Konfigurieren von FMC mit Ansible zur Erstellung einer FTD-Hochverfügbarkeit

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Automatisierung von FirePOWER Management Center (FMC) zur Erstellung von FirePOWER Threat Defense (FTD) High Availability mit Ansible beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Ansible
- Ubuntu-Server
- Cisco FirePOWER Management Center (FMC) - Virtuell
- Cisco FirePOWER Threat Defense (FTD) - virtuell

Im Kontext dieser Laborsituation wird Ansible unter Ubuntu bereitgestellt.

Es ist wichtig sicherzustellen, dass Ansible erfolgreich auf jeder von Ansible unterstützten Plattform installiert wird, um die in diesem Artikel genannten Ansible-Befehle auszuführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

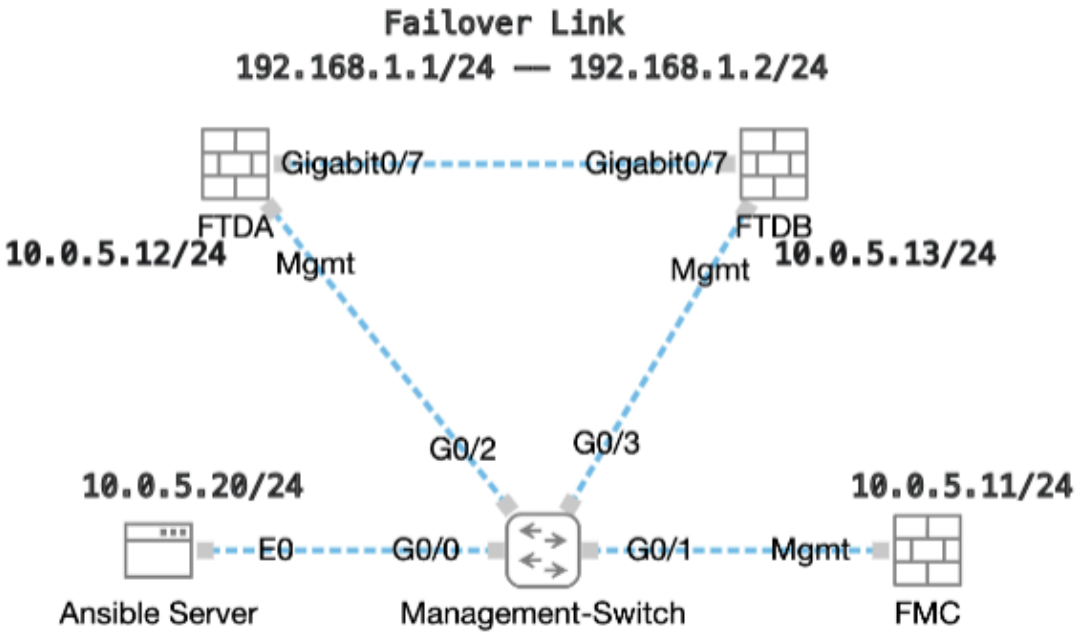
Hintergrundinformationen

Ansible ist ein äußerst vielseitiges Tool, das eine erhebliche Effizienz bei der Verwaltung von Netzwerkgeräten demonstriert. Für die Ausführung automatisierter Aufgaben mit Ansible können zahlreiche Methoden eingesetzt werden. Das in diesem Artikel verwendete Verfahren dient als Referenz für Testzwecke.

In diesem Beispiel werden die FTD-Hochverfügbarkeit und die Standby-IP-Adresse erstellt, nachdem das Beispiel des strategischen Leitfadens erfolgreich ausgeführt wurde.

Konfigurieren

Netzwerkdiagramm



Topologie

Konfigurationen

Da Cisco keine Beispiel-Skripte oder vom Kunden erstellte Skripte unterstützt, gibt es einige Beispiele, die Sie je nach Ihren Anforderungen testen können.

Es muss unbedingt sichergestellt werden, dass die vorläufige Überprüfung ordnungsgemäß abgeschlossen wurde.

