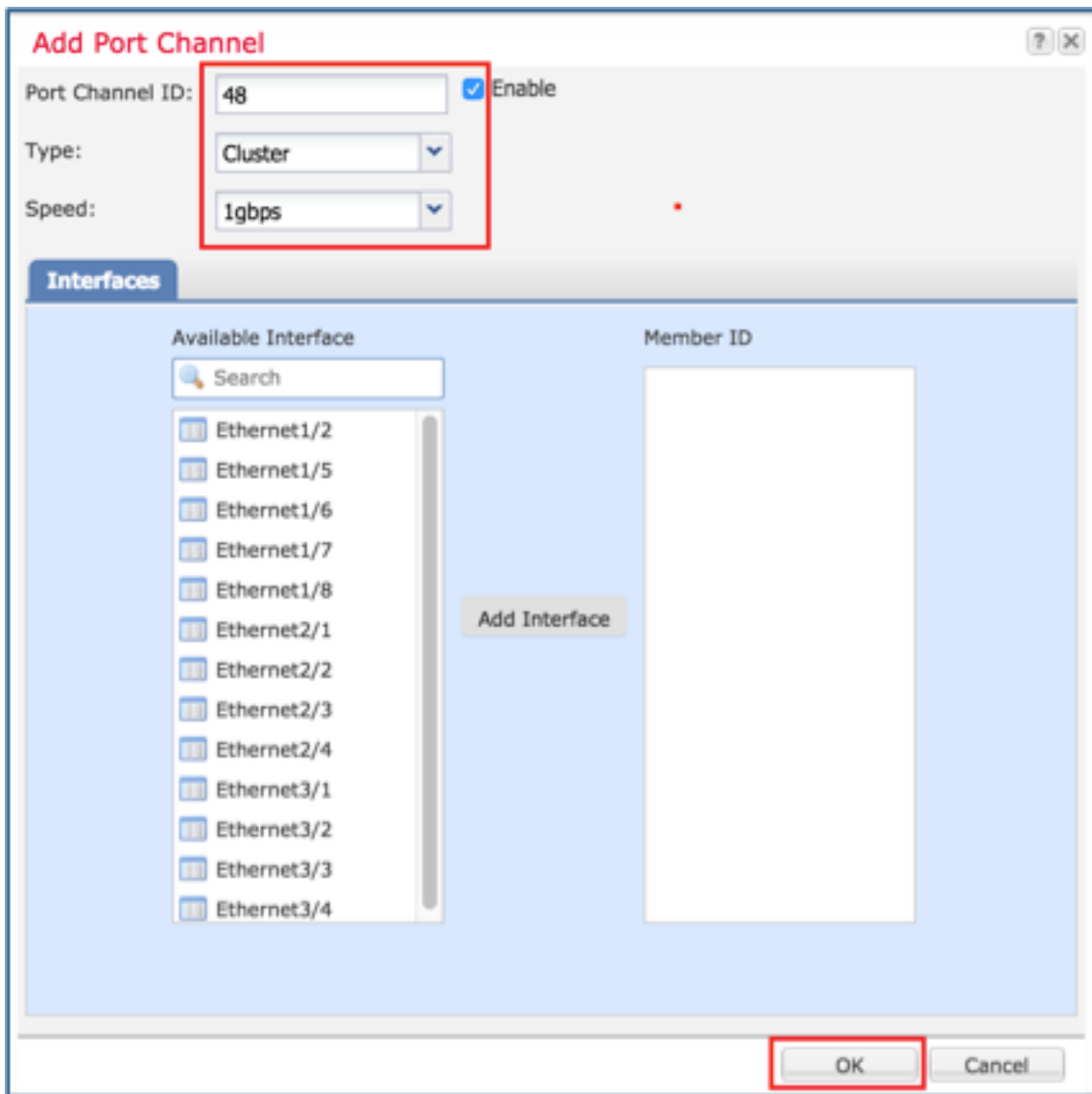
[OK]をクリックし、図に示すように設定を保存します。



ステップ3 : クラスタ制御リンクインターフェイスを作成します。

図に示すように、[Add Port Channel]ボタンをクリックし、これらのパラメータを使用して新しいポートチャネルインターフェイスを作成します。

Port Channel ID	48
Type	クラスタ
Enable	Yes
Member ID	-



## 作業2:FTDクラスタの作成

タスク要件 :

