Remplacement de l'unité défectueuse dans le pare-feu sécurisé Défense contre les menaces de haute disponibilité

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Avant de commencer

Identification de l'unité défectueuse

Remplacement d'une unité défectueuse par une unité de secours

Remplacement d'une unité défectueuse sans sauvegarde

Informations connexes

Introduction

Ce document décrit comment remplacer un module de défense contre les menaces de pare-feu sécurisé défectueux qui fait partie d'une configuration haute disponibilité (HA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Système d'exploitation extensible Cisco Firepower (FXOS)
- Cisco Secure Firewall Threat Defense (FTD)

Composants utilisés

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

- Firepower 4110 exécute FXOS v2.12(0.498)
- Le périphérique logique exécute Cisco Secure Firewall v7.2.5
- Secure Firewall Management Center 2600 exécute v7.4
- Connaissance du protocole Secure Copy (SCP)

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

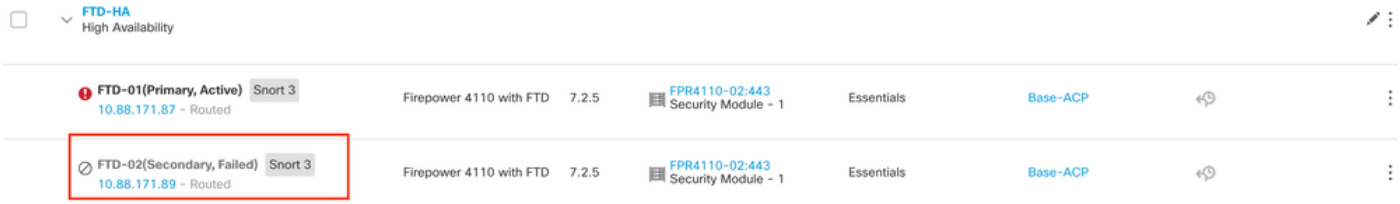
Cette procédure est prise en charge sur les appliances :

- Appliances Cisco Secure Firewall 1000
- Appliances Cisco Secure Firewall 2100
- Appliances Cisco Secure Firewall 3100
- Appliances Cisco Secure Firewall 4100
- Appliances Cisco Secure Firewall 4200
- Appliance Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense pour VMWare

Avant de commencer

Ce document exige que la nouvelle unité soit configurée avec les mêmes versions FXOS et FTD.

Identification de l'unité défectueuse

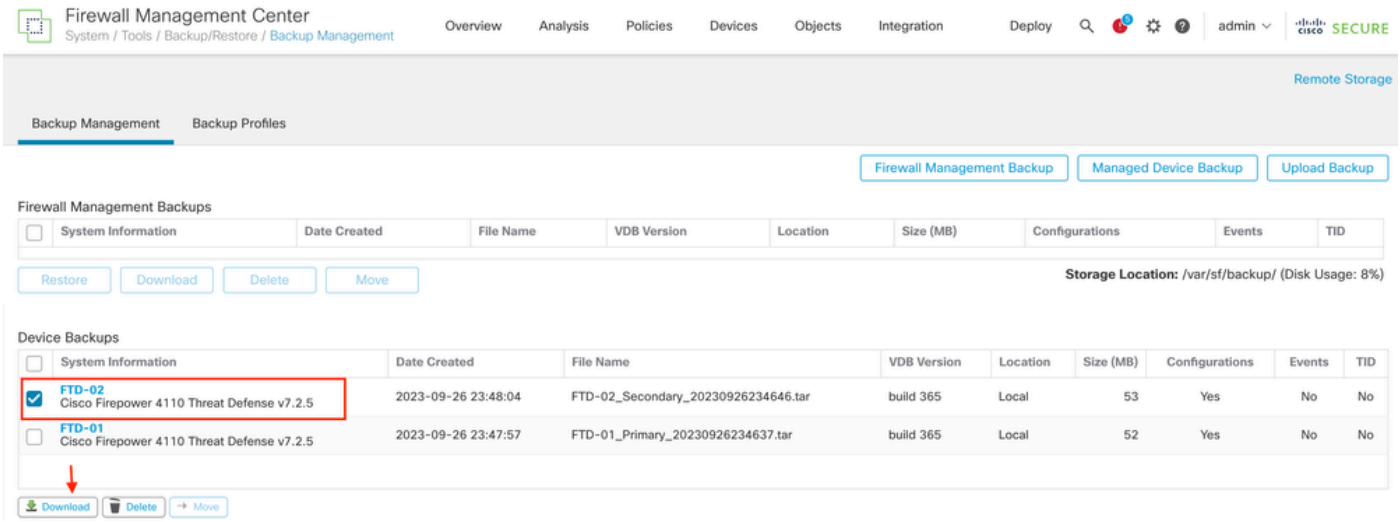


Dans ce scénario, l'unité secondaire (FTD-02) est à l'état d'échec.

Remplacement d'une unité défectueuse par une unité de secours

Vous pouvez utiliser cette procédure pour remplacer l'unité principale ou secondaire. Ce guide suppose que vous disposez d'une sauvegarde de l'unité défectueuse que vous allez remplacer.

Étape 1 : téléchargement du fichier de sauvegarde à partir de FMC Accédez à System > Tools > Restore > Device Backups et sélectionnez la sauvegarde appropriée. Cliquez sur Télécharger :



Étape 2. Téléchargez la sauvegarde FTD dans le répertoire /var/sf/backup/ du nouveau FTD :

2.1 À partir du test-pc (client SCP), téléchargez le fichier de sauvegarde vers le FTD sous le répertoire /var/tmp/ :

```
@test-pc ~ % scp FTD-02_Secondary_20230926234646.tar cisco@10.88.243.90:/var/tmp/
```

2.2 À partir du mode expert CLI FTD, déplacez le fichier de sauvegarde de /var/tmp/ vers /var/sf/backup/ :

```
root@firepower:/var/tmp# mv FTD-02_Secondary_20230926234646.tar /var/sf/backup/
```

Étape 3. Restaurer la sauvegarde FTD-02, en appliquant la commande suivante à partir du mode interférence :

