Configurar o FMC com Ansible para criar alta disponibilidade do FTD

Contents

Introdução

Este documento descreve as etapas para automatizar o Firepower Management Center (FMC) para criar o Firepower Threat Defense (FTD) High Availability com Ansible.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ansible
- Servidor Ubuntu
- Cisco Firepower Management Center (FMC) Virtual
- Cisco Firepower Threat Defense (FTD) Virtual

No contexto desta situação de laboratório, Ansible é implantado no Ubuntu.

É essencial garantir que o Ansible seja instalado com êxito em qualquer plataforma suportada pelo Ansible para executar os comandos Ansible referenciados neste artigo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor Ubuntu 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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

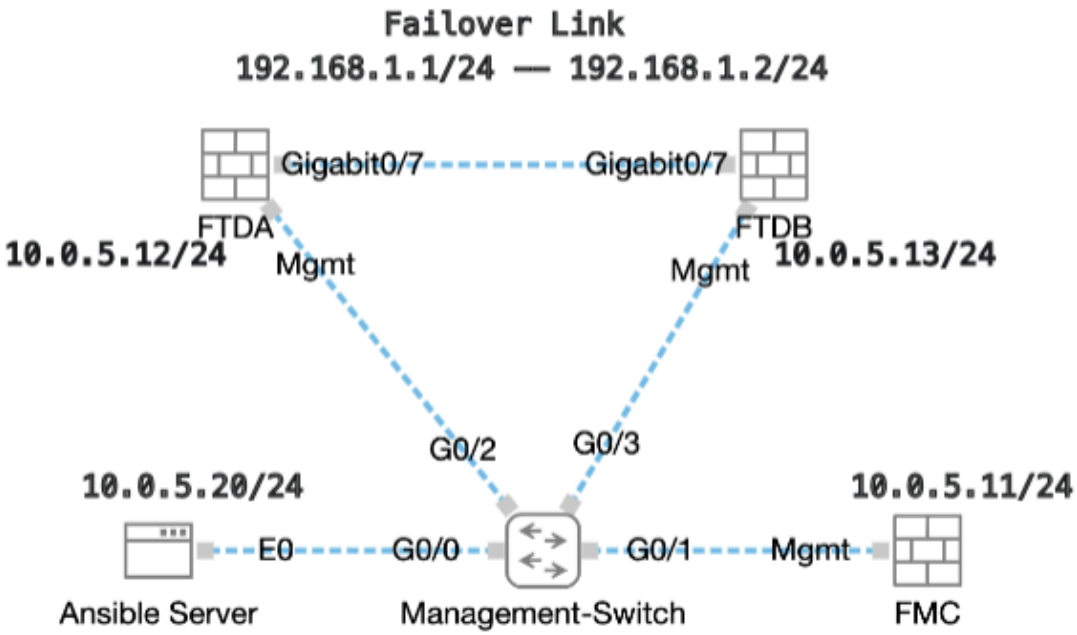
Informações de Apoio

O Ansible é uma ferramenta altamente versátil que demonstra uma eficiência significativa no gerenciamento de dispositivos de rede. Várias metodologias podem ser empregadas para executar tarefas automatizadas com a Ansible. O método utilizado neste artigo serve de referência para fins de teste.

Neste exemplo, a Alta disponibilidade de FTD e o endereço IP de espera dele são criados após a execução bem-sucedida do exemplo de manual de atividades.

Configurar

Diagrama de Rede



Topologia

Configurações

Como a Cisco não oferece suporte a scripts de exemplo ou scripts escritos por clientes, temos alguns exemplos que você pode testar de acordo com suas necessidades.

É essencial assegurar que a verificação preliminar foi devidamente concluída.

- Um servidor possível possui conectividade com a Internet.
- Um servidor Ansible pode se comunicar com êxito com a porta GUI do FMC (a porta padrão da GUI do FMC é 443).
- Dois dispositivos de FTD são registrados com êxito no FMC.
- O FTD principal é configurado com o endereço IP da interface.

Etapa 1. Conecte-se ao CLI do servidor Ansible via SSH ou console.

Etapa 2. Execute o comandoansible-galaxy collection install cisco.fmcansible para instalar a coleção Ansible do FMC em seu servidor Ansible.

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

Etapa 3. Execute o comandomkdir /home/cisco/fmc_ansible para criar uma nova pasta para armazenar os arquivos relacionados. Neste exemplo, o diretório inicial é /home/cisco/, o nome da nova pasta é fmc_ansible.

