Configurer FMC avec Ansible pour créer une haute disponibilité FTD

Table des matières

Introduction

Ce document décrit les étapes d'automatisation de Firepower Management Center (FMC) pour créer Firepower Threat Defense (FTD) High Availability avec Ansible.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Ansible
- Serveur Ubuntu
- Cisco Firepower Management Center (FMC) virtuel
- Cisco Firepower Threat Defense (FTD) virtuel

Dans le cadre de cette situation de laboratoire, Ansible est déployé sur Ubuntu.

Il est essentiel de s'assurer que Ansible est correctement installé sur toute plate-forme prise en charge par Ansible pour exécuter les commandes Ansible mentionnées dans cet article.

Composants utilisés

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

- Serveur Ubuntu 22.04
- Ansible 2.10.8
- Python 3.10
- Cisco Firepower Threat Defense Virtual 7.4.1
- Cisco Firepower Management Center Virtual 7.4.1

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.

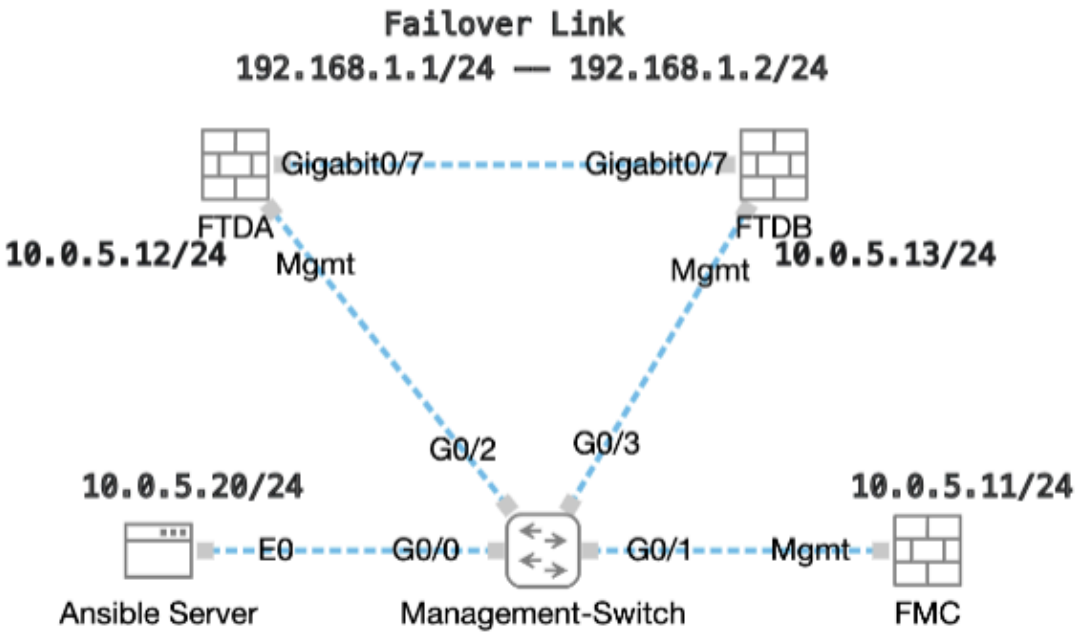
Informations générales

Ansible est un outil très polyvalent, qui démontre une efficacité significative dans la gestion des périphériques réseau. De nombreuses méthodologies peuvent être utilisées pour exécuter des tâches automatisées avec Ansible. La méthode utilisée dans cet article sert de référence aux fins de l'essai.

Dans cet exemple, la haute disponibilité FTD et son adresse IP de secours sont créées après l'exécution de l'exemple de guide.

Configurer

Diagramme du réseau



Topologie

Configurations

Étant donné que Cisco ne prend pas en charge les scripts d'exemple ou les scripts écrits par le client, nous avons quelques exemples que vous pouvez tester en fonction de vos besoins.

Il est essentiel de veiller à ce que la vérification préliminaire ait été dûment menée à bien.

