使用Ansible設定FMC以建立FTD高可用性

目錄

簡介

本文檔介紹自動化Firepower管理中心(FMC)的步驟，以使用Ansible建立Firepower威脅防禦(FTD)高可用性。

必要條件

需求

思科建議您瞭解以下主題：

- 阿尼塞
- Ubuntu伺服器
- Cisco Firepower管理中心(FMC)虛擬
- Cisco Firepower威脅防禦(FTD)虛擬

在這種實驗室情況下，Ansible被部署在Ubuntu。

必須確保Ansible成功安裝在Ansible支援的任何平台上，以便運行本文中引用的Ansible命令。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Ubuntu伺服器22.04
- 阿尼塞2.10.8
- Python 3.10
- Cisco Firepower威脅防禦虛擬7.4.1

- Cisco Firepower管理中心虛擬7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

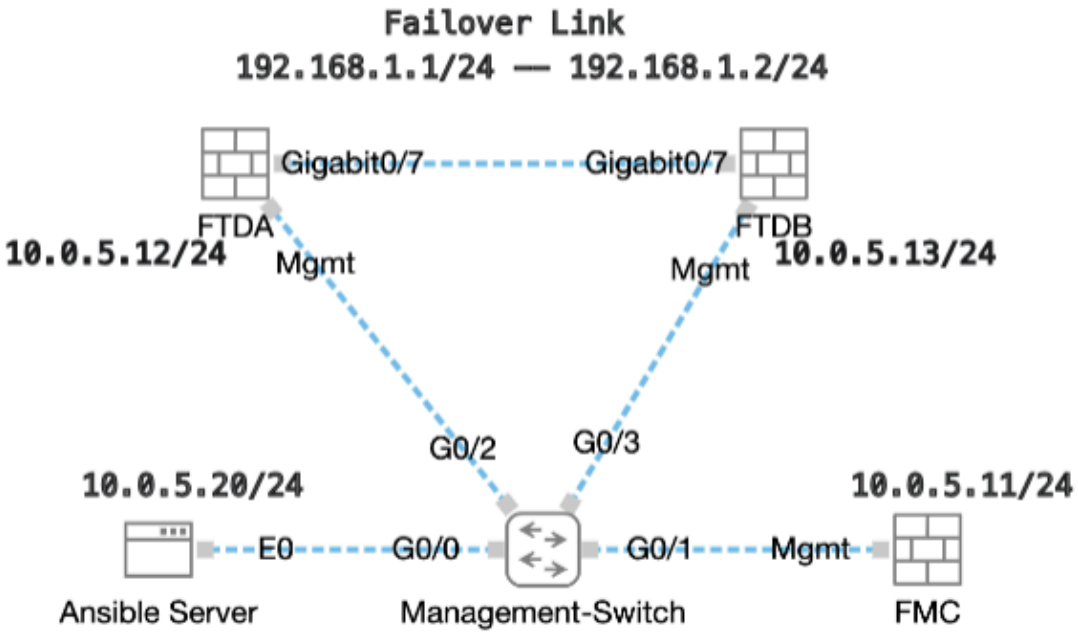
背景資訊

Ansible是一個功能非常豐富的工具，在管理網路裝置方面展現了極大的效率。使用Ansible可以採用多種方法來運行自動化任務。本文所採用的方法為試驗提供了參考。

在本範例中，FTD的高可用性及備用IP位址是在成功執行手冊范例後建立的。

設定

網路圖表



拓撲

組態

由於Cisco不支援示例指令碼或客戶編寫的指令碼，我們提供了一些可根據您的需求進行測試的示例。

必須確保適當完成初步核查。

- Ansible伺服器具有internet連線。
- Ansible伺服器能夠與FMC GUI埠成功通訊（FMC GUI的預設埠是443）。
- 兩台FTD裝置已順利註冊到FMC。
- 主要FTD設定為介面IP位址。

步驟 1. 透過SSH或控制檯連線到Ansible伺服器的CLI。

步驟 2.運行命令ansible-galaxy collection install cisco.fmcansible以在Ansible伺服器上安裝FMC的Ansible集合。

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

步驟 3.運行命令mkdir /home/cisco/fmc_ansible以建立一個新資料夾來儲存相關檔案。在本示例中，主目錄是/home/cisco/ ，新資料夾名稱為fmc_ansible。

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

步驟 4. 導航到資料夾/home/cisco/fmc_ansible，建立資產檔案。在本示例中，資產檔名為inventory.ini。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