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

Etapa 4. Navegue até a pasta /home/cisco/fmc_ansible, crie o arquivo de inventário. Neste exemplo, o nome do arquivo de inventário é inventory.ini.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

Você pode duplicar esse conteúdo e colá-lo para utilização, alterando as seções em **negrito** com os parâmetros precisos.

<#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

Etapa 5. Navegue para a pasta /home/cisco/fmc_ansible, crie o arquivo de variável para criar FTD HA. Neste exemplo, o nome do arquivo de variável é 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

Você pode duplicar esse conteúdo e colá-lo para utilização, alterando as seções em **negrito** com os parâmetros precisos.

<#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

'

Etapa 6. Navegue para a pasta /home/cisco/fmc_ansible, crie o arquivo de manual para criar o HA do FTD. Neste exemplo, o nome do arquivo de playbook é 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

Você pode duplicar esse conteúdo e colá-lo para utilização, alterando as seções em **negrito** com os parâmetros precisos.

<#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

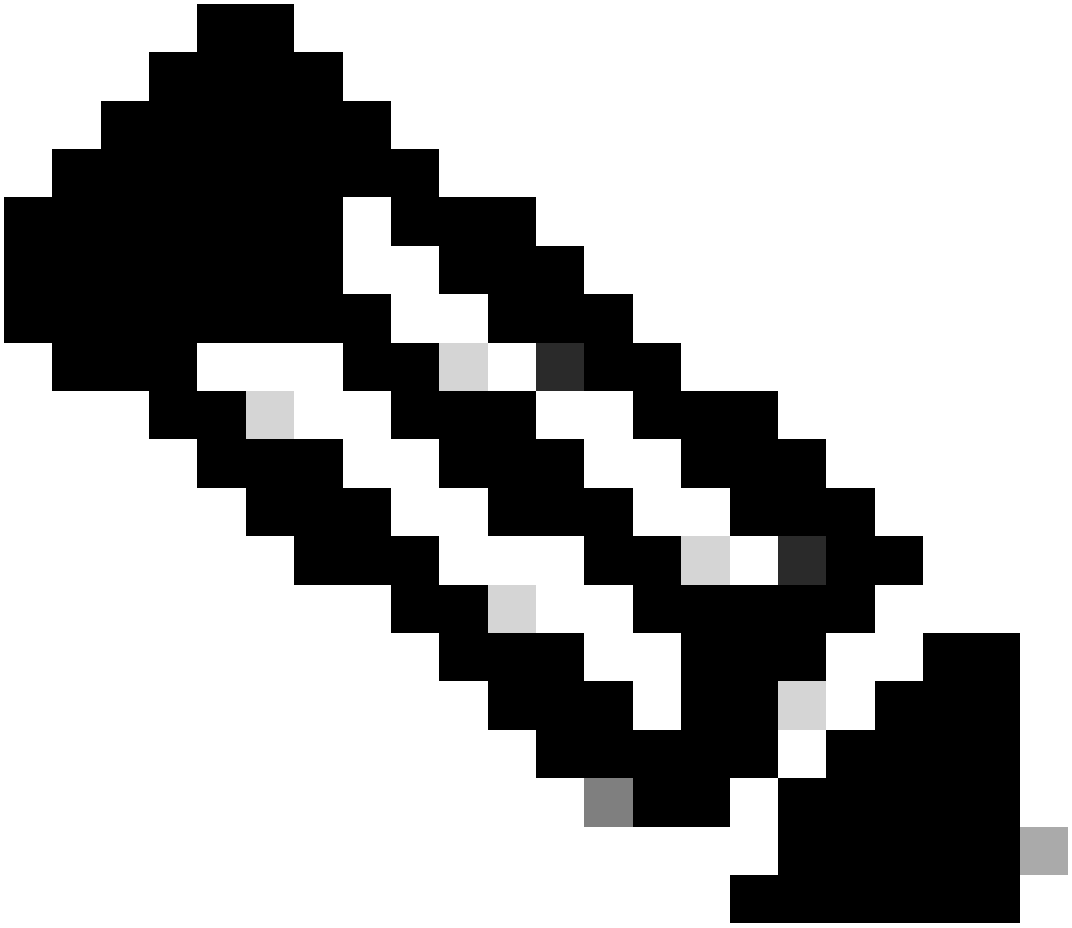
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



Observação: os nomes em negrito neste manual de atividades de exemplo servem como variáveis. Os valores correspondentes para essas variáveis são preservados no arquivo de variáveis.

Passo 7. Navegue para a pasta **/home/cisco/fmc_ansible**, execute o comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"para reproduzir a tarefa ansible.