- Le serveur Ansible possède une connectivité Internet.
- Le serveur Ansible est capable de communiquer avec le port de l'interface graphique FMC (le port par défaut de l'interface graphique FMC est 443).
- Deux périphériques FTD sont correctement enregistrés auprès de FMC.
- Les FTD principaux sont configurés avec une adresse IP d'interface.

Étape 1. Connectez-vous à la CLI du serveur Ansible via SSH ou la console.

Étape 2. Exécutez la commande`ansible-galaxy collection install cisco.fmcansible` afin d'installer la collection Ansible de FMC sur votre serveur Ansible.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Étape 3. Exécutez la commande`mkdir /home/cisco/fmc_ansible` afin de créer un nouveau dossier pour stocker les fichiers associés. Dans cet exemple, le répertoire de base est /home/cisco/, le nouveau nom de dossier est fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Étape 4. Accédez au dossier /home/cisco/fmc_ansible, create inventory file. Dans cet exemple, le nom du fichier d'inventaire est inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/


ccisco@inserthostname-here:~/fmc_ansible$

ls


inventory.ini
```

Vous pouvez dupliquer ce contenu et le coller pour l'utiliser, en modifiant les sections **en gras** avec les paramètres précis.

<#root>

[fmc]

10.0.5.11

[fmc:vars]
ansible_user=

cisco

ansible_password=

cisco

ansible_httpapi_port=443
ansible_httpapi_use_ssl=True
ansible_httpapi_validate_certs=False
network_type=HOST
ansible_network_os=cisco.fmcansible.fmc

Étape 5. Accédez au dossier /home/cisco/fmc_ansible, create variable file for creation FTD HA. Dans cet exemple, le nom de fichier de la variable est fmc-create-ftd-ha-vars.yml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-create-ftd-ha-vars.yml

inventory.ini

Vous pouvez dupliquer ce contenu et le coller pour l'utiliser, en modifiant les sections **en gras** avec les paramètres précis.

<#root>

user: domain: 'Global' device_name: ftd1: '

FTDA

' ftd2: '

FTDB

' ftd_ha: name: '

FTD_HA

' active_ip: '

192.168.1.1

' standby_ip: '

192.168.1.2

' key:

cisco

mask24: '

255.255.255.0

'

