Configuration de la haute disponibilité multiinstance FTD sur Firepower 4100

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Diagramme du réseau

Configurations

- Étape 1. Pré-configuration des interfaces
- Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur.
- Étape 3. (Facultatif) Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur.
- Étape 4. Ajouter une instance autonome.
- Étape 5. Configuration des interfaces
- Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.

Vérifier

Dépannage

Référence

Introduction

Ce document décrit comment configurer le basculement dans les instances de conteneur FTD (multi-instance).

Conditions préalables

Exigences

Cisco vous recommande de connaître Firepower Management Center et Firewall Threat Defense.

Composants utilisés

Cisco Firepower Management Center Virtual 7.2.5
Périphérique de pare-feu de nouvelle génération Cisco Firepower 4145 (FTD) 7.2.5
Système d'exploitation extensible Firepower (FXOS) 2.12 (0.498)
Windows 10

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.

Avant de déployer FTD Multi-Instance, il est important de comprendre l'impact que cela peut avoir sur les performances de votre système et de planifier en conséquence. Reportez-vous toujours à la documentation officielle de Cisco ou consultez un représentant technique Cisco pour garantir un déploiement et une configuration optimaux.

Informations générales

Multi-Instance est une fonctionnalité de Firepower Threat Defense (FTD) qui est similaire au mode de contexte multiple ASA. Il vous permet d'exécuter plusieurs instances de conteneur distinctes de FTD sur un seul composant matériel. Chaque instance de conteneur permet une séparation des ressources matérielles, une gestion de la configuration séparée, des rechargements séparés, des mises à jour logicielles distinctes et une prise en charge complète des fonctions de défense contre les menaces. Cela est particulièrement utile pour les entreprises qui ont besoin de politiques de sécurité différentes pour différents services ou projets, mais qui ne souhaitent pas investir dans plusieurs appliances matérielles distinctes. La fonctionnalité Multi-Instance est actuellement prise en charge sur les appliances de sécurité des gammes Firepower 4100 et 9300 exécutant FTD 6.4 et versions ultérieures.

Ce document utilise Firepower4145 qui prend en charge un maximum de 14 instances de conteneur. Pour connaître le nombre maximal d'instances prises en charge dans l'appliance Firepower, veuillez vous reporter à Nombre maximal d'instances de conteneur et ressources par modèle.

Diagramme du réseau

Ce document présente la configuration et la vérification de la haute disponibilité dans Multi-Instance sur ce schéma.

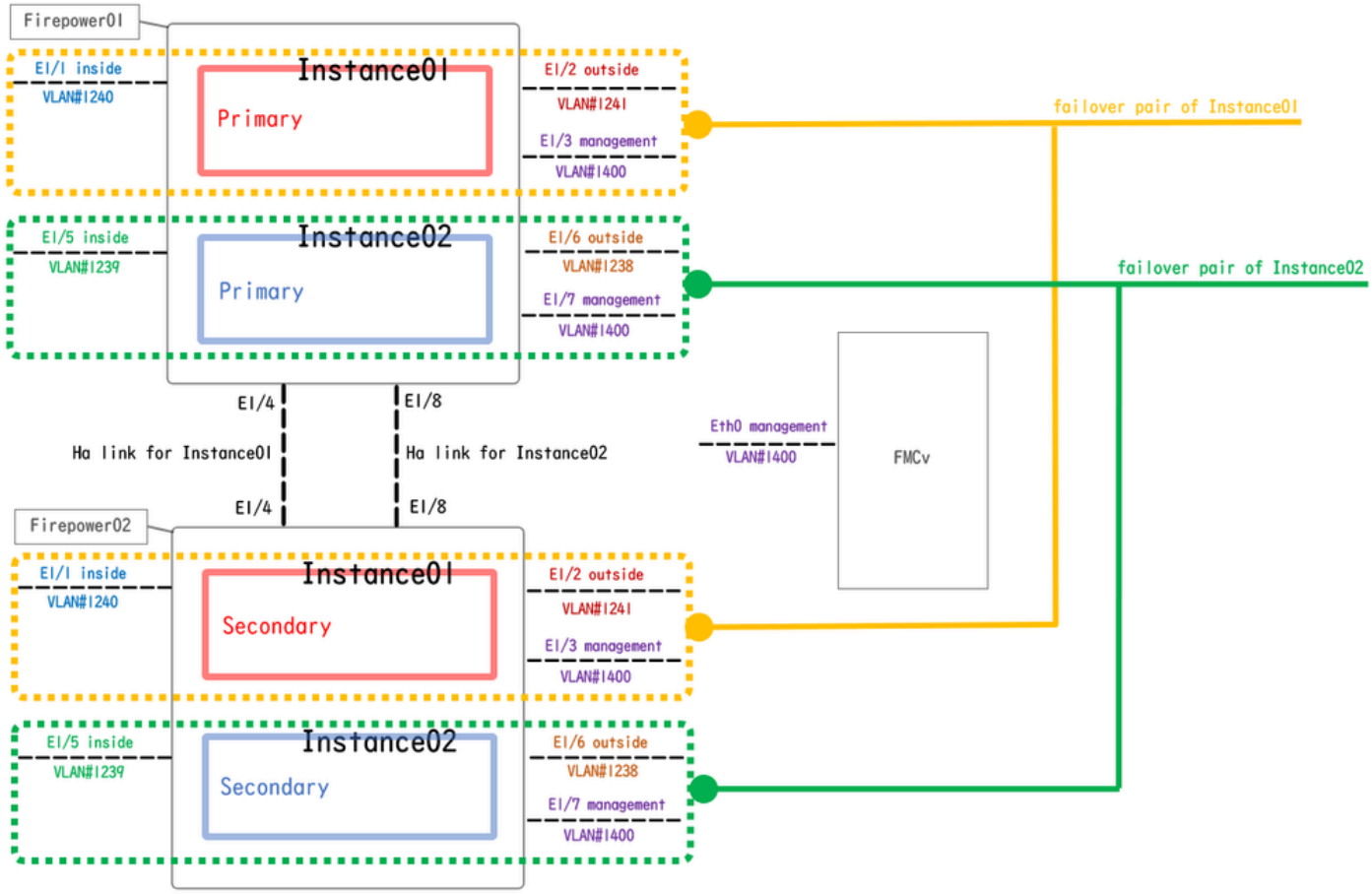


Diagramme de configuration logique

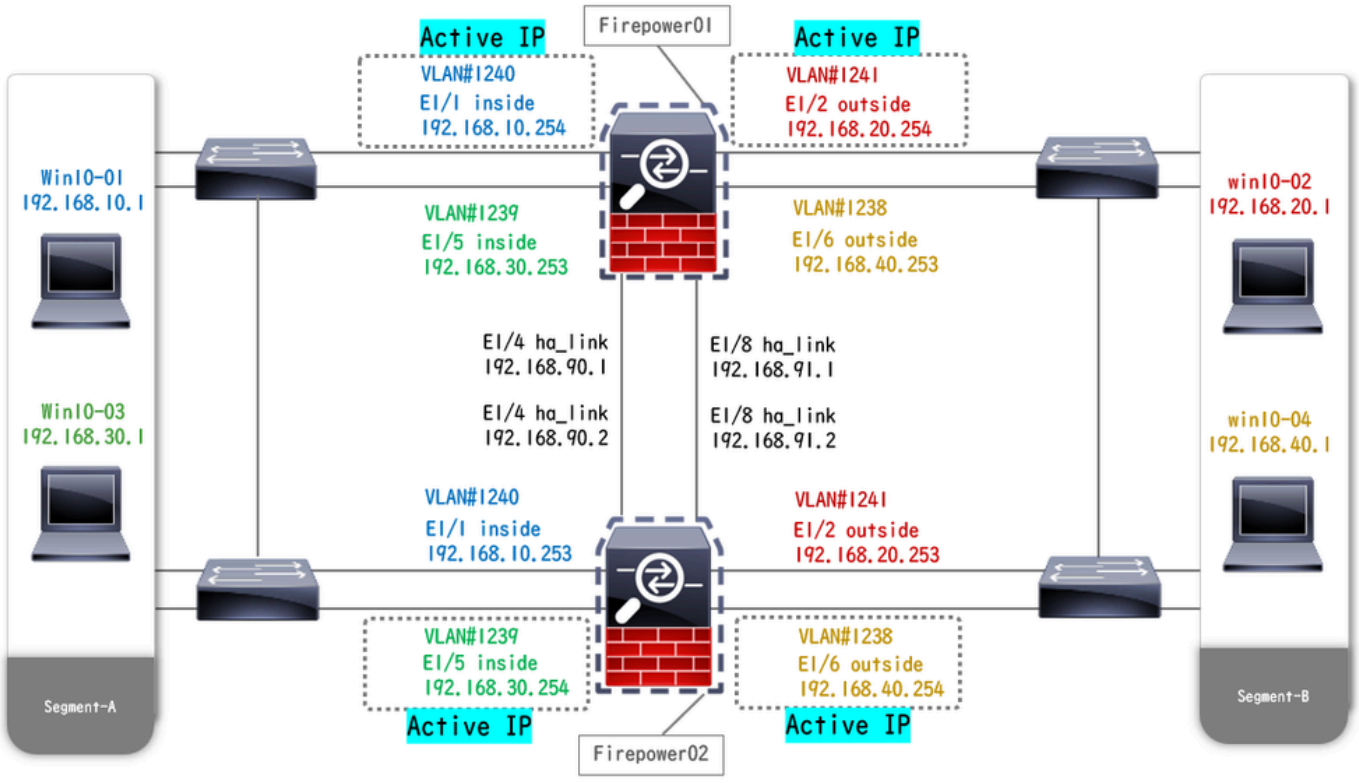
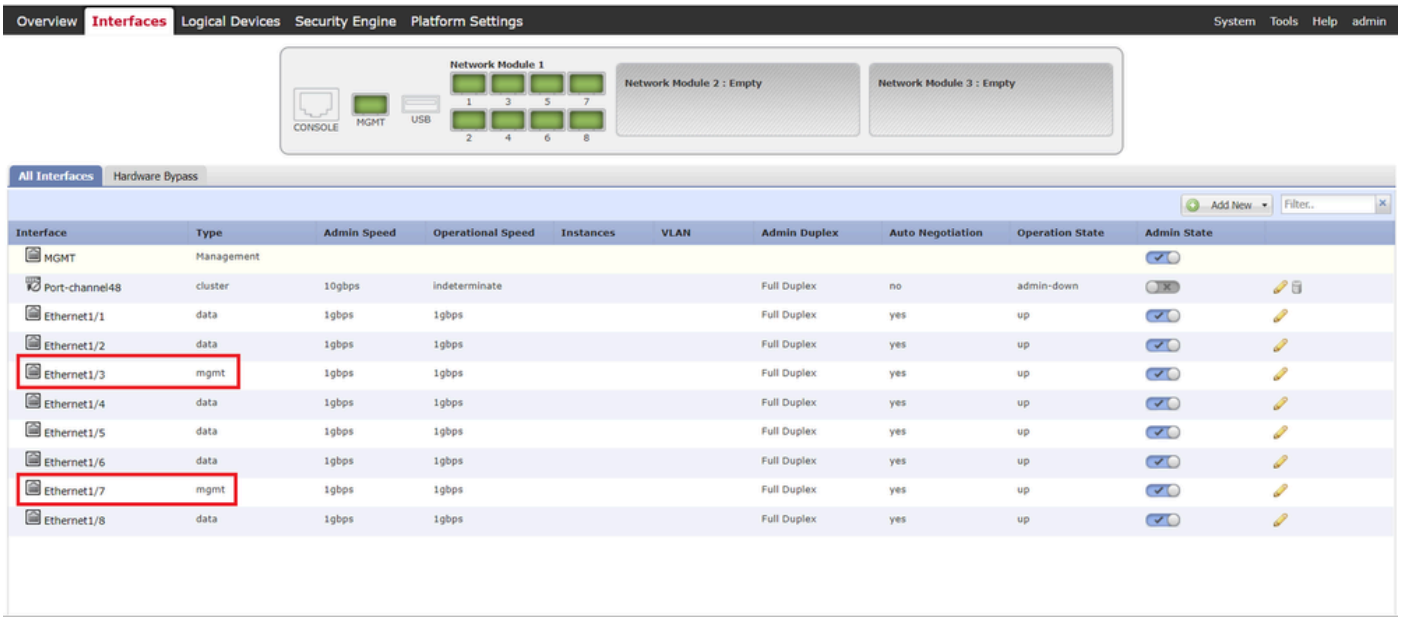