FTDクラスタユニットを作成します。

ソリューション :

ステップ1:[Logical Devices]に移動し、[Add Device]ボタンをクリックします。

次のようにFTDクラスタリングを作成します。

Device Name	FTD_cluster
Template	Cisco Firepower Threat Defense
Image Version	6.0.1.1213
デバイスモード	クラスタ

デバイスを追加するには、図に示すように[OK]をクリックします。

## Add Device

Device Name:

Template:

Image Version:

Device Mode:  Standalone  Cluster

ステップ2:FTDクラスタを設定および導入します。

FTDデバイスを作成すると、[Provisioning- device\_name]ウィンドウにリダイレクトされます。

図に示すように、デバイスアイコンをクリックして設定を開始します。

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

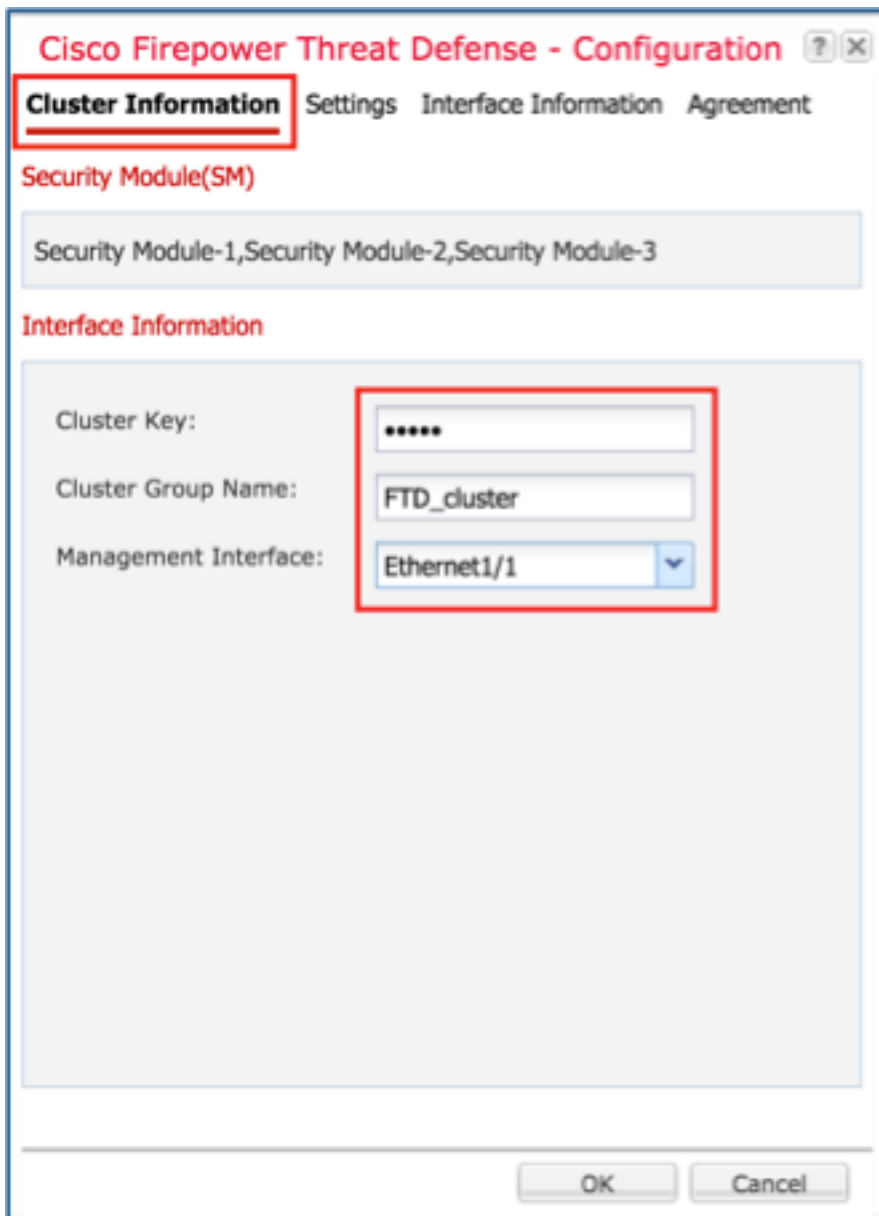
- Ethernet1/2
- Ethernet1/5
- Ethernet1/6
- Ethernet1/7
- Ethernet1/8
- Ethernet2/1
- Ethernet2/2
- Ethernet2/3
- Ethernet2/4
- Ethernet3/1
- Ethernet3/2
- Ethernet3/3
- Ethernet3/4
- Port-channel5