您可以複製此內容並貼上它以供使用，並使用準確引數更改**粗體**部分。

<#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

步驟 5. 導航到資料夾/home/cisco/fmc_ansible，建立用於建立FTD HA的變數檔案。在此範例中，變數檔案名稱為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

您可以複製此內容並貼上它以供使用，並使用準確引數更改**粗體**部分。

<#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

'

步驟 6. 導航到資料夾/home/cisco/fmc_ansible，建立用於建立FTD HA的手冊檔案。在本示例中，播放手冊檔名為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

您可以複製此內容並貼上它以供使用，並使用準確引數更改**粗體**部分。

<#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'

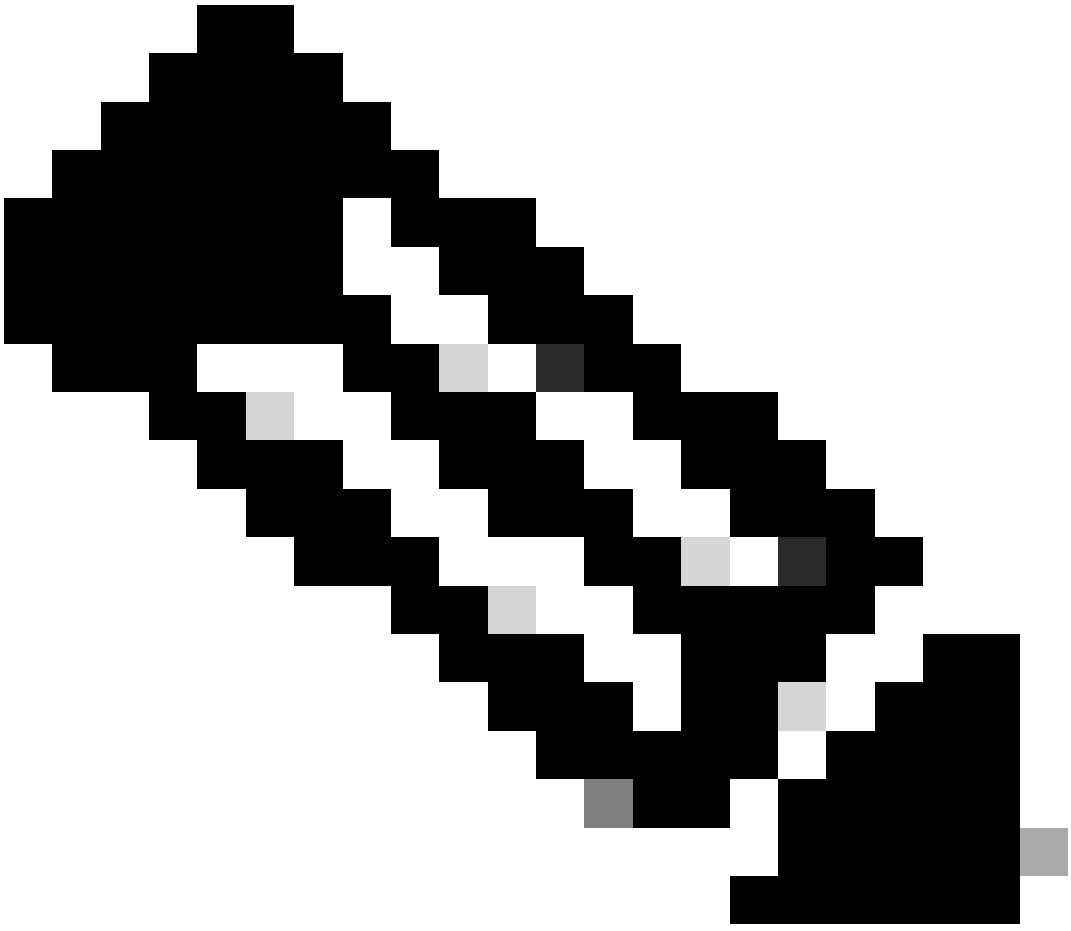
ftd_ha.standby_ip

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

ftd_ha.active_ip

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

---



注意：本示例攻略中的粗體名稱用作變數。這些變數的對應值會保留在變數檔案中。

步驟 7. 導航到資料夾**/home/cisco/fmc_ansible**，運行命令ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"以播放ansible任務。

在本示例中，該命令是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:~/f

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

PLAY [FMC Create FTD HA] **

步驟 8. 導航到資料夾/home/cisco/fmc_ansible，建立用於更新FTD HA備用IP地址的變數檔案。在本示例中，變數檔名是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