Étape 6. Accédez au dossier /home/cisco/fmc_ansible, create playbook file for creation FTD HA. Dans cet exemple, le nom du fichier du playbook est fmc-create-ftd-ha-playbook.yaml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-create-ftd-ha-playbook.yaml

fmc-create-ftd-ha-vars.yml inventory.ini

Vous pouvez dupliquer ce contenu et le coller pour l'utiliser, en modifiant les sections **en gras** avec les paramètres précis.

<#root>

--- - name: FMC Create FTD HA hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configuration: operation:

user.domain

}}" register_as: domain - name: Task02 - Get FTD1 cisco.fmcansible.fmc_configuration: operation: getAl

device_name.ftd1

}}" register_as: ftd1_list - name: Task03 - Get FTD2 cisco.fmcansible.fmc_configuration: operation: ge

device_name.ftd2

}}" register_as: ftd2_list - name: Task04 - Get Physical Interfaces cisco.fmcansible.fmc_configuration

ftd_ha.name

}}" type: "DeviceHAPair" ftdHABootstrap: { 'isEncryptionEnabled': false, 'encKeyGenerationScheme': 'CU

ftd_ha.key

}}", 'useSameLinkForFailovers': true, 'lanFailover': { 'useIPv6Address': false, 'subnetMask': "{{

ftd_ha.mask24

}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

ftd_ha.standby_ip

}}", 'logicalName': 'LAN-INTERFACE', 'activeIP': "{{

ftd_ha.active_ip

}}" }, 'statefulFailover': { 'useIPv6Address': false, 'subnetMask': "{{

ftd_ha.mask24

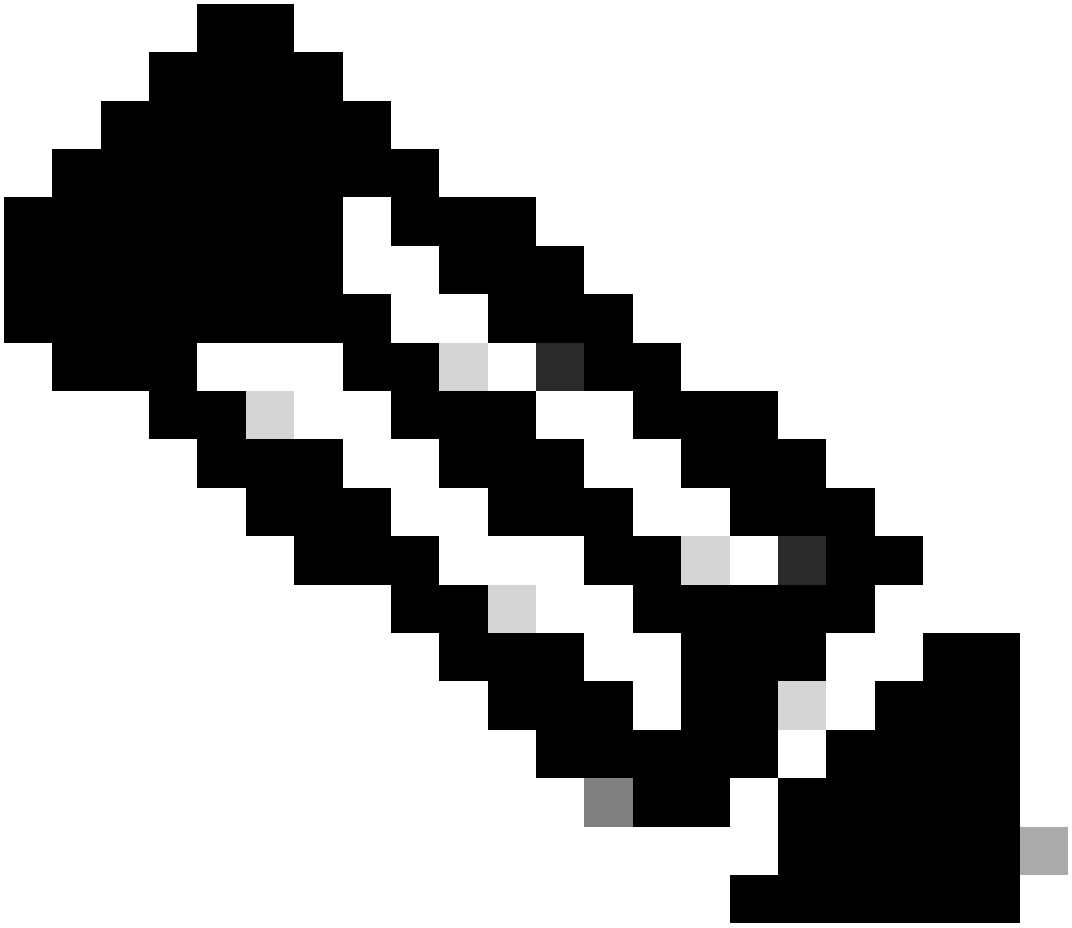
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

ftd_ha.standby_ip

}}", 'logicalName': 'STATEFUL-INTERFACE', 'activeIP': "{{

ftd_ha.active_ip

}}" } } path_params: domainUUID: "{{ domain[0].uuid }}" - name: Task06 - Wait for FTD HA Ready ansible



Remarque : les noms en gras dans cet exemple de guide servent de variables. Les valeurs correspondantes de ces variables sont conservées dans le fichier de variables.

Étape 7. Accédez au dossier **/home/cisco/fmc_ansible**, run command ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"afin de lire la tâche ansible.

Dans cet exemple, la commande est ansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yml" .

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