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				

図に示すように、FTDクラスタ情報タブを次の設定で構成します。

クラスタキー	cisco
クラスタグループ名	FTD_cluster
Management Interface	Ethernet1/1



図に示すように、FTDの[Settings]タブを設定します。

登録キー	cisco
Password	Admin123
Firepower Management Center の IP	10.62.148.73
Search domains	cisco.com
Firewall Mode	Routed
DNS Servers	173.38.200.100
Fully Qualified Hostname	ksec-fpr9k-1-1-3.cisco.com
Eventing Interface	なし

**Cisco Firepower Threat Defense - Configuration** ? X

Cluster Information **Settings** Interface Information Agreement

Registration Key: \*\*\*\*\*

Password: \*\*\*\*\*

Firepower Management Center IP: 10.62.148.73

Search domains: cisco.com

Firewall Mode: Routed

DNS Servers: 173.38.200.100

Fully Qualified Hostname: ksec-fpr9k-1-1-3.cisco.com

Eventing Interface: None

OK Cancel

図に示すように、これらの設定を使用して[FTDインターフェイス情報]タブを設定します。

Address Type	IPv4のみ
<b>セキュリティモジュール1</b>	
Management IP	10.62.148.67
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1
<b>セキュリティモジュール2</b>	
Management IP	10.62.148.68
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1
<b>セキュリティモジュール3</b>	
Management IP	10.62.148.69
Network Mask	255.255.255.128
ゲートウェイ	10.62.148.1



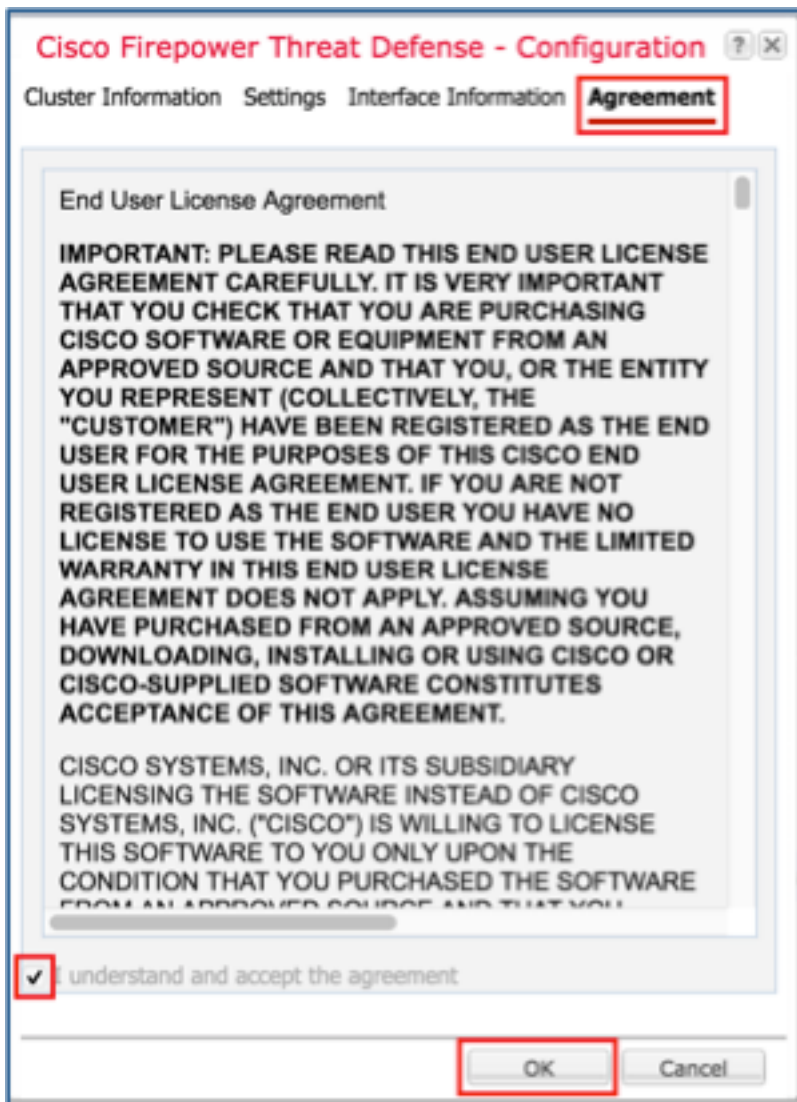
Cisco Firepower Threat Defense - Configuration ? ×