可以複製此內容並貼上以供使用，並使用準確引數更改**粗體**部分。

<#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

'

步驟 9. 導航到資料夾**/home/cisco/fmc_ansible**，建立用於更新FTD HA備用IP地址的手冊檔案。在本示例中，手冊檔名為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

您可以複製此內容並貼上它以供使用，並使用準確引數更改**粗體**部分。

<#root>

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

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

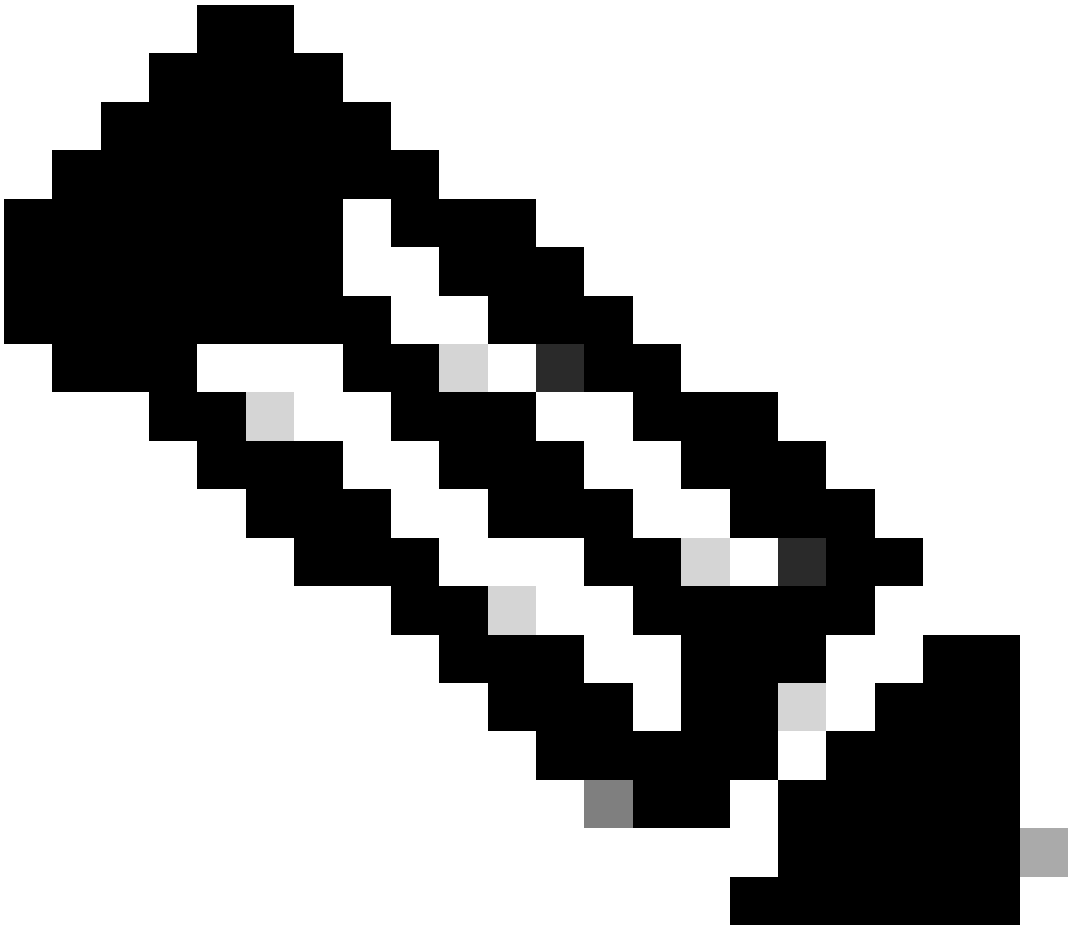
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{
```



