

# Firepower 4100でのFTDマルチインスタンス高可用性の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[ステップ 1: インターフェイスの事前設定](#)

[ステップ 2: コンテナインスタンスに2つのリソースプロファイルを追加します。](#)

[ステップ 3: \(オプション\) コンテナインスタンスインターフェイスの仮想MACアドレスのMACプールプレフィックスを追加します。](#)

[ステップ 4: スタンドアロンインスタンスを追加します。](#)

[ステップ 5: インターフェイスの設定](#)

[手順 6: 各インスタンスにハイアベイラビリティペアを追加します。](#)

[確認](#)

[トラブルシューティング](#)

[参考](#)

---

## はじめに

このドキュメントでは、FTDコンテナインスタンス ( マルチインスタンス ) でフェールオーバーを設定する方法について説明します。

## 前提条件

### 要件

Firepower Management Center(FMC)およびファイアウォール脅威対策に関する知識があることが推奨されます。

### 使用するコンポーネント

Cisco Firepower Management Center(FMC)仮想7.2.5

Cisco Firepower 4145 NGFWアプライアンス(FTD)7.2.5

Firepower eXtensibleオペレーティングシステム(FXOS)2.12(0.498)

Windows 10

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、クリアな（デフォルト）設定で作業を開始しています。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。

FTDマルチインスタンスを導入する前に、それがシステムのパフォーマンスに与える影響を理解し、それに応じて計画を立てることが重要です。最適な導入と設定を行うには、必ずシスコの公式文書を参照するか、シスコの技術担当者に相談してください。

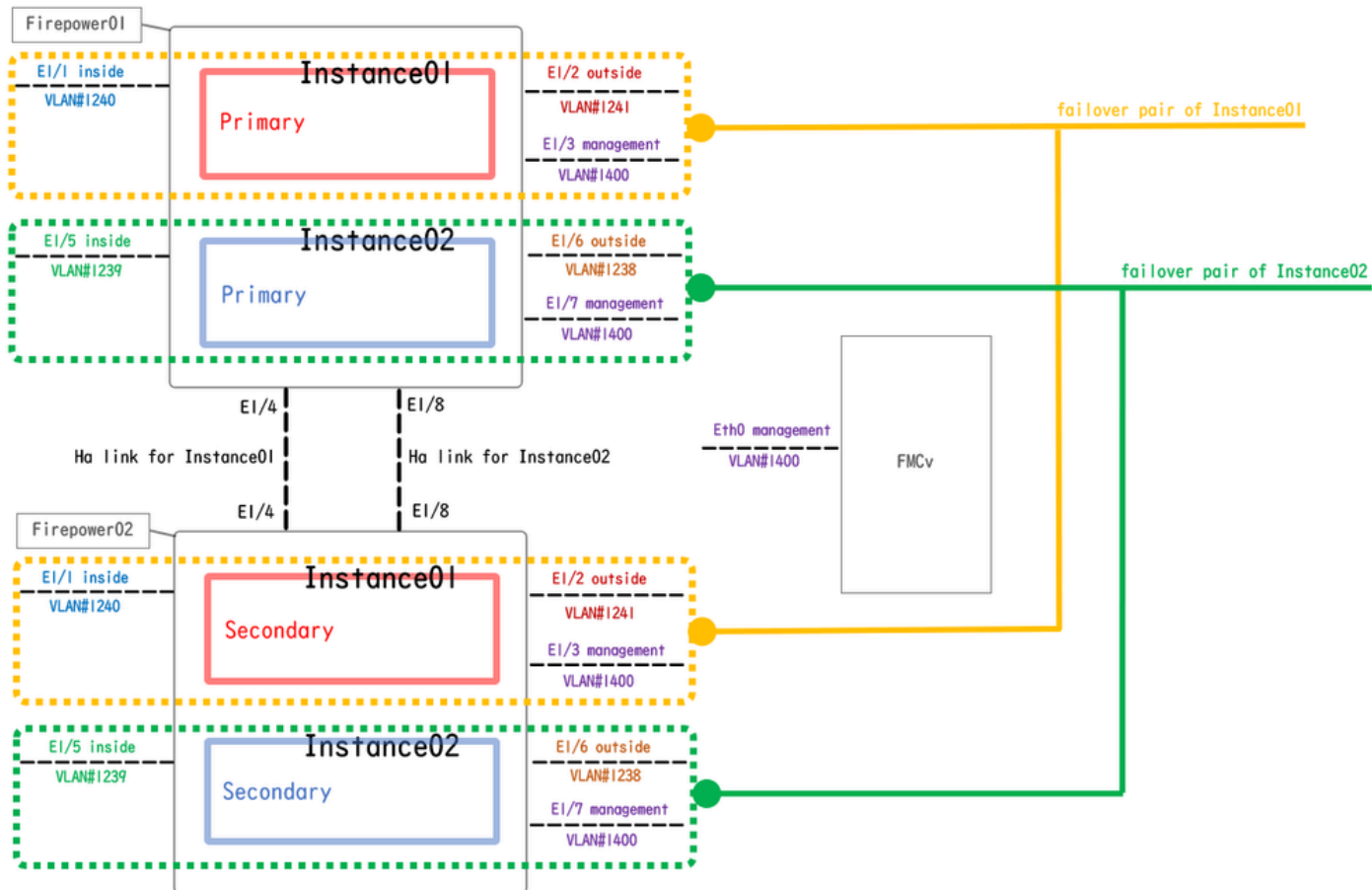
## 背景説明

マルチインスタンスは、ASAマルチコンテキストモードと同様のFirepower Threat Defense(FTD)の機能です。これにより、単一のハードウェア上でFTDの複数の個別コンテナインスタンスを実行できます。各コンテナインスタンスでは、リソースの分離、構成管理、リロードの分離、ソフトウェアアップデートの分離、脅威に対する防御機能の完全なサポートが可能です。これは、部門やプロジェクトごとに異なるセキュリティポリシーを必要とするが、複数のハードウェアアプライアンスに個別に投資したくない組織に特に役立ちます。マルチインスタンス機能は現在、FTD 6.4以降を実行するFirepower 4100および9300シリーズセキュリティアプライアンスでサポートされています。

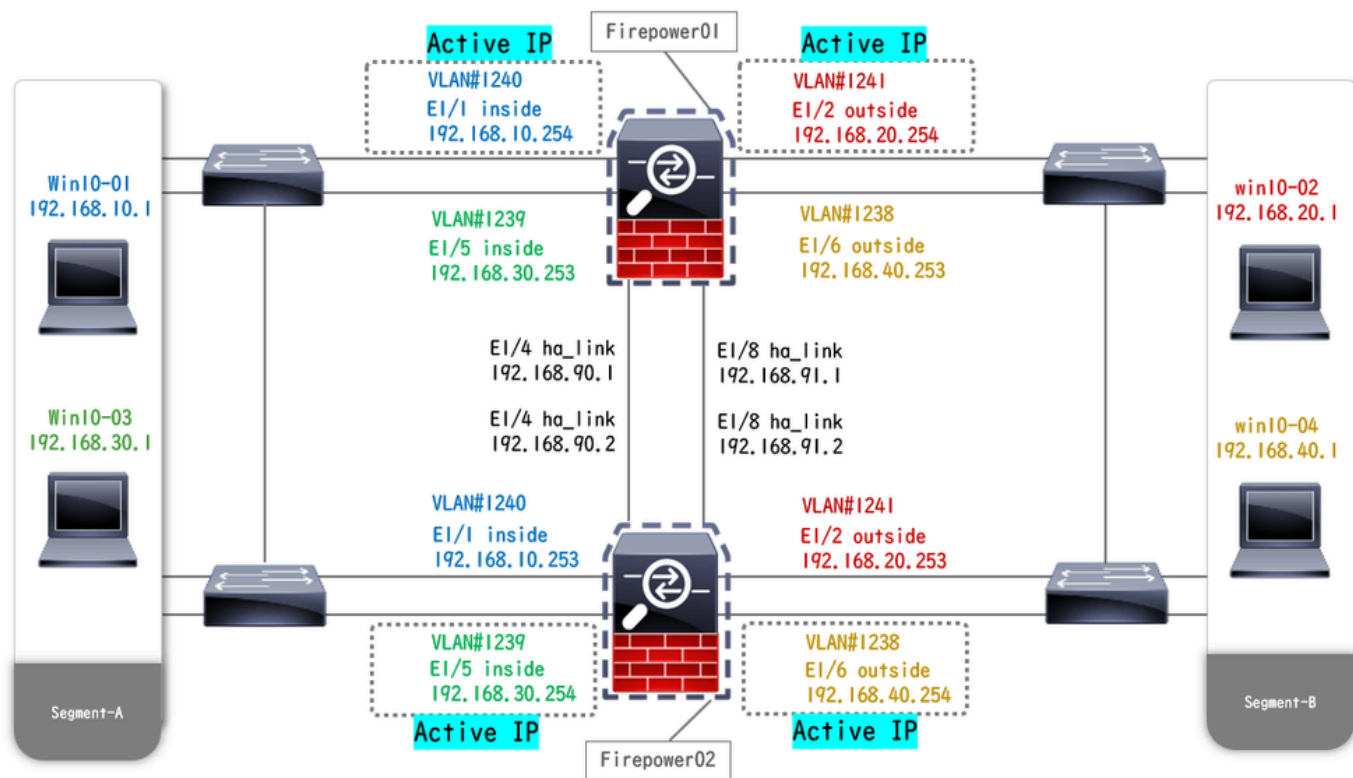
このドキュメントでは、最大14のコンテナインスタンスをサポートするFirepower4145を使用します。Firepowerアプライアンスでサポートされる最大インスタンス数については、[「モデルごとのコンテナインスタンスおよびリソースの最大数」](#)を参照してください。