```
 ccisco@inserthostname-here:~/fmc_ansible$
ls
 fmc-create-ftd-ha-playbook.yaml fmc-create-ftd-ha-vars.yml inventory.ini cisco@inserthostname-here:~/fm
ansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yml"
 PLAY [FMC Create FTD HA] ********************************************************************************
```

Étape 8. Accédez au dossier /home/cisco/fmc_ansible, créez un fichier variable pour mettre à jour l'adresse IP de secours FTD HA. Dans cet exemple, le nom du fichier variable est fmc-create-ftd-ha-standby-ip-vars.yml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-create-ftd-ha-playbook.yaml

fmc-create-ftd-ha-standby-ip-vars.yml

fmc-create-ftd-ha-vars.yml inventory.ini

Vous pouvez dupliquer ce contenu et le coller pour l'utiliser, en modifiant les sections **en gras** avec les paramètres précis.

<#root>

user: domain: 'Global' ftd_data: outside_name: '

Outside

' inside_name: '

Inside

' outside_ip: '10.1.1.1' inside_ip: '10.1.2.1' mask24: '255.255.255.0' ftd_ha: name: '

FTD_HA

' outside_standby: '

10.1.1.2

' inside_standby: '

10.1.2.2

'

Étape 9. Accédez au dossier **/home/cisco/fmc_ansible**, créez un fichier de guide de mise à jour de l'adresse IP de secours FTD HA. Dans cet exemple, le nom du fichier du playbook est fmc-create-ftd-ha-standby-ip-playbook.yaml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-create-ftd-ha-playbook.yaml

fmc-create-ftd-ha-standby-ip-playbook.yaml

