FMC configureren met Ansible om FTD hoge beschikbaarheid te maken

Inhoud

Inleiding

In dit document worden de stappen beschreven om Firepower Management Center (FMC) te automatiseren voor het maken van Firepower Threat Defence (FTD) High Availability met Ansible.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- anabel
- Ubuntu server
- Cisco Firepower Management Center (FMC) virtueel
- Cisco Firepower Threat Defence (FTD) virtueel

In de context van deze laboratoriumsituatie wordt Ansible ingezet op Ubuntu.

Het is van essentieel belang om ervoor te zorgen dat Ansible met succes wordt geïnstalleerd op elk platform dat wordt ondersteund door Ansible voor het uitvoeren van de Ansible commando's waarnaar in dit artikel wordt verwezen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Ubuntu server 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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

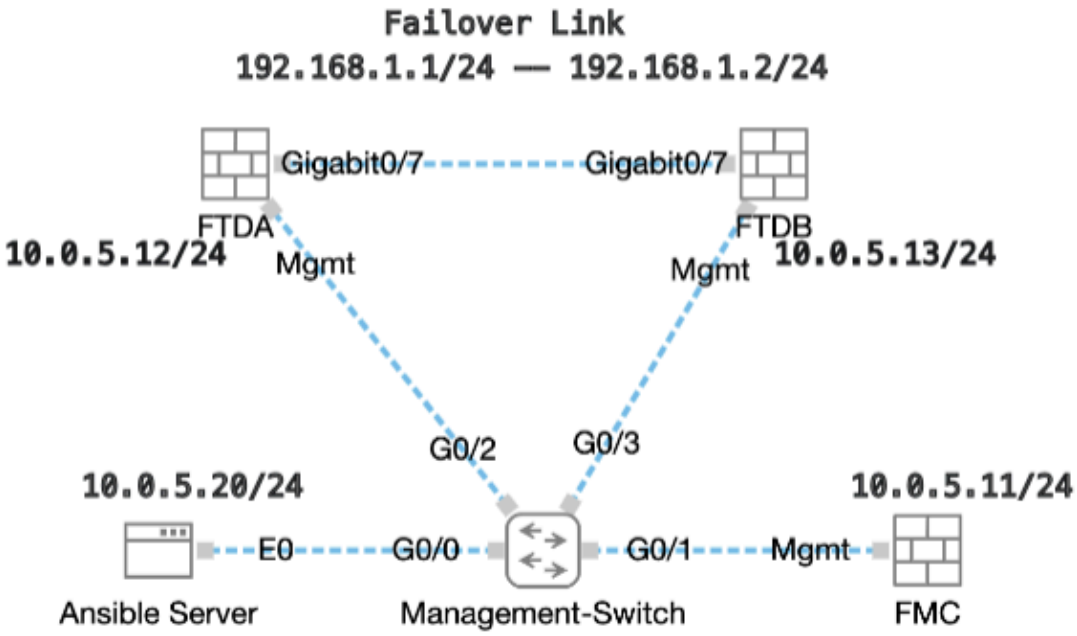
Achtergrondinformatie

Ansible is een zeer veelzijdig hulpmiddel, dat significante doeltreffendheid in het beheer van netwerkapparaten aantoont. Er kunnen tal van methodologieën worden gebruikt om geautomatiseerde taken uit te voeren met Ansible. De in dit artikel gebruikte methode dient als referentie voor testdoeleinden.

In dit voorbeeld, de FTD Hoge Beschikbaarheid en het standby IP adres van het worden gecreëerd na het uitvoeren van het playbookvoorbeeld met succes.

Configureren

Netwerkdiagram



Topologie

Configuraties

Omdat Cisco voorbeeldscripts of door de klant geschreven scripts niet ondersteunt, hebben we enkele voorbeelden die u kunt testen afhankelijk van uw behoeften.

Het is van essentieel belang ervoor te zorgen dat de voorafgaande verificatie naar behoren is uitgevoerd.