## ネットワーク図

このドキュメントでは、この図のマルチインスタンスのHAの設定と検証を紹介します。



論理構成図

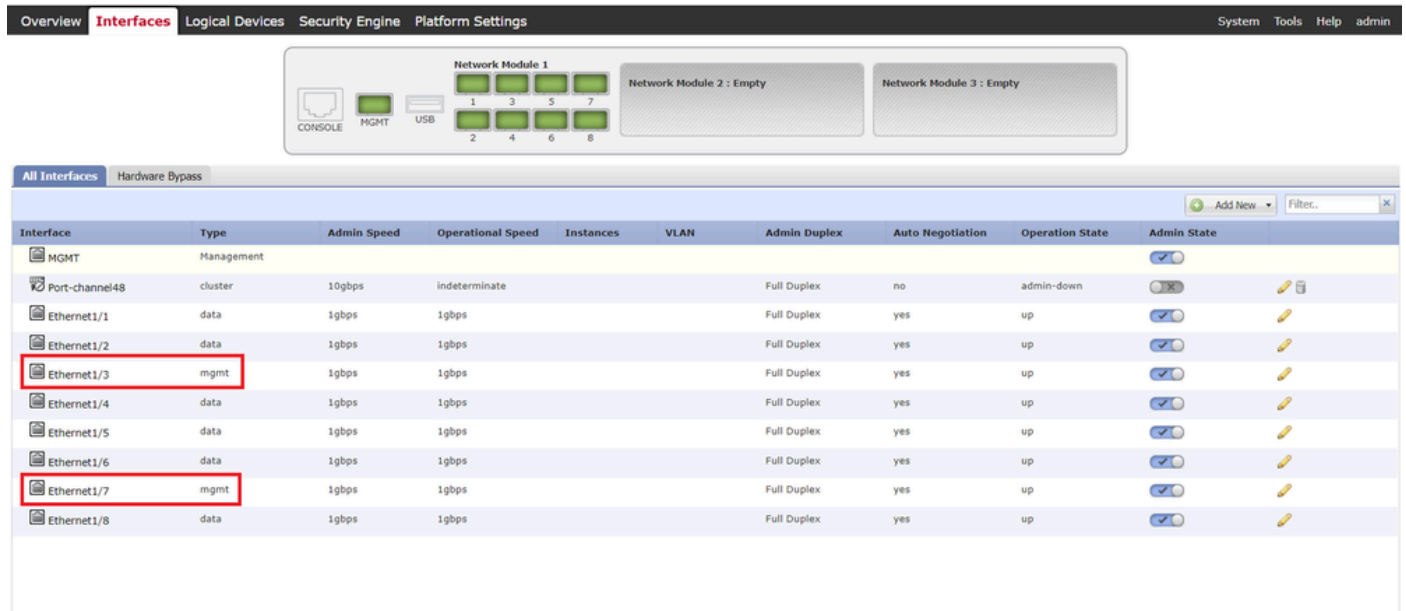


物理構成図

# コンフィギュレーション

## ステップ 1：インターフェイスの事前設定

a. FCMのインターフェイスに移動します。管理インターフェイスを2つ設定します。この例では、Ethernet1/3とEthernet1/7です。



The screenshot shows the configuration page for network interfaces. At the top, there are tabs for Overview, Interfaces (selected), Logical Devices, Security Engine, and Platform Settings. Below the tabs is a diagram of Network Module 1 with ports 1-8, and Network Module 2 and 3 are empty. Below the diagram is a table of interfaces.

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State
MGMT	Management								<input checked="" type="checkbox"/>
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	<input type="checkbox"/>
Ethernet1/1	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/2	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/3	mgmt	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/4	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/5	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/6	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/7	mgmt	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>
Ethernet1/8	data	1gbps	1gbps			Full Duplex	yes	up	<input checked="" type="checkbox"/>

インターフェイスの事前設定

ステップ 2：コンテナインスタンスに2つのリソースプロファイルを追加します。

a. FCMで、Platform Settings > Resource Profiles > Addの順に移動します。1番目のリソースプロファイルを設定します。