fmc-create-ftd-ha-standby-ip-vars.yml fmc-create-ftd-ha-vars.yml inventory.ini

Vous pouvez dupliquer ce contenu et le coller pour l'utiliser, en modifiant les sections **en gras** avec les paramètres précis.

<#root>

--- - name: FMC Update FTD HA Interface Standby IP hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_conf

user.domain

}}" register_as: domain - name: Task02 - Get FTD HA Object cisco.fmcansible.fmc_configuration: operati

ftd_data.outside_name

}}" register_as: outside_interface - name: Task04 - Get Inside Interface cisco.fmcansible.fmc_configur

ftd_data.inside_name

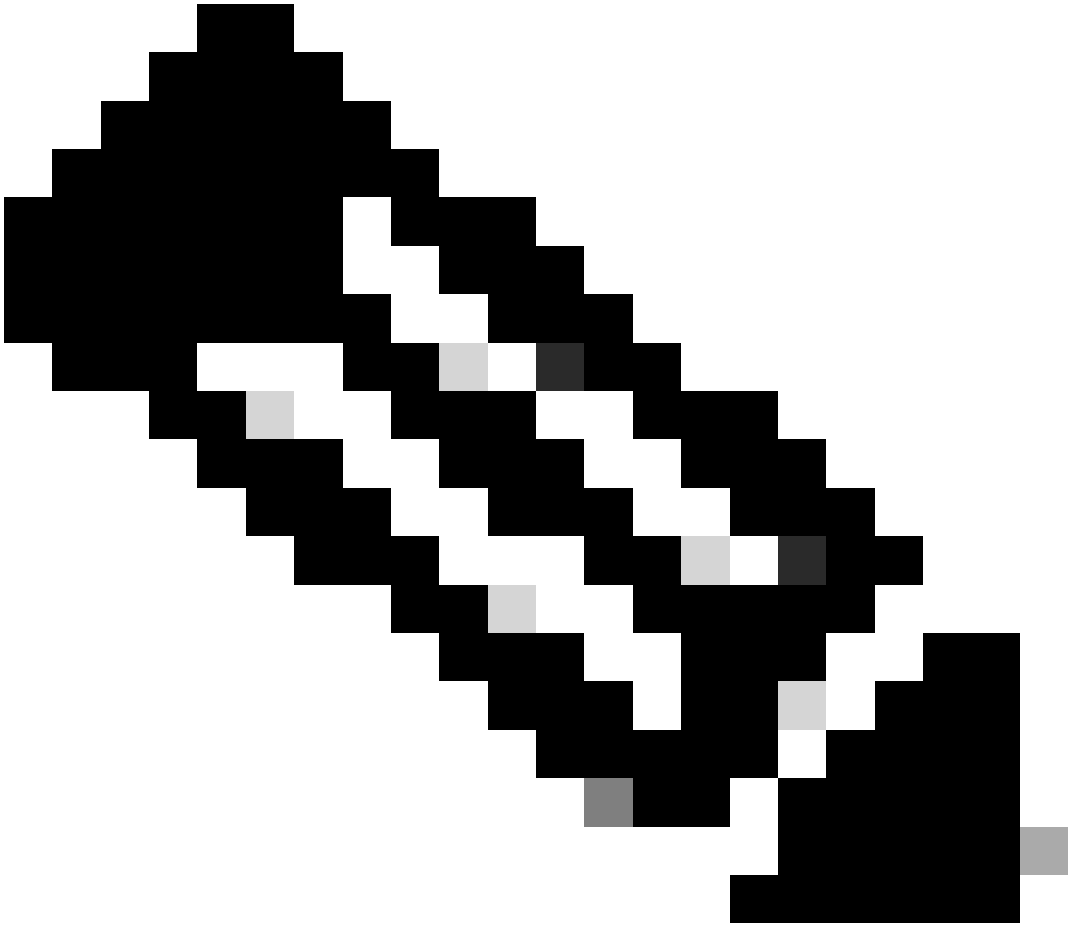
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

ftd_ha.outside_standby

}}"} monitorForFailures: true path_params: objectId: "{{ outside_interface[0].id }}" containerUUID: "{

ftd_ha.inside_standby

}}"} monitorForFailures: true path_params: objectId: "{{ inside_interface[0].id }}" containerUUID: "{{



Remarque : les noms en gras dans cet exemple de guide servent de variables. Les valeurs correspondantes de ces variables sont conservées dans le fichier de variables.

Étape 10. Accédez au dossier **/home/cisco/fmc_ansible**, run command ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"afin de lire la tâche ansible.

Dans cet exemple, la commande est ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

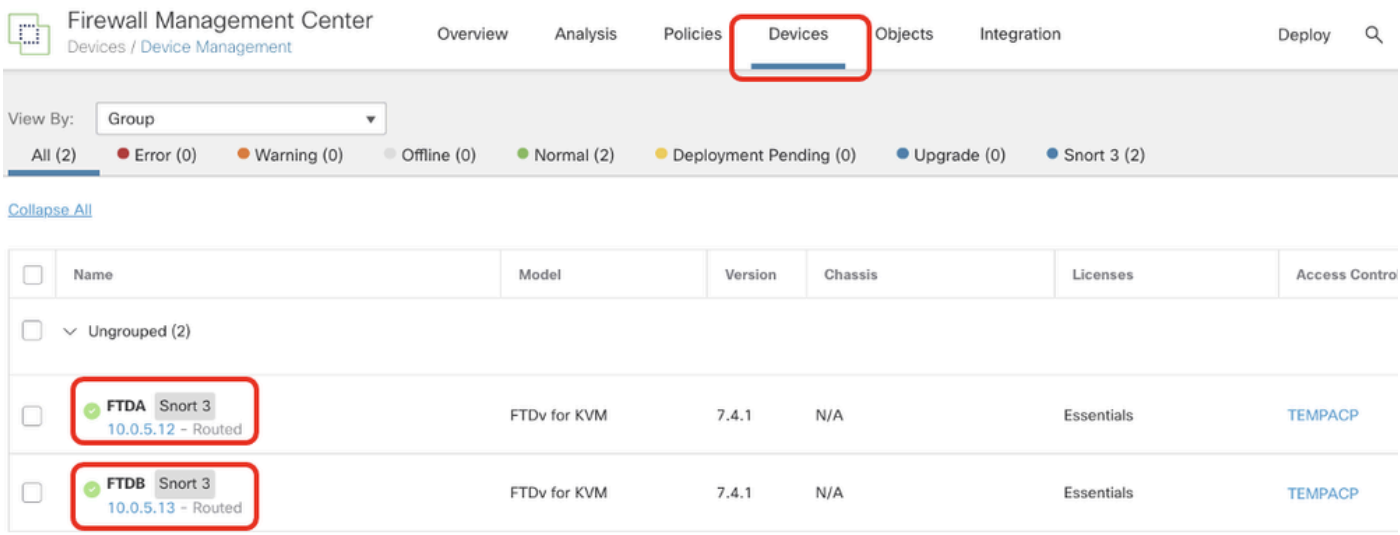
<#root>

cisco@inserthostname-here:~$