- Ein möglicher Server verfügt über eine Internetverbindung.
- Ein möglicher Server kann erfolgreich mit dem FMC GUI-Port kommunizieren (der Standardport für die FMC GUI ist 443).
- Zwei FTD-Geräte wurden erfolgreich bei FMC registriert.
- Primäre FTDs werden mit der Schnittstellen-IP-Adresse konfiguriert.

Schritt 1: Stellen Sie über SSH oder die Konsole eine Verbindung mit der CLI des Ansible-Servers her.

Schritt 2: Führen Sie den Befehl ansible-galaxy collection install cisco.fmcansible aus, um die Ansible-Sammlung von FMC auf dem Ansible-Server zu installieren.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Schritt 3: Führen Sie den Befehlmkdir /home/cisco/fmc_ansible aus, um einen neuen Ordner zum Speichern der zugehörigen Dateien zu erstellen. In diesem Beispiel ist das Basisverzeichnis /home/cisco/, und der neue Ordnername lautet fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Schritt 4: Navigieren Sie zum Ordner /home/cisco/fmc_ansible, und erstellen Sie eine Inventardatei. In diesem Beispiel lautet der Name der Bestandsdatei Inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/


ccisco@inserthostname-here:~/fmc_ansible$

ls
```

inventory.ini

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **fett gedruckten** Abschnitte mit genauen Parametern ändern.

<#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

Schritt 5: Navigieren Sie zum Ordner /home/cisco/fmc_ansible, erstellen Sie eine variable Datei zum Erstellen von FTD HA. In diesem Beispiel lautet der Dateiname der Variablen 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

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **fett gedruckten** Abschnitte mit genauen Parametern ändern.

<#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

'

Schritt 6: Navigieren Sie zum Ordner /home/cisco/fmc_ansible, und erstellen Sie einen strategischen Leitfaden zum Erstellen von FTD HA. In diesem Beispiel lautet der Dateiname des strategischen Leitfadens 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

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **fett gedruckten** Abschnitte mit genauen Parametern ändern.

<#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

