使用Ansible配置FMC以创建FTD高可用性

目录

简介

本文档介绍自动运行Firepower管理中心(FMC)以使用Ansible创建Firepower威胁防御(FTD)高可用性的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Ansible
- Ubuntu服务器
- Cisco Firepower管理中心(FMC)虚拟
- Cisco Firepower威胁防御(FTD)虚拟

在这种实验室情况下，Ansible被部署在Ubuntu上。

必须确保Ansible成功安装在Ansible支持的任何平台上，才能运行本文中引用的Ansible命令。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Ubuntu服务器22.04
- Ansible 2.10.8
- Python 3.10
- 思科Firepower威胁防御虚拟7.4.1

- 思科Firepower管理中心虚拟7.4.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

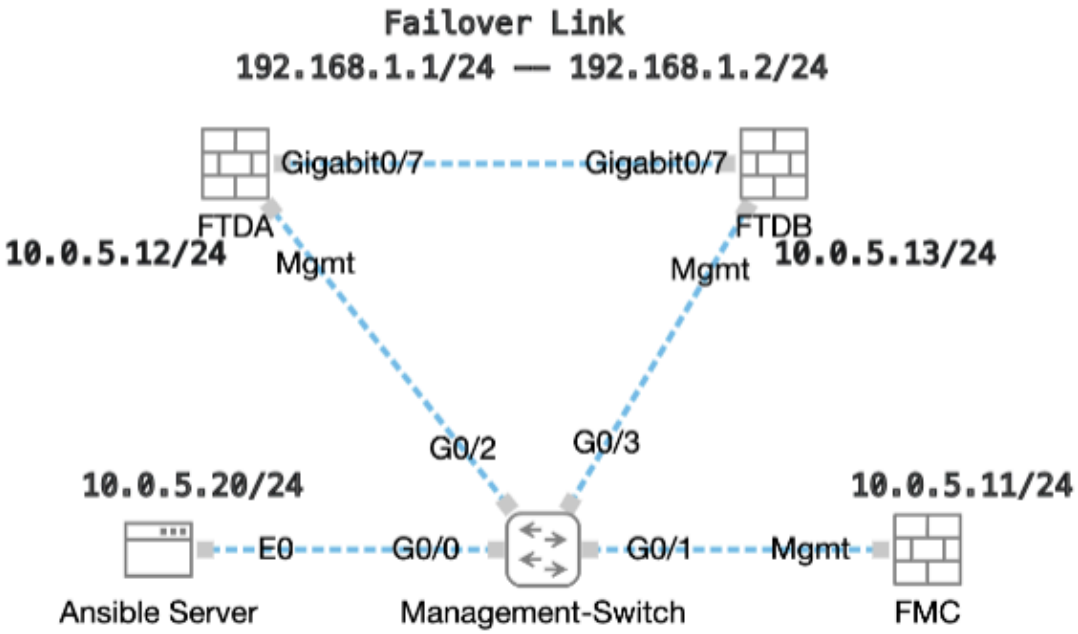
背景信息

Ansible是一个功能非常全面的工具，在管理网络设备时显示了显著的功效。通过Ansible，可以采用多种方法运行自动化任务。本文所采用的方法为试验提供了参考。

在本示例中，在成功运行攻略示例后创建其FTD高可用性和备用IP地址。

配置

网络图



拓扑

配置

由于思科不支持示例脚本或客户编写的脚本，我们提供了一些您可以根据需要进行测试的示例。

必须确保适当完成初步核查。

- Ansible服务器具有Internet连接。
- Ansible服务器能够与FMC GUI端口成功通信（FMC GUI的默认端口为443）。
- 两个FTD设备已成功注册到FMC。
- 使用接口IP地址配置主FTD。

步骤1: 通过SSH或控制台连接到Ansible服务器的CLI。

第二步：运行命令ansible-galaxy collection install cisco.fmcansible以在Ansible服务器上安装FMC的Ansible集合。

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

第三步：运行命令mkdir /home/cisco/fmc_ansible以创建一个新文件夹来存储相关文件。在本示例中，主目录为/home/cisco/，新文件夹名称为fmc_ansible。

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

第四步： 导航到文件夹/home/cisco/fmc_ansible，创建资产文件。在本示例中，资产文件名为inventory.ini。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

您可以复制此内容并粘贴以备不时之需，并使用准确参数更改**粗体**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