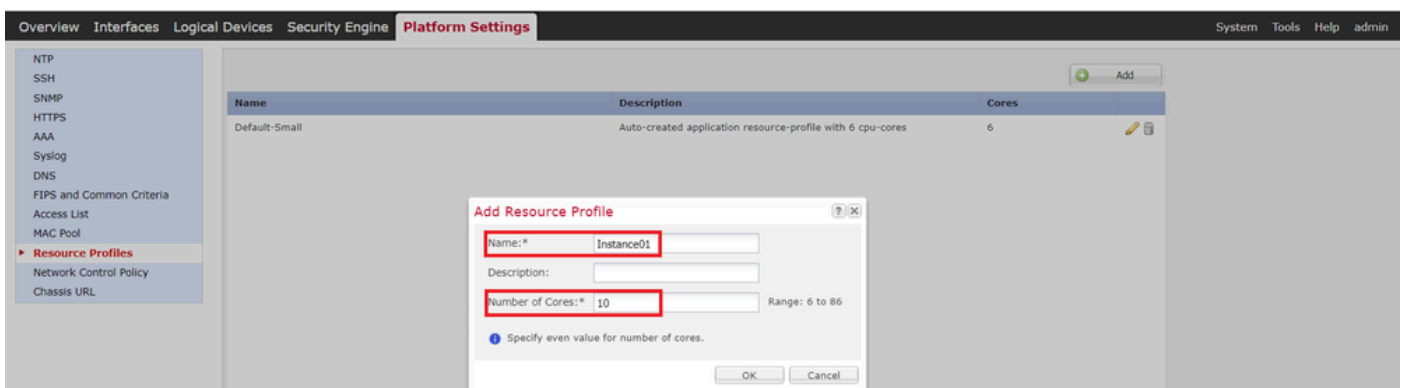
この例では、

- ・ 名前：Instance01
- ・ コア数：10

注：コンテナインスタンスペアのHAの場合、同じリソースプロファイル属性を使用する必要があります。

プロファイルの名前を1～64文字に設定します。このプロファイルを追加した後は、このプロファイルの名前を変更できないことに注意してください。

プロファイルのコアの数6から最大の間で設定します。

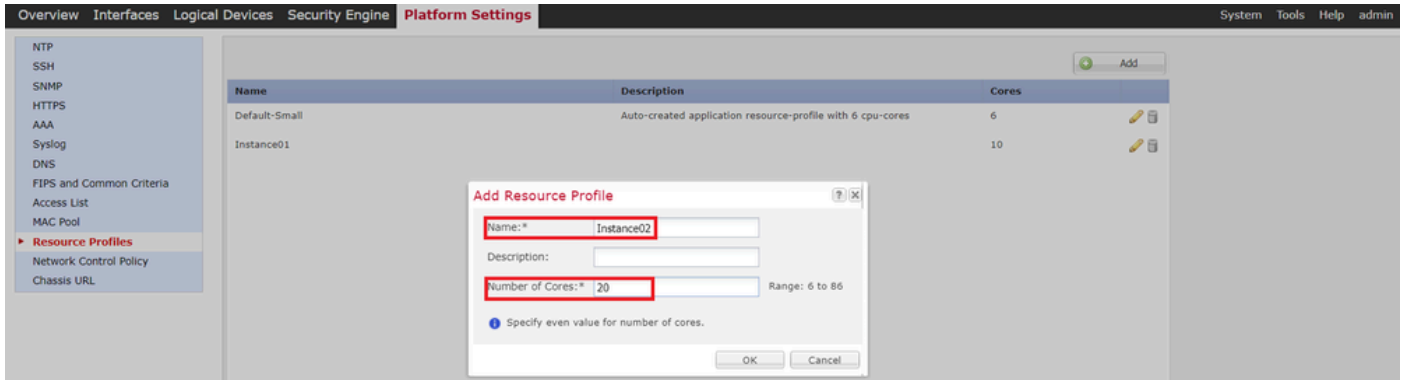


1番目のリソースプロファイルの追加

b.ステップ2のa.を繰り返して、2番目のリソースプロファイルを設定します。

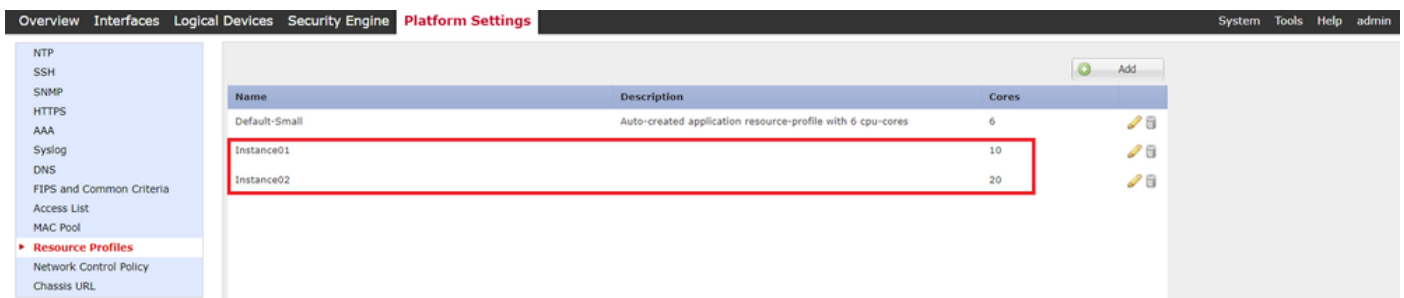
この例では、

- ・ 名前 : Instance02
- ・ コア数 : 20コア



2番目のリソースプロファイルの追加

c. 2つのリソースプロファイルが正常に追加されたことを確認します。



リソースプロファイルの確認

ステップ3: ( オプション ) コンテナインスタンスインターフェイスの仮想MACアドレスのMACプールプレフィックスを追加します。

アクティブ/スタンバイインターフェイスの仮想MACアドレスは手動で設定できます。マルチインスタンス機能のために仮想MACアドレスが設定されていない場合 ( デフォルト )、シャーシは自動的にインスタンスインターフェイスのMACアドレスを生成し、各インスタンスの共有インターフェイスが一意的MACアドレスを使用することを保証します。

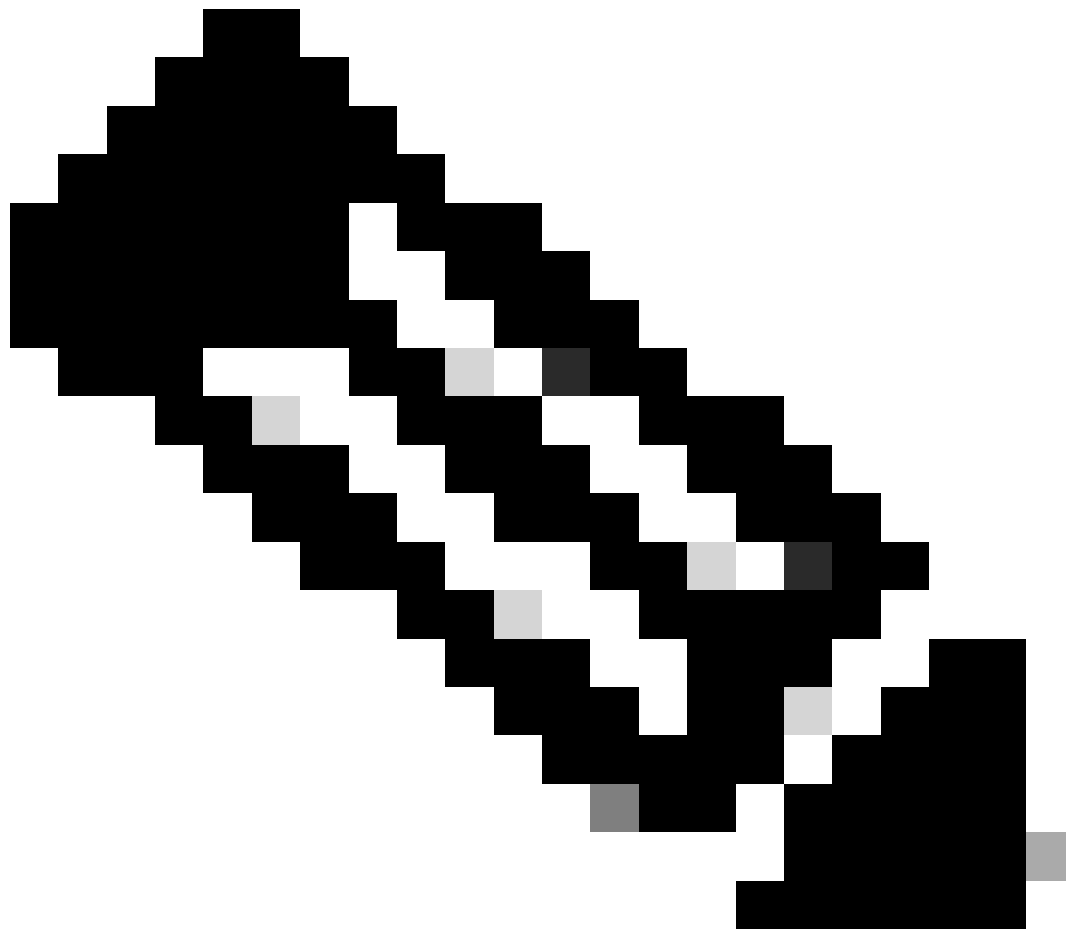
MACアドレスの詳細については、「[MACプールプレフィックスの追加とコンテナインスタンスインターフェイスのMACアドレスの表示](#)」を参照してください。

ステップ 4 : スタンドアロンインスタンスを追加します。

a. Logical Devices > Add Standaloneの順に移動します。第1インスタンスを設定します。

この例では、

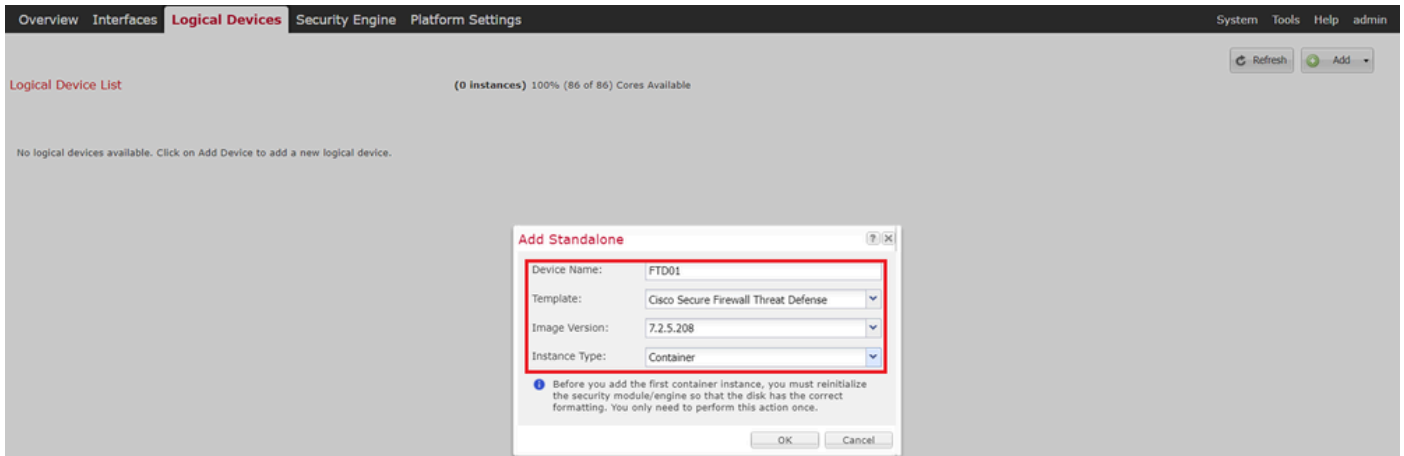
- ・ デバイス名 : FTD01



注 : コンテナアプリケーションを導入する唯一の方法は、インスタンスタイプをコンテナに設定したアプリケーションインスタンスを事前導入することです。Containerを選択したことを確認します。