- Een omkeerbare server beschikt over internetverbinding.
- Een omkeerbare server kan met succes communiceren met de FMC GUI-poort (de standaardpoort voor FMC GUI is 443).
- Twee FTD-apparaten zijn geregistreerd bij het VCC.
- Primaire FTD wordt geconfigureerd met IP-interfaceadres.

Stap 1. Maak verbinding met de CLI van de Ansible server via SSH of console.

Stap 2. Voer de opdracht ansible-galaxy collection install cisco.fmcansible uit om de Ansible Collection van FMC op uw Ansible Server te installeren.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Stap 3. Start de opdracht mkdir /home/cisco/fmc_ansible om een nieuwe map te maken voor het opslaan van de bijbehorende bestanden. In dit voorbeeld is de home directory /home/cisco/, de nieuwe mapnaam is fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Stap 4. Navigeer naar de map /home/cisco/fmc_ansible en maak een voorraadbestand. In dit voorbeeld, de inventaris bestandsnaam is inventaris.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/


ccisco@inserthostname-here:~/fmc_ansible$

ls


inventory.ini
```

U kunt deze inhoud dupliceren en plakken voor gebruik, door de **vetgedrukte** secties te veranderen met de nauwkeurige parameters.

<#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

Stap 5. Navigeer naar de map /home/cisco/fmc_ansible, maak een variabele bestand voor het maken van FTD HA. In dit voorbeeld is de variabele bestandsnaam fmc-creation-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