第五步： 导航到文件夹/home/cisco/fmc_ansible，创建用于创建FTD HA的变量文件。在本示例中，变量文件名为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

您可以复制此内容并粘贴以备不时之需，并使用准确参数更改**粗体**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

'

第六步： 导航到文件夹/home/cisco/fmc_ansible，创建用于创建FTD HA的攻略文件。在本示例中，手册文件名为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

您可以复制此内容并粘贴以备不时之需，并使用准确参数更改**粗体**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'

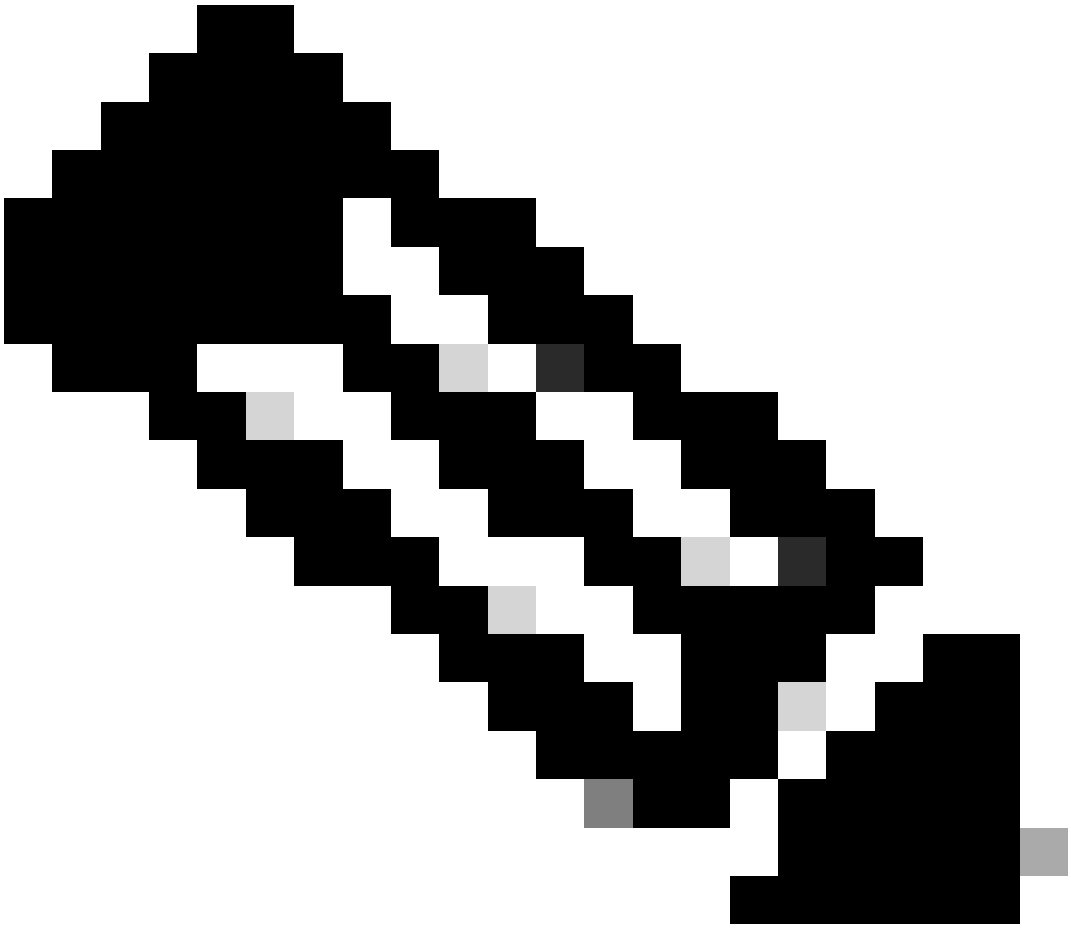
ftd_ha.standby_ip

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

ftd_ha.active_ip

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

---



注意：本示例手册中粗体显示的名称用作变量。这些变量的对应值保留在变量文件中。

步骤 7. 导航到文件夹/**home/cisco/fmc_ansible**，run commandansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"以播放ansible任务。

在本示例中，该命令是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] **

步骤 8 导航到文件夹/home/cisco/fmc_ansible，创建用于更新FTD HA备用IP地址的变量文件。在本示例中，变量文件名为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

您可以复制此内容并粘贴以供使用，并使用准确参数更改**粗体**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

'

步骤 9 导航到文件夹**/home/cisco/fmc_ansible**，创建用于更新FTD HA备用IP地址的攻略文件。在本示例中，手册文件名为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