Neste exemplo, o comando é 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] **

Etapa 8. Navegue para a pasta /home/cisco/fmc_ansible, crie um arquivo de variável para atualizar o endereço IP em espera HA do FTD. Neste exemplo, o nome do arquivo de variável é 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

Você pode duplicar esse conteúdo e colá-lo para utilização, alterando as seções **bold** com os parâmetros precisos.

<#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

'

Etapa 9. Navegue para a pasta **/home/cisco/fmc_ansible**, crie o arquivo de manual para atualizar o endereço IP de espera HA do FTD. Neste exemplo, o nome do arquivo de playbook é 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

Você pode duplicar esse conteúdo e colá-lo para utilização, alterando as seções em **negrito** com os parâmetros precisos.

<#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

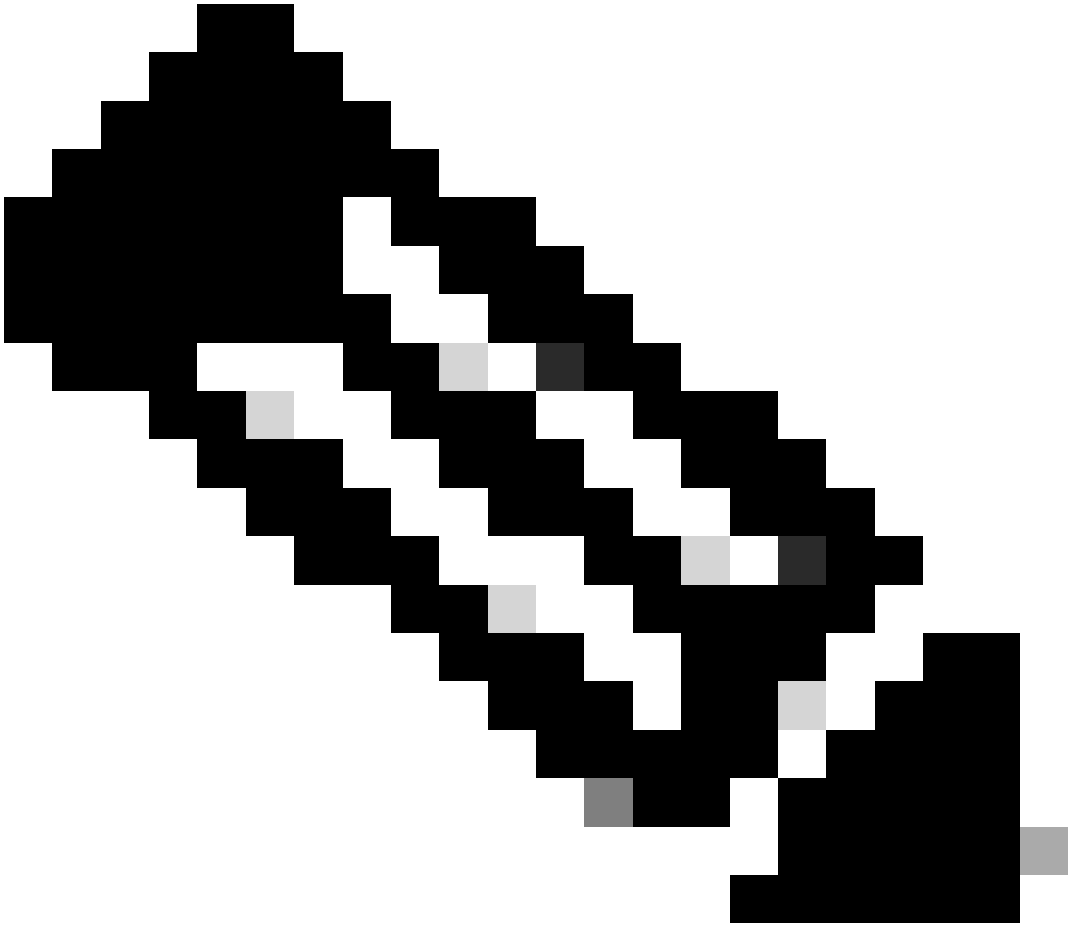
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



Observação: os nomes em negrito neste manual de atividades de exemplo servem como variáveis. Os valores correspondentes para essas variáveis são preservados no arquivo de variáveis.

Etapa 10. Navegue para a pasta **/home/cisco/fmc_ansible**, execute o comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"para reproduzir a tarefa ansible.