U kunt deze inhoud dupliceren en plakken voor gebruik, door de **vetgedrukte** secties te veranderen met de nauwkeurige parameters.

<#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

'

Stap 6. Navigeer naar de map /home/cisco/fmc_ansible en maak een afspeelboekbestand voor het maken van FTD HA. In dit voorbeeld is de bestandsnaam van het afspeelboek fmc-creation-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

U kunt deze inhoud dupliceren en plakken voor gebruik, door de **vetgedrukte** secties te veranderen met de nauwkeurige parameters.

<#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

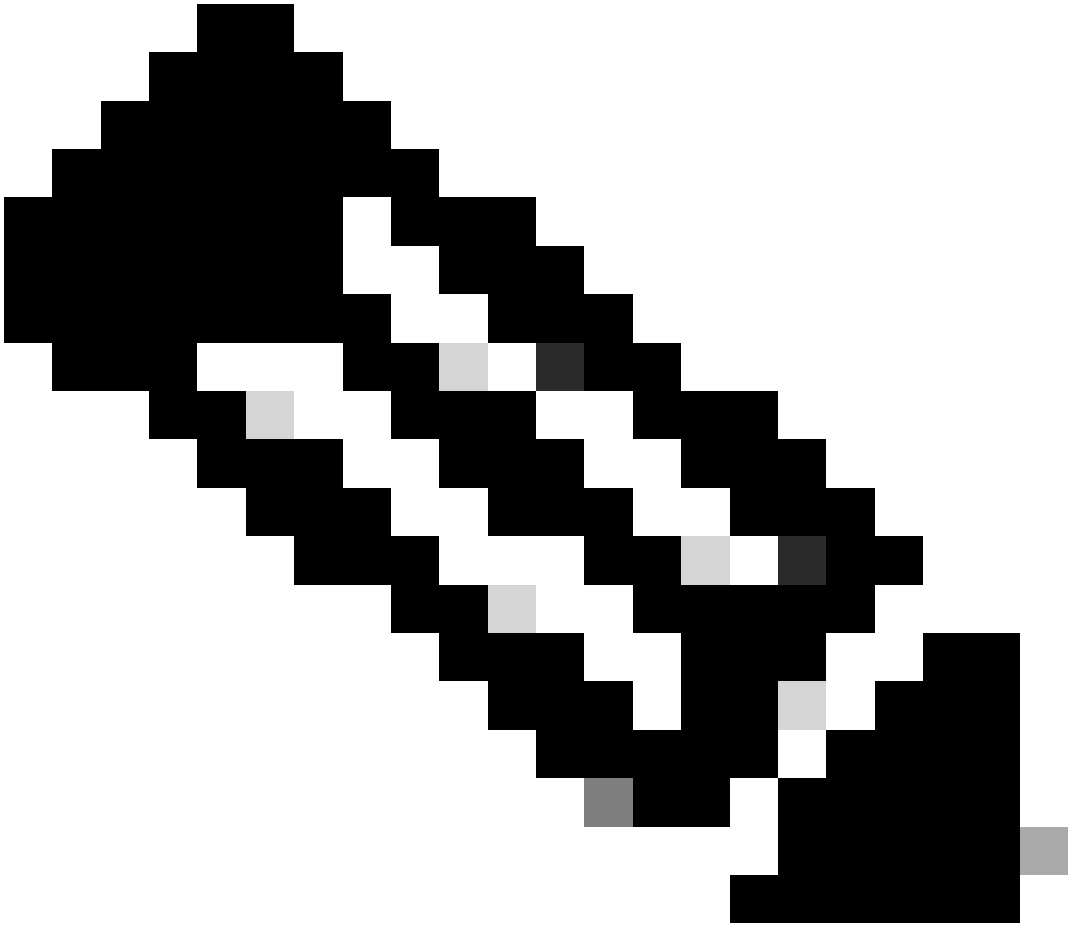
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



Opmerking: de vetgedrukte namen in dit voorbeeldafspeelboek dienen als variabelen. De corresponderende waarden voor deze variabelen blijven in het variabele bestand bewaard.

Stap 7. Navigeer naar de map **/home/cisco/fmc_ansible**, voer de opdracht ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"uit om de taak ansible af te spelen.

In dit voorbeeld is de opdracht 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:~/fr

ansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yml"

PLAY [FMC Create FTD HA] **

Stap 8. Navigeer naar de map /home/cisco/fmc_ansible, maak een variabele bestand voor het bijwerken van FTD HA standby ip-adres. In dit voorbeeld is de variabele bestandsnaam fmc-creation-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