您可以复制此内容并粘贴以备不时之需，并使用准确参数更改**粗体**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

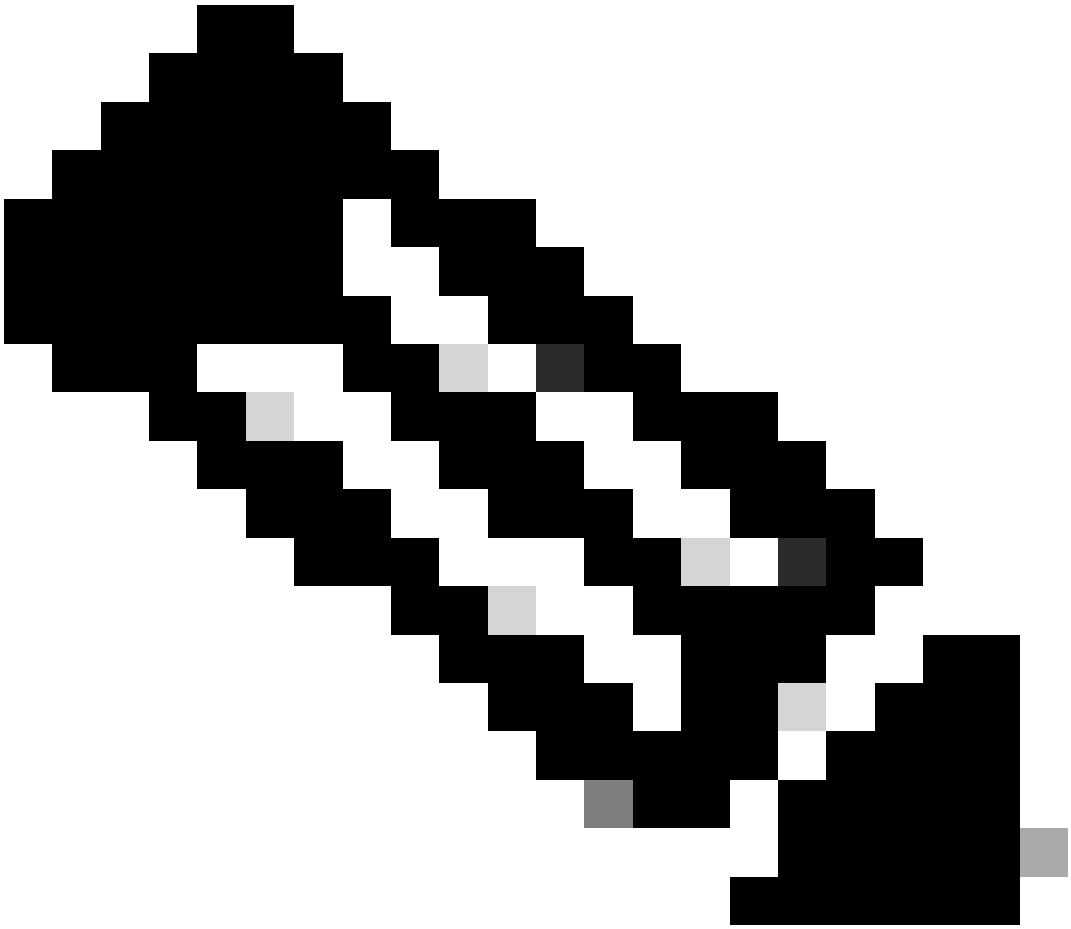
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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：本示例手册中粗体显示的名称用作变量。这些变量的对应值保留在变量文件中。

步骤 10 导航到文件夹**/home/cisco/fmc_ansible**，run commandansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"以播放ansible任务。