注意：本示例攻略中的粗體名稱用作變數。這些變數的對應值會保留在變數檔案中。

步驟 10. 導航到資料夾**/home/cisco/fmc_ansible**，運行命令ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"以播放ansible任務。

在本示例中，該命令是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

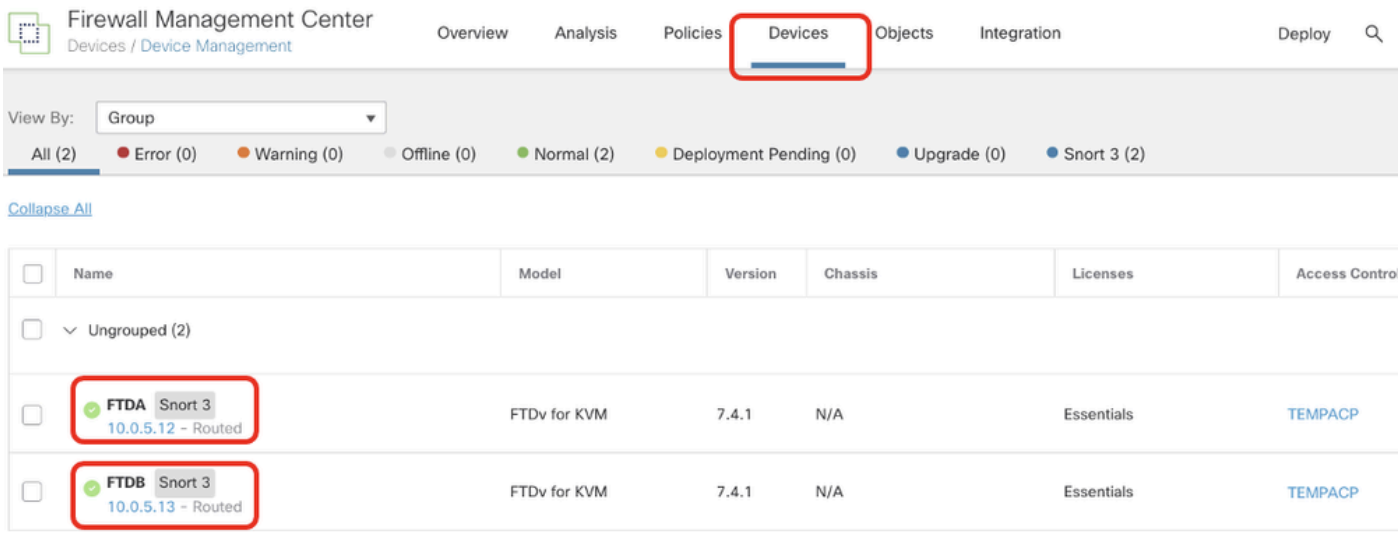
cisco@inserthostname-here:~/fmc_ansible$

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] **********

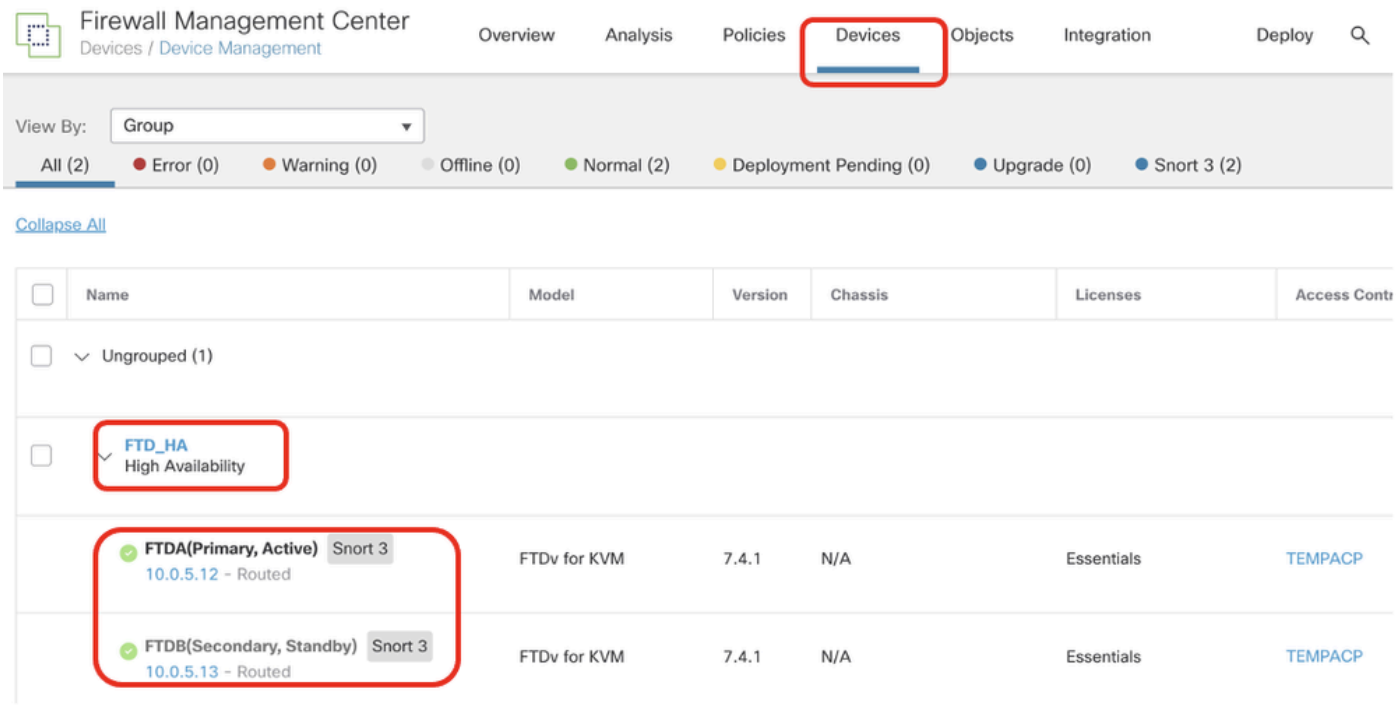
驗證

在運行ansible任務之前，請登入FMC GUI。導覽至**Devices** > **Device Management**，兩個FTD已在FMC上成功註冊，且已設定存取控制原則。



