Configurare FMC con Ansible per creare disponibilità elevata FTD

Sommario

Introduzione

In questo documento viene descritto come automatizzare Firepower Management Center (FMC) per creare Firepower Threat Defense (FTD) High Availability con Ansible.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Ansioso
- Server Ubuntu
- Virtual Cisco Firepower Management Center (FMC)
- Virtual Cisco Firepower Threat Defense (FTD)

Nel contesto di questa situazione di laboratorio, Ansible è schierato su Ubuntu.

È essenziale assicurarsi che Ansible sia installato correttamente su qualsiasi piattaforma supportata da Ansible per l'esecuzione dei comandi Ansible a cui si fa riferimento in questo articolo.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

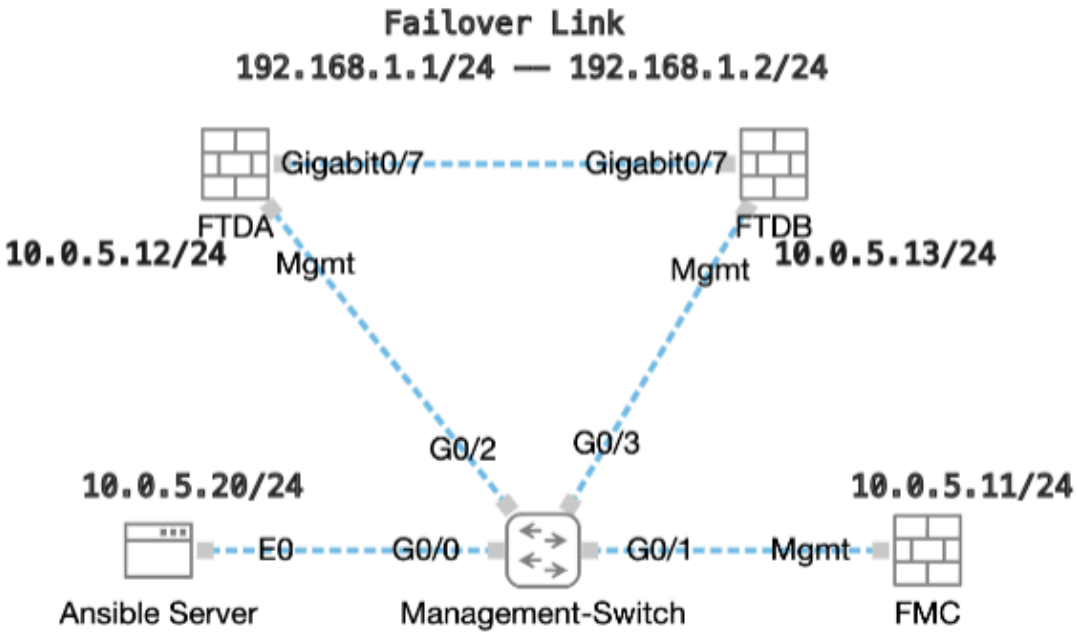
Premesse

Ansible è uno strumento estremamente versatile che dimostra una notevole efficacia nella gestione dei dispositivi di rete. Numerose metodologie possono essere impiegate per eseguire operazioni automatizzate con Ansible. Il metodo utilizzato in questo articolo serve da riferimento ai fini della prova.

In questo esempio, la disponibilità elevata FTD e l'indirizzo IP di standby dell'FTD vengono creati dopo l'esecuzione corretta dell'esempio di playbook.

Configurazione

Esempio di rete



Topologia

Configurazioni

Poiché Cisco non supporta gli script di esempio o quelli scritti dal cliente, sono disponibili alcuni esempi che è possibile verificare in base alle esigenze.

È essenziale garantire che la verifica preliminare sia stata debitamente completata.