Cluster Information Settings **Interface Information** Agreement

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

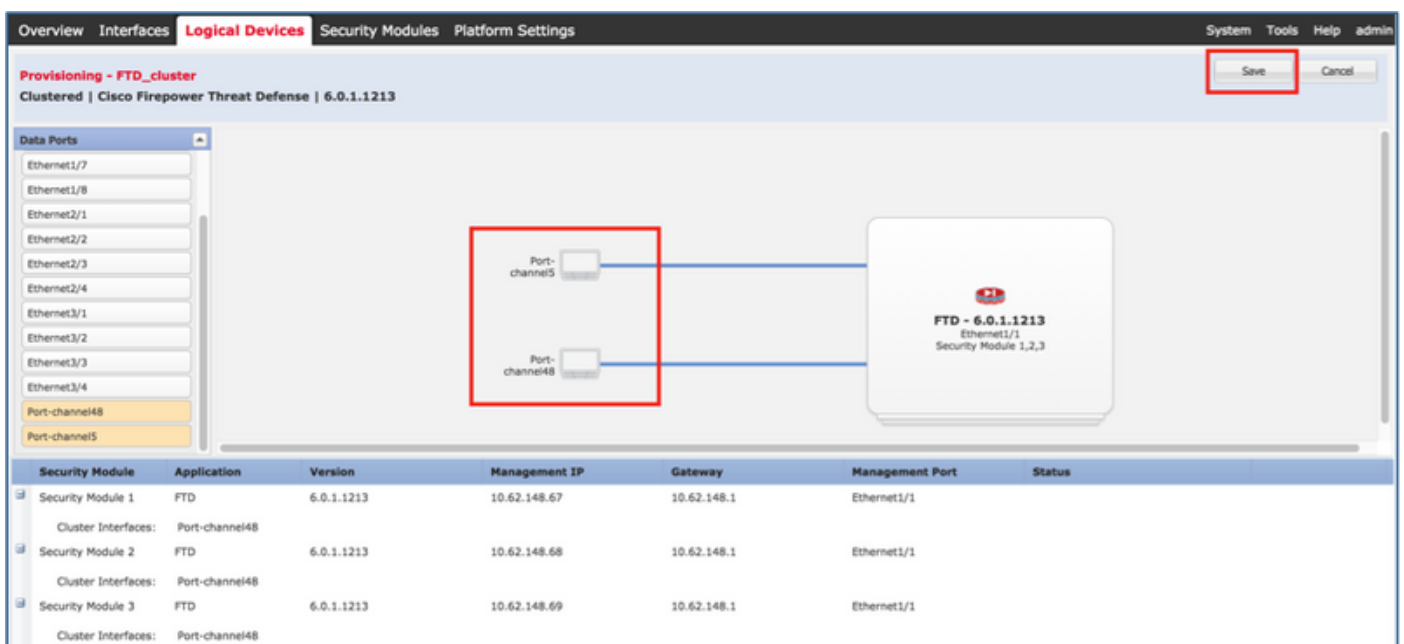
OK Cancel

[Agreement]タブの[Agreement]に同意し、図に示すように[OK]をクリックします。



ステップ3:FTDへのデータインターフェイスの割り当て

[Data Ports] 領域を展開し、FTD に割り当てる各インターフェイスをクリックします。完了したら、[Save]を選択して、図に示すようにFTDクラスタを作成します。