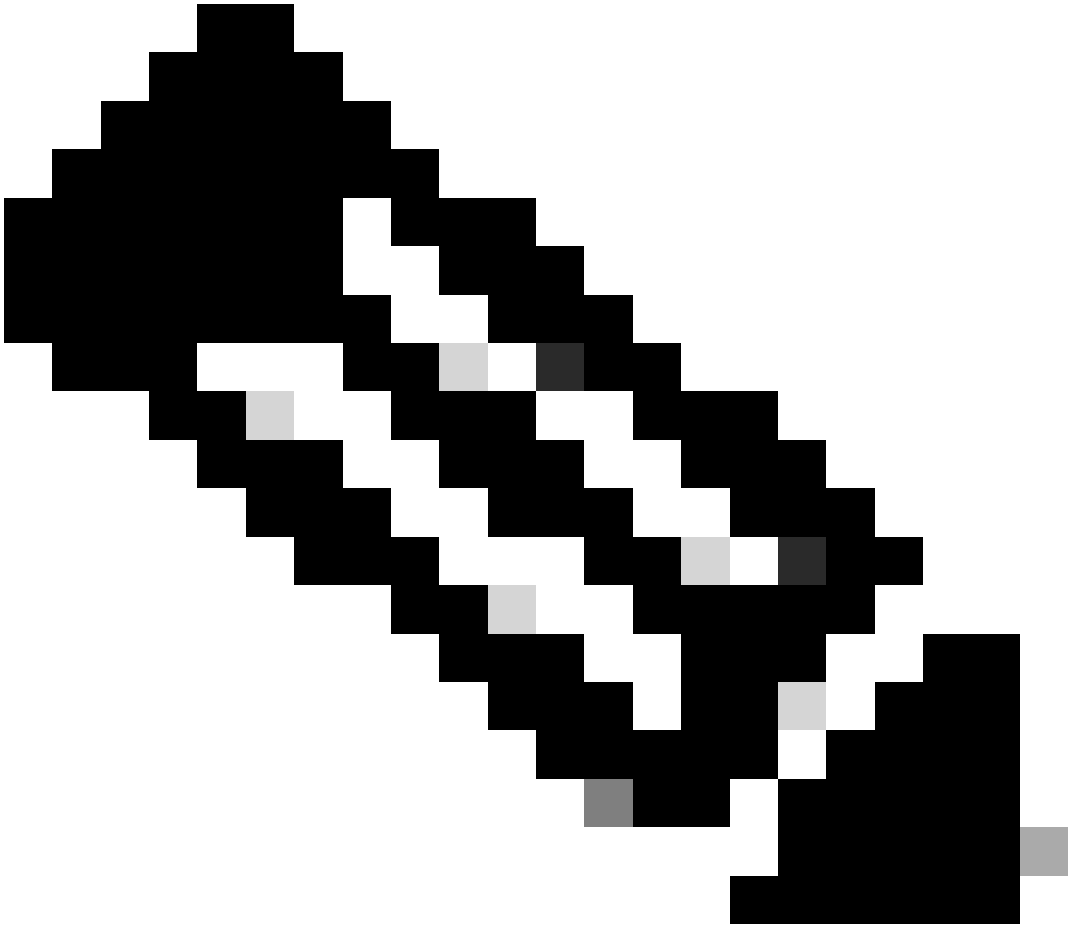
```
>restore remote-manager-backup FTD-02_Secondary_20230926234646.tar

Device model from backup :: Cisco Firepower 4110 Threat Defense
This Device Model  :: Cisco Firepower 4110 Threat Defense
************************************************
Backup Details
************************************************
Model = Cisco Firepower 4110 Threat Defense
Software Version = 7.2.5
Serial = FLM22500791
Hostname = firepower
Device Name = FTD-02_Secondary
IP Address = 10.88.171.89
Role = SECONDARY
VDB Version = 365
SRU Version =
FXOS Version = 2.12(0.498)
Manager IP(s) = 10.88.243.90
Backup Date = 2023-09-26 23:46:46
Backup Filename = FTD-02_Secondary_20230926234646.tar
************************************************

********************* Caution ****************************
Verify that you are restoring a valid backup file.
Make sure that FTD is installed with same software version and matches versions from backup manifest be
Restore operation will overwrite all configurations on this device with configurations in backup.
If this restoration is being performed on an RMA device then ensure old device is removed from network
************************************************************
Are you sure you want to continue (Y/N)Y
Restoring device . . . . . .
Added table audit_log with table_id 1
Added table health_alarm_syslog with table_id 2
Added table dce_event with table_id 3
Added table application with table_id 4
Added table rna_scan_results_tableview with table_id 5
Added table rna_event with table_id 6
Added table ioc_state with table_id 7
Added table third_party_vulns with table_id 8
Added table user_ioc_state with table_id 9
Added table rna_client_app with table_id 10
Added table rna_attribute with table_id 11
Added table captured_file with table_id 12
Added table rna_ip_host with table_id 13
Added table flow_chunk with table_id 14
Added table rua_event with table_id 15
Added table wl_dce_event with table_id 16
Added table user_identities with table_id 17
Added table whitelist_violations with table_id 18
Added table remediation_status with table_id 19
Added table syslog_event with table_id 20
Added table rna_service with table_id 21
Added table rna_vuln with table_id 22
Added table SRU_import_log with table_id 23
Added table current_users with table_id 24
```

```
Broadcast message from root@firepower (Wed Sep 27 15:50:12 2023):

The system is going down for reboot NOW!
```

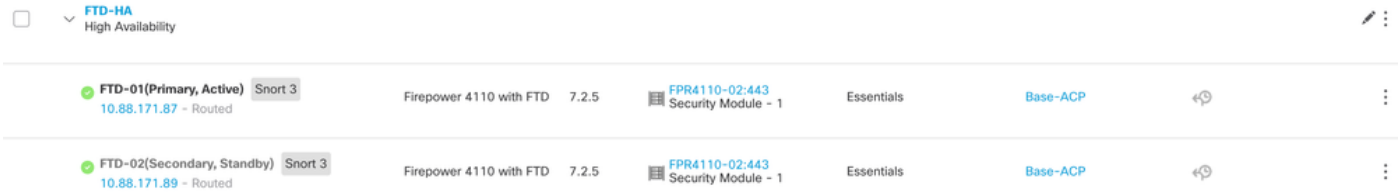


> Remarque : Une fois la restauration terminée, le périphérique vous déconnecte de l'interface de ligne de commande, redémarre et se connecte automatiquement au FMC. À ce stade, le périphérique va apparaître obsolète.