- Il server ansibile dispone di connettività Internet.
- Ansible Server è in grado di comunicare con la porta GUI FMC (la porta predefinita per l'interfaccia GUI FMC è 443).
- Due dispositivi FTD sono stati registrati nel FMC.
- L'FTD primario è configurato con l'indirizzo IP dell'interfaccia.

Passaggio 1. Connettersi alla CLI del server Ansible tramite SSH o console.

Passaggio 2. Eseguire il comando ansible-galaxy collection install cisco.fmcansible per installare la raccolta Ansible di FMC nel server Ansible.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Passaggio 3. Eseguire il comando mkdir /home/cisco/fmc_ansible per creare una nuova cartella in cui archiviare i file correlati. In questo esempio, la home directory è /home/cisco/, il nome della nuova cartella è fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Passaggio 4. Passare alla cartella /home/cisco/fmc_ansible, Crea file di inventario. In questo esempio, il nome del file di inventario è inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini
```

Potete duplicare questo contenuto e incollarlo per utilizzarlo, modificando le sezioni **in grassetto** con parametri accurati.

<#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

Passaggio 5. Passare alla cartella /home/cisco/fmc_ansible, creare un file variabile per la creazione di FTD HA. In questo esempio, il nome del file della variabile è 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

Potete duplicare questo contenuto e incollarlo per utilizzarlo, modificando le sezioni **in grassetto** con parametri accurati.

<#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

'

Passaggio 6. Passare alla cartella /home/cisco/fmc_ansible, creare il file della playbook per la creazione di FTD HA. In questo esempio, il nome del file della playbook è 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

Potete duplicare questo contenuto e incollarlo per utilizzarlo, modificando le sezioni **in grassetto** con parametri accurati.

<#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