Schéma de configuration physique

Configurations

Étape 1. Pré-configuration des interfaces

a. Accédez à Interfaces sur FCM. Définissez 2 interfaces de gestion. Dans cet exemple, Ethernet1/3 et Ethernet1/7.



Pré-configuration des interfaces

Étape 2. Ajoutez 2 profils de ressources pour les instances de conteneur.

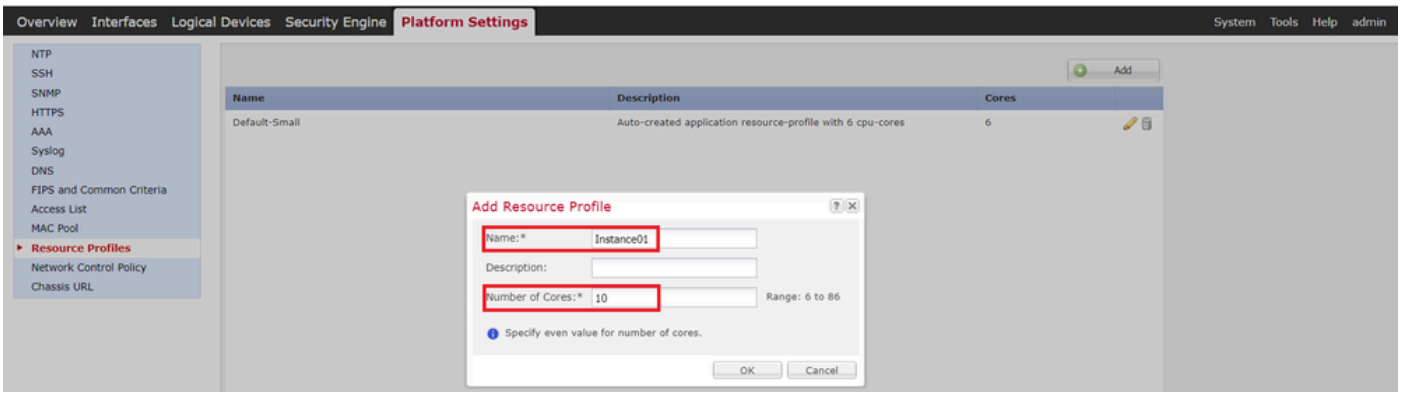
a. Accédez à Platform Settings > Resource Profiles > Add on FCM. Définissez le 1er profil de ressource.

Dans cet exemple :
·Nom : Instance01
· Nombre de coeurs : 10

Remarque : pour la haute disponibilité d'une paire d'instances de conteneur, ils doivent utiliser les mêmes attributs de profil de ressource.

Définissez le nom du profil entre 1 et 64 caractères. Notez que vous ne pouvez pas modifier le nom de ce profil après l'avoir ajouté.

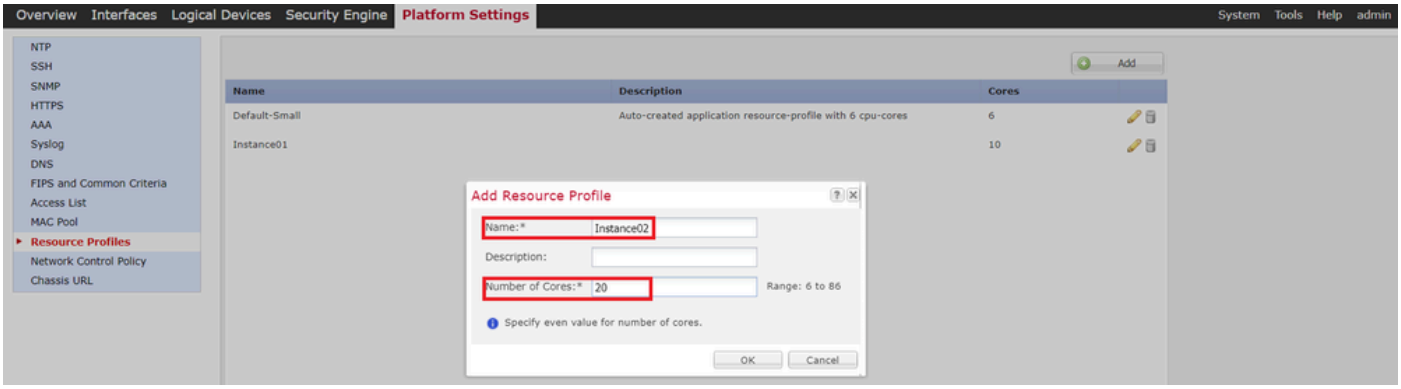
Définissez le nombre de coeurs pour le profil, entre 6 et le maximum.



Ajouter le 1er profil de ressource

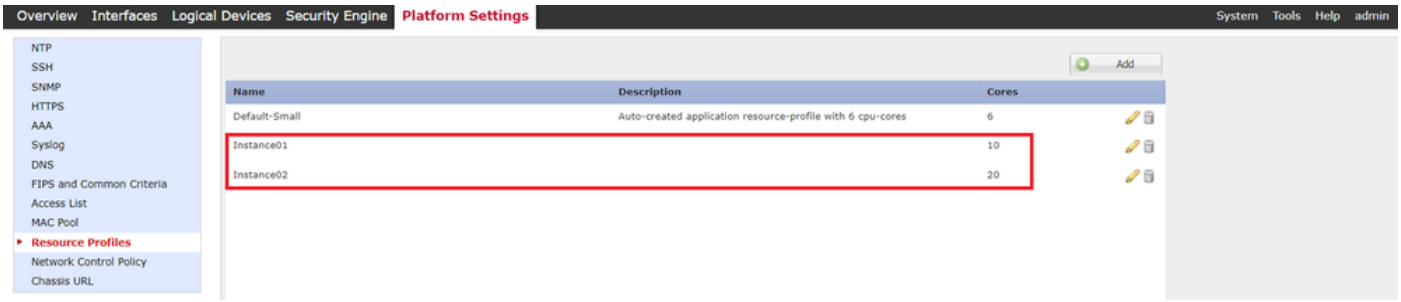
b. Répétez la procédure a. à l'étape 2, pour configurer le 2e profil de ressources.

Dans cet exemple :
·Nom : Instance02
· Nombre de coeurs : 20



Ajouter un 2e profil de ressources

c. Vérifiez que 2 profils de ressources ont bien été ajoutés.



Confirmer le profil de ressource

Étape 3. (Facultatif)Ajoutez un préfixe de pool MAC d'adresse MAC virtuelle pour les interfaces d'instance de conteneur.

Vous pouvez définir manuellement l'adresse MAC virtuelle pour l'interface active/veille. Si les adresses MAC virtuelles ne sont pas définies pour la fonctionnalité multi-instance , le châssis génère automatiquement des adresses MAC pour les interfaces d'instance et garantit qu'une interface partagée dans chaque instance utilise une adresse MAC unique.