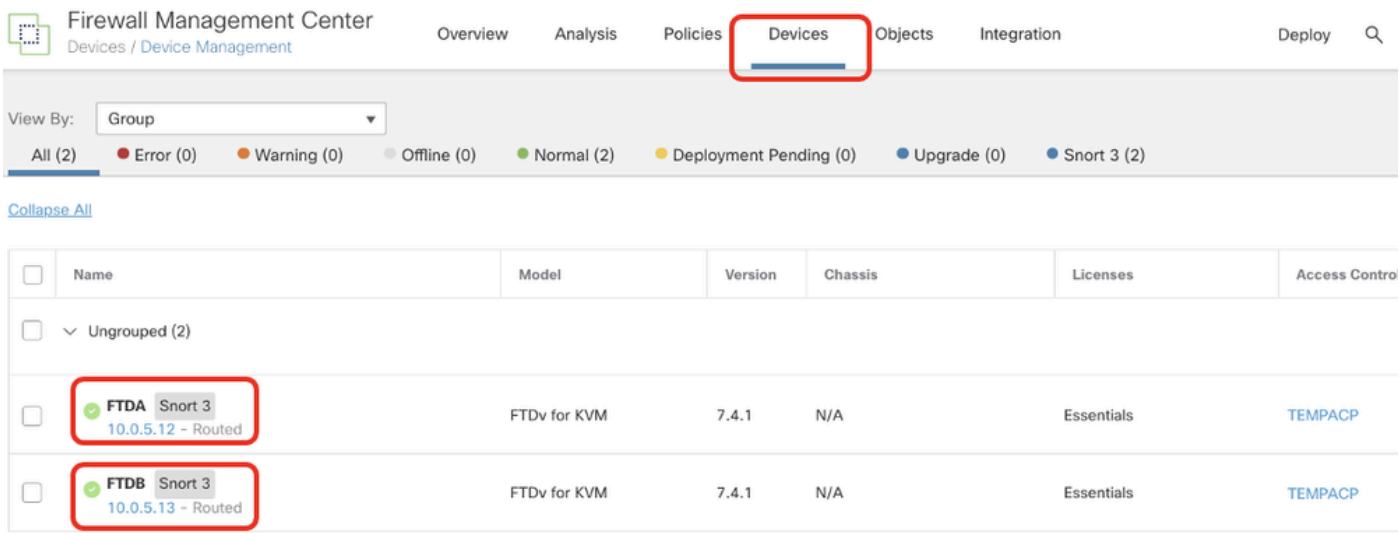
在本示例中，该命令是ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml"。