クラスタが展開されるまで数分間待機し、その後にマスターユニットの選択が行われます。

検証：

- 図に示すように、FPR9300 GUIから。

Security Module	Application	Version	Management IP	Gateway	Management Port	Status
Security Module 1	FTD	6.0.1.1213	10.62.148.67	10.62.148.1	Ethernet1/1	online
<b>Ports:</b>						
Data Interfaces:	Port-channel5					
Cluster Interfaces:	Port-channel48					
<b>Attributes:</b>						
Cluster Operational Status : in-cluster						
Firepower Management IP : 10.62.148.67						
Cluster Role : primary						
Management URL : https://10.62.148.73/						
UUID : b2a42bba-5da0-11e6-af1e-efdb623eeb1						
Security Module 2	FTD	6.0.1.1213	10.62.148.68	10.62.148.1	Ethernet1/1	online
<b>Ports:</b>						
Data Interfaces:	Port-channel5					
Cluster Interfaces:	Port-channel48					
<b>Attributes:</b>						
Cluster Operational Status : in-cluster						
Firepower Management IP : 10.62.148.68						
Cluster Role : secondary						
Management URL : https://10.62.148.73/						
UUID : b2c13764-5da0-11e6-8795-e46a69566c19						
Security Module 3	FTD	6.0.1.1213	10.62.148.69	10.62.148.1	Ethernet1/1	online
<b>Ports:</b>						
Data Interfaces:	Port-channel5					
Cluster Interfaces:	Port-channel48					
<b>Attributes:</b>						
Cluster Operational Status : in-cluster						
Firepower Management IP : 10.62.148.69						
Cluster Role : secondary						
Management URL : https://10.62.148.73/						
UUID : beb6ca08-5da0-11e6-b8d6-d506b11d340						

- FPR9300 CLIから

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

```
FPR9K-1-A# scope ssa
```

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

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version
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					

- LINA(ASA)CLIから

```
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#
```

## 作業3:FTDクラスタのFMCへの登録

タスク要件 :

論理デバイスをFMCに追加し、クラスタにグループ化します。

ソリューション :

ステップ1 : 論理デバイスをFMCに追加します。FMCバージョン6.3と同様に、1つのFTDデバイスだけを登録する必要があります ( マスターとして推奨 )。残りのFTDはFMCによって自動検出されます。

FMCにログインし、[Devices] > [Device Management]タブに**移動し**、[Add Device]をクリック**します**。

図に示されている設定で、最初の論理デバイスを追加します。

登録を開始するには**登録**をクリックしてください。

**Add Device**

Host: 10.62.148.67

Display Name: FTD1

Registration Key: cisco

Group: None

Access Control Policy: FTD9300

**Smart Licensing**

Malware:

Threat:

URL Filtering:

**Advanced**

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

Register Cancel

図に確認を示します。

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
<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
<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

## 作業4:FMCでのポートチャンネルサブインターフェイスの設定

タスク要件 :

ポートチャンネルデータインターフェイスのサブインターフェイスを設定します。

ソリューション :