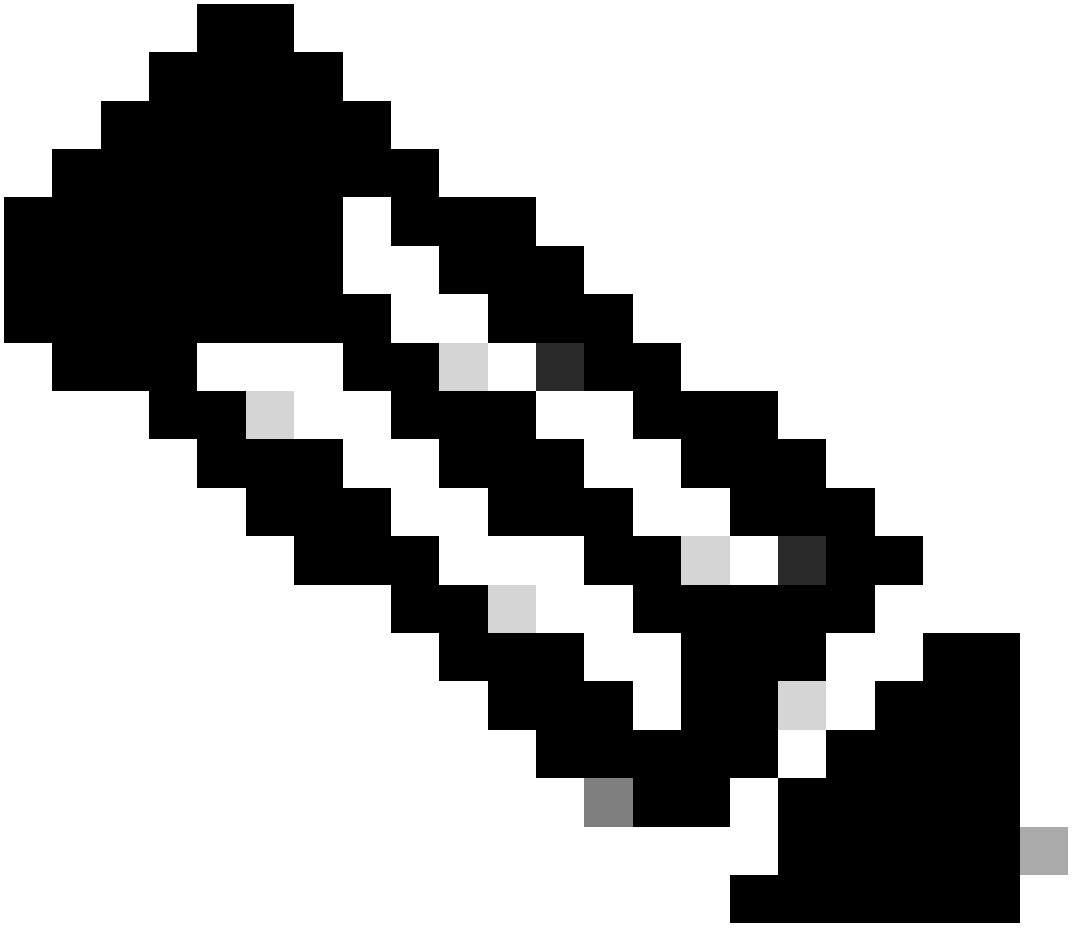
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



Nota: i nomi in grassetto in questo esempio di playbook fungono da variabili. I valori corrispondenti per queste variabili vengono mantenuti nel file delle variabili.

Passaggio 7. Passare alla cartella **/home/cisco/fmc_ansible**, eseguire il comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"per eseguire l'attività andibile.

Nell'esempio, il comando è 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] **

Passaggio 8. Passare alla cartella /home/cisco/fmc_ansible, creare un file di variabili per l'aggiornamento dell'indirizzo IP di standby FTD HA.
In questo esempio, il nome del file della variabile è 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

È possibile duplicare il contenuto e incollarlo per utilizzarlo, modificando le sezioni in **grassetto** con i parametri accurati.

<#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

'