<#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] **********************************************************
```

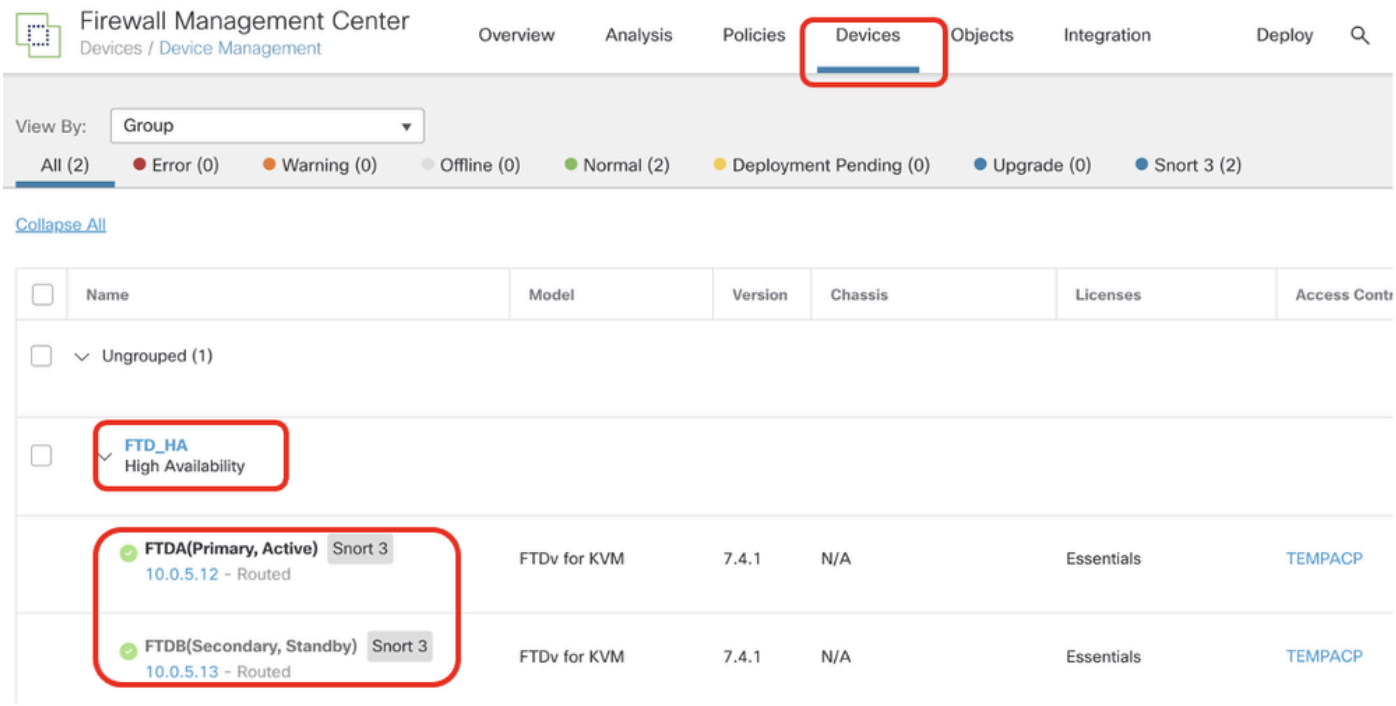
验证

在运行ansible任务之前，请登录FMC GUI。导航到设备>设备管理，两个FTD在FMC上使用配置的访问控制策略成功注册。



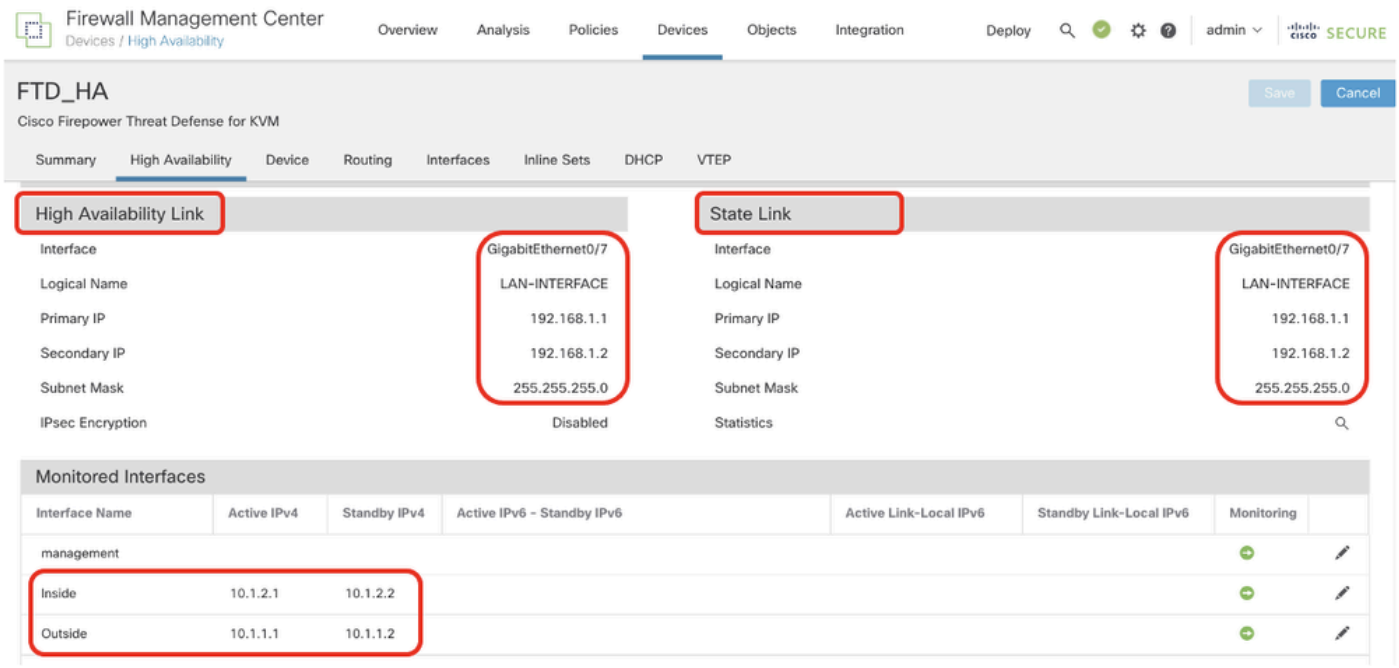
在运行*Ansible*任务之前

在运行ansible任务后，登录FMC GUI。导航到设备>设备管理，已成功创建FTD HA。



成功运行Ansible任务后

单击FTD HA的Edit，成功配置了故障切换IP地址和接口备用IP地址。



FTD高可用性详细信息

故障排除

本部分提供的信息可用于对配置进行故障排除。

要查看ansible攻略的更多日志，您可以使用-vvv运行ansible攻略。

<#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

相关信息

Cisco Devnet FMC Ansible

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。