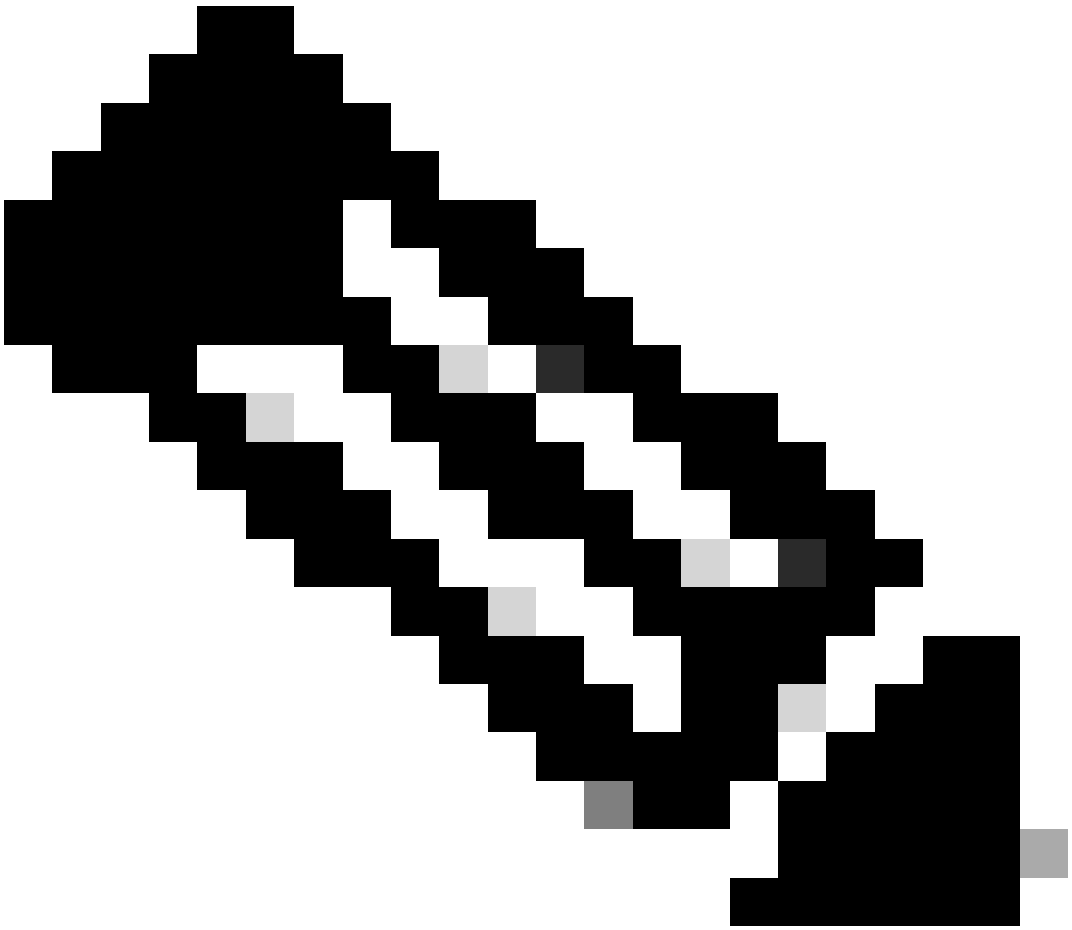
Veuillez vérifier Ajouter un préfixe de pool MAC et Afficher les adresses MAC pour les interfaces d'instance de conteneur pour plus de détails sur l'adresse MAC.

Étape 4. Ajouter une instance autonome.

a. Accédez à Logical Devices > Add Standalone. Définissez la 1ère instance.

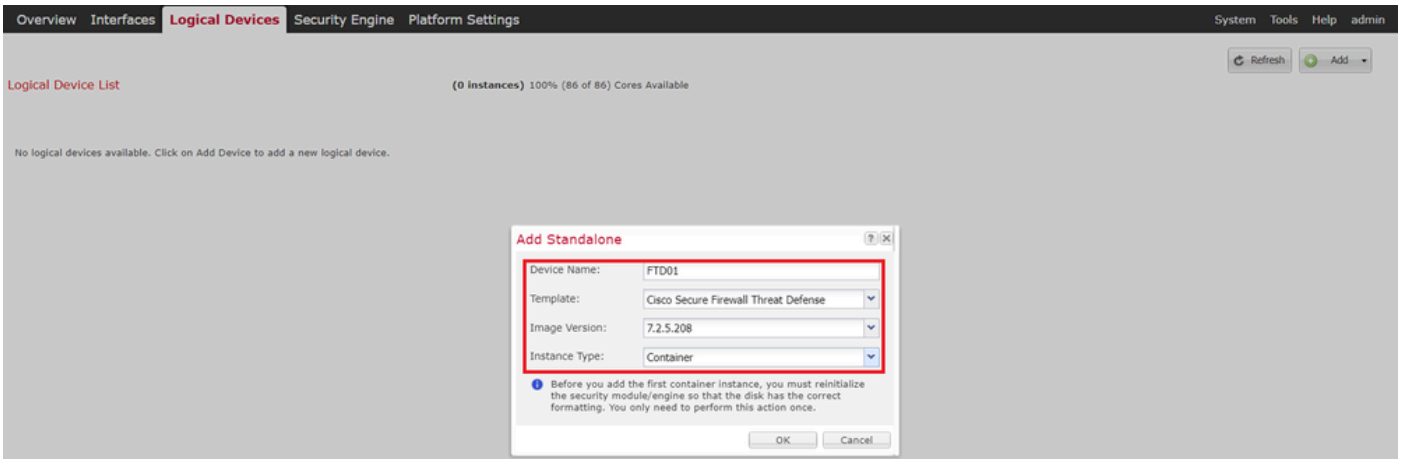
Dans cet exemple :
· Nom du périphérique : FTD01

· Type d'instance : conteneur



Remarque : la seule façon de déployer une application conteneur est de prédéployer une instance d'application avec le type d'instance défini sur Conteneur. Assurez-vous de sélectionner Container.

Vous ne pouvez pas modifier ce nom après avoir ajouté le périphérique logique.

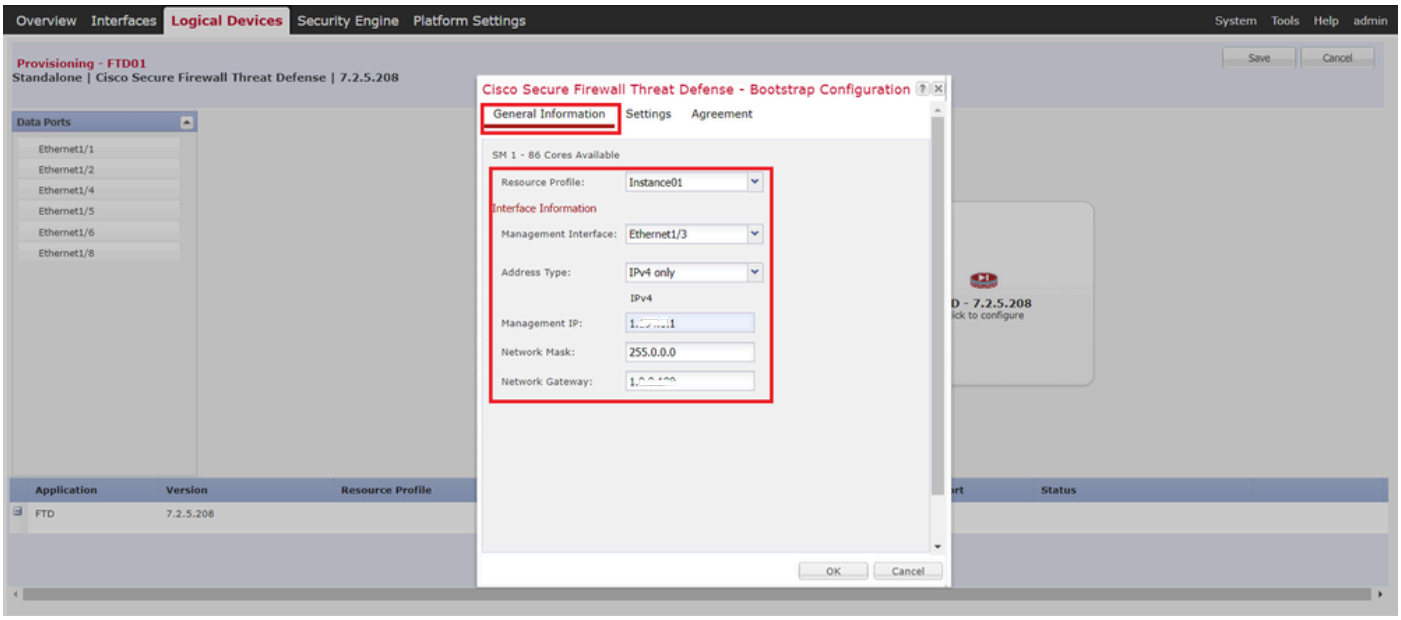


Ajouter une instance

Étape 5. Configuration des interfaces

a. Définissez Profil de ressource, Interface de gestion, IP de gestion pour Instance01.

Dans cet exemple :
· Profil de ressource : Instance01
· Interface de gestion : Ethernet1/3
·IP de gestion : x.x.1.1



Configuration du profil/interface de gestion/IP de gestion

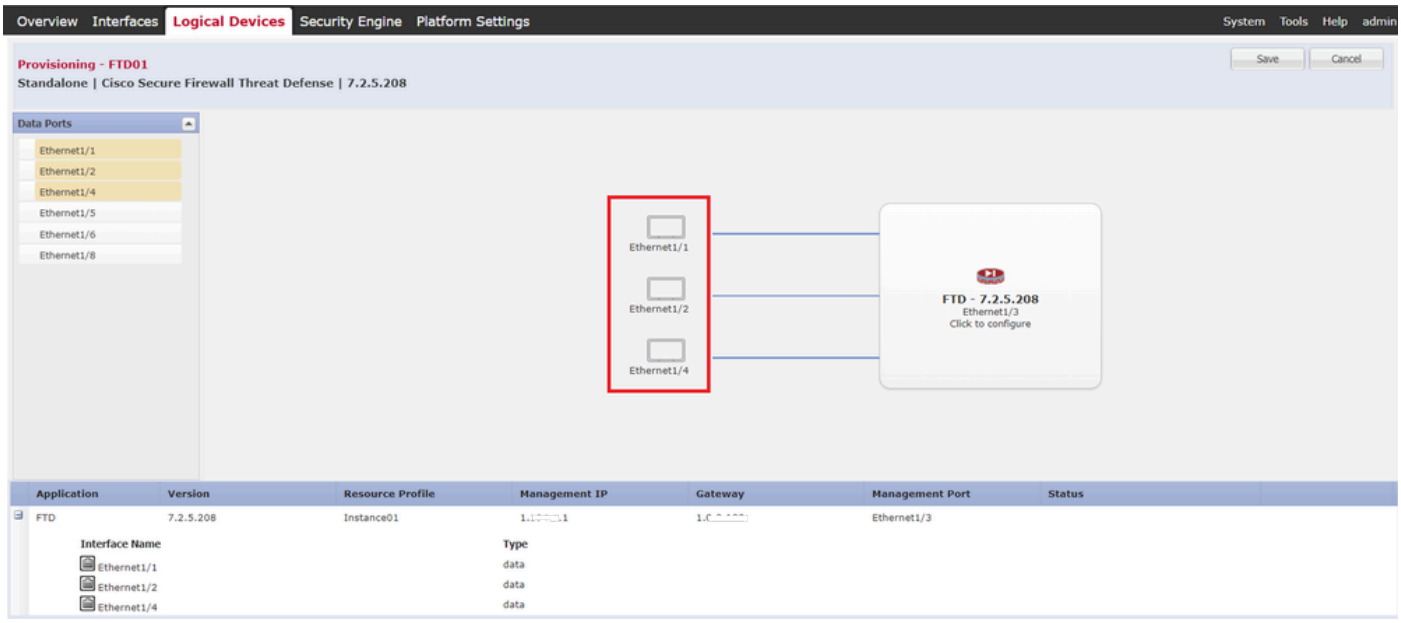
b. Définissez les interfaces de données.