U kunt deze inhoud dupliceren en plakken voor gebruik, door de **vetgedrukte** secties met de nauwkeurige parameters te wijzigen.

<#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

'

Stap 9. Navigeer naar de map **/home/cisco/fmc_ansible**, maak een afspeelboekbestand voor het bijwerken van het FTD HA stand-by ip adres. In dit voorbeeld is de bestandsnaam van het afspeelboek fmc-creation-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

U kunt deze inhoud dupliceren en plakken voor gebruik, door de **vetgedrukte** secties te veranderen met de nauwkeurige parameters.

<#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

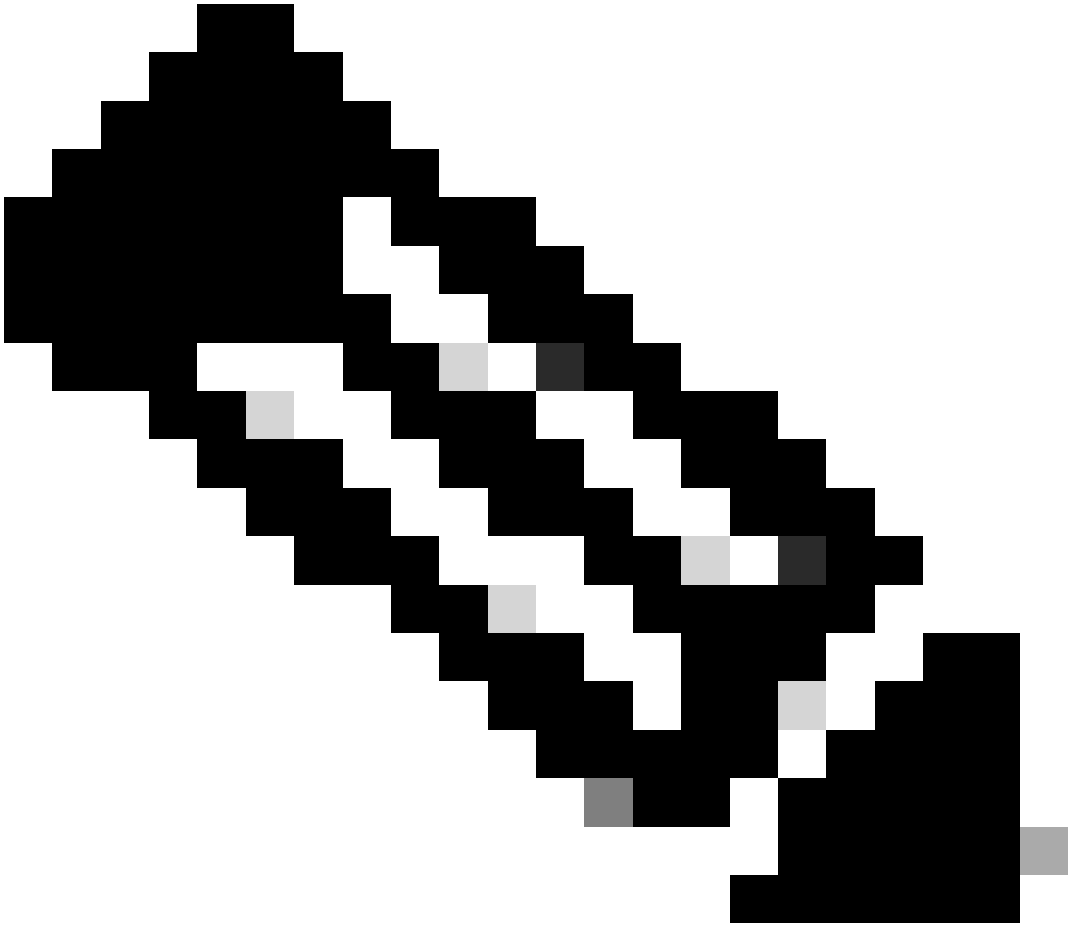
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



Opmerking: de vetgedrukte namen in dit voorbeeldafspeelboek dienen als variabelen. De corresponderende waarden voor deze variabelen blijven in het variabele bestand bewaard.

Stap 10. Navigeer naar de map **/home/cisco/fmc_ansible**, voer de opdracht ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"uit om de taak ansible af te spelen.

In dit voorbeeld is de opdracht ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

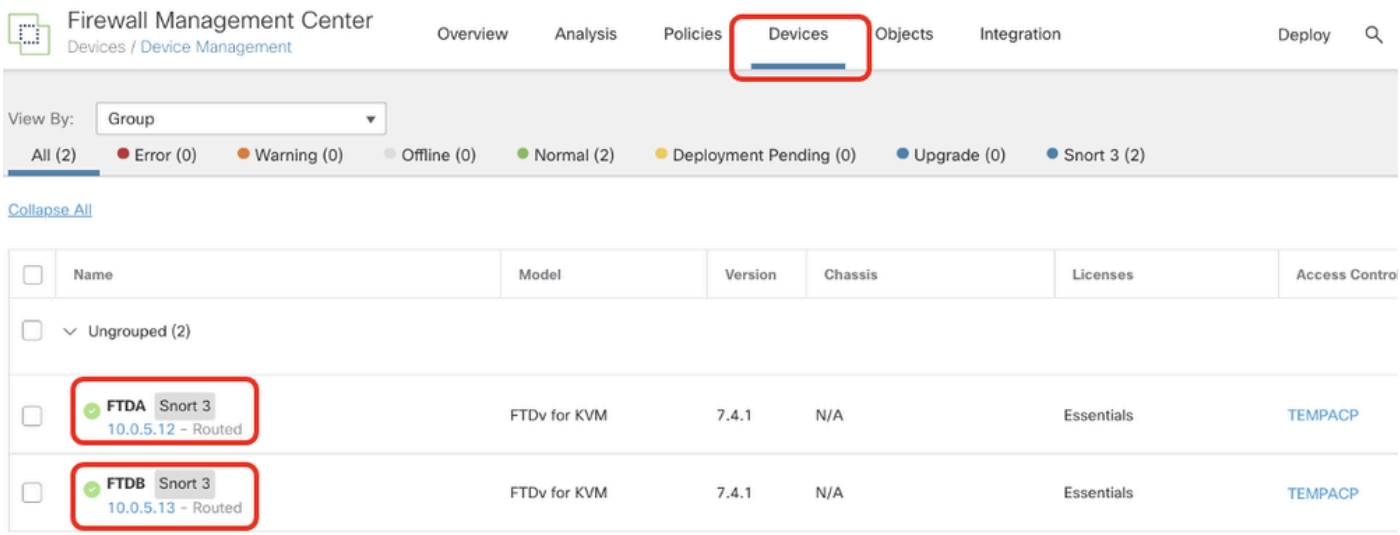
<#root>

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] **********************************************************
```