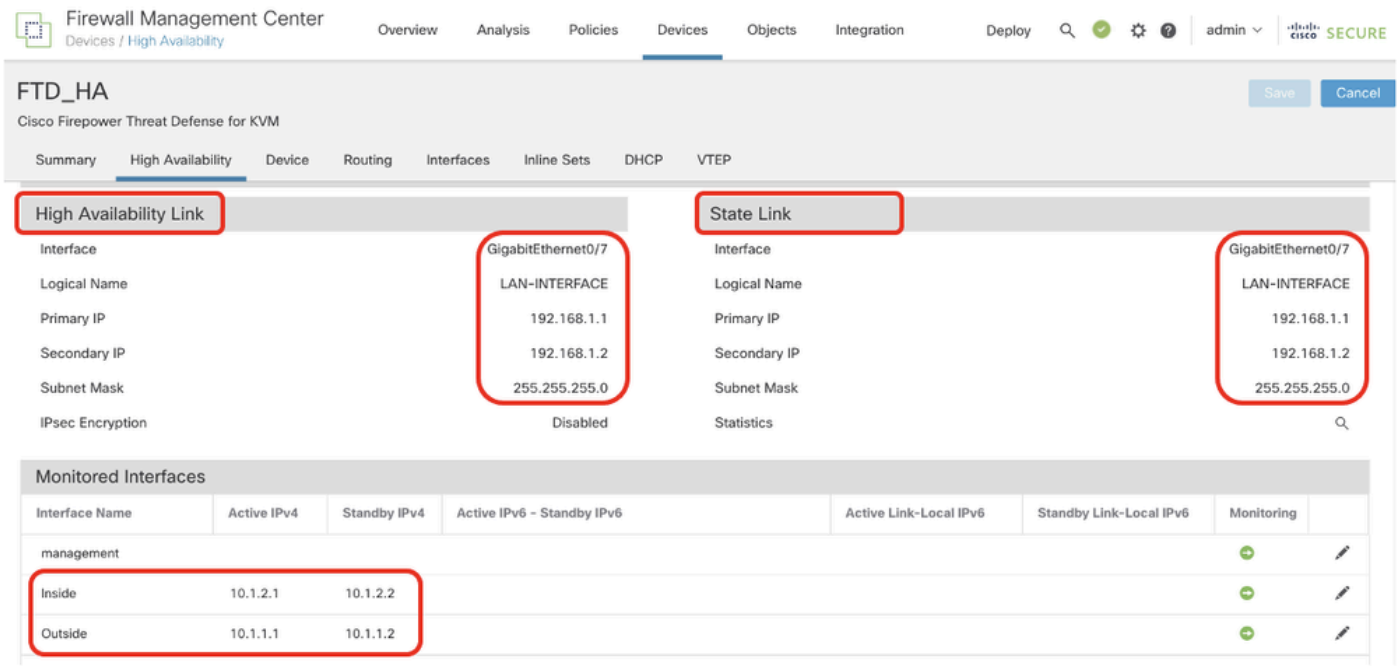
執行*Ansible*工作之前

運行ansible任務後，登入FMC GUI。導覽至**Devices** > **Device Management**，FTD HA已成功建立。



成功執行*Ansible*工作之後

按一下**Edit** of FTD HA，故障切換IP地址和介面備用IP地址已成功配置。



*FTD*高可用性明細

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要檢視更多有關ansible實戰手冊的記錄，您可以使用-vvv執行ansible實戰手冊。

<#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

相關資訊

Cisco Devnet FMC Ansible

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。