Étape 4. Reprendre la synchronisation haute disponibilité. Dans l'interface de ligne de commande FTD, entrez configure high-availability resume :

```
>configure high-availability resume
```

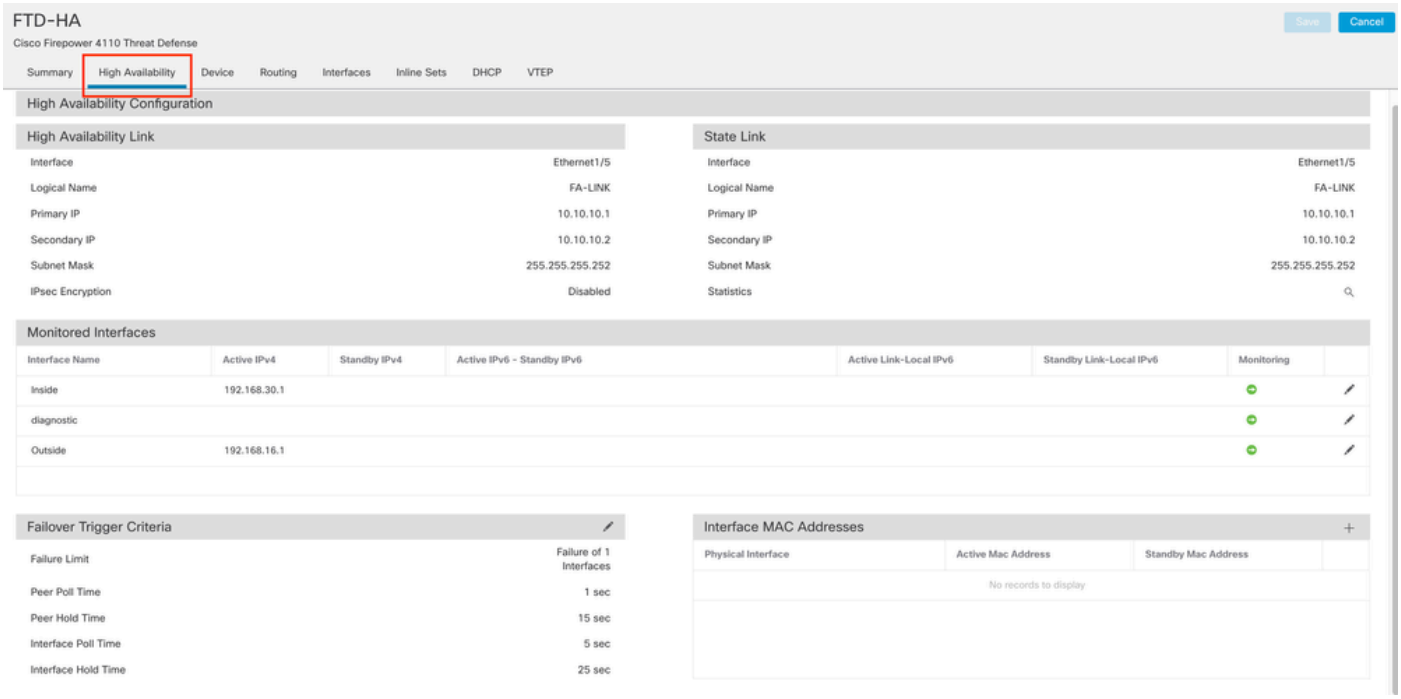
La configuration de la haute disponibilité FTD est maintenant terminée :



Remplacement d'une unité défectueuse sans sauvegarde

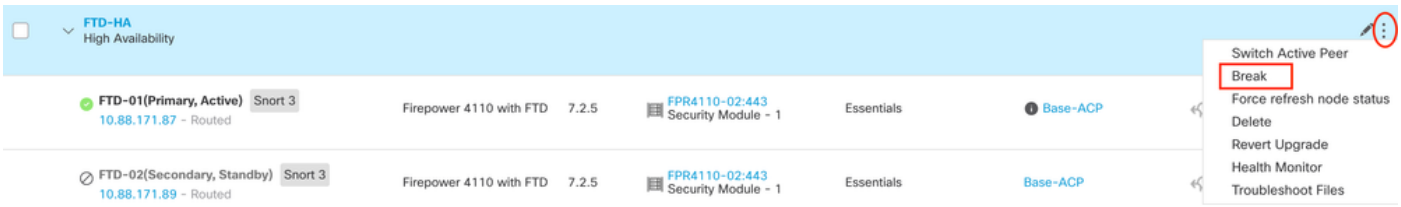
Si vous ne disposez pas d'une sauvegarde du périphérique défaillant, vous pouvez poursuivre avec ce guide. Vous pouvez remplacer l'unité principale ou secondaire,Le processus varie selon que le périphérique est principal ou secondaire. Toutes les étapes décrites dans ce guide consistent à restaurer une unité secondaire défectueuse. Si vous souhaitez restaurer une unité principale défectueuse, à l'étape 5, configurez la haute disponibilité, en utilisant l'unité secondaire/active existante comme périphérique principal et le périphérique de remplacement comme périphérique secondaire/de secours lors de l'enregistrement.

Étape 1. Effectuez une capture d'écran (sauvegarde) de la configuration haute disponibilité en accédant à Device > Device Management. Modifiez la paire FTD HA appropriée (cliquez sur l'icône représentant un crayon), puis cliquez sur l'option Haute disponibilité :