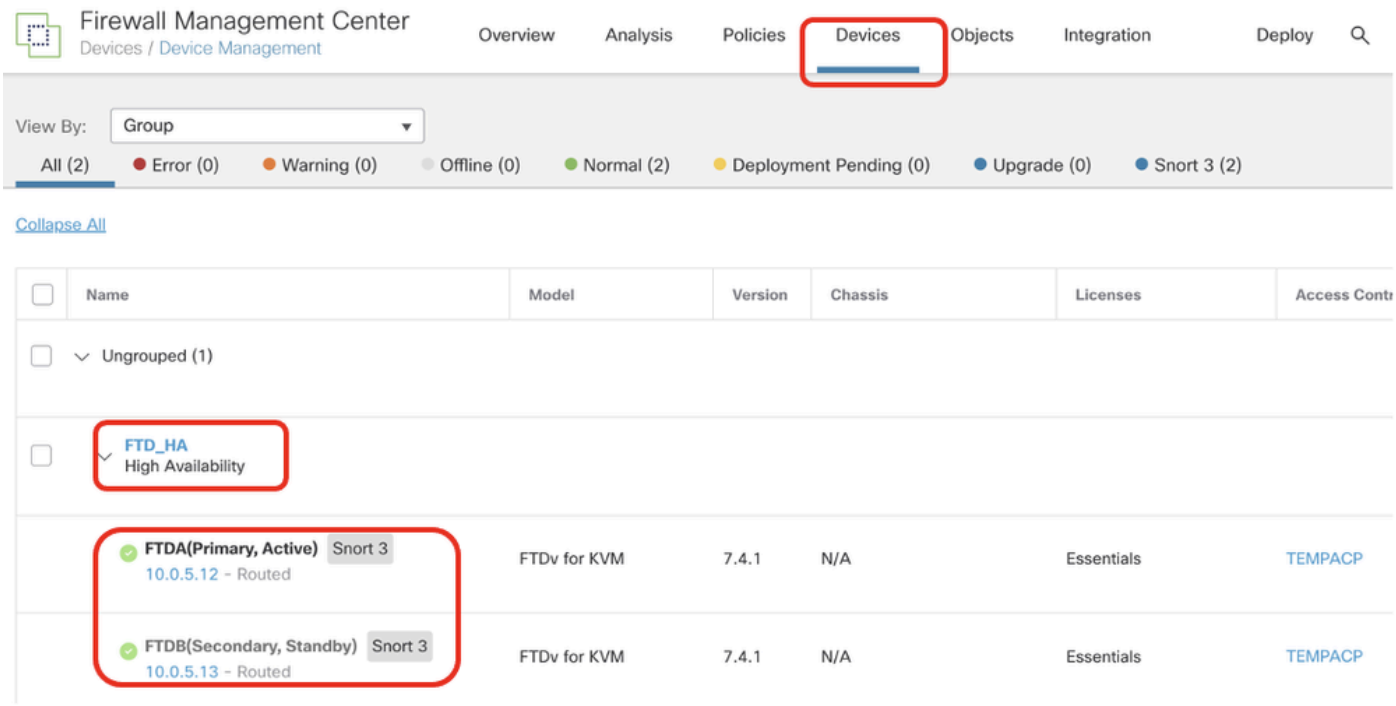
Verifiëren

Log in de FMC GUI voordat u de verstelbare taak uitvoert. Navigeren naar **Apparaten > Apparaatbeheer,** twee FTD met succes geregistreerd op FMC met geconfigureerd toegangscontrolebeleid.