ステップ1:FMCのGUIで、[FTD\_cluster Edit]ボタンを選択します。

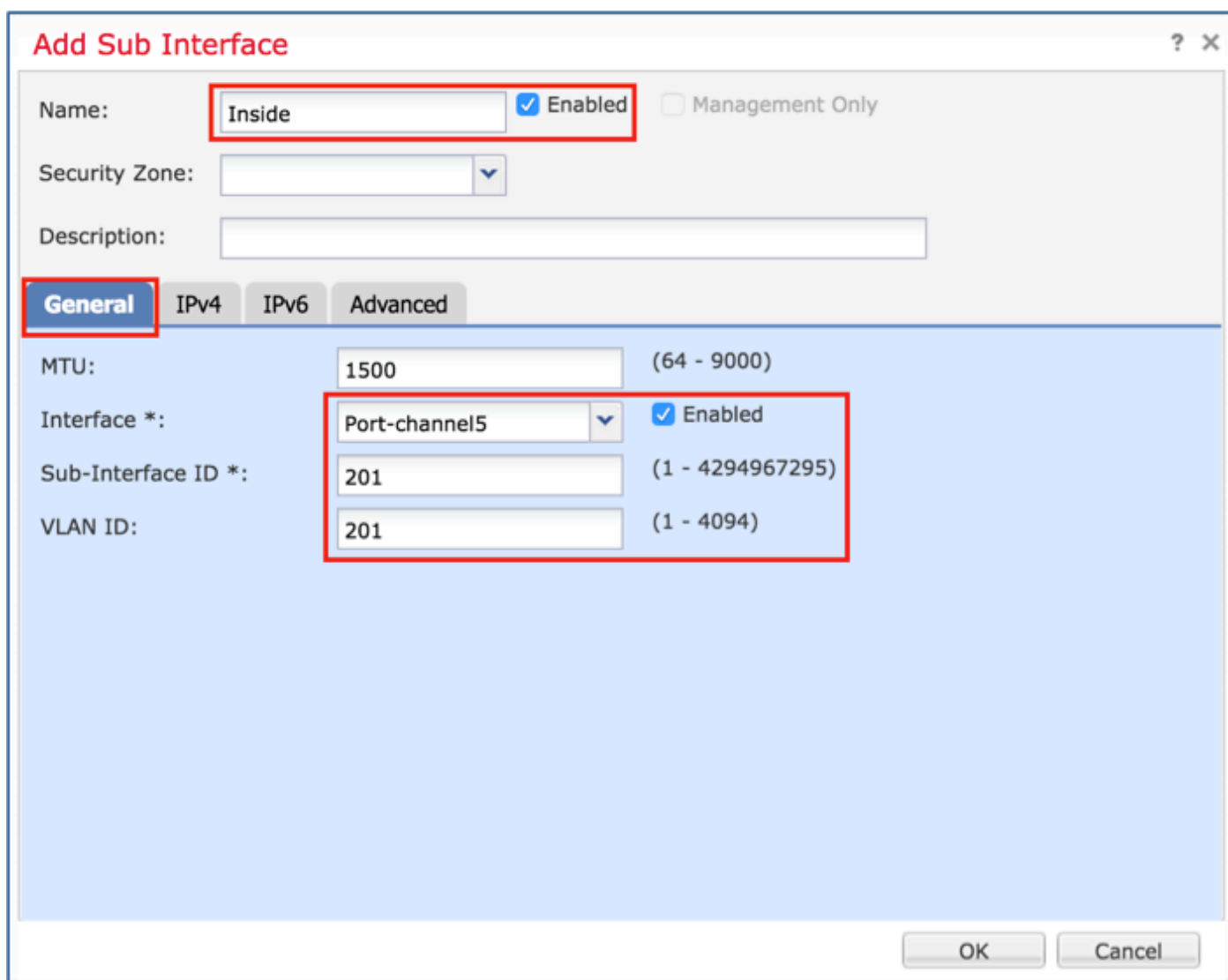
[Interfaces]タブに移動し、図に示すように[Add Interfaces] > [Sub Interface]をクリックします。





次の詳細を使用して、最初のサブインターフェイスを設定します。[OK]を選択して、変更を適用します（図を参照）。

[名前(Name)]                                   INSIDE  
**[General] タブ**  
 インターフェイス                           ポートチャンネル5  
 サブインターフェイスID                  201  
 VLAN ID                                       201  
**[IPv4]タブ**  
 IPタイプ                                     スタティックIPの使用  
 iSCSIポータルの                            192.168.75.10/24

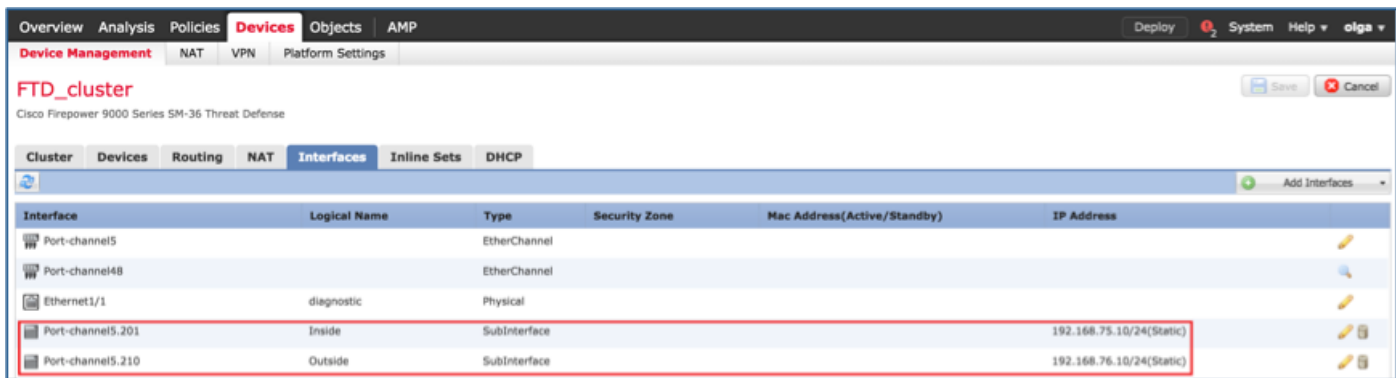


次の詳細を使用して、2番目のサブインターフェイスを設定します。

[名前(Name)]	OUTSIDE
[General] タブ	
インターフェイス	ポートチャンネル5
サブインターフェイスID	210
VLAN ID	210
[IPv4]タブ	
IPタイプ	スタティックIPの使用
iSCSIポータルの	192.168.76.10/24