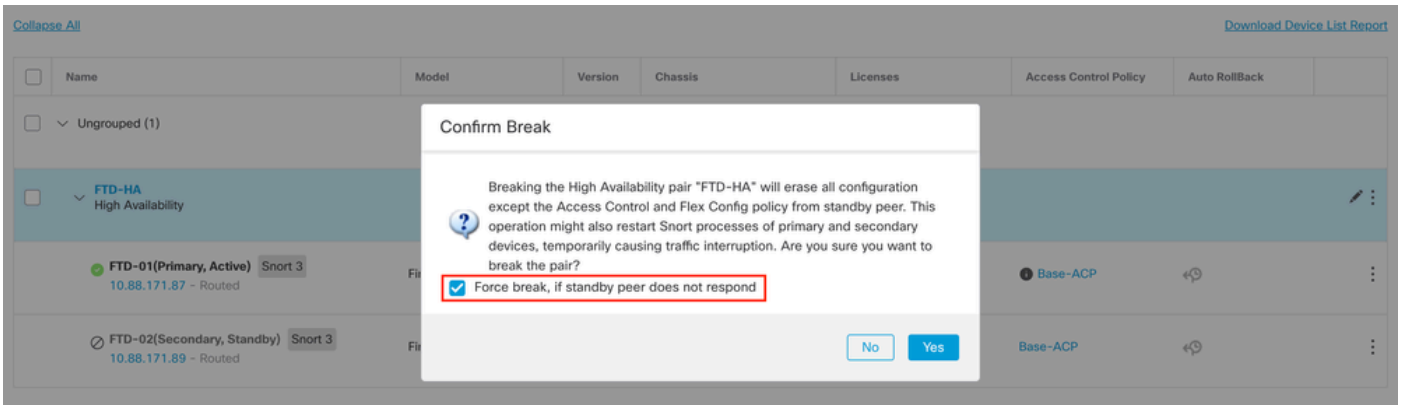


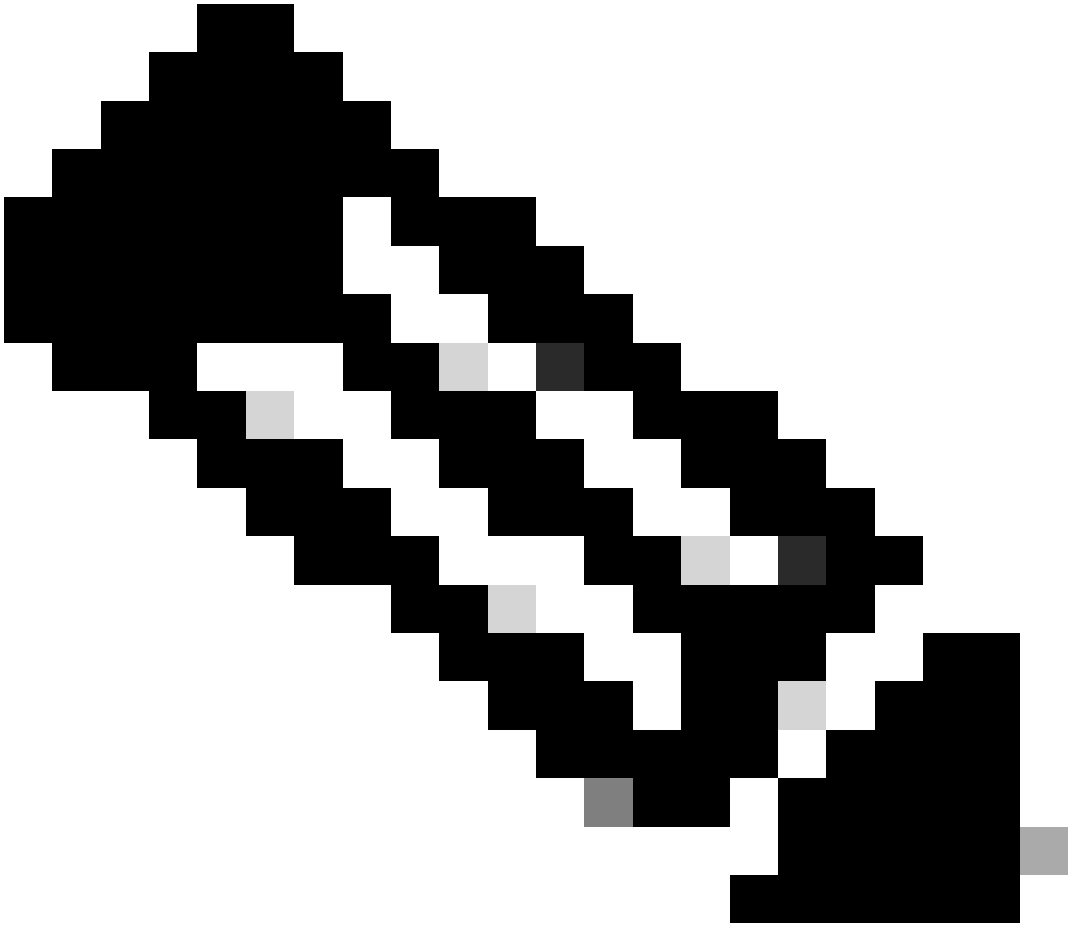
Étape 2 : interruption de la haute disponibilité

2.1 Accédez à Devices > Device Management, puis cliquez sur le menu à trois points dans l'angle supérieur droit. Cliquez ensuite sur l'option Break :



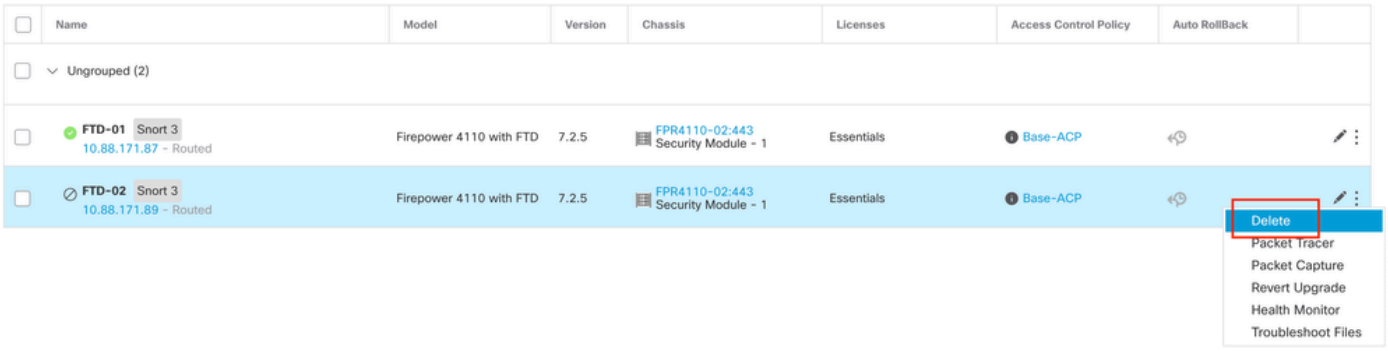
2.2. Sélectionnez l'option Forcer l'interruption si l'homologue en veille ne répond pas :