論理デバイスを追加した後で、この名前を変更することはできません。

---



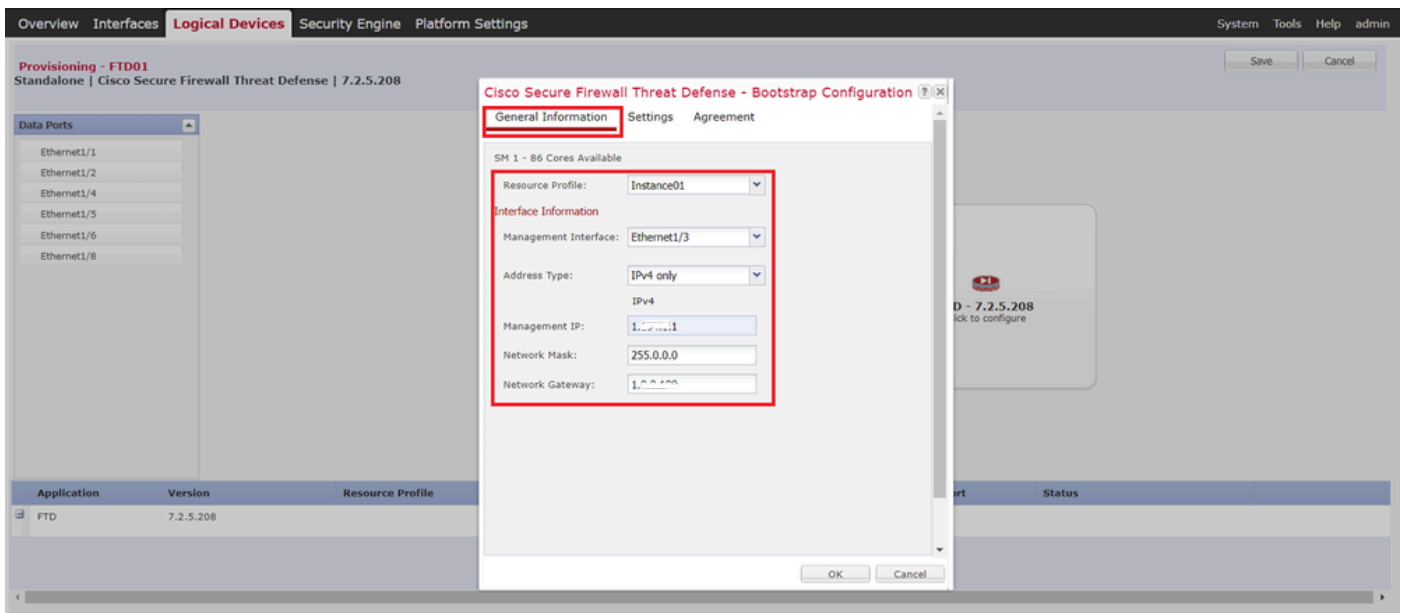
インスタンスの追加

## ステップ 5： インターフェイスの設定

a. Instance01のリソースプロファイル、管理インターフェイス、管理IPを設定します。

この例では、

- ・ リソースプロファイル： Instance01
- ・ 管理インターフェイス： Ethernet1/3
- ・ 管理IP： x.x.1.1



プロファイル/管理インターフェイス/管理IPの設定

b. データインターフェイスを設定します。

この例では、

- ・ Ethernet1/1 ( 内部で使用 )
- ・ Ethernet1/2 ( 外部用 )
- ・ Ethernet1/4 ( HAリンクに使用 )



Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208	Instance01	1.1.1.1	1.1.1.1	Ethernet1/3	Installing

データインターフェイスの設定

c. Logical Devicesに移動します。インスタンスのブートアップを待機しています。

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.2.5.208	Instance01	1.1.1.1	1.1.1.1	Ethernet1/3	Installing

Instance01のステータスの確認

d.手順4.aと手順5.a ~ cのa.を繰り返して2つ目のインスタンスを追加し、そのインスタンスの詳細を設定します。

この例では、

- ・ デバイス名 : FTD11
- ・ インスタンスタイプ : コンテナ
- ・ リソースプロファイル : Instance02
- ・ 管理インターフェイス : Ethernet1/7
- ・ 管理IP : x.x.10.1
- ・ Ethernet1/5 =内部
- ・ Ethernet1/6 =外部
- ・ Ethernet1/8 = HAリンク

e. FCMで2つのインスタンスがオンライン状態であることを確認します。

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available		
<b>FTD11</b>	Standalone	Status:ok							
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status			
FTD	7.2.5.208	Instance02	10.1	1.0.0.0	Ethernet1/7	Online			
<b>FTD01</b>	Standalone	Status:ok							
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status			
FTD	7.2.5.208	Instance01	10.1	1.0.0.0	Ethernet1/3	Online			

プライマリデバイスのインスタンスステータスの確認

f. ( オプション ) scope ssa を実行し、scope slot 1 および show app-Instance コマンドを実行して、2つのインスタンスが Firepower CLI でオンラインステータスであることを確認します。

<#root>

FPR4145-ASA-K9#

scope ssa

FPR4145-ASA-K9 /ssa #

scope slot 1

FPR4145-ASA-K9 /ssa/slot #

show app-Instance

```
Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deploy
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11
```

```
Online
```

```
7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online
```

g. セカンダリデバイスでも同じ操作を行います。2つのインスタンスがオンライン状態であることを確認します。

Logical Device List							(2 Container Instances) 66% (56 of 86) Cores Available		
<b>FTD12</b>	Standalone	Status:ok							
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status			
FTD	7.2.5.208	Instance02	10.2	1.0.0.0	Ethernet1/7	Online			
<b>FTD02</b>	Standalone	Status:ok							
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status			
FTD	7.2.5.208	Instance01	10.2	1.0.0.0	Ethernet1/3	Online			