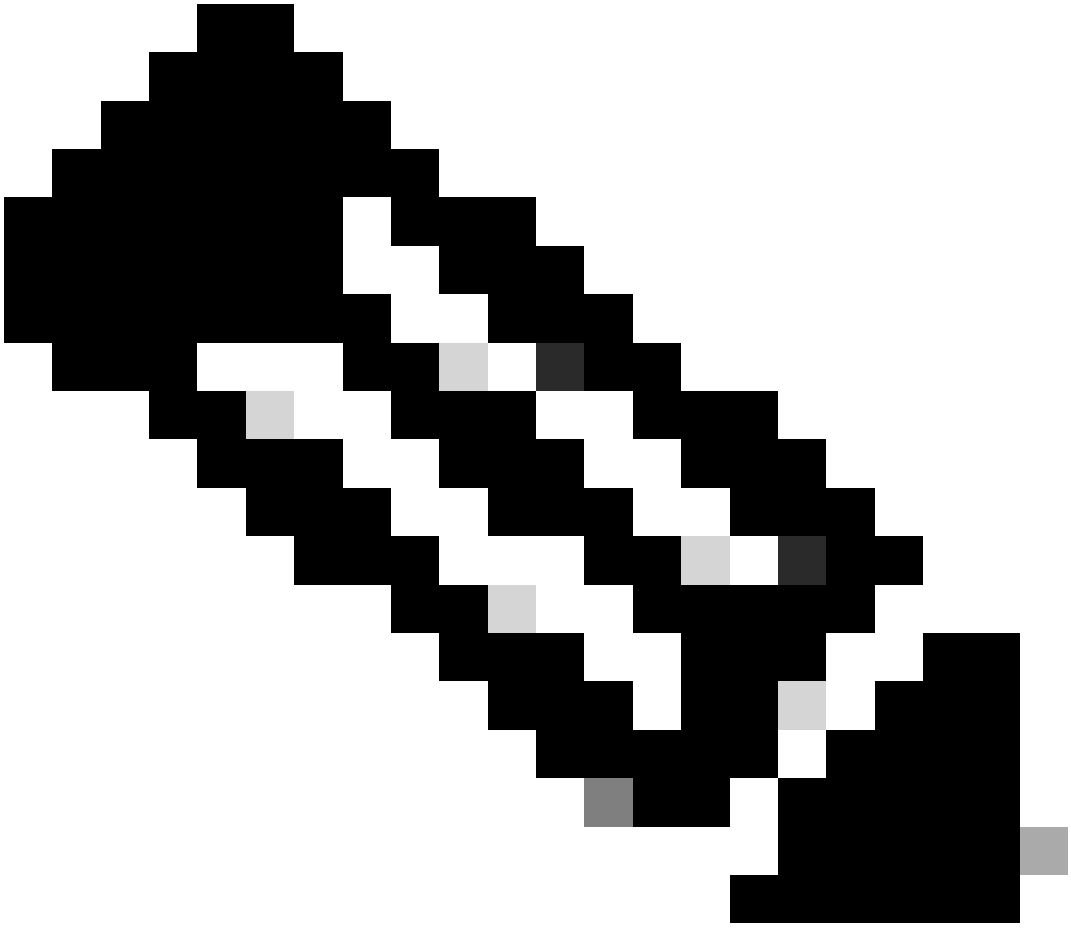
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



Hinweis: Die in diesem strategischen Leitfaden fett formatierten Namen dienen als Variablen. Die entsprechenden Werte für diese Variablen werden innerhalb der Variablendatei beibehalten.

Schritt 7. Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, führen Sie den Befehl ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"aus, um die ansible Aufgabe abzuspielen.

In diesem Beispiel lautet der Befehl 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] **********

Schritt 8: Navigieren Sie zum Ordner /home/cisco/fmc_ansible, und erstellen Sie eine variable Datei zum Aktualisieren der FTD HA-Standby-IP-Adresse. In diesem Beispiel lautet der Dateiname der Variablen 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

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **fett gedruckten** Abschnitte mit genauen Parametern ändern.

<#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

'