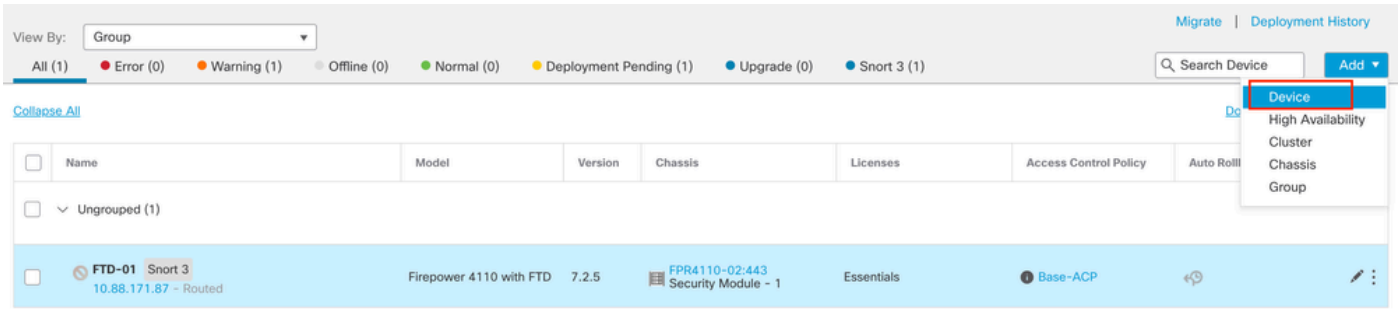
Remarque : Comme l'unité ne répond pas, vous devez forcer la rupture de la haute disponibilité. Lorsque vous rompez une paire haute disponibilité, le périphérique actif conserve toutes les fonctionnalités déployées. Le périphérique de secours perd ses configurations de basculement et d'interface et devient un périphérique autonome.

Étape 3 : suppression du FTD défectueux Identifiez le FTD à remplacer, puis cliquez sur le menu à trois points. Cliquez sur Supprimer :



Étape 4. Ajout du nouveau FTD

4.1. Accédez à Devices > Device Management > Add, puis cliquez sur Device :



4.2. Sélectionnez la méthode d'approvisionnement, dans ce cas, Clé d'enregistrement, configurez Hôte, Nom d'affichage, Clé d'enregistrement. Configurez une stratégie de contrôle d'accès et cliquez sur Enregistrer.

Add Device

Select the Provisioning Method:

(•) Registration Key ( ) Serial Number

[ ] CDO Managed Device

Host:†

10.88.171.89

Display Name:

FTD-02

Registration Key:*

••••••••

Group:

None

Access Control Policy:*

Base-ACP

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

[ ] Carrier
[ ] Malware Defense
[ ] IPS
[ ] URL

Advanced

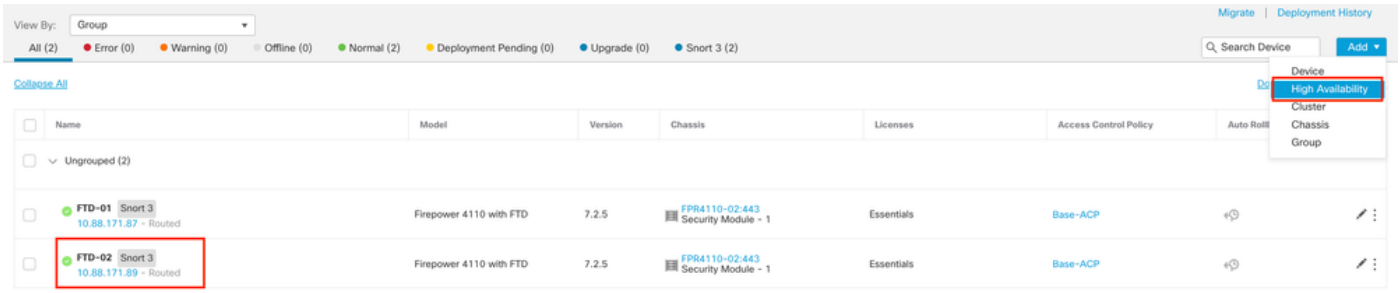
Unique NAT ID:†

[ ] Transfer Packets

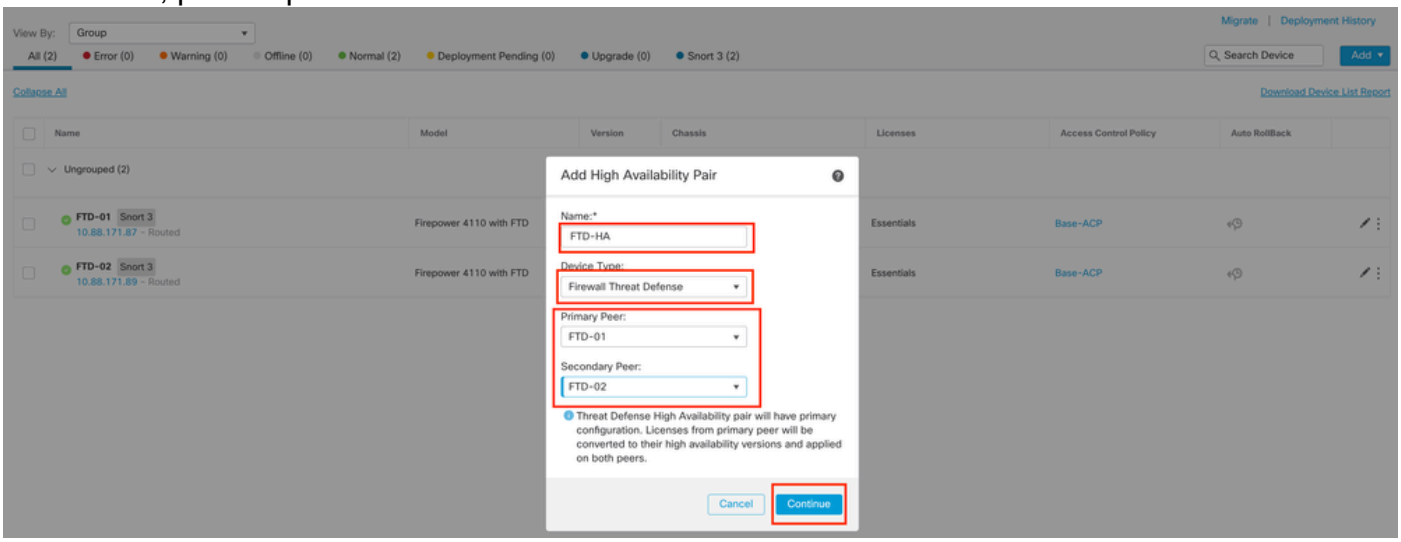
Cancel Register

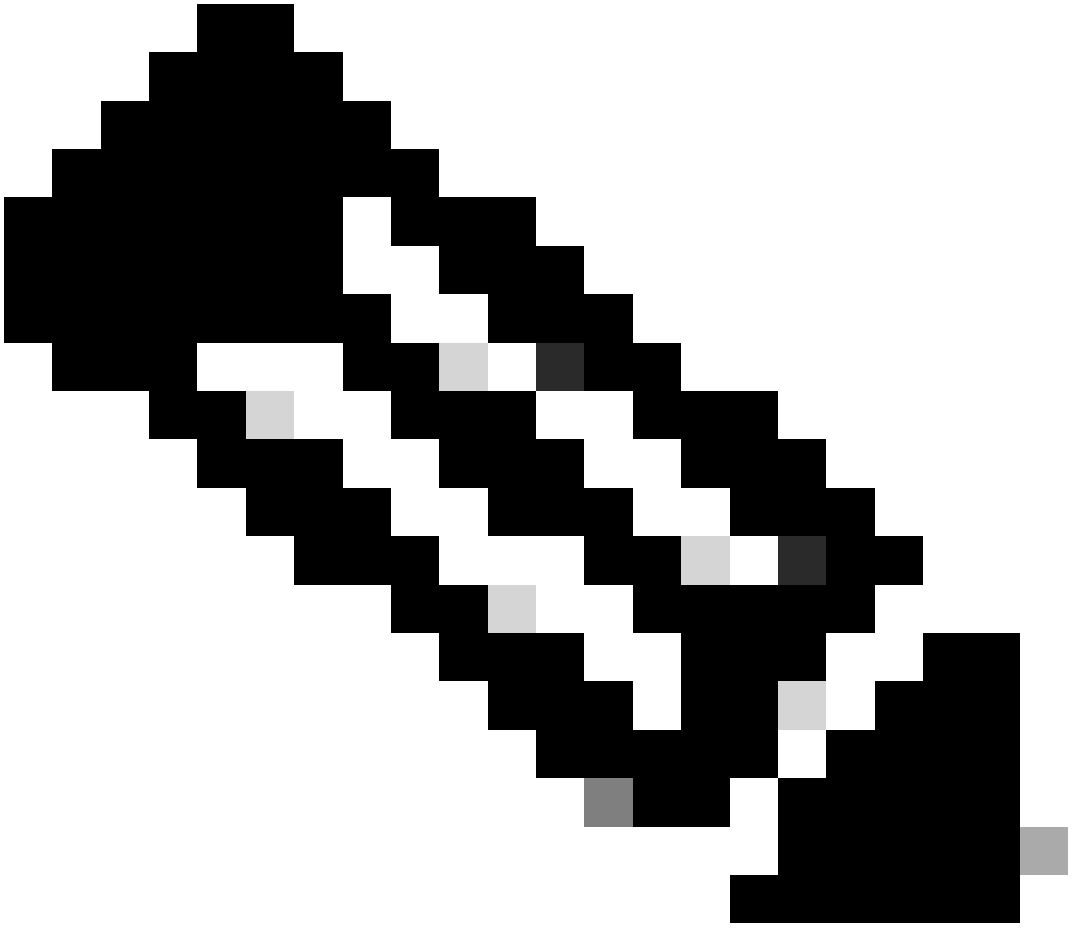
Étape 5. Création de la haute disponibilité

5.1 Accédez à Devices > Device Management > Add et cliquez sur l'option High Availability.



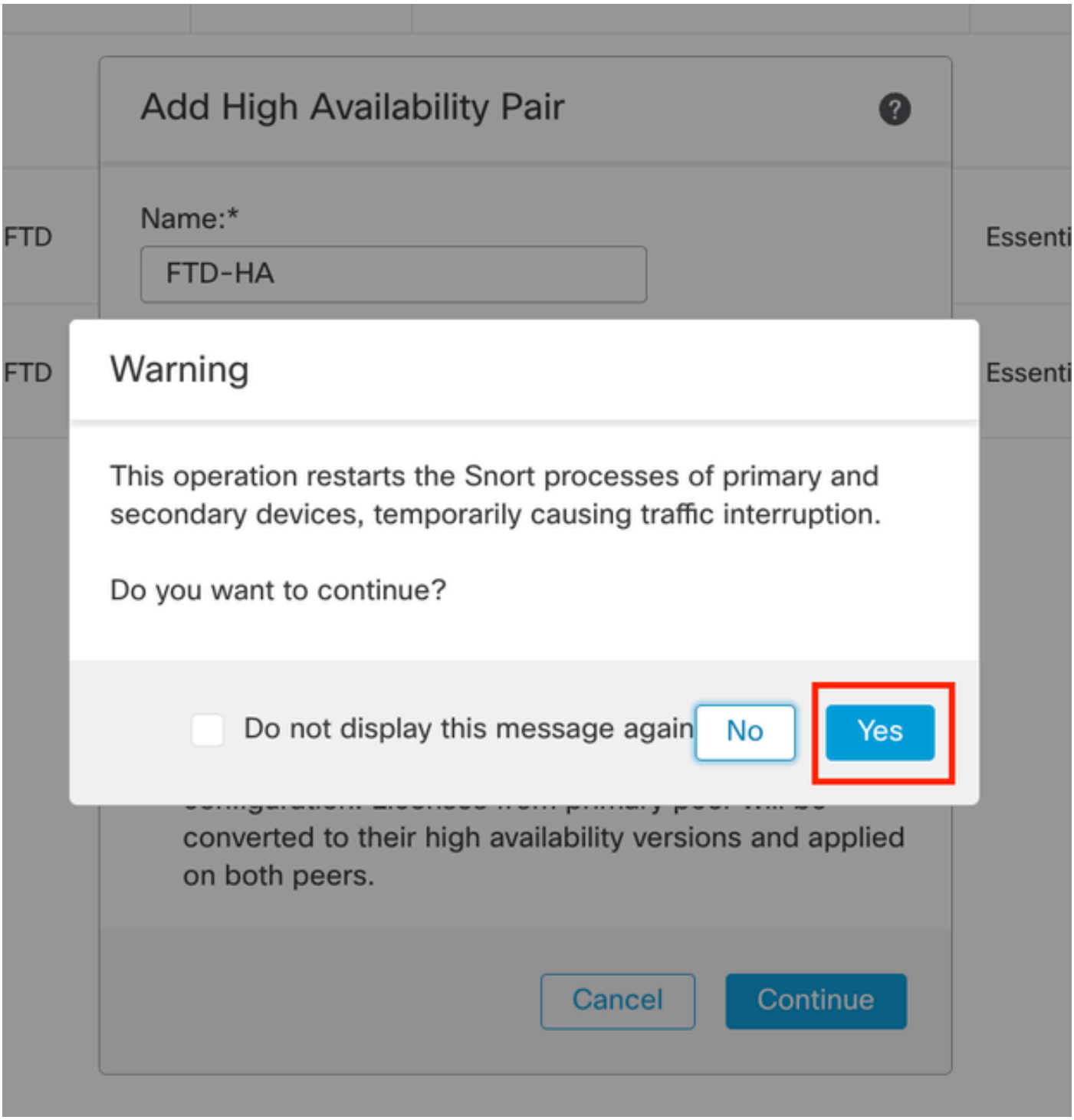
5.2. Configuration de la paire Ajouter haute disponibilité Configurez le nom, le type de périphérique, sélectionnez FTD-01 comme homologue principal et FTD-02 comme homologue secondaire, puis cliquez sur Continuer.