セカンダリデバイスのインスタンスステータスの確認

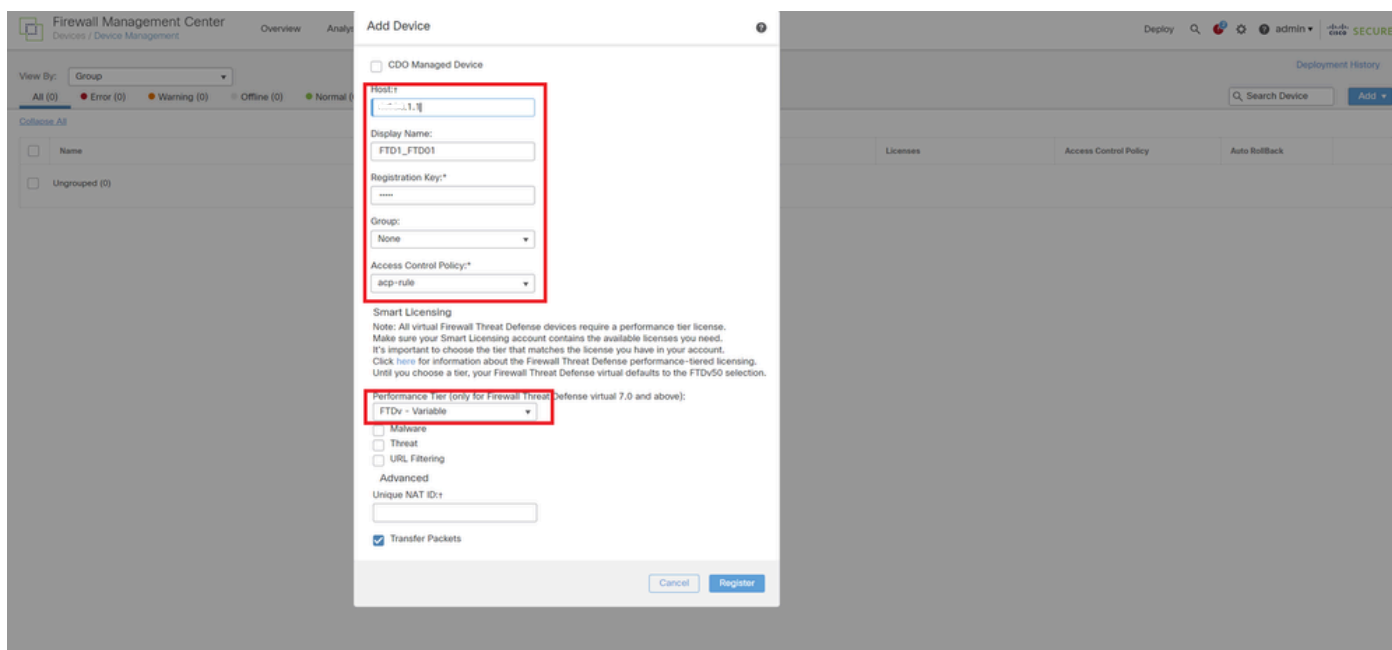
手順 6 : 各インスタンスにハイアベイラビリティペアを追加します。

A. FMCで、Devices > Add Deviceの順に移動します。FMCにすべてのインスタンスを追加します。

この例では、

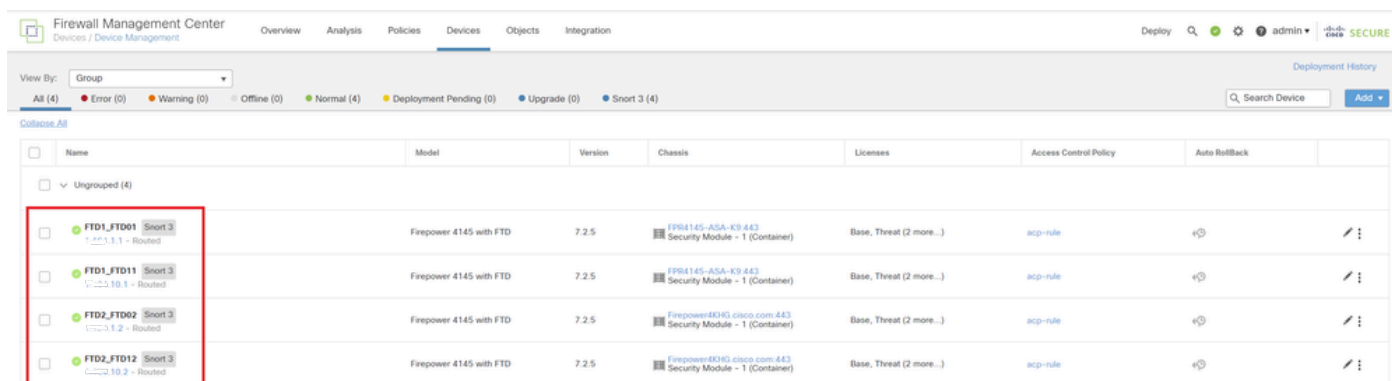
- ・ FTD1のInstance01の表示名：FTD1\_FTD01
- ・ FTD1のInstance02の表示名：FTD1\_FTD11
- ・ FTD2のInstance01の表示名：FTD2\_FTD02
- ・ FTD2のInstance02の表示名：FTD2\_FTD12