Passaggio 9. Passare alla cartella **/home/cisco/fmc_ansible**, creare il file della playbook per aggiornare l'indirizzo IP di standby FTD HA. In questo esempio, il nome del file della playbook è 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

Potete duplicare questo contenuto e incollarlo per utilizzarlo, modificando le sezioni **in grassetto** con parametri accurati.

<#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

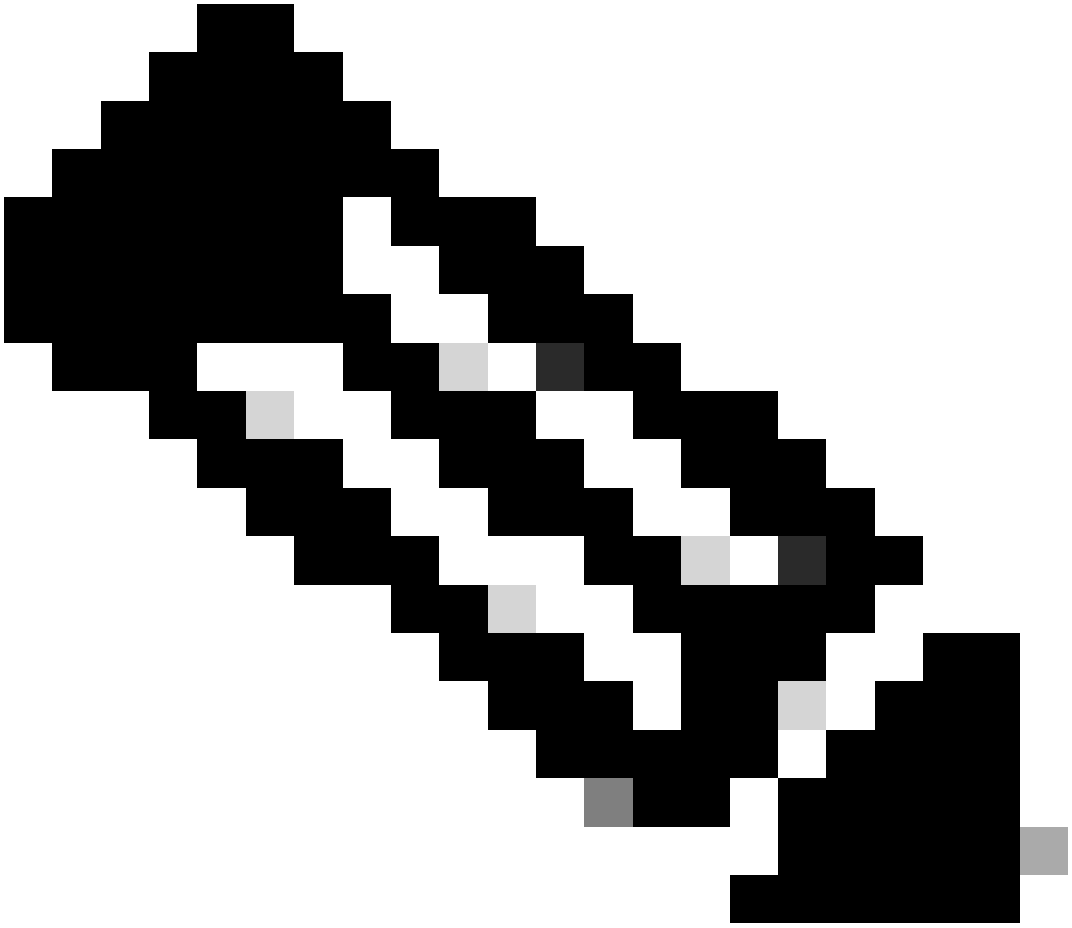
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



Nota: i nomi in grassetto in questo esempio di playbook fungono da variabili. I valori corrispondenti per queste variabili vengono mantenuti nel file delle variabili.

Passaggio 10. Passare alla cartella **/home/cisco/fmc_ansible**, eseguire il comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"per eseguire l'attività andibile.

Nell'esempio, il comando è ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

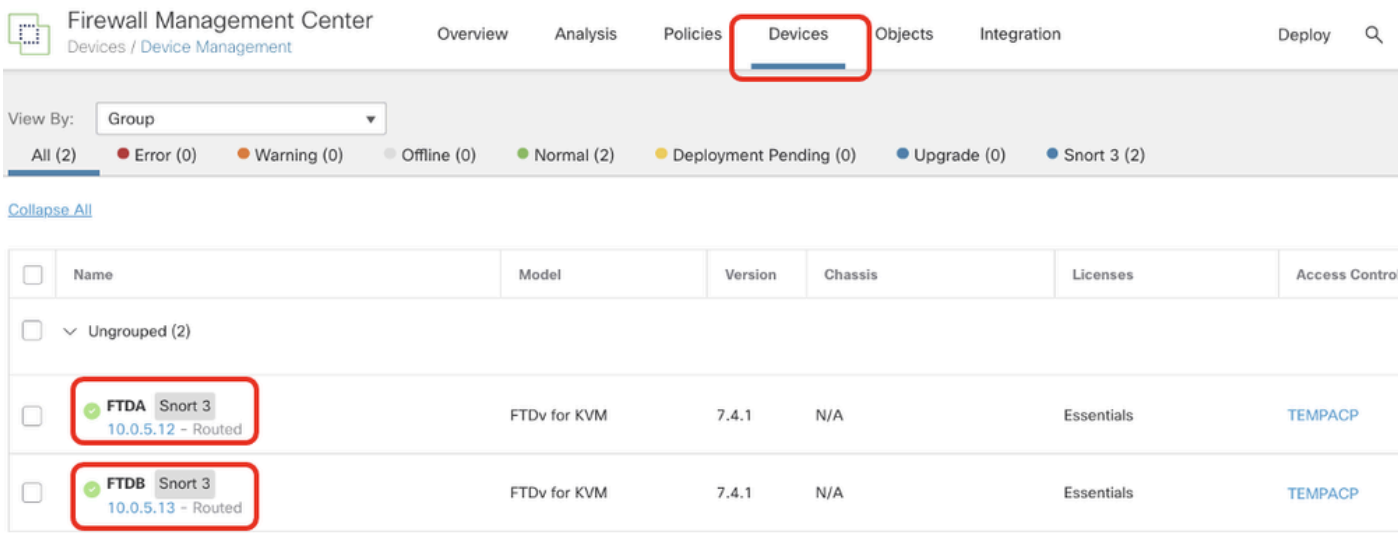
<#root>

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

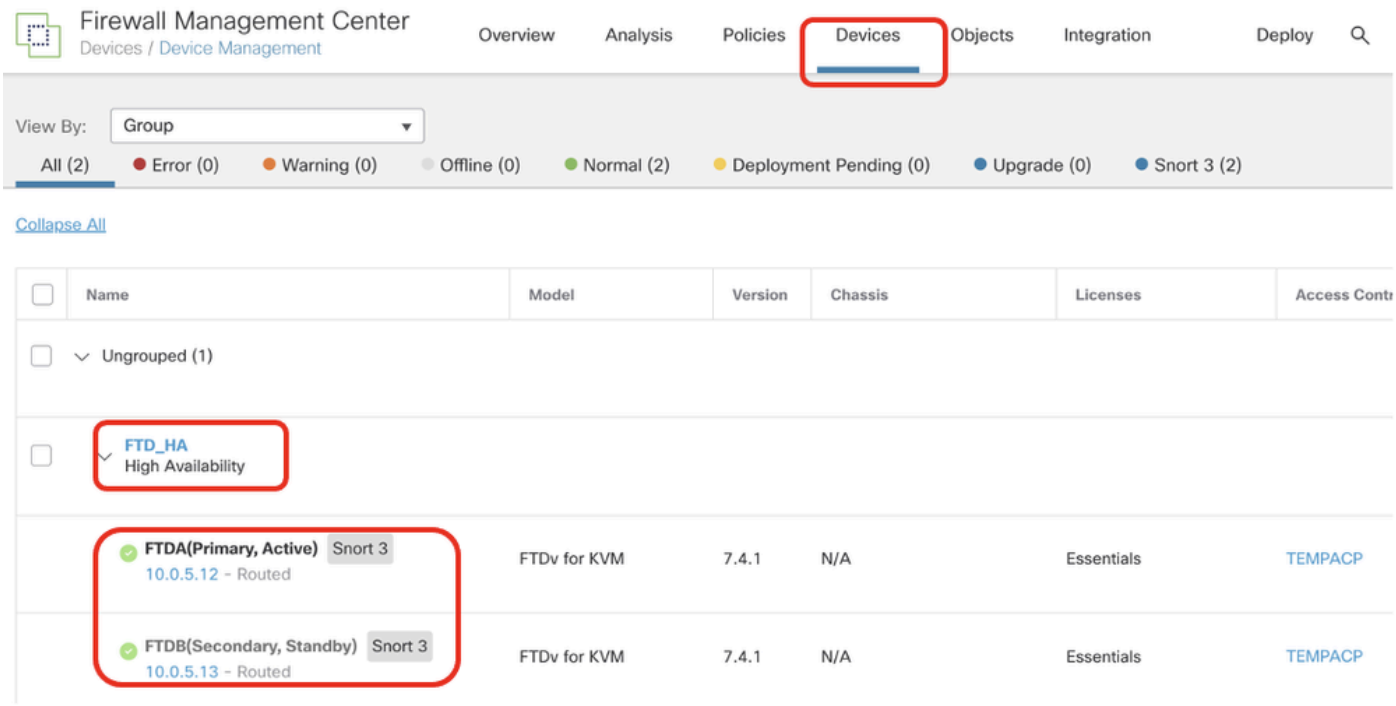