Neste exemplo, o comando é ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

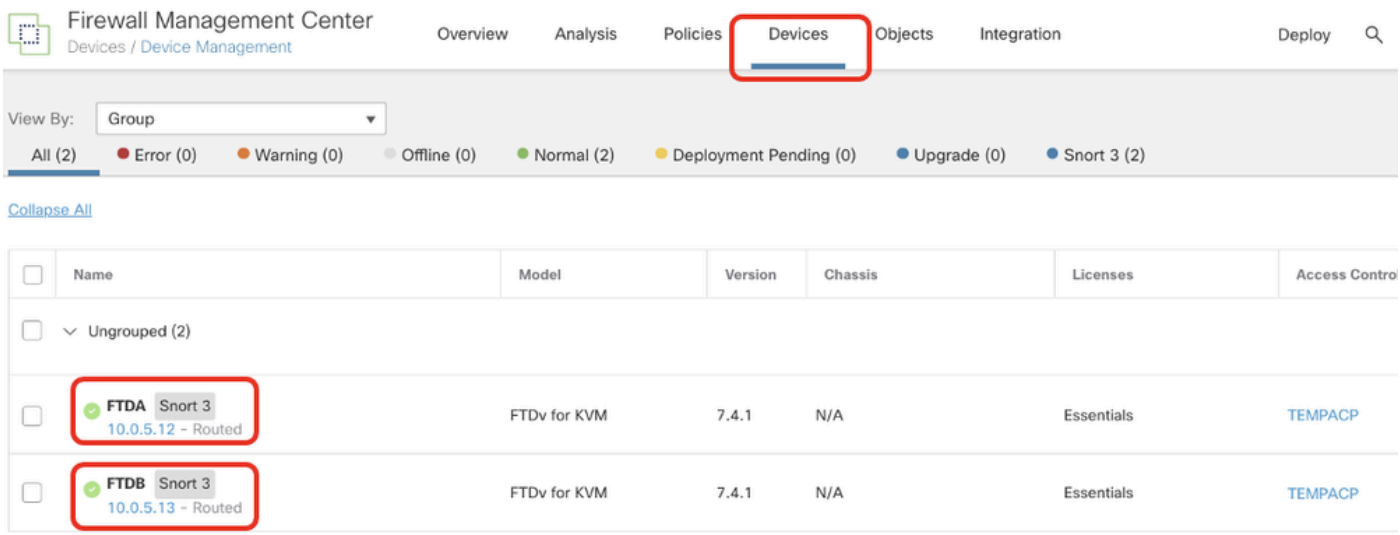
<#root>

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

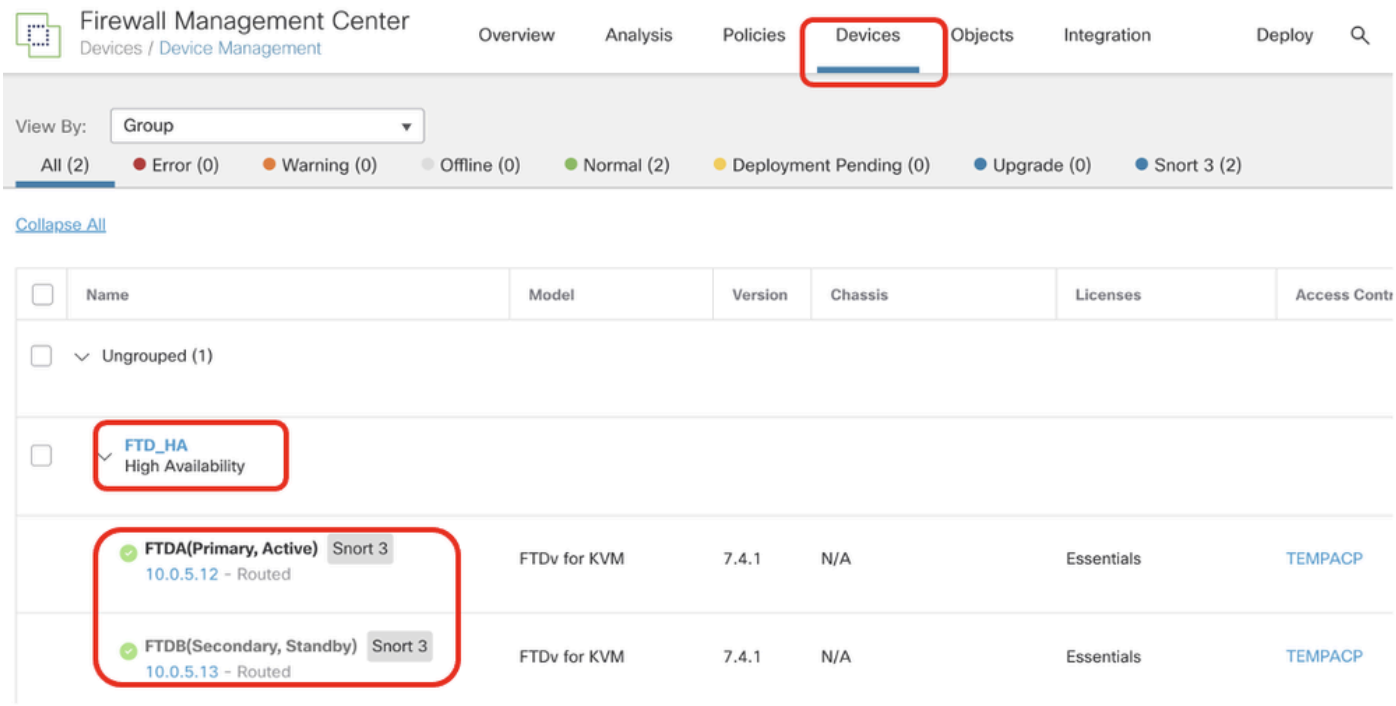
Verificar

Antes de executar a tarefa analisável, faça login na GUI do FMC. Navegue até **Devices > Device Management,** dois FTD registrados com êxito no FMC com política de controle de acesso configurada.



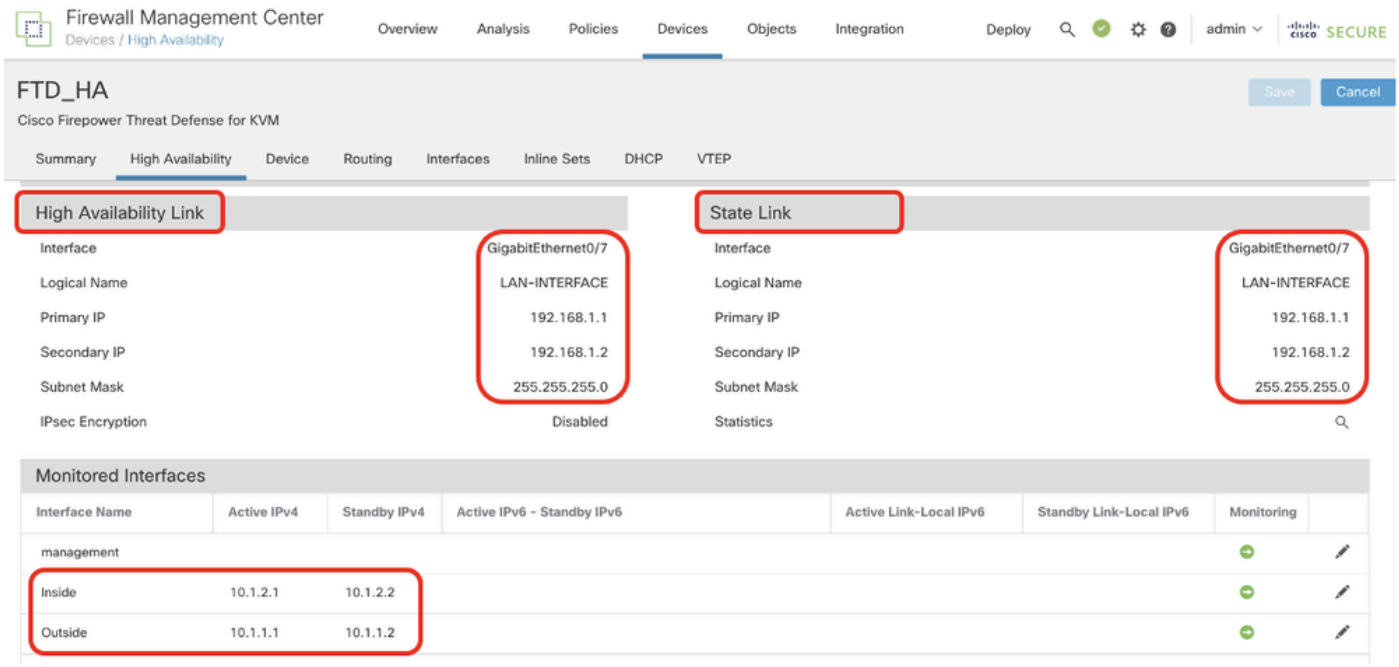
Antes de Executar Tarefa Ansible

Após executar a tarefa analisável, faça login na GUI do FMC. Navegue até **Devices > Device Management,** FTD HA é criado com sucesso.



Após Executar Tarefa Responsável com Êxito

Clique em **Edit** of FTD HA, failover ip address e interface standby ip address estão configurados com êxito.



Detalhes de Alta Disponibilidade do FTD

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para ver mais registros de um manual de atividades possível, você pode executar um manual de atividades com o - vvv.

<#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

Informações Relacionadas

Cisco Devnet FMC Ansible

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.