Schritt 9. Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, und erstellen Sie eine Playbook-Datei für die Aktualisierung der FTD HA-Standby-IP-Adresse. In diesem Beispiel lautet der Dateiname des strategischen Leitfadens 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

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **fett gedruckten** Abschnitte mit genauen Parametern ändern.

<#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

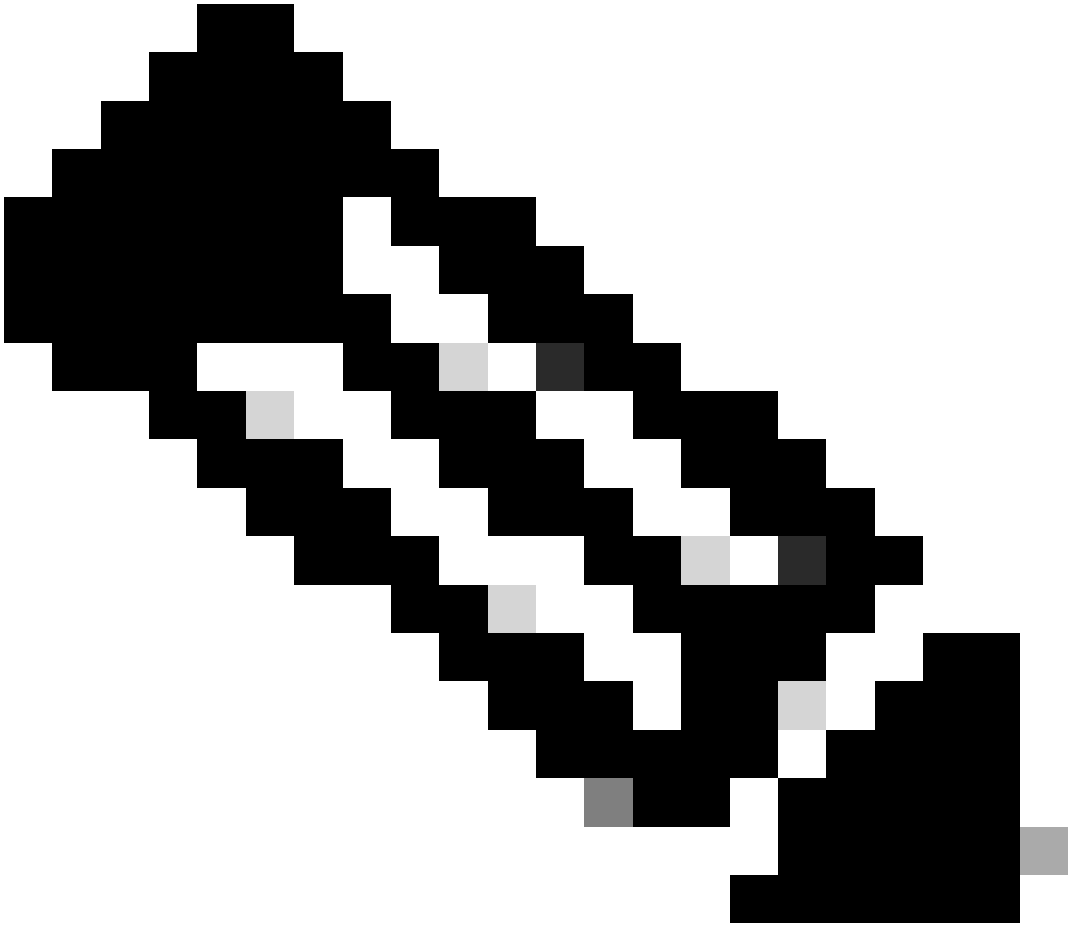
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



Hinweis: Die in diesem strategischen Leitfaden fett formatierten Namen dienen als Variablen. Die entsprechenden Werte für diese Variablen werden innerhalb der Variablendatei beibehalten.

Schritt 10. Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, führen Sie den Befehl ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"aus, um die ansible Aufgabe abzuspielen.

In diesem Beispiel lautet der Befehl ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

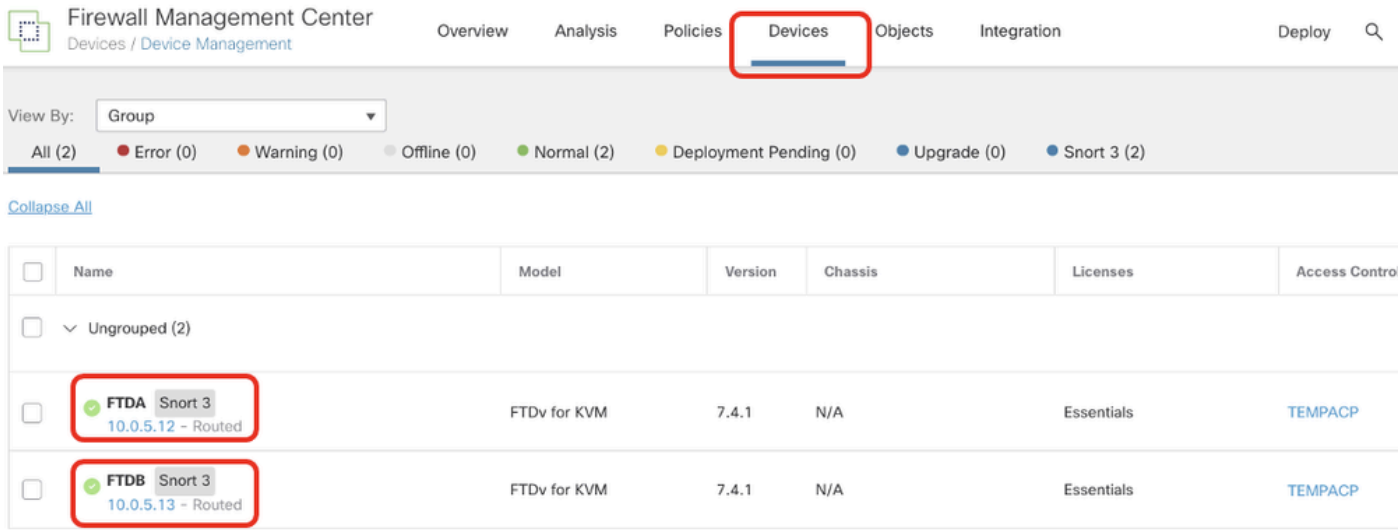
<#root>

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

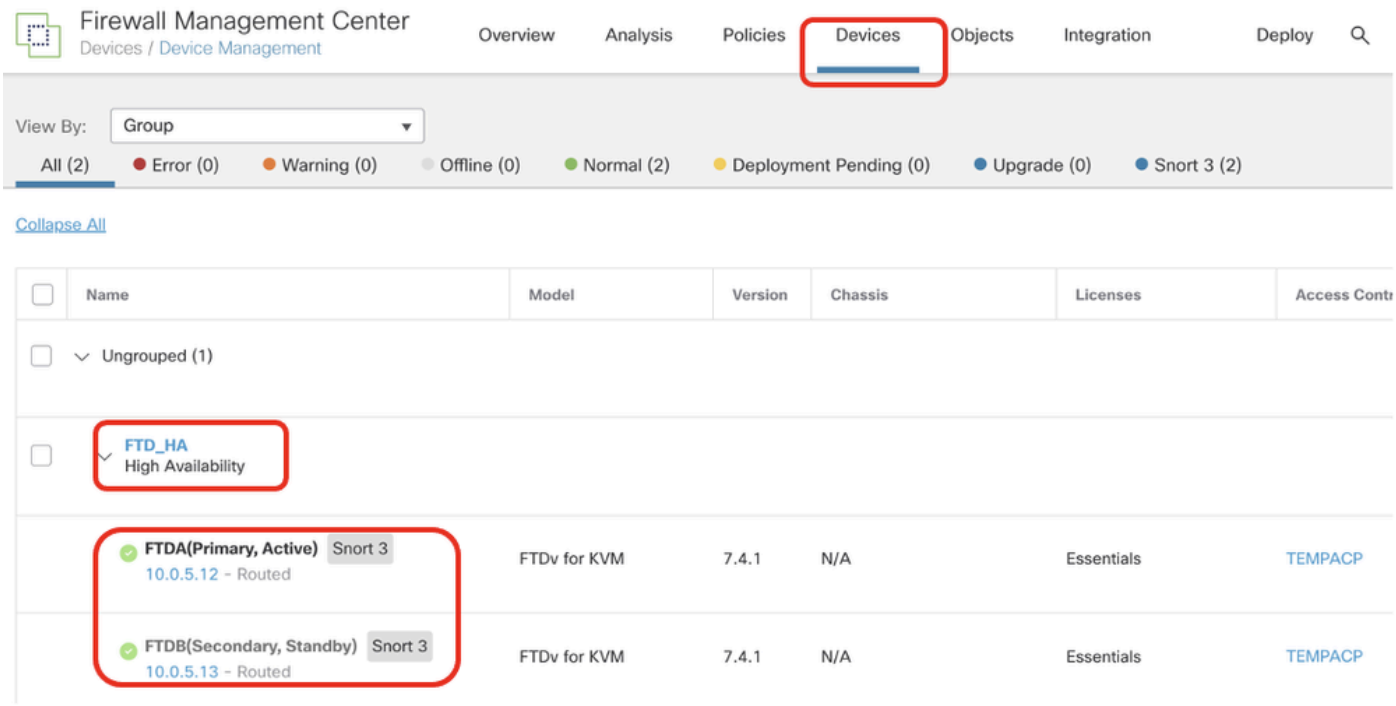