次の図にFTD1\_FTD01の設定を示します。



FMCへのFTDインスタンスの追加

b. すべてのインスタンスが正常であることを確認します。

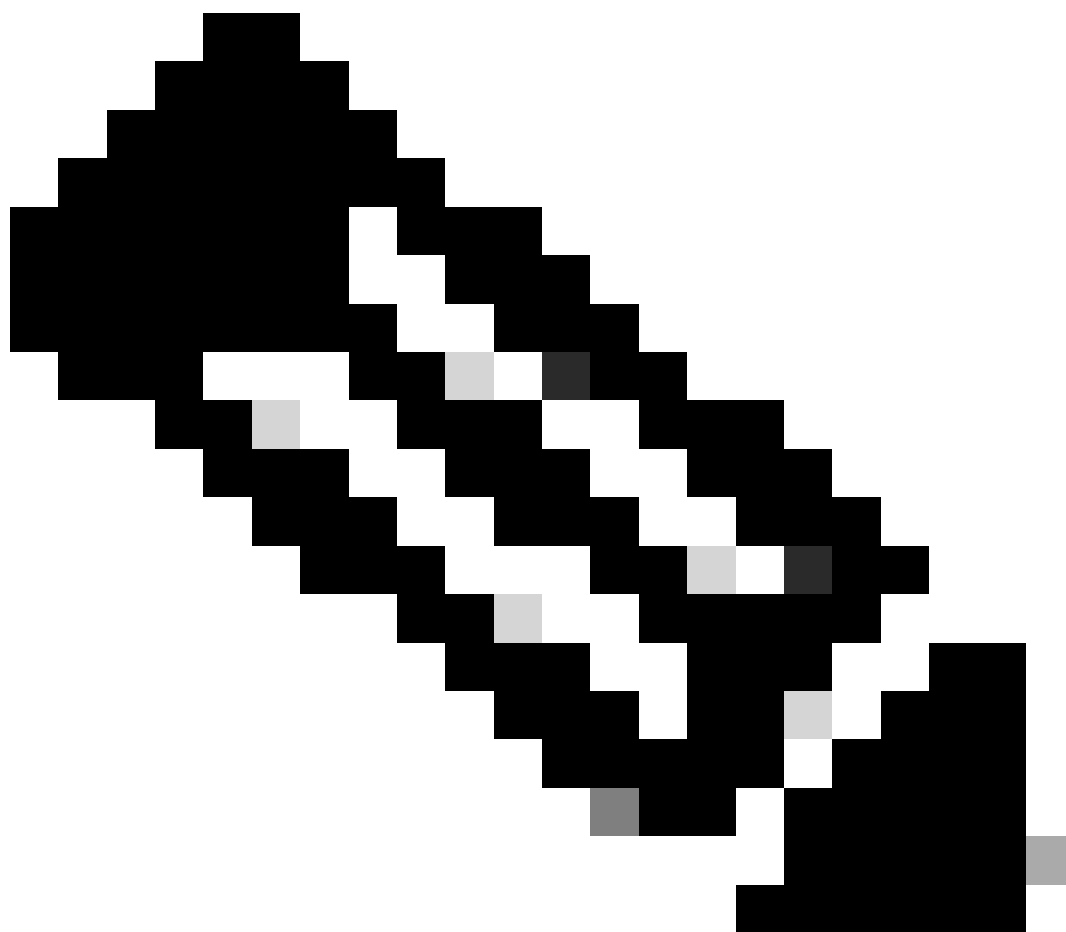


FMCでのインスタンスステータスの確認

c. Devices > Add High Availabilityの順に移動します。1番目のフェールオーバーペアを設定します。

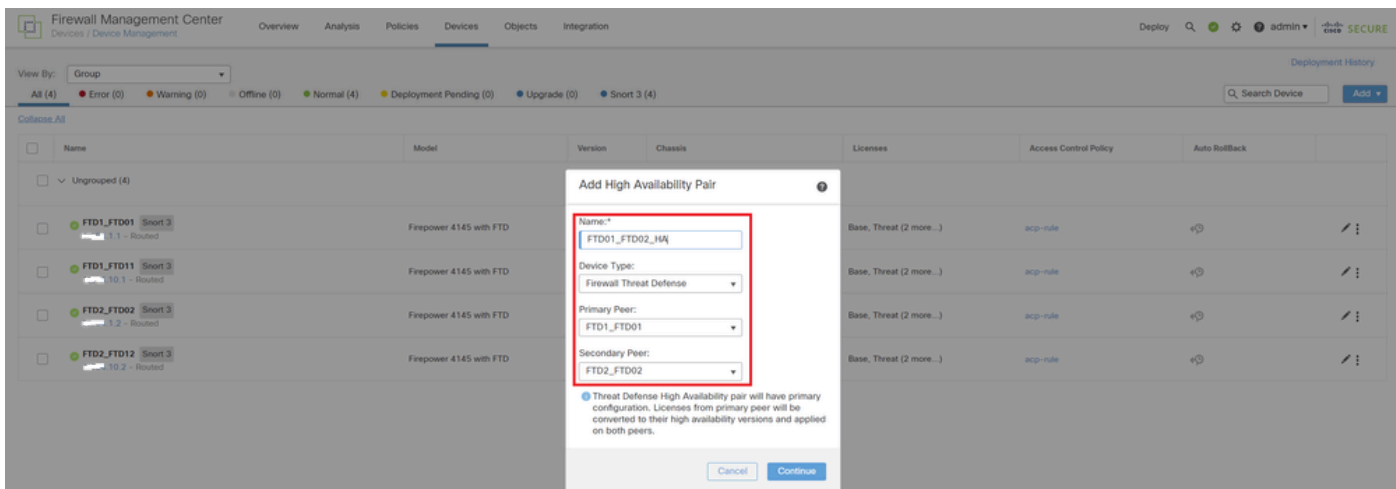
この例では、

- ・ 名称：FTD01\_FTD02\_HA
- ・ プライマリピア：FTD1\_FTD01



注 : 正しいユニットをプライマリユニットとして選択してください。

---

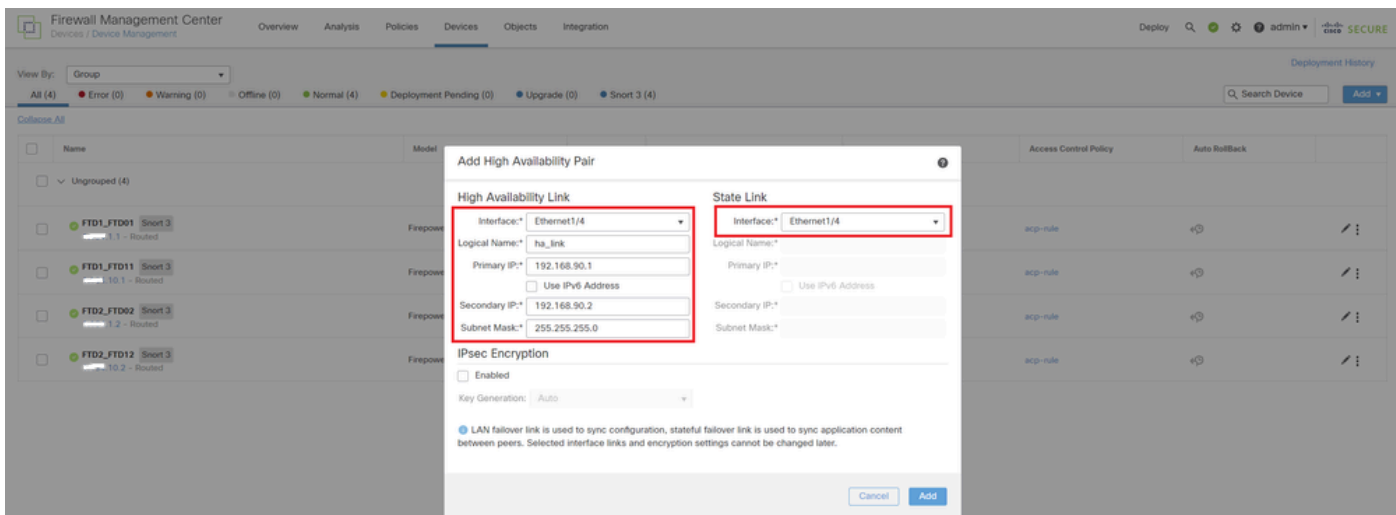


1番目のフェールオーバーペアの追加

d. 1番目のフェールオーバーペアのフェールオーバーリンクのIPを設定します。

この例では、

- ・ ハイアベイラビリティリンク : **Ethernet1/4**
- ・ ステートリンク : **Ethernet1/4**
- ・ プライマリIP:**192.168.90.1/24**
- ・ セカンダリIP:**192.168.90.2/24**



1番目のフェールオーバーペア用のHAインターフェイスとIPの設定

e. フェールオーバーのステータスを確認します

- ・ **FTD1\_FTD01** : プライマリ、アクティブ
- ・ **FTD2\_FTD02** : セカンダリ、スタンバイ

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Un grouped (3)						
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Active) v7.2.5 - Routed	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD2_FTD02(Secondary, Standby) v7.2.5 - Routed	Firepower 4145 with FTD	7.2.5	Firepower403HG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD1_FTD01 v7.2.5, 10.1 - Routed	Firepower 4145 with FTD	7.2.5	FP04145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+
FTD2_FTD02 v7.2.5, 10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower403HG.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+

最初のフェールオーバーペアのステータスの確認

f. **Devices**に移動し、**FTD01\_FTD02\_HA** (この例の場合) をクリックし、**Interfaces**をクリックします。データインターフェイスのアクティブIPを設定します。

この例では、

- Ethernet1/1 (内部) :192.168.10.254/24
- Ethernet1/2 (外部) :192.168.20.254/24
- Ethernet1/3 (診断) :192.168.80.1/24

次の図に、**Ethernet1/1**のアクティブIPの設定を示します。

FTD1\_FTD01  
Cisco Firepower 4145 Threat Defense

Summary High Availability Device Routing **Interfaces** Inline Se...

Interface	Log...
Ethernet1/1	inside
Ethernet1/2	outside
Ethernet1/3	diagnostic
Ethernet1/4	

**Edit Physical Interface**

General IPv4 IPv6 Path Monitoring Advanced

Name: inside

Enabled

Description:

Mode: None

Security Zone: inside\_zone

Interface ID: Ethernet1/1

MTU: 1500

Priority: 0

Propagate Security Group Tag:

NVE Only:

**Edit Physical Interface**

General IPv4 IPv6 Path Monitoring Advanced

IP Type: Use Static IP

IP Address: 192.168.10.254/24

Cancel OK

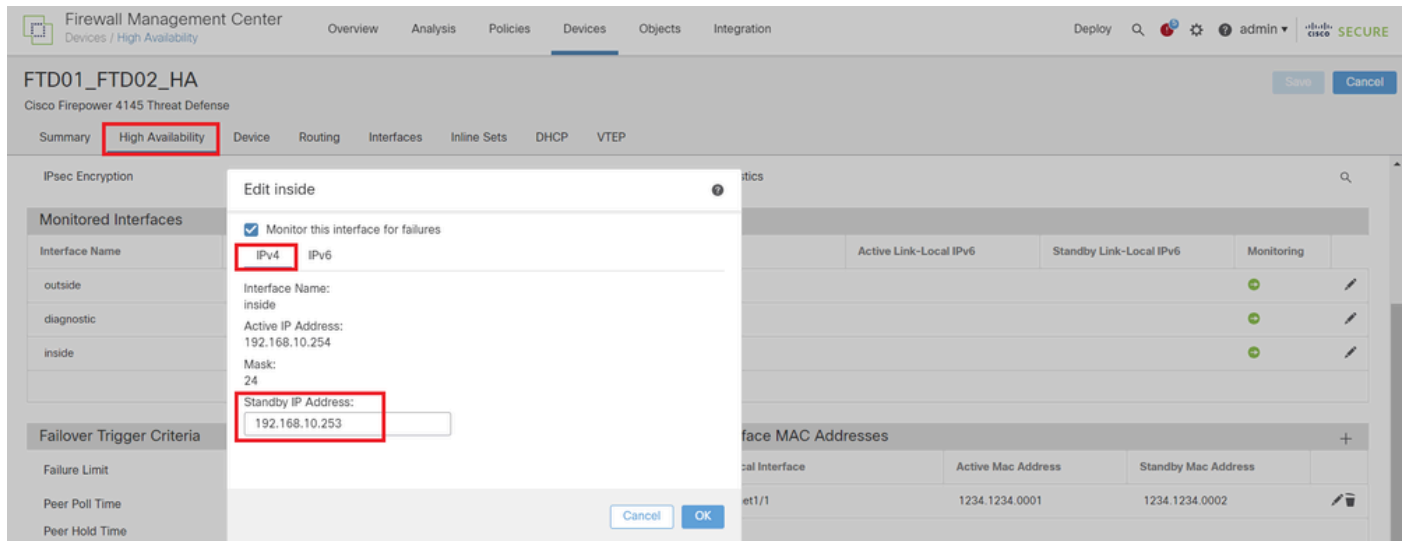
データインターフェイスのアクティブIPの設定

g. **Devices** > **Click FTD01\_FTD02\_HA** (この例の場合) > **High Availability**の順に移動します。データインターフェイスのスタンバイIPを設定します。

この例では、

- Ethernet1/1 (内部) :192.168.10.253/24
- Ethernet1/2 (外部) :192.168.20.253/24
- Ethernet1/3 (診断) :192.168.80.2/24

次の図に、Ethernet1/1のスタンバイIPの設定を示します。



データインターフェイスのスタンバイIPの設定

h.ステップ6.c ~ gを繰り返して、2番目のフェールオーバーペアを追加します。

この例では、

- ・ 名称 : FTD11\_FTD12\_HA
- ・ プライマリピア : FTD1\_FTD11
- ・ セカンダリピア : FTD2\_FTD12
  
- ・ ハイアベイラビリティリンク : Ethernet1/8
- ・ ステートリンク : Ethernet1/8
- ・ Ethernet1/8 ( ha\_linkアクティブ ) :192.168.91.1/24
  
- ・ Ethernet1/5 ( 内部アクティブ ) :192.168.30.254/24
- ・ Ethernet1/6 ( 外部アクティブ ) :192.168.40.254/24
- ・ Ethernet1/7 ( 診断アクティブ ) :192.168.81.1/24
  
- ・ Ethernet1/8 ( ha\_linkスタンバイ ) :192.168.91.2/24
  
- ・ Ethernet1/5 ( 内部スタンバイ ) :192.168.30.253/24
- ・ Ethernet1/6 ( 外部スタンバイ ) :192.168.40.253/24
- ・ Ethernet1/7 ( 診断スタンバイ ) :192.168.81.2/24

i. Logical Devices > Add Standaloneの順に移動します。内部から外部へのトラフィックを許可するようにACPルールを設定します

。

## ACPルールの設定

j. 設定をFTDに展開します。

k. CLIでのHAステータスの確認

各インスタンスのHAステータスは、ASAと同じFirepower CLIでも確認されます。

**show running-config failover** および **show failover** コマンドを実行して、FTD1\_FTD01 (プライマリインスタンス01) のHAステータスを確認します。

<#root>

```
// confirm HA status of FTD1_FTD01 (Instance01 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/4 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host: P
..... Other host: Secondary - Standby Ready <---- Instance01 of FPR02 is Standby Interface diagnostic
```