Dans cet exemple :

·Ethernet1/1 (utilisé pour l'intérieur)

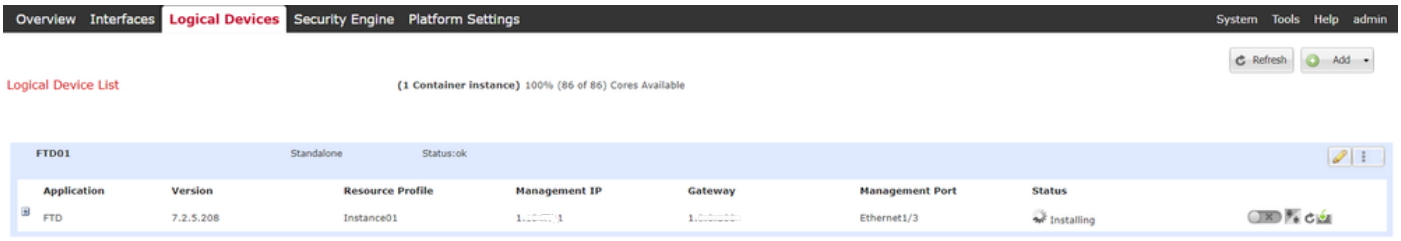
·Ethernet1/2 (utilisé pour l'extérieur)

·Ethernet1/4 (utilisé pour la liaison haute disponibilité)



Définition des interfaces de données

c. Accédez à Logical Devices. Attente du démarrage de l'instance.



Confirmer l'état de Instance01

d. Répétez a. aux étapes 4.a et 5.a à c pour ajouter la 2e instance et définir les détails correspondants.

Dans cet exemple :

·Nom du périphérique : FTD11
·Type d'instance : Conteneur

·Profil de ressource : Instance02
·Interface de gestion : Ethernet1/7
·IP de gestion : x.x.10.1

·Ethernet1/5 = interne

·Ethernet1/6 = extérieur

·Ethernet1/8 = liaison haute disponibilité

e. Confirmez que 2 instances sont en ligne sur FCM.