```
 cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$
ls

fmc-create-ftd-ha-playbook.yaml
fmc-create-ftd-ha-standby-ip-playbook.yaml

fmc-create-ftd-ha-standby-ip-vars.yml
 fmc-create-ftd-ha-vars.yml
inventory.ini

cisco@inserthostname-here:~/fmc_ansible$
ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-stand
 PLAY [FMC Update FTD HA Interface Standby IP] **********************************************************
```

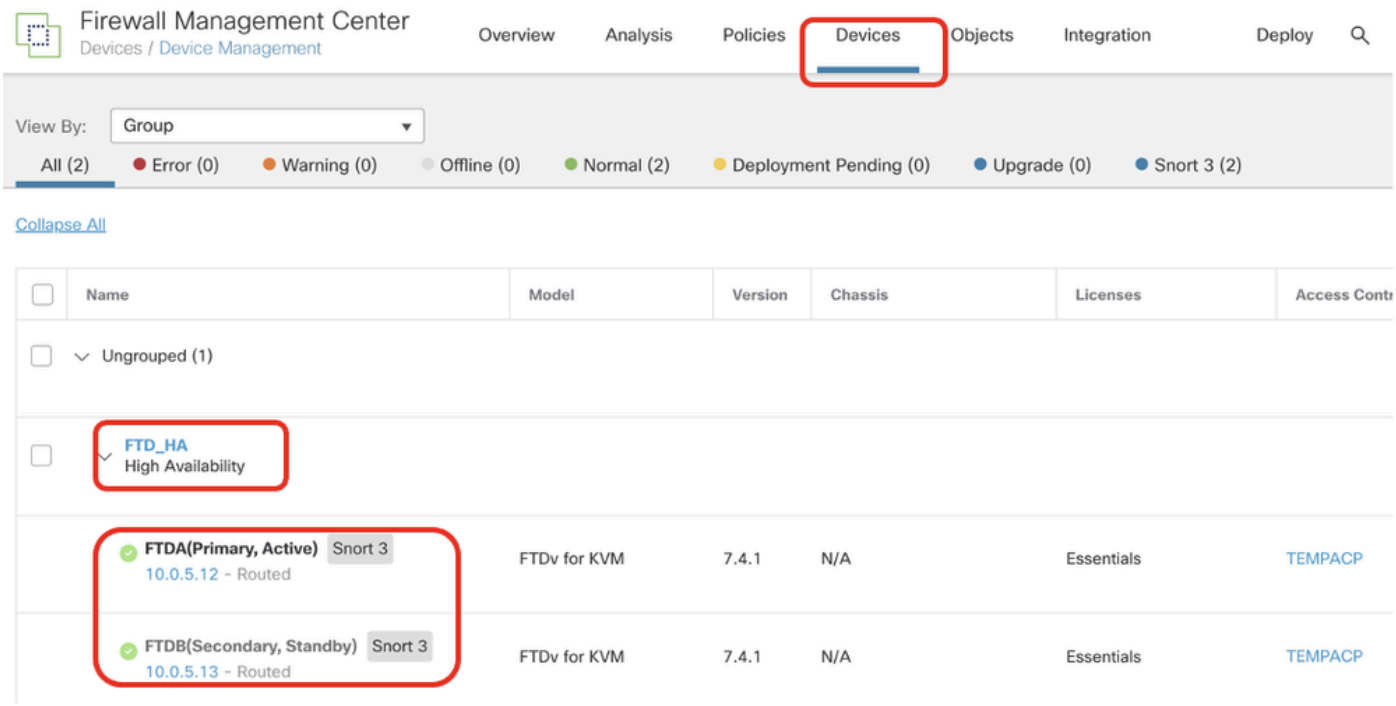
Vérifier

Avant d'exécuter la tâche d'analyse, connectez-vous à l'interface utilisateur FMC. Accédez à **Devices > Device Management,** deux FTD enregistrés avec succès sur FMC avec la stratégie de contrôle d'accès configurée.



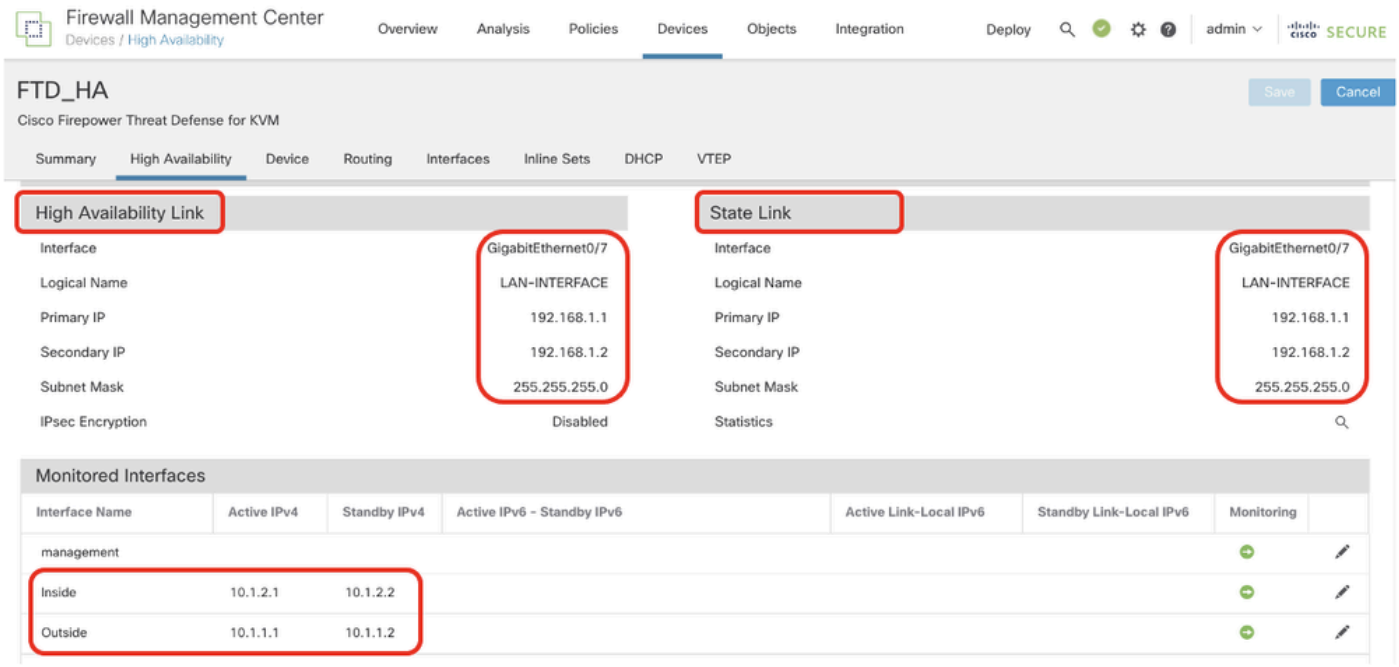
Avant d'exécuter une tâche réactive

Après avoir exécuté la tâche d'analyse, connectez-vous à l'interface utilisateur FMC. Accédez à **Périphériques > Gestion des périphériques,** FTD HA est créé avec succès.



Après exécution réussie d'une tâche réactive

Cliquez sur **Edit** of FTD HA, failover ip address et interface standby ip address are configured successfully.



Détail de la haute disponibilité FTD

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de voir plus de journaux de playbook ansible, vous pouvez exécuter le playbook ansible avec -vvv.

<#root>

cisco@inserthostname-here:~/fmc_ansible$ ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-

-vvv

Informations connexes

Cisco Devnet FMC Ansible

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.