**show running-config failover** および **show failover** コマンドを実行して、FTD1\_FTD11のHAステータス (プライマリInstance02) を確認します。

<#root>

```
// confirm HA status of FTD1_FTD11 (Instance02 of Primary Device) >
```

```
show running-config failover
```

```
failover failover lan unit primary failover lan interface ha_link Ethernet1/8 failover replication http
```

```
show failover
```

```
Failover On Failover unit Primary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host: P
Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16
```

**show running-config failover** および **show failover** コマンドを実行して、FTD2\_FTD02 (セカンダリインスタンス01) のHAステータスを確認します。



<#root>

// confirm HA status of FTD2\_FTD02 (Instance01 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/4 failover replication h

show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host:  
Other host: Primary - Active <---- Instance01 of FPR01 is Active Active time: 31651 (sec) slot 0: UCSB-

show running-config failover および show failover コマンドを実行して、FTD2\_FTD12 (セカンダリInstance02) のHAステータスを確認します。

<#root>

// confirm HA status of FTD2\_FTD12 (Instance02 of Secondary Device) >

show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/8 failover replication h  
Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

#### 1. ライセンス消費の確認

すべてのライセンスは、コンテナインスタンスごとではなく、セキュリティエンジン/シャーシごとに消費されます。

- ・ ベースライセンスは自動的に割り当てられます : セキュリティエンジン/シャーシごとに1つ。
- ・ 機能ライセンスは各インスタンスに手動で割り当てられますが、使用するライセンスは機能エンジン/シャーシあたり1つだけです。特定の機能ライセンスに必要なライセンスは、使用中のインスタンスの数に関係なく、合計1つだけです。

次の表に、このドキュメントでライセンスがどのように消費されるかを示します。

FPR01	インスタンス01	ベース、URLフィルタリング、マルウェア、脅威
	インスタンス02	ベース、URLフィルタリング、マルウェア、脅威
FPR02	インスタンス01	ベース、URLフィルタリング、マルウェア、脅威
	インスタンス02	ベース、URLフィルタリング、マルウェア、脅威

## ライセンスの総数

ベース	URL フィルタリング	マルウェア	脅威
2	2	2	2

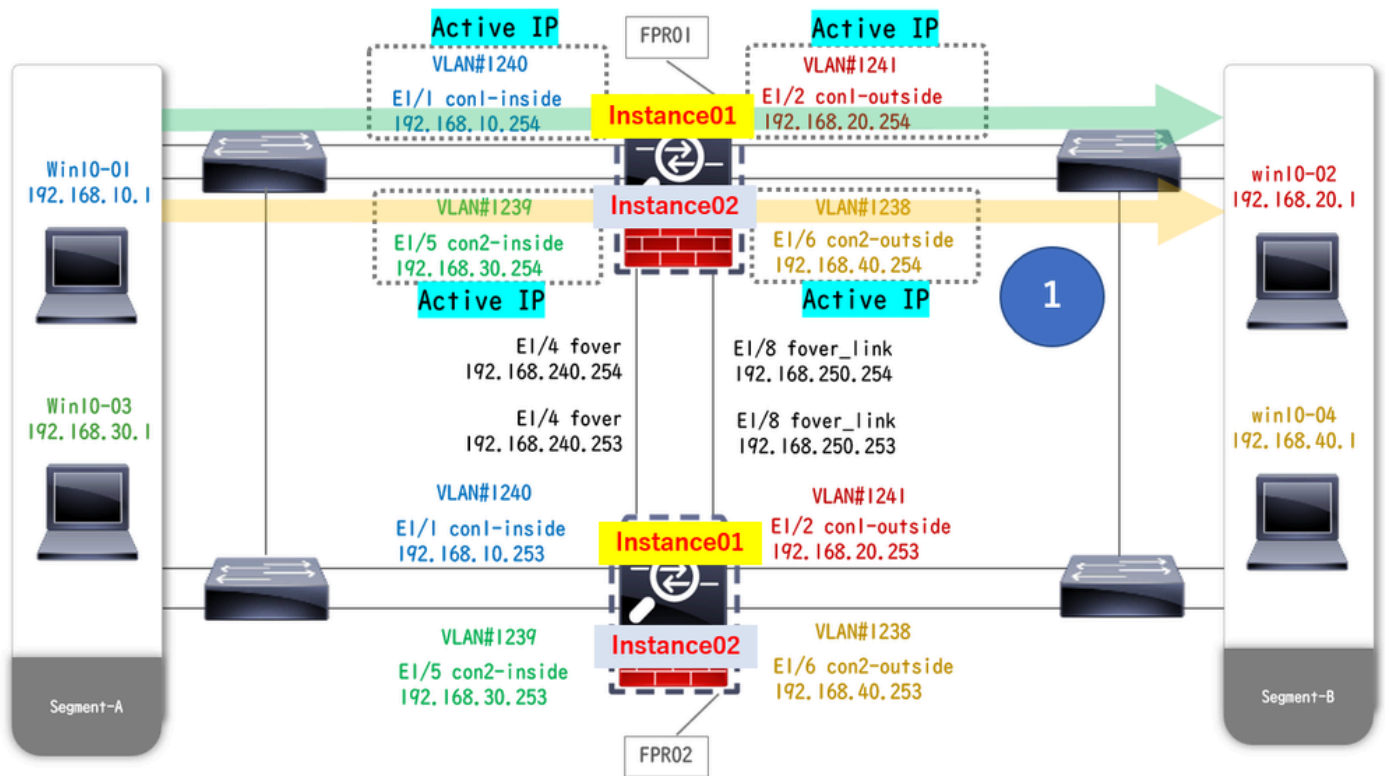
FMC GUIで消費されたライセンス数を確認します。

License Type/Device Name	License Status	Device Type	Domain	Group
Base (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Malware (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
Threat (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
URL Filtering (2)	In-Compliance			
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Threat Defense	Global	N/A