Confirmer l'état des instances dans le périphérique principal

f. (Facultatif) Exécutez scope ssa , **scope slot 1** et **show app-Instance** commande pour confirmer que 2 instances sont en ligne sur l'interface de ligne de commande Firepower.

```
<#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 Deplo

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. Procédez de la même manière sur le périphérique secondaire. Confirmez que 2 instances ont l'état En ligne.

Confirmer l'état de l'instance dans le périphérique secondaire

Étape 6. Ajoutez Une Paire Haute Disponibilité Pour Chaque Instance.

a. Accédez à **Devices** > **Add Device** sur FMC. Ajoutez toutes les instances à FMC.

Dans cet exemple :

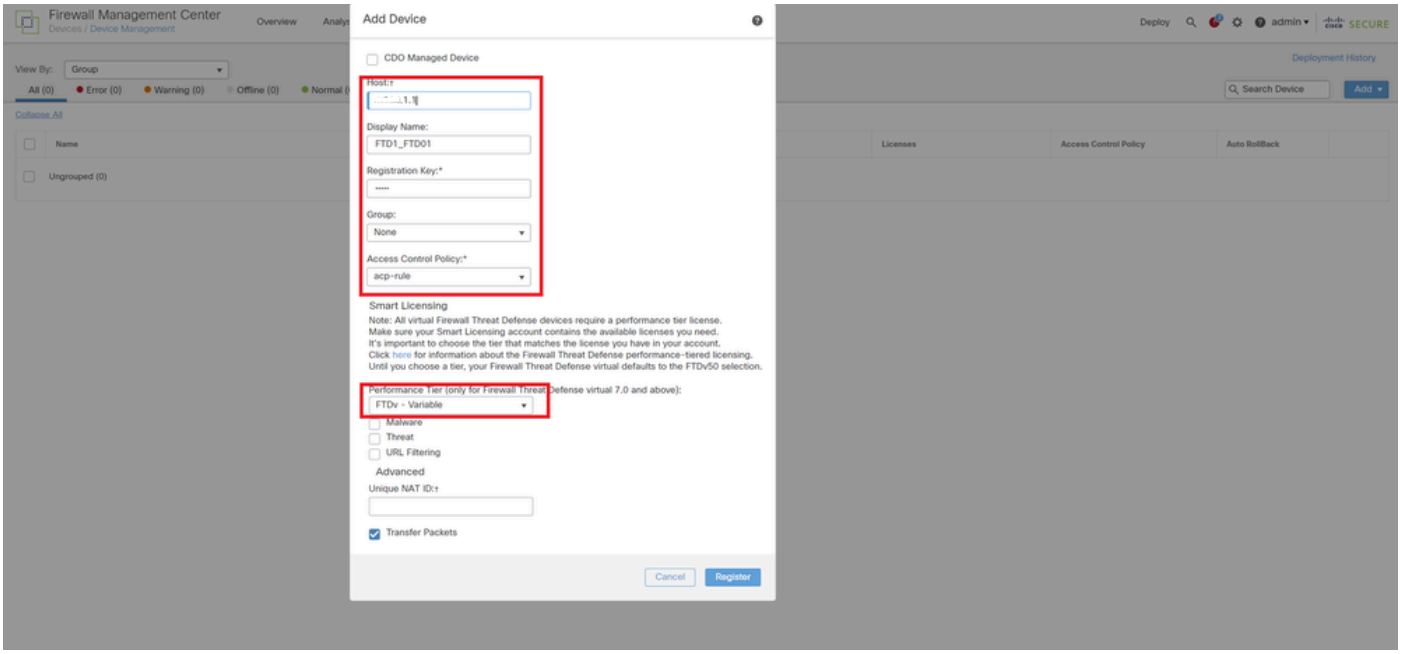
·Nom d'affichage pour Instance01 de FTD1 : FTD1_FTD01

·Nom d'affichage pour Instance02 de FTD1 : FTD1_FTD11

·Nom d'affichage pour Instance01 de FTD2 : FTD2_FTD02

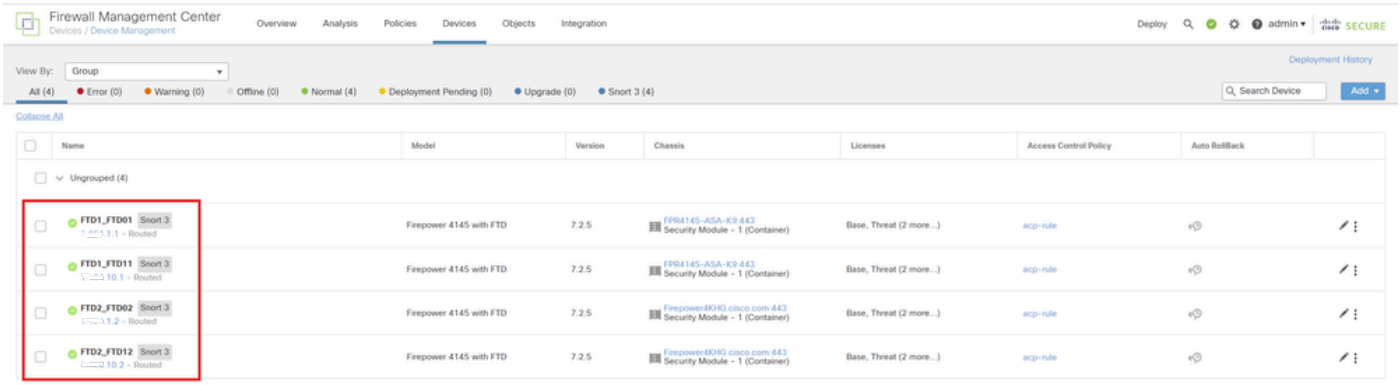
·Nom d'affichage pour Instance02 de FTD2 : FTD2_FTD12

Cette image présente le paramètre de **FTD1_FTD01**.



Ajouter une instance FTD à FMC

b. Vérifiez que toutes les instances sont normales.



Confirmer l'état des instances dans FMC

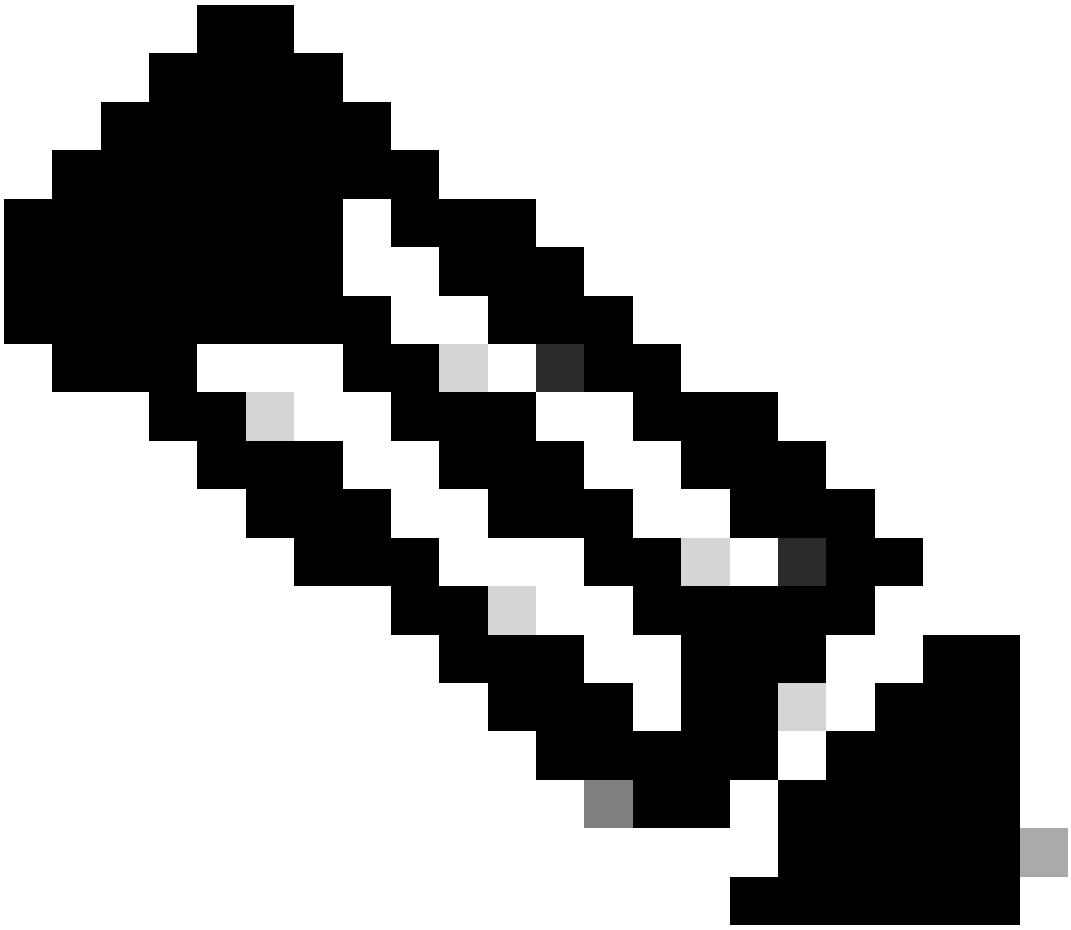
c. Accédez à **Devices** > **Add High Availability**. Définissez la 1ère paire de basculement.

Dans cet exemple :

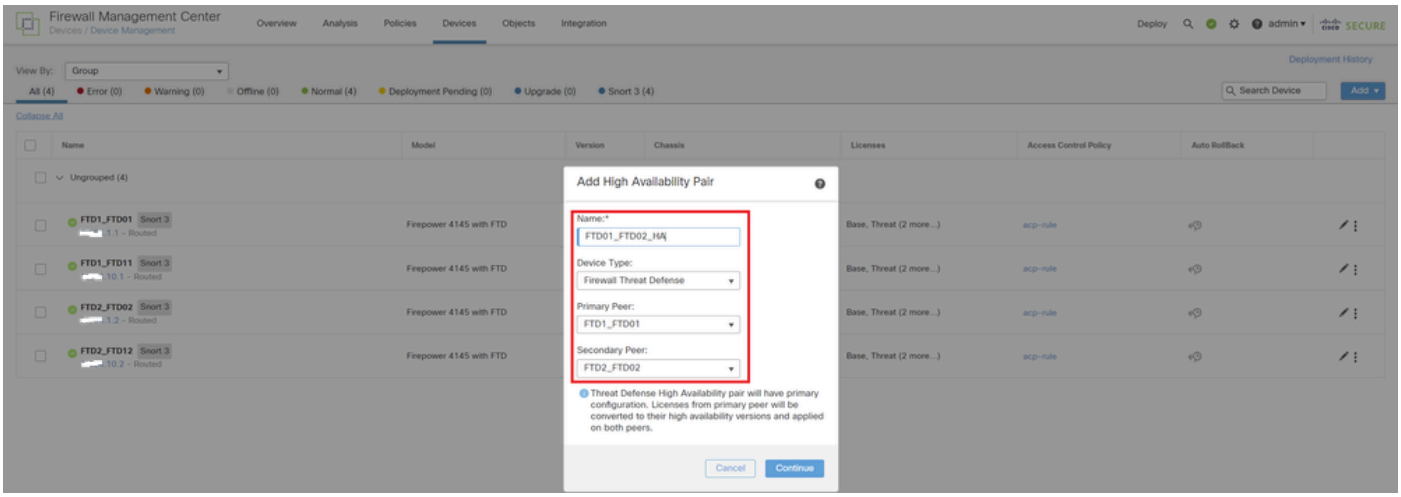
·**Nom : FTD01_FTD02_HA**

· **Homologue principal : FTD1_FTD01**

· **Homologue secondaire : FTD2_FTD02**



Remarque : assurez-vous de sélectionner l'unité appropriée comme unité principale.



Ajouter la première paire de basculement

d. Définissez l'adresse IP du lien de basculement dans la première paire de basculement.

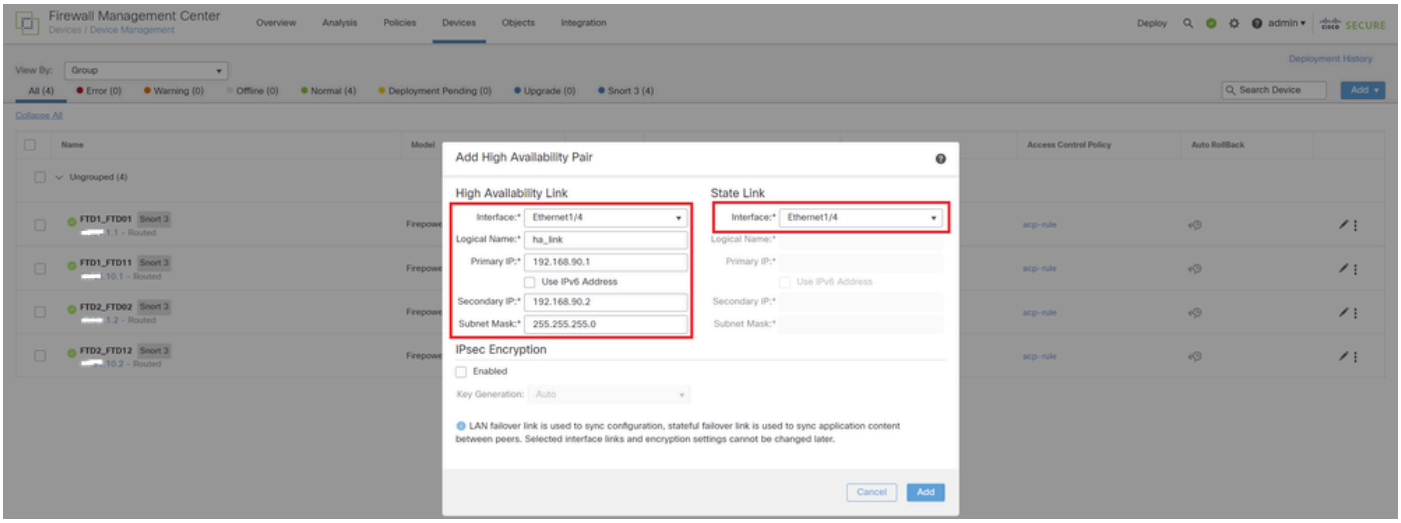
Dans cet exemple :

· **Liaison haute disponibilité : Ethernet1/4**

· **Liaison d'état : Ethernet1/4**

· **IP principale : 192.168.90.1/24**

· **IP secondaire : 192.168.90.2/24**

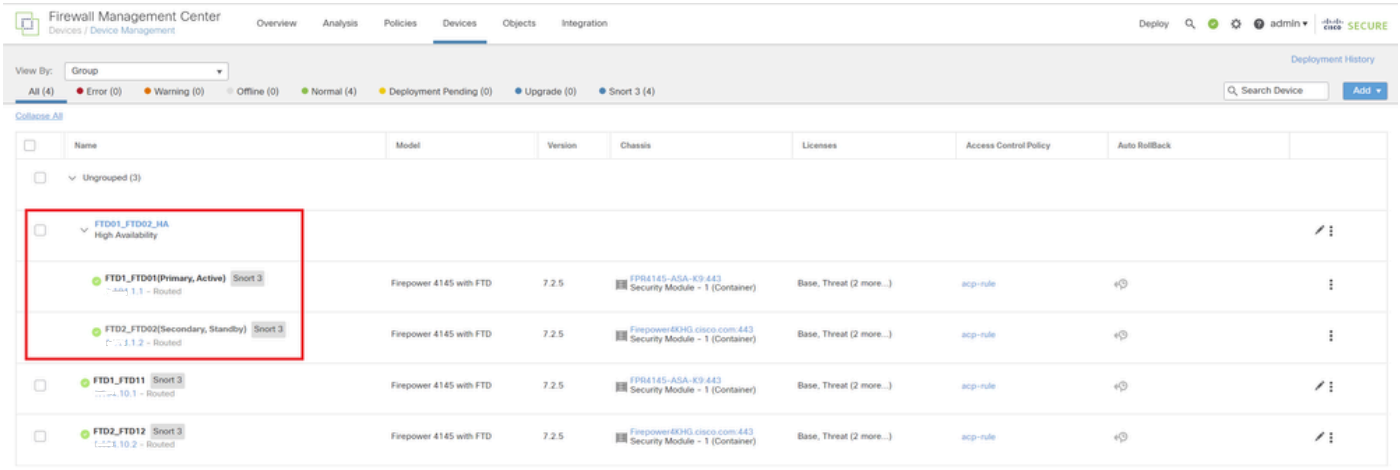


Définir l'interface haute disponibilité et IP pour la première paire de basculement

e. Confirmer l'état du basculement

·**FTD1_FTD01 : Primaire, actif**

·**FTD2_FTD02 : secondaire, veille**



Confirmer l'état de la première paire de basculement