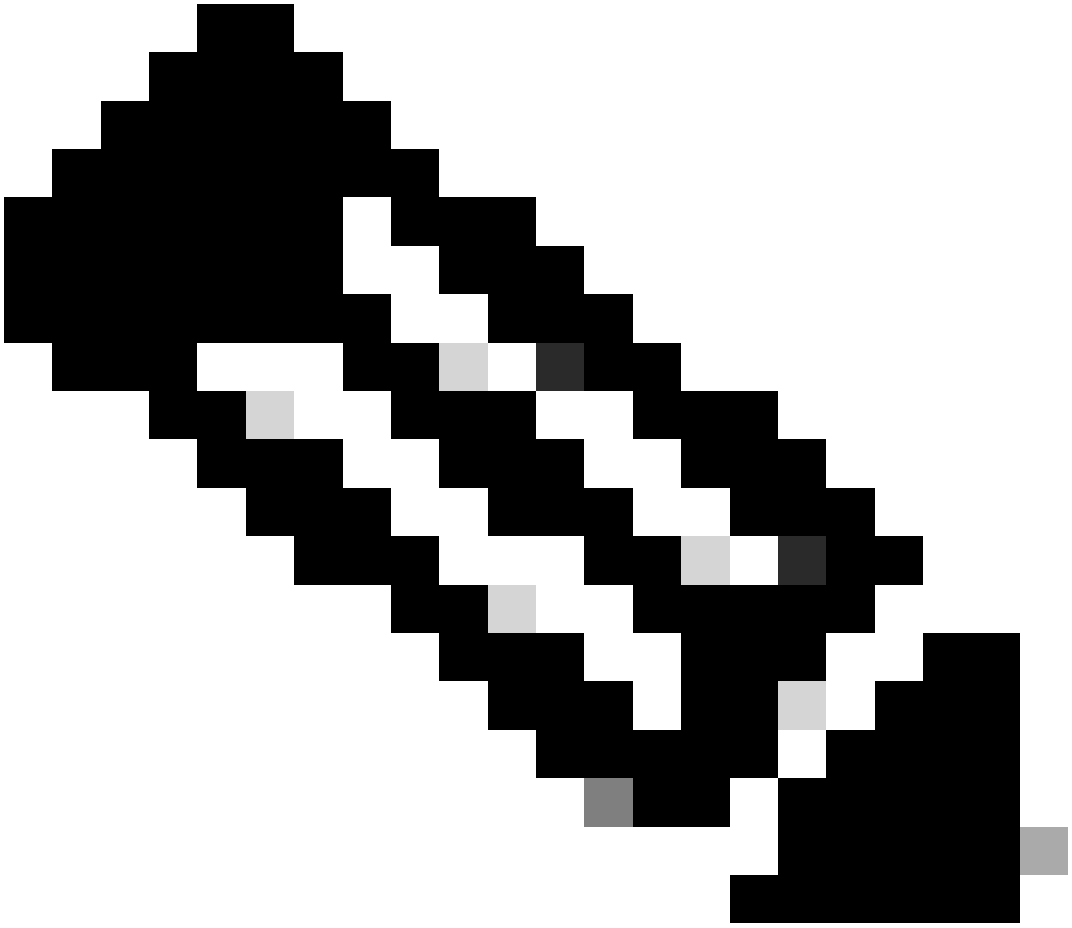




Remarque : N'oubliez pas de sélectionner l'unité principale comme périphérique qui a toujours la configuration, dans ce cas, FTD-01.

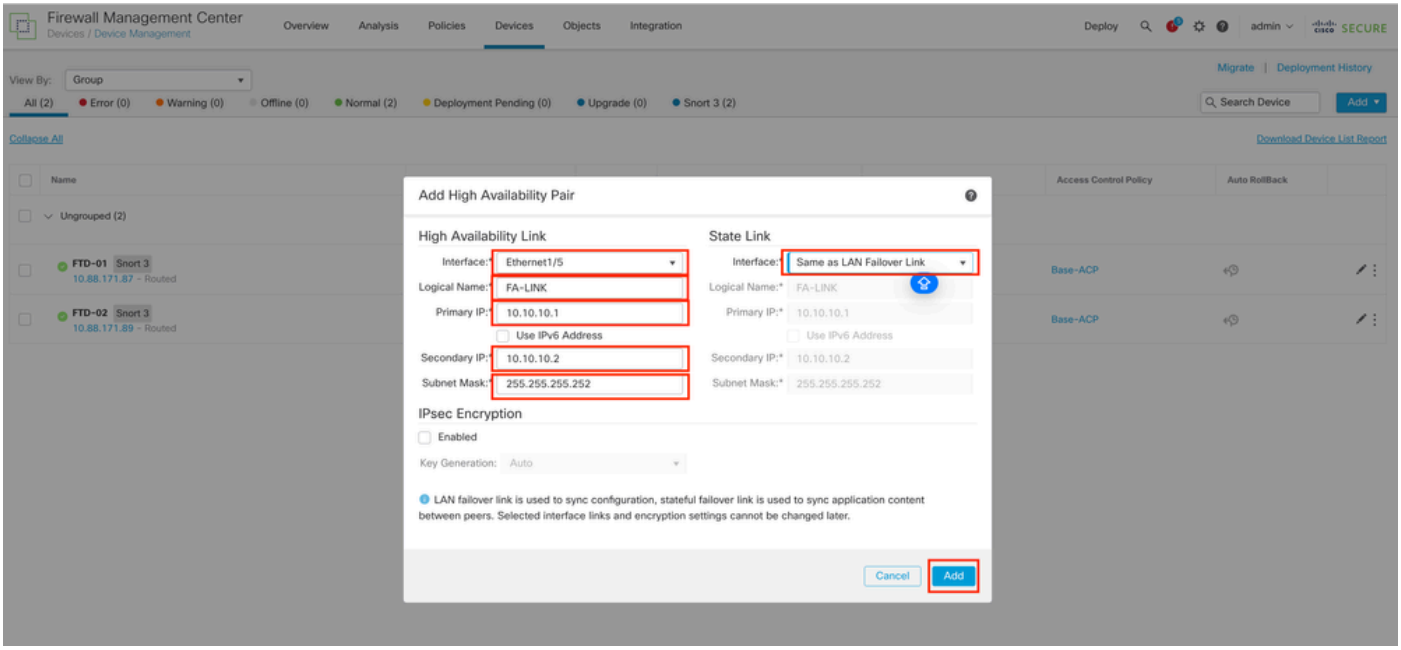
5.3. Confirmez la création de la haute disponibilité, puis cliquez sur Oui.