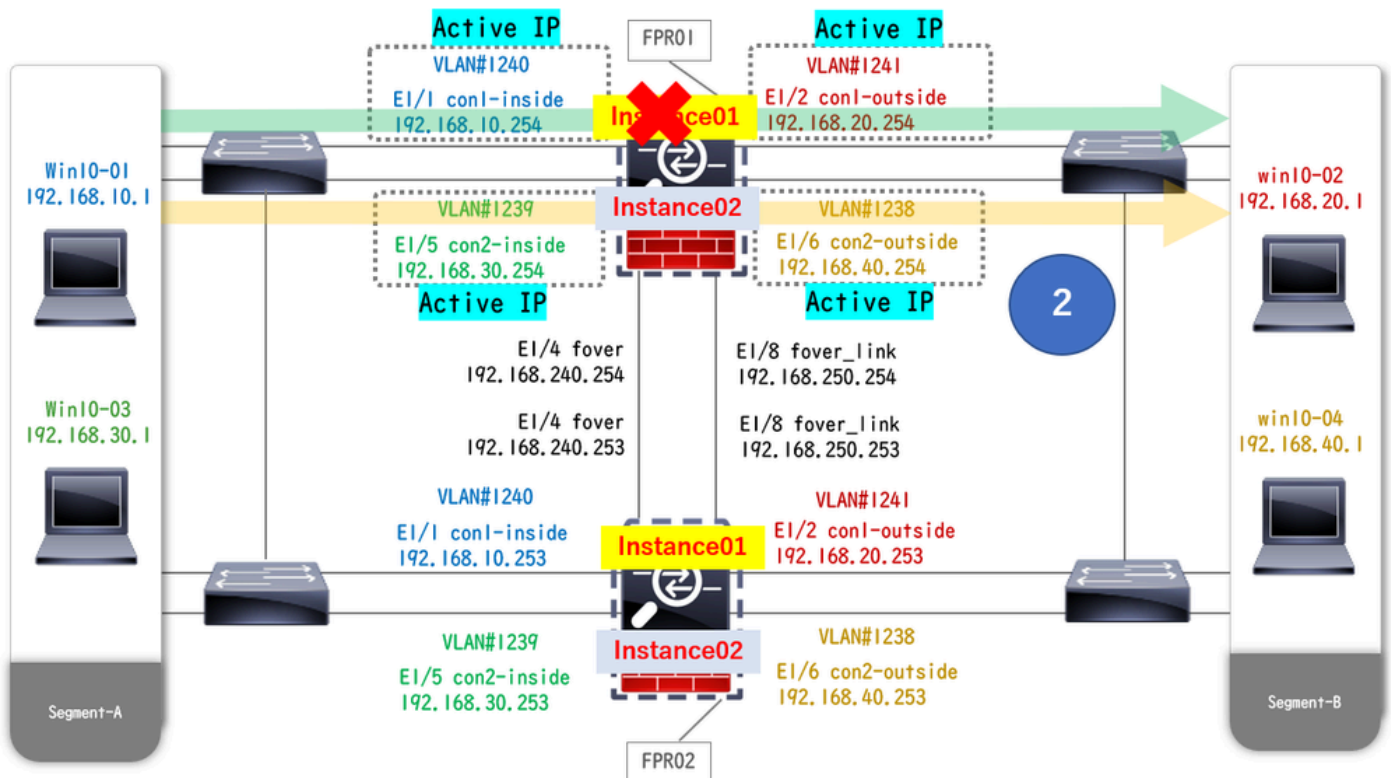
## 使用したライセンスの確認

### 確認

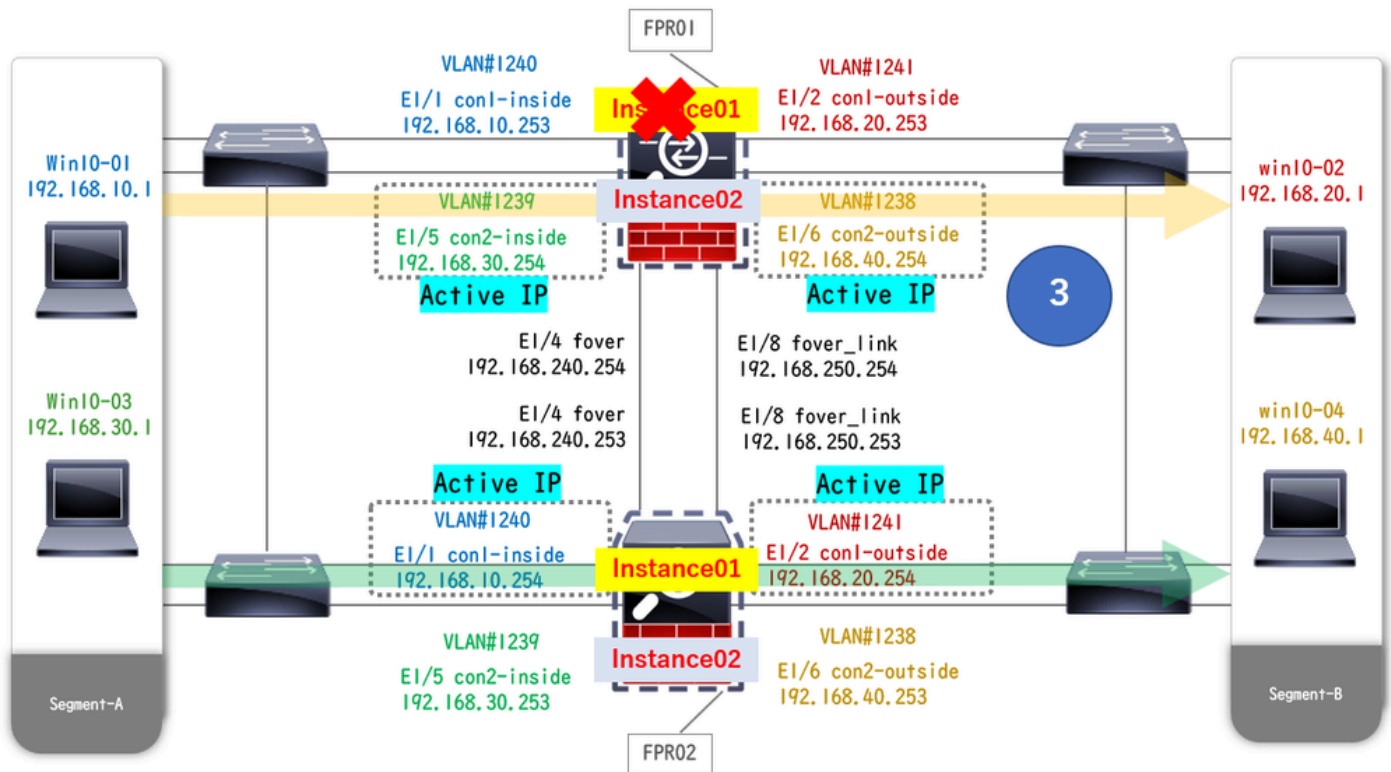
FTD1\_FTD01 (プライマリインスタンス01) でクラッシュが発生すると、インスタンス01のフェールオーバーがトリガーされ、スタンバイ側のデータインターフェイスが元のアクティブインターフェイスのIP/MACアドレスを引き継いで、トラフィック(このドキュメントではFTP接続)がFirepowerによって継続的に渡されるようになります。



クラッシュ前



クラッシュ中



フェールオーバーがトリガーされる

ステップ 1 : Win10-01からWin10-02へのFTP接続を開始します。

ステップ 2 : show conn コマンドを実行して、Instance01の両方でFTP接続が確立されていることを確認します。

<#root>

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

ステップ 3 : Win10-03からWin10-04へのFTP接続を開始します。

ステップ 4 : show conn コマンドを実行して、FTP接続が両方のInstance02で確立されていることを確認します。

<#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm
```

```
show conn
```

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1
```

ステップ 5 : connect ftd FTD01コマンドおよび system support diagnostic-cliコマンドを実行して、ASA CLIに入ります。 enableおよび crashinfo force watchdog コマンドを実行して、プライマリ/アクティブ装置のInstance01を強制的にクラッシュさせます。

```
<#root>
```

```
Firepower-module1>
```

```
connect ftd FTD01
```

```
>
```

```
system support diagnostic-cli
```

```
FTD01>
```

```
enable
```

```
Password: FTD01# FTD01#
```

```
crashinfo force watchdog
```

```
reboot. Do you wish to proceed? [confirm]:
```

手順 6 : Instance01でフェールオーバーが発生し、FTP接続は中断されません。 show failoverコマンドおよび show connコマンドを実行して、FPR02でのInstance01のステータスを確認します。

```
<#root>
```

```
>
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/4 (up) ..... This host:
Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside (
```

```
show conn
```

```
TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1
```

手順 7 : Instance01で発生したクラッシュは、Instance02には影響を及ぼしませんでした。 show failoverコマンドおよび show connコマンドを実行して、Instance02のステータスを確認します。

```
<#root>
```

```
>
```

```
show failover
```

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host:  
Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1

ステップ 8 : FMCで、Devices > Allの順に移動します。HAステータスを確認します。

- ・ FTD1\_FTD01 : プライマリ、スタンバイ
- ・ FTD2\_FTD02 : セカンダリ、アクティブ

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Un grouped (2)						
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145G.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD11_FTD12_HA High Availability						
FTD1_FTD11(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD12(Secondary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145G.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞

HAステータスの確認

ステップ9: ( オプション ) FPR01のInstance01が通常に戻った後で、手動でHAのステータスを切り替えることができます。これは、FMC GUIまたはFRP CLIのいずれかによって実行できます。

FMCで、Devices > Allの順に移動します。Switch Active Peerをクリックして、FTD01\_FTD02\_HAのHAステータスをスイッチします。

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Un grouped (2)						
FTD01_FTD02_HA High Availability						
FTD1_FTD01(Primary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD02(Secondary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145G.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD11_FTD12_HA High Availability						
FTD1_FTD11(Primary, Active) Snort 3	Firepower 4145 with FTD	7.2.5	FPR0145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞
FTD2_FTD12(Secondary, Standby) Snort 3	Firepower 4145 with FTD	7.2.5	Firepower4145G.cisco.com:443 Security Module - 1 (Container)	Base, Threat (2 more...)	acp-rule	+⊞

スイッチのHAステータス

Firepower CLIで、connect ftd FTD01コマンドと system support diagnostic-cliコマンドを実行し、ASA CLIに入ります。  
FTD01\_FTD02\_HAのHAをスイッチするために、enableおよび failover active コマンドを実行します。

```
<#root>
```

```
Firepower-module1>
```

```
connect ftd FTD01
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of available commands.
```

```
enable
```

```
firepower#
```

```
failover active
```

トラブルシューティング

フェールオーバーのステータスを検証するには、show failover コマンドと show failover history コマンドを実行します。

```
<#root>
```

```
>
```

```
show failover
```

```
Failover On Failover unit Secondary Failover LAN Interface: ha_link Ethernet1/8 (up) ..... This host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (192.168.81.1) (up) .....
```

```
>
```

```
show failover history
```

```
===== From State To State Reason =====
```

debug fover コマンドを実行して、フェールオーバーのデバッグログを有効にします。

```
<#root>
```

```
>
```

```
debug fover
```

```
auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution
```

## 参考

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html>

[https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance\\_solution.html](https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance_solution.html)

<https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497>



## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。