f. Accédez à **Devices** > **Cliquez sur FTD01_FTD02_HA** (dans cet exemple) > **Interfaces.** Définissez l'adresse IP active pour l'interface de données.

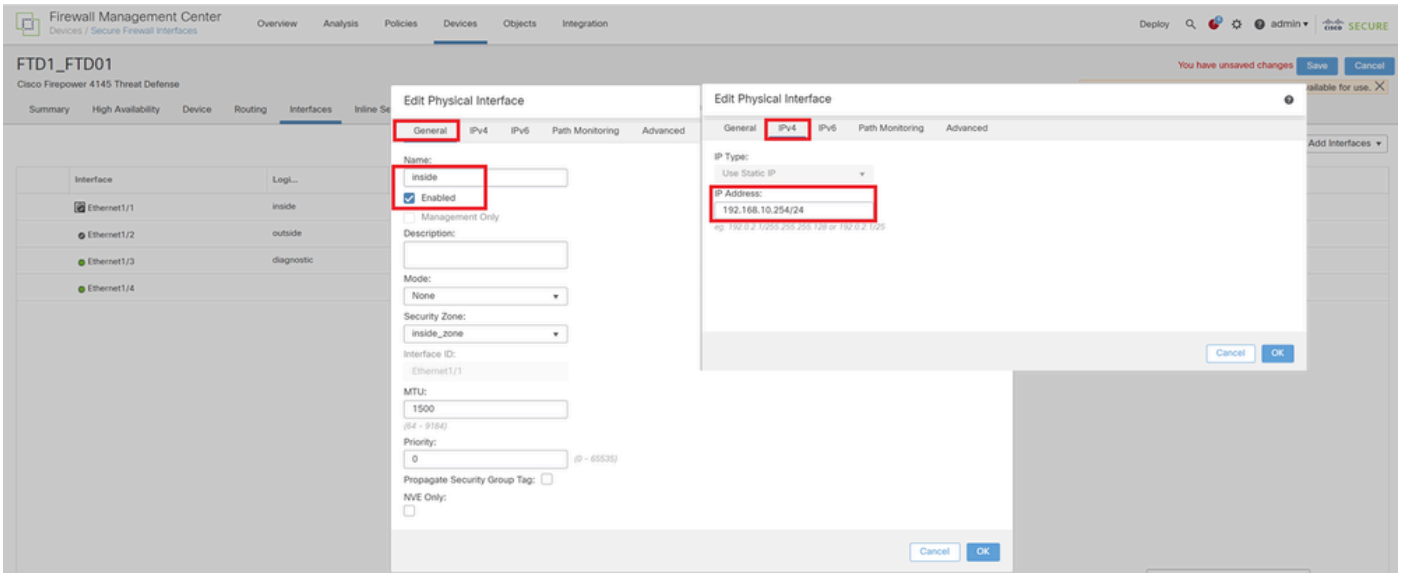
Dans cet exemple :

·Ethernet1/1 (interne) : 192.168.10.254/24

·Ethernet1/2 (extérieur) : 192.168.20.254/24

·Ethernet1/3 (diagnostic) : 192.168.80.1/24

Cette image montre le paramètre de l'adresse IP active d'**Ethernet1/1**.



Définir l'adresse IP active pour l'interface de données

g. Accédez à **Devices** > **Cliquez sur FTD01_FTD02_HA** (dans cet exemple) > **High Availability.** Définissez l'IP de secours pour l'interface de données.

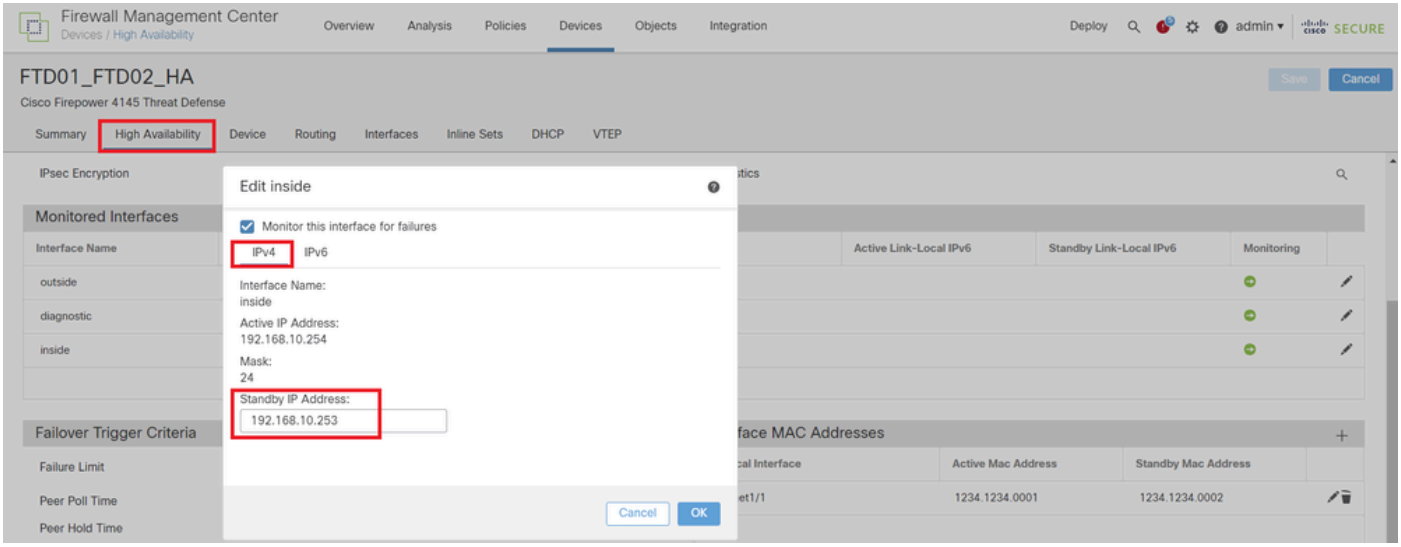
Dans cet exemple :

·Ethernet1/1 (interne) : 192.168.10.253/24

·Ethernet1/2 (extérieur) : 192.168.20.253/24

·Ethernet1/3 (diagnostic) : 192.168.80.2/24

Cette image montre le paramètre de l'adresse IP de secours d'**Ethernet1/1**.



Définir l'IP de secours pour l'interface de données

h. Répétez les étapes 6.c à g pour ajouter une deuxième paire de basculement.

Dans cet exemple :

·Nom : FTD11_FTD12_HA
·Pair principal : FTD1_FTD11
·Homologue secondaire : FTD2_FTD12

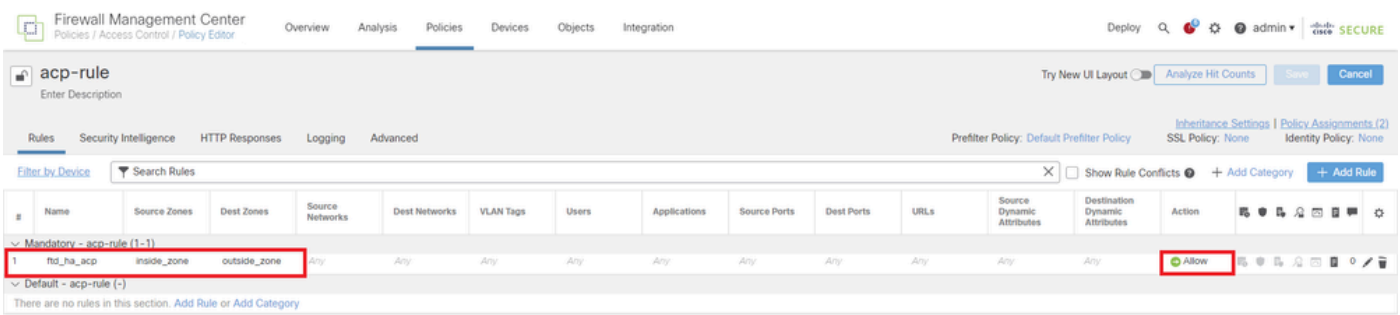
·Liaison haute disponibilité : Ethernet1/8
·Liaison d'état : Ethernet1/8
·Ethernet1/8 (ha_link Active) : 192.168.91.1/24

·Ethernet1/5 (interne actif) : 192.168.30.254/24
·Ethernet1/6 (extérieur actif) : 192.168.40.254/24
·Ethernet1/7 (diagnostic actif) : 192.168.81.1/24

·Ethernet1/8 (ha_link Standby) : 192.168.91.2/24

·Ethernet1/5 (en veille) : 192.168.30.253/24
·Ethernet1/6 (hors veille) : 192.168.40.253/24
·Ethernet1/7 (diagnostic Standby) : 192.168.81.2/24

i. Accédez à **Logical Devices** > **Add Standalone**. Définissez la règle ACP pour autoriser le trafic de l'intérieur vers l'extérieur.



Définir la règle ACP

j. Déployez le paramètre sur FTD.

k. Confirmer le statut HA dans CLI

L'état de haute disponibilité de chaque instance est également confirmé dans l'interface de ligne de commande Firepower, qui est identique à ASA.

Exécutez **show running-config failover** et **show failover** exécutez la commande pour confirmer l'état de haute disponibilité de FTD1_FTD01 (instance principale01) .