Add High Availability Pair
Name:*
FTD-HA
FTD
Essenti
FTD
Essenti
Warning
This operation restarts the Snort processes of primary and secondary devices, temporarily causing traffic interruption.
Do you want to continue?
Do not display this message again
No
Yes
converted to their high availability versions and applied on both peers.
Cancel
Continue

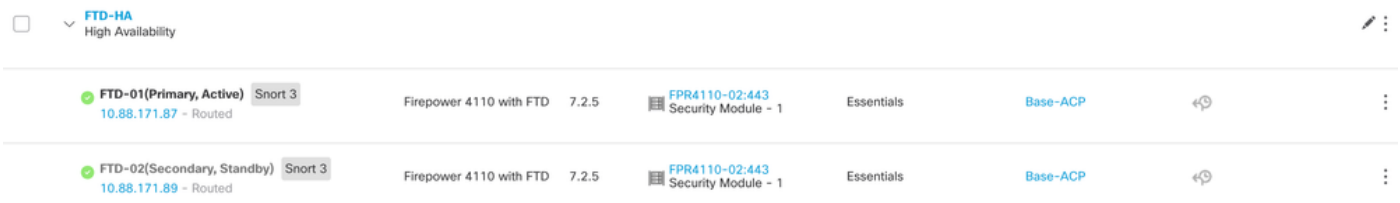


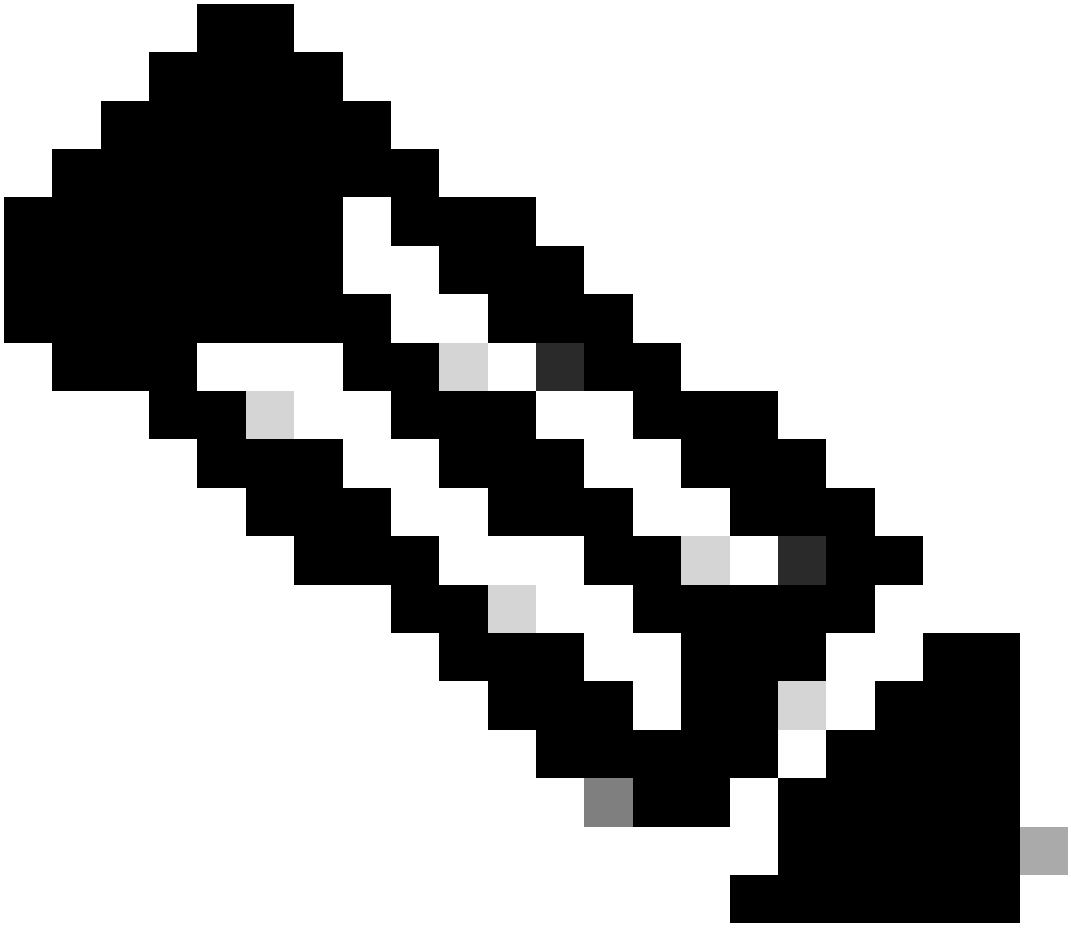
Remarque : La configuration de la haute disponibilité redémarre le moteur Snort des deux unités, ce qui peut entraîner une interruption du trafic.

5.4. Configurez les paramètres de haute disponibilité définis à l'étape 2, puis cliquez sur l'option Add :



6. La configuration de la haute disponibilité FTD est maintenant terminée :





Remarque : Si vous ne configurez pas d'adresses MAC virtuelles, vous devez effacer les tables ARP sur les routeurs connectés pour rétablir le flux de trafic en cas de remplacement de l'unité principale. Pour plus d'informations, consultez Adresses MAC et adresses IP en haute disponibilité.

Informations connexes

- Assistance technique de Cisco et téléchargements

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.