[OK]をクリックして、サブインターフェイスを作成します。[Save]をクリックして、図に示すように[Deploy changes to the FTD\_cluster]をクリックします。

検証：



## 作業5.基本接続の確認

タスク要件：

キャプチャを作成し、2つのVM間の接続を確認します。

ソリューション：

ステップ1：すべてのクラスタユニットでキャプチャを作成します。

マスターユニットのLINA(ASA)CLIに移動し、内部インターフェイスと外部インターフェイスのキャプチャを作成します。

```
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:*****
```

検証：

```
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#

```

手順2:VM1からVM2へのpingテストを実行します。

4パケットでテストを実行します。テスト後のキャプチャ出力を確認します。

```

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#

```

特定のユニットのキャプチャ出力を確認するには、次のコマンドを実行します。

```

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#
```

この作業が完了したら、次のコマンドでキャプチャを削除します。

```
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:*****
```

ステップ3:VM2からVM1にファイルをダウンロードします。

VM1はFTPサーバとして事前設定され、VM2はFTPクライアントとして事前設定されました。

次の内容で新しいキャプチャを作成します。

```
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:*****
```

FTPクライアントを使用して、VM2からVM1にファイルをダウンロードします。

show connの出力をチェックします。

```
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
```

Show captureの出力 :

```
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

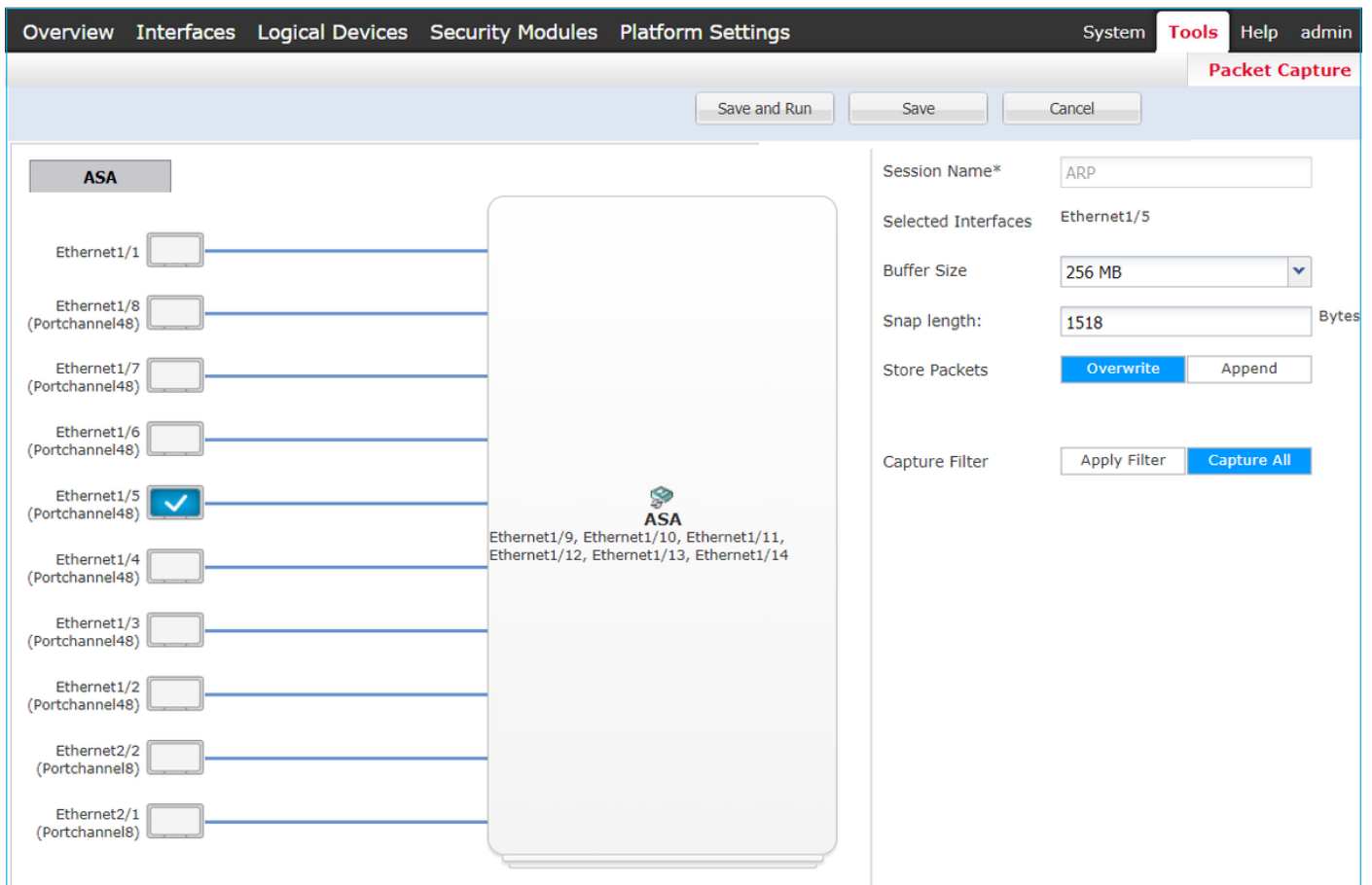
```