Überprüfung

Melden Sie sich vor dem Ausführen der ansible Aufgabe in der FMC-GUI an. Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung),** zwei FTDs wurden erfolgreich auf dem FMC registriert und haben die Zugriffskontrollrichtlinie konfiguriert.



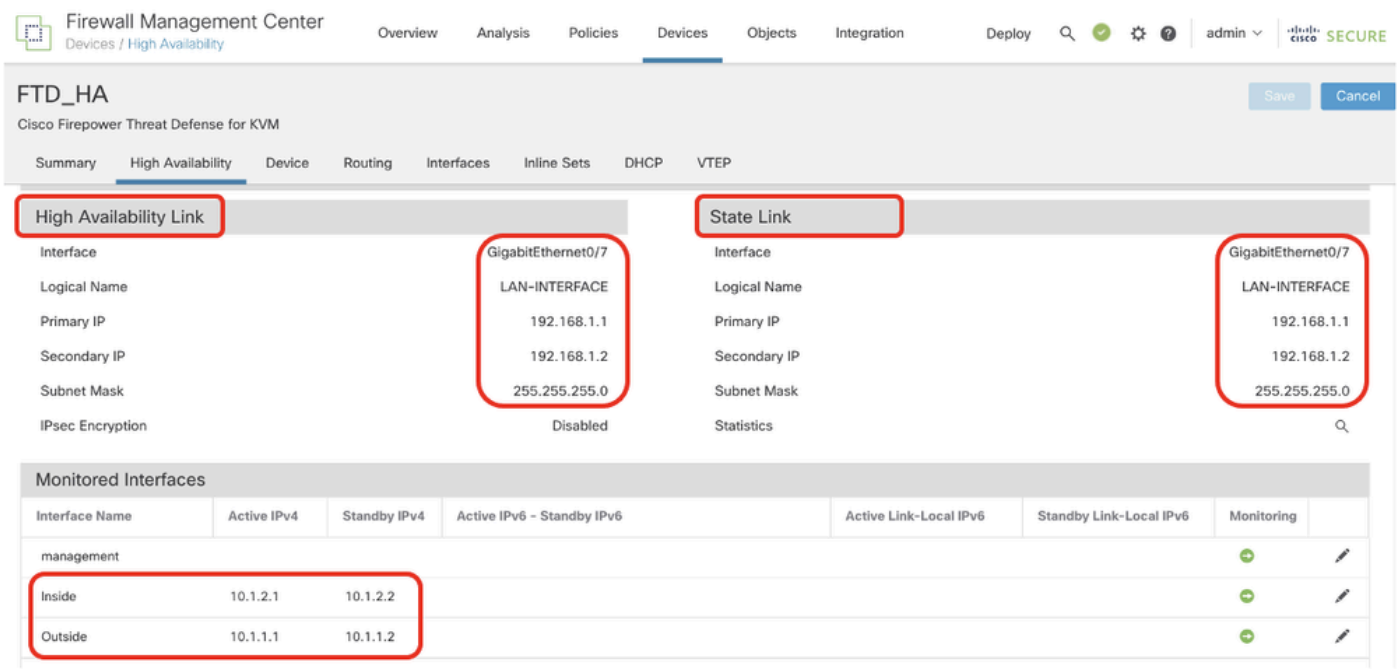
Vor dem Ausführen einer möglichen Aufgabe

Melden Sie sich nach dem Ausführen der Task "Ansible" in der FMC-GUI an. Navigieren Sie zu **Devices > Device Management (Geräte > Geräteverwaltung).** FTD HA wurde erfolgreich erstellt.



Nach erfolgreicher Ausführung der ansible Aufgabe

Klicken Sie auf **Edit** of FTD HA (FTD-HA bearbeiten), die Failover-IP-Adresse und die Standby-IP-Adresse der Schnittstelle wurden erfolgreich konfiguriert.



FTD - Details zur Hochverfügbarkeit

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Um mehr Logs von ansible playbook zu sehen, können Sie ansible playbook mit -vvv ausführen.

<#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

Zugehörige Informationen

Cisco DevNet FMC-fähig

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.