```
<#root>
```

// confrim 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 htt

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
```

Exécutez **show running-config failover** et **show failover** exécutez la commande pour confirmer l'état de haute disponibilité de FTD1_FTD11 (instance principale02) .

```
<#root>
```

// confrim 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 htt

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
```

Exécutez **show running-config failover** et **show failover** exécutez la commande pour confirmer l'état de haute disponibilité de FTD2_FTD02 (instance secondaire01) .

```
<#root>
```

// confrim 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-
```

Exécutez **show running-config failover** la **show failover** commande permettant de confirmer l'état de haute disponibilité de FTD2_FTD12 (instance secondaire02) .

<#root>

// confrim 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-
```

l. Confirmer la consommation de licence

Toutes les licences sont utilisées par moteur/châssis de sécurité et non par instance de conteneur.

· Les licences de base sont automatiquement attribuées : une par moteur/châssis de sécurité.

· Les licences de fonction sont attribuées manuellement à chaque instance, mais vous ne consommez qu'une seule licence par moteur/châssis de sécurité. Pour une licence de fonction spécifique, vous n'avez besoin que d'une licence au total, quel que soit le nombre d'instances utilisées.

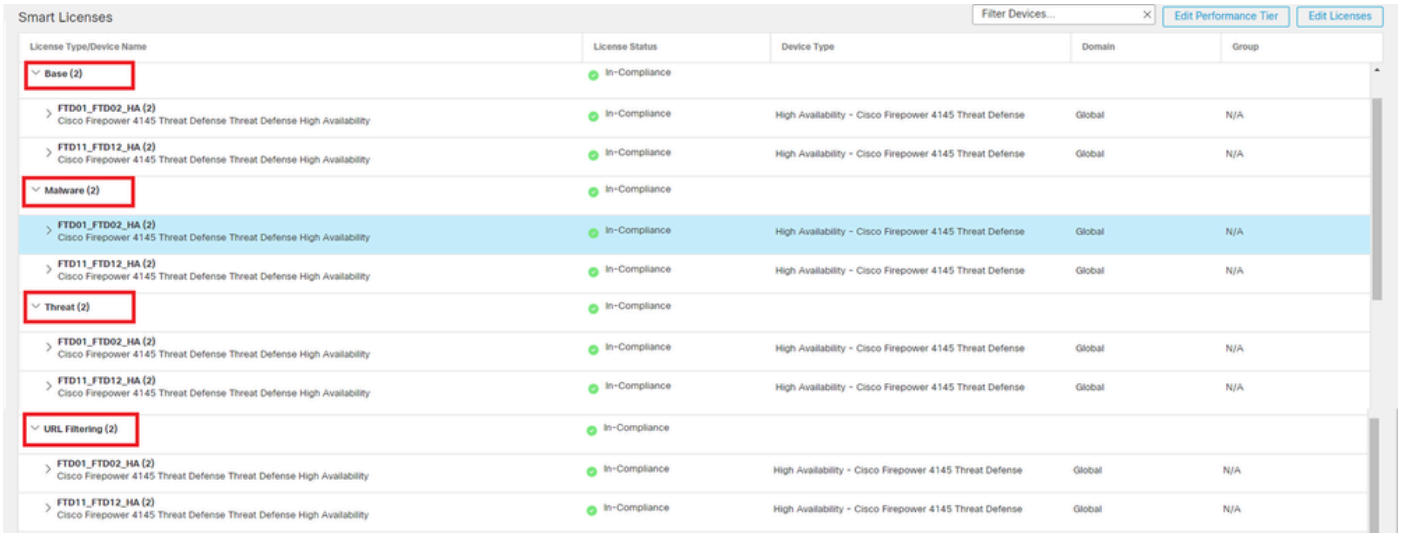
Ce tableau montre comment les licences sont utilisées dans ce document.

RP01	Instance01	Base, filtrage des URL, programmes malveillants, menace
	Instance02	Base, filtrage des URL, programmes malveillants, menace
RP02	Instance01	Base, filtrage des URL, programmes malveillants, menace
	Instance02	Base, filtrage des URL, programmes malveillants, menace

Nombre total de licences

Base	Filtrage des URL	Programme malveillant	Menace
2	2	2	2

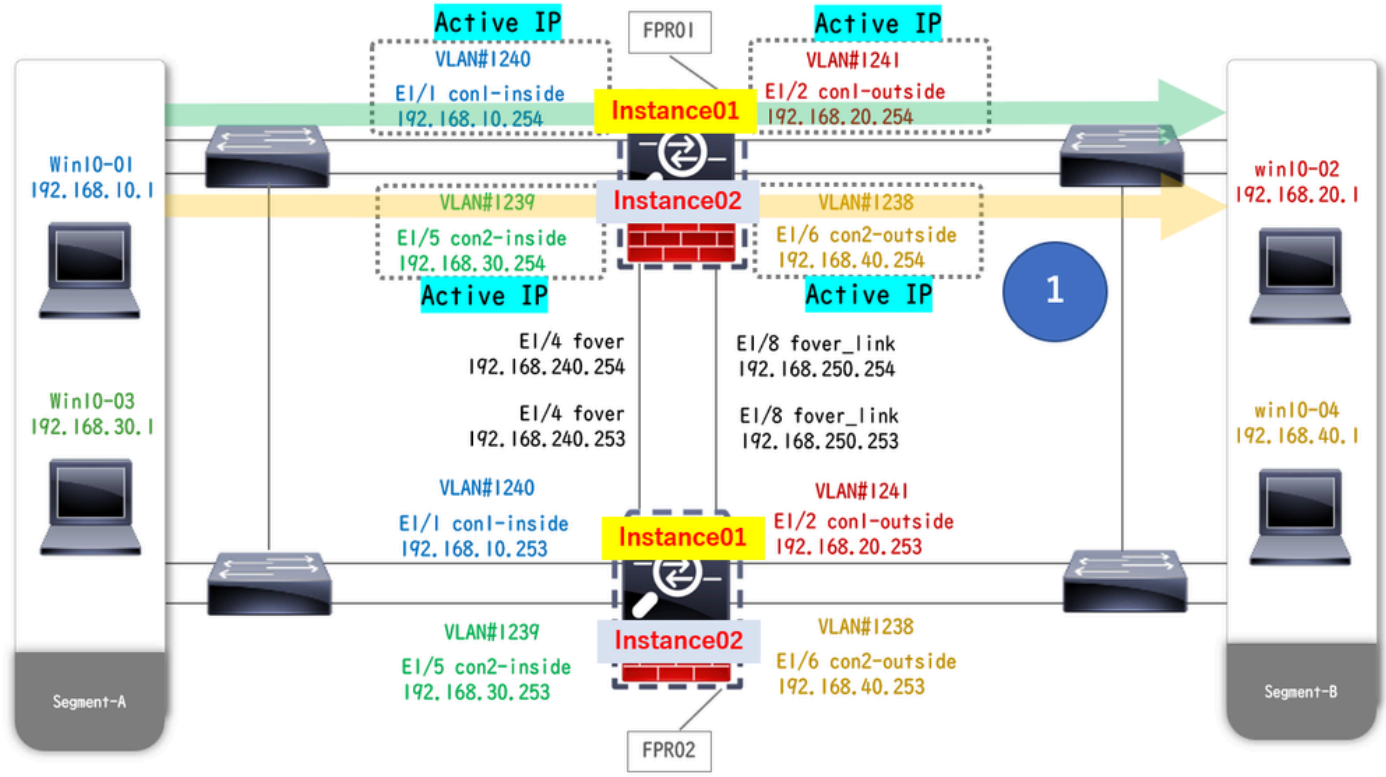
Confirmez le nombre de licences consommées dans l'interface utilisateur graphique FMC.



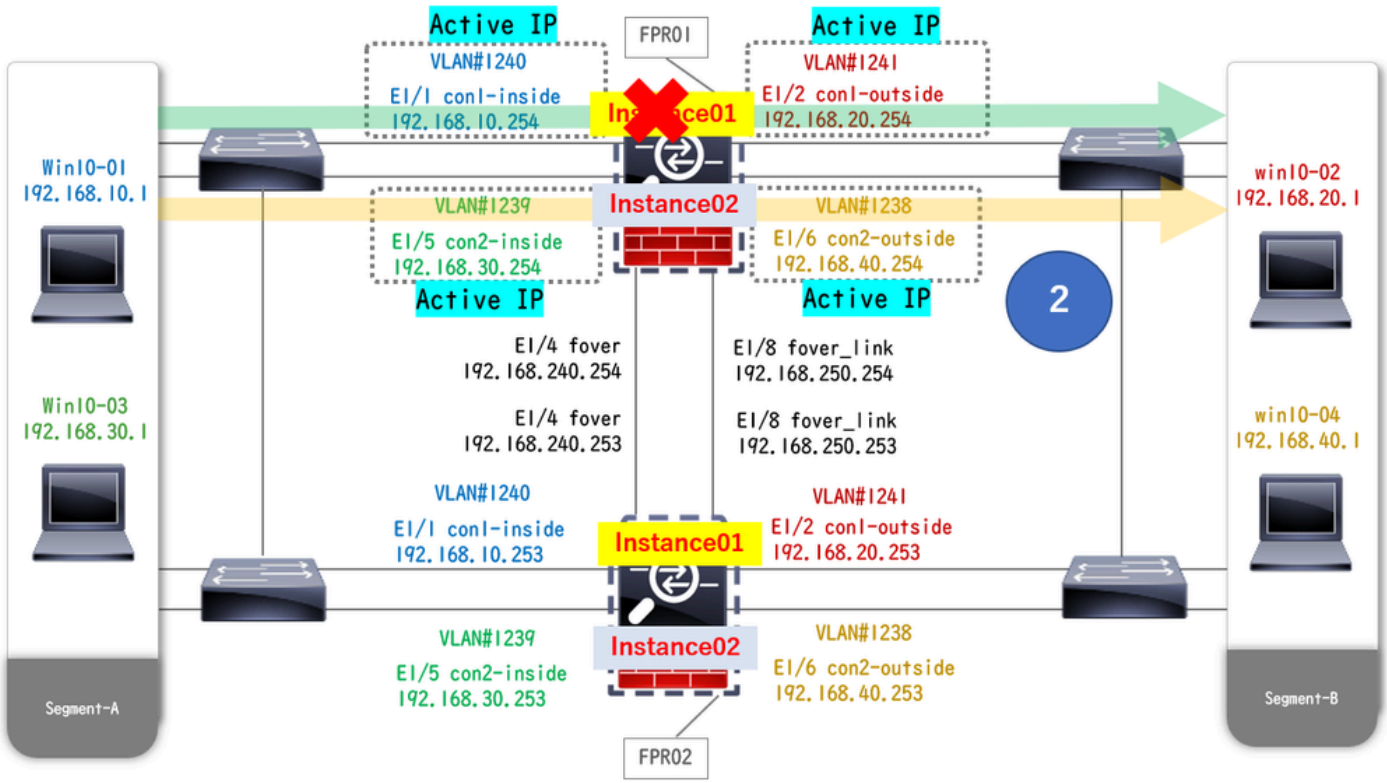
Confirmer les licences consommées

Vérifier

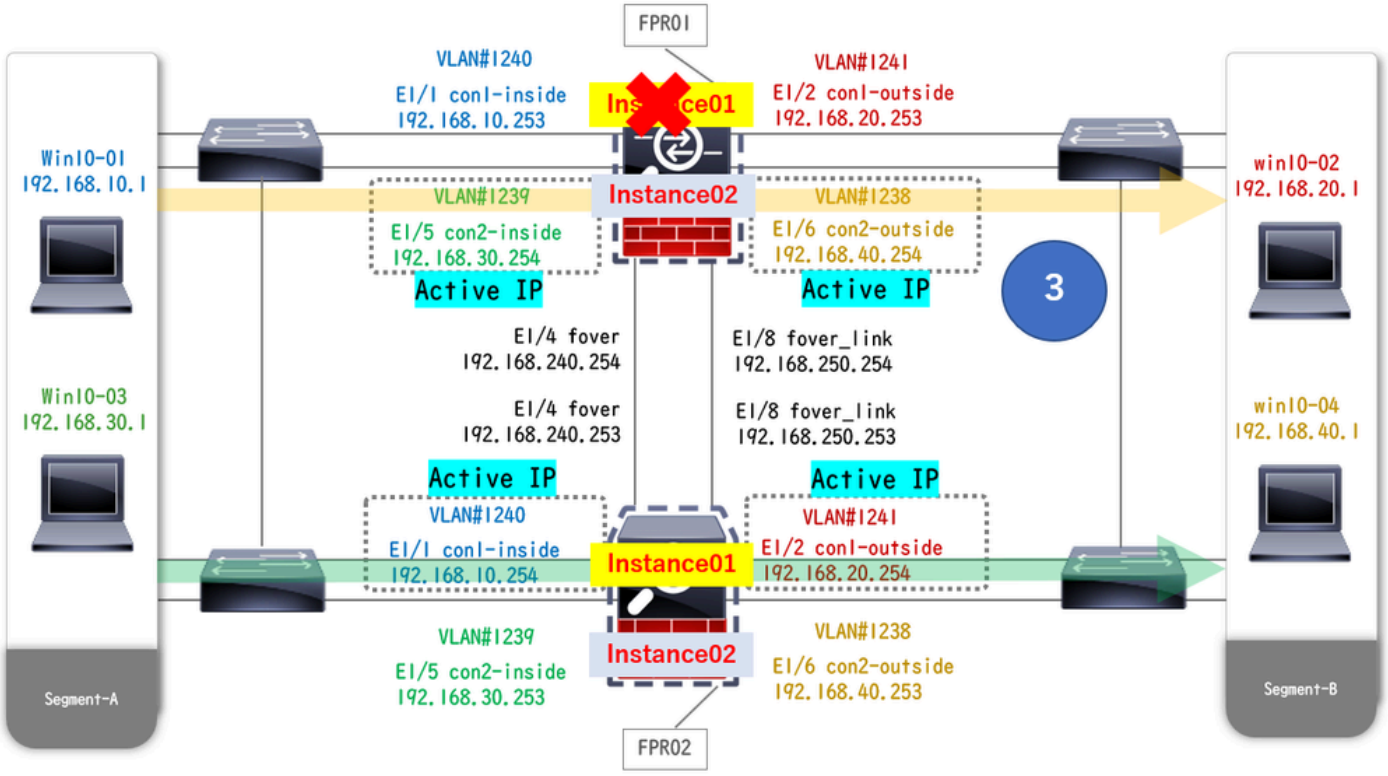
En cas de panne sur FTD1_FTD01 (instance principale01), le basculement de l'instance01 est déclenché et les interfaces de données côté veille prennent le relais de l'adresse IP/MAC de l'interface active d'origine, assurant ainsi le passage continu du trafic (connexion FTP dans ce document) par Firepower.



Avant le crash



Pendant le crash



Le basculement est déclenché

Étape 1. Lancez la connexion FTP de Win10-01 à Win10-02.

Étape 2. Exécutez la show conn commande pour confirmer que la connexion FTP est établie dans les deux instances de Instance01.

<#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
```