Verifica

Prima di eseguire l'attività ansibile, accedere all'interfaccia utente di FMC. Passare a **Dispositivi > Gestione dispositivi,** due FTD registrati correttamente sul FMC con criteri di controllo di accesso configurati.



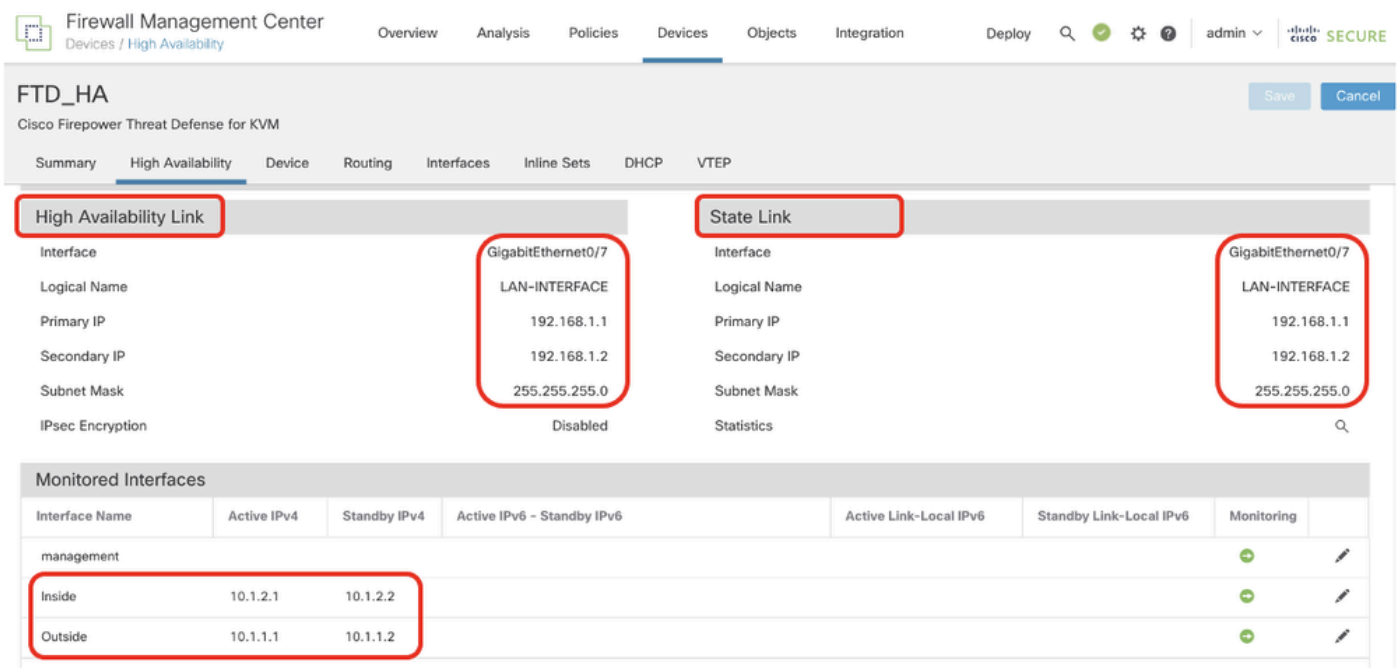
Prima di eseguire un'attività flessibile

Dopo aver eseguito l'attività ansibile, accedere all'interfaccia utente di FMC. Passare a **Dispositivi > Gestione dispositivi.** FTD HA è stato creato correttamente.



Dopo l'esecuzione di Ansible Task

Fare clic su **Edit** of FTD HA (Modifica di FTD HA) per configurare correttamente l'indirizzo IP di failover e l'indirizzo IP di standby dell'interfaccia.



Dettagli alta disponibilità FTD

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Per visualizzare più registri di un playbook andibile, è possibile eseguire un playbook ansibile con -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

Informazioni correlate

Cisco Devent FMC Ansible

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).