## Chassis Manager UIからのクラスタキャプチャ

次の図では、2つのポートチャネル（8および48）を備えたFPR9300上の3ユニットクラスタを確認できます。論理デバイスはASAですが、FTDの場合は同じ概念になります。重要な点は、クラスタユニットは3つありますが、キャプチャの観点から見ると、論理デバイスは1つしかありません。

The screenshot shows the 'Logical Devices' tab in the Chassis Manager UI. The 'Logical Device List' displays three clustered ASA security modules. Each module is shown with its configuration details, including ports, data interfaces, cluster interfaces, and attributes.

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
<b>Ports:</b>		<b>Attributes:</b>				
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
<b>Ports:</b>		<b>Attributes:</b>				
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
<b>Ports:</b>		<b>Attributes:</b>				
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				



## 作業6：クラスタからのスレーブデバイスの削除

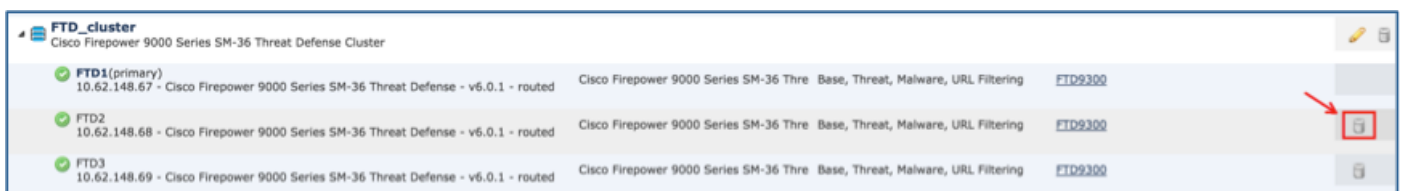
タスク要件：

FMCにログインし、クラスタからスレーブユニットを削除します。

ソリューション：

ステップ1:FMCにログインし、[Device] > [Device Management]に移動します。

図に示すように、スレーブユニットの横にあるごみ箱アイコンをクリックします。



確認ウィンドウが表示されます。図に示すように、[Yes]を選択して確認します。





検証：

- 図に示すように、FMCから実行します。



- FXOS CLIから。

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

Application Name	Slot ID	Admin State	Operational State	Running Version	Startup Version
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					

- LINA(ASA)CLIから。

```
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#
```

注：デバイスはFMCから登録解除されましたが、FPR9300のクラスタメンバーのままです。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

検証が完了し、個々のタスクでカバーされます。

## トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- Cisco Firepower Management Centerコンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

[https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id\\_47280](https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280) にアクセスしてください。

- FXOS Chassis ManagerおよびCLIコンフィギュレーションガイドのすべてのバージョンは、次の場所にあります。

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

- Cisco Global Technical Assistance Center(TAC)では、このビジュアルガイドを使用して、Cisco Firepower次世代セキュリティテクノロジーに関する詳細な実務知識を得ることを強く推奨しています。このガイドには、次の内容が含まれます。

<http://www.ciscopress.com/title/9781587144806> にアクセスしてください。

- Firepowerテクノロジーに関連するすべての設定およびトラブルシューティングのテクニカルノート。

<https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html> にアクセスしてください。

- [テクニカル サポートとドキュメント – Cisco Systems](#)