Étape 3. Lancez la connexion FTP de Win10-03 à Win10-04.

Étape 4. Exécutez la **show conn** commande pour confirmer que la connexion FTP est établie dans les deux instances de Instance02.

<#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
```

Étape 5. Exécutez connect ftd FTD01 et entrez system support diagnostic-cli la commande dans l'interface de ligne de commande ASA. Exécuter enable et **crashinfo force watchdog** commander pour forcer la panne Instance01 dans l'unité principale/active.

```
<#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]:
```

Étape 6. Le basculement se produit dans Instance01 et la connexion FTP n'est pas interrompue. Exécutez show failover et show conn la commande pour confirmer l'état de Instance01 dans FPR02.

```
<#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
```

Étape 7. Le plantage survenu dans Instance01 n'a eu aucun effet sur Instance02. Exécutez show failover et show conn la commande pour confirmer l'état d'Instance02.

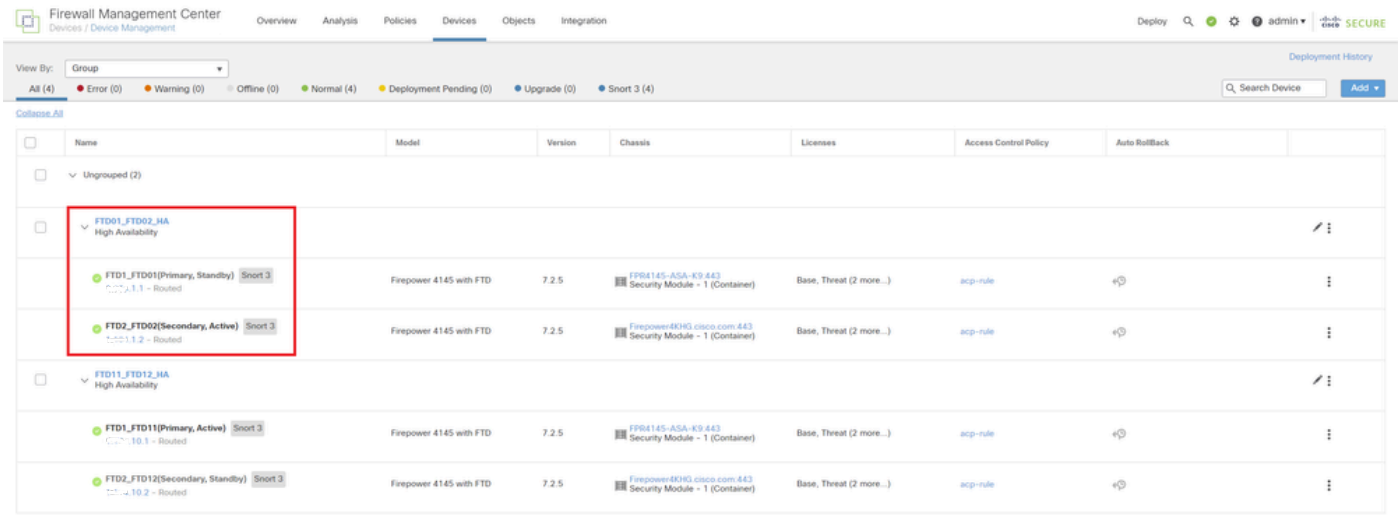
```
<#root>
>
show failover
```

```
 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
```

Étape 8. Accédez à **Devices** > **All** sur FMC. Confirmez l'état HA.

·**FTD1_FTD01 : principal, veille**

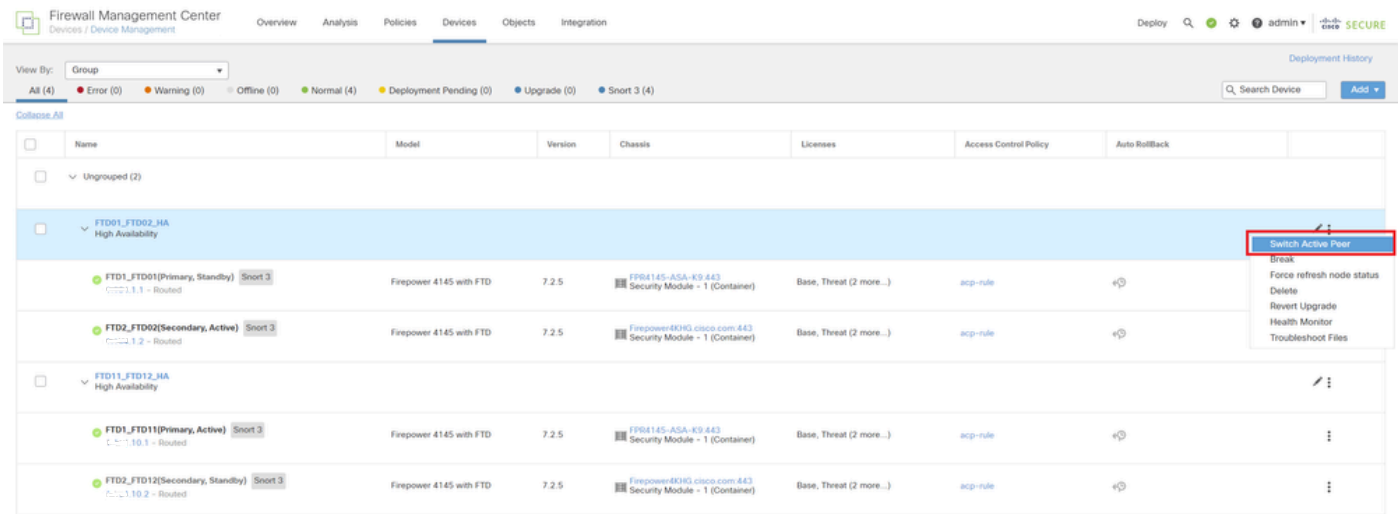
·**FTD2_FTD02 : secondaire, actif**



Confirmer l'état HA

Étape 9. (Facultatif)Une fois que l'Instance01 de FPR01 est revenue à la normale, vous pouvez changer manuellement l'état de la haute disponibilité. Cela peut être effectué par l'interface graphique FMC ou l'interface de ligne de commande FRP.

Sur FMC, accédez à **Devices** > **All**. Cliquez sur **Commuter l'homologue actif** pour commuter l'état de haute disponibilité pour **FTD01_FTD02_HA**.



État HA du commutateur

Sur l'interface de ligne de commande Firepower, exécutez connect ftd FTD01 et system support diagnostic-cli la commande pour entrer dans

l'interface de ligne de commande ASA. Exécutez enable et la **failover active** commande pour commuter la haute disponibilité pour FTD01_FTD02_HA.

<#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 availab

enable

firepower#

failover active

Dépannage

Afin de valider l'état du basculement, exécutez **show failover** et **show failover history** commande.

<#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 failover history

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

Exécutez la commande debug fover <option> pour activer le journal de débogage du basculement.

<#root>

>

debug fover

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

Référence

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/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.