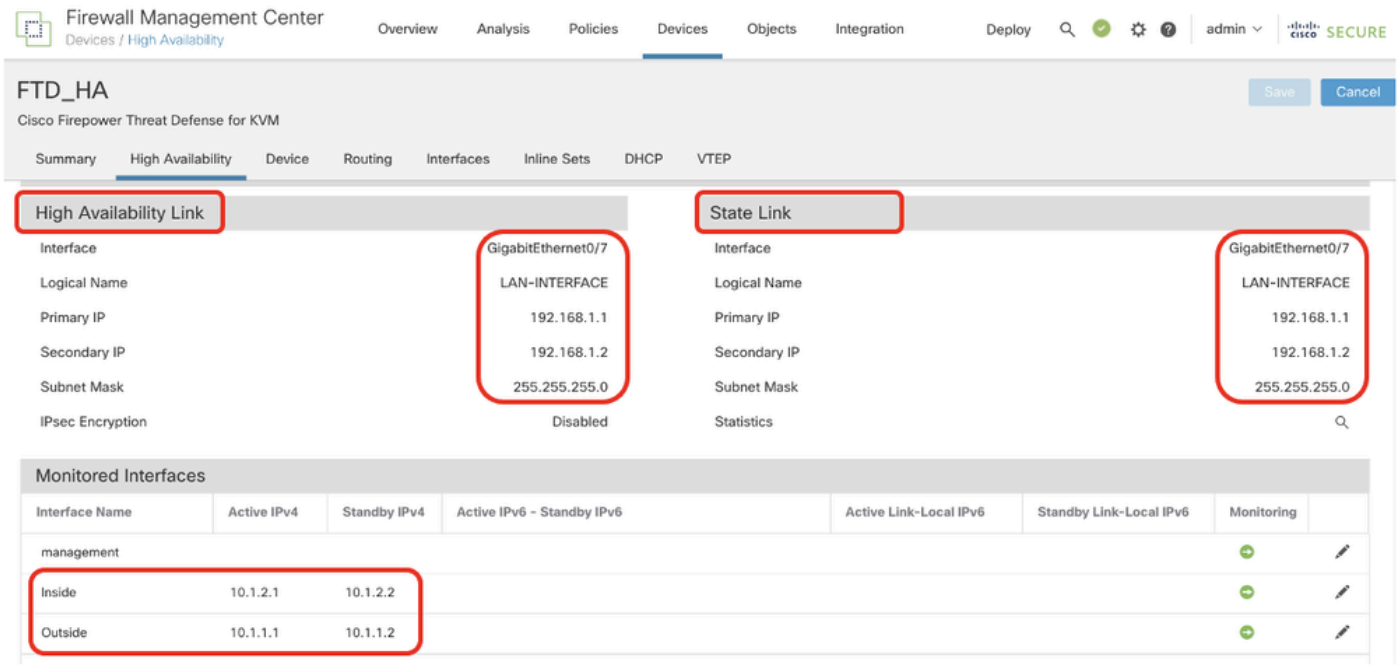
Voordat u een willekeurige taak uitvoert

Log na het uitvoeren van de verstelbare taak in op FMC GUI. Navigeren naar **Apparaten > Apparaatbeheer,** FTD HA is gemaakt.



Na het uitvoeren van een omkeerbare taak

Klik op **Bewerken** van FTD HA, failover IP-adres en interface standby ip-adres worden met succes geconfigureerd.



FTD - Detail met hoge beschikbaarheid

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Om meer logboeken van ansible playbook te zien, kunt u ansible playbook uitvoeren met -vv.

<#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

Gerelateerde informatie

Cisco Devnet FMC Ansible

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.