Configuración de FMC con Ansible para crear alta disponibilidad de FTD

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Diagrama de la red
- Configuraciones

Verificación

Troubleshoot

Información Relacionada

Introducción

En este documento se describen los pasos para automatizar Firepower Management Center (FMC) a fin de crear una alta disponibilidad de Firepower Threat Defence (FTD) con Ansible.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

En el contexto de esta situación de laboratorio, Ansible está desplegado en Ubuntu.

Es esencial asegurarse de que Ansible se instale correctamente en cualquier plataforma compatible con Ansible para ejecutar los comandos Ansible a los que se hace referencia en este artículo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y 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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

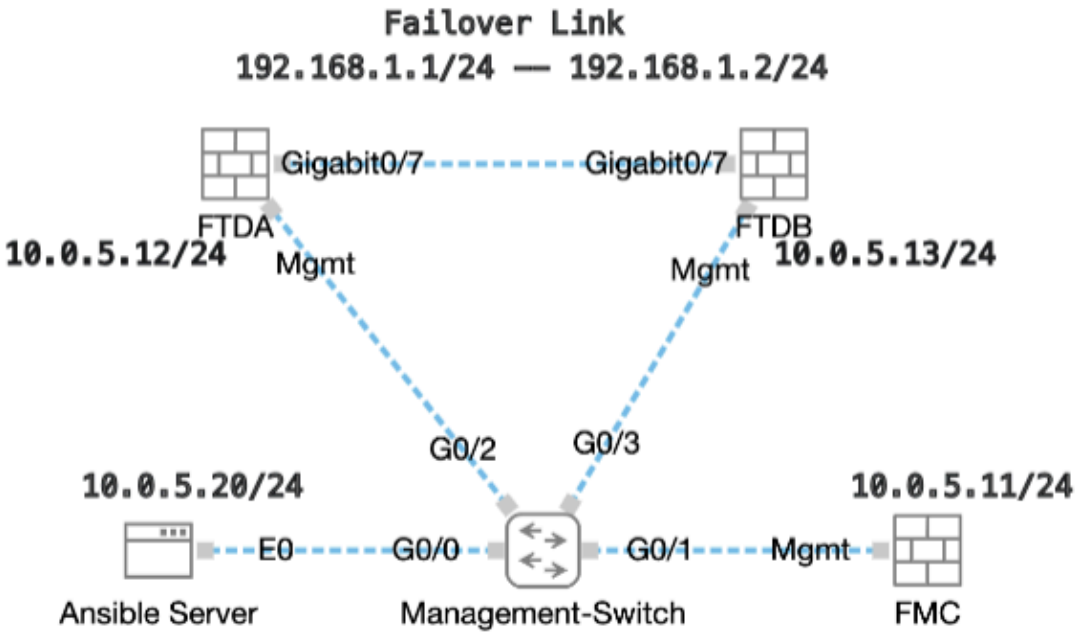
Antecedentes

Ansible es una herramienta muy versátil que demuestra una eficacia significativa en la gestión de dispositivos de red. Se pueden emplear numerosas metodologías para ejecutar tareas automatizadas con Ansible. El método empleado en este artículo sirve de referencia a efectos de ensayo.

En este ejemplo, la alta disponibilidad de FTD y la dirección IP en espera de la misma se crean después de ejecutar el ejemplo del cuaderno de campaña correctamente.

Configurar

Diagrama de la red



Topología

Configuraciones

Como Cisco no admite scripts de ejemplo ni scripts escritos por el cliente, tenemos algunos ejemplos que puede probar según sus necesidades.

Es esencial garantizar que la verificación preliminar se ha completado debidamente.

- El servidor Ansible posee conectividad a Internet.
- El servidor Ansible puede comunicarse correctamente con el puerto GUI de FMC (el puerto predeterminado para la GUI de FMC es 443).
- Dos dispositivos FTD se han registrado correctamente en FMC.
- El FTD principal se configura con la dirección IP de la interfaz.

Paso 1. Conéctese a la CLI del servidor Ansible mediante SSH o la consola.

Paso 2. Ejecute ansible-galaxy collection install cisco.fmcansible el comando para instalar la colección Ansible de FMC en su servidor Ansible.

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

Paso 3. Ejecute mkdir /home/cisco/fmc_ansible el comando para crear una nueva carpeta para almacenar los archivos relacionados. En este ejemplo, el directorio principal es /home/cisco/, el nuevo nombre de carpeta es fmc_ansible.

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

Paso 4. Vaya a la carpeta /home/cisco/fmc_ansible, crear archivo de inventario. En este ejemplo, el nombre del archivo de inventario es Inventory.ini.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones en **negrita** con los parámetros 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

Paso 5. Vaya a la carpeta /home/cisco/fmc_ansible, cree un archivo de variables para crear FTD HA. En este ejemplo, el nombre de archivo de la variable es 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

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones en **negrita** con los parámetros 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

'

Paso 6. Desplácese hasta la carpeta /home/cisco/fmc_ansible, crear archivo de cuaderno para crear FTD HA. En este ejemplo, el nombre del archivo del cuaderno es 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

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones en **negrita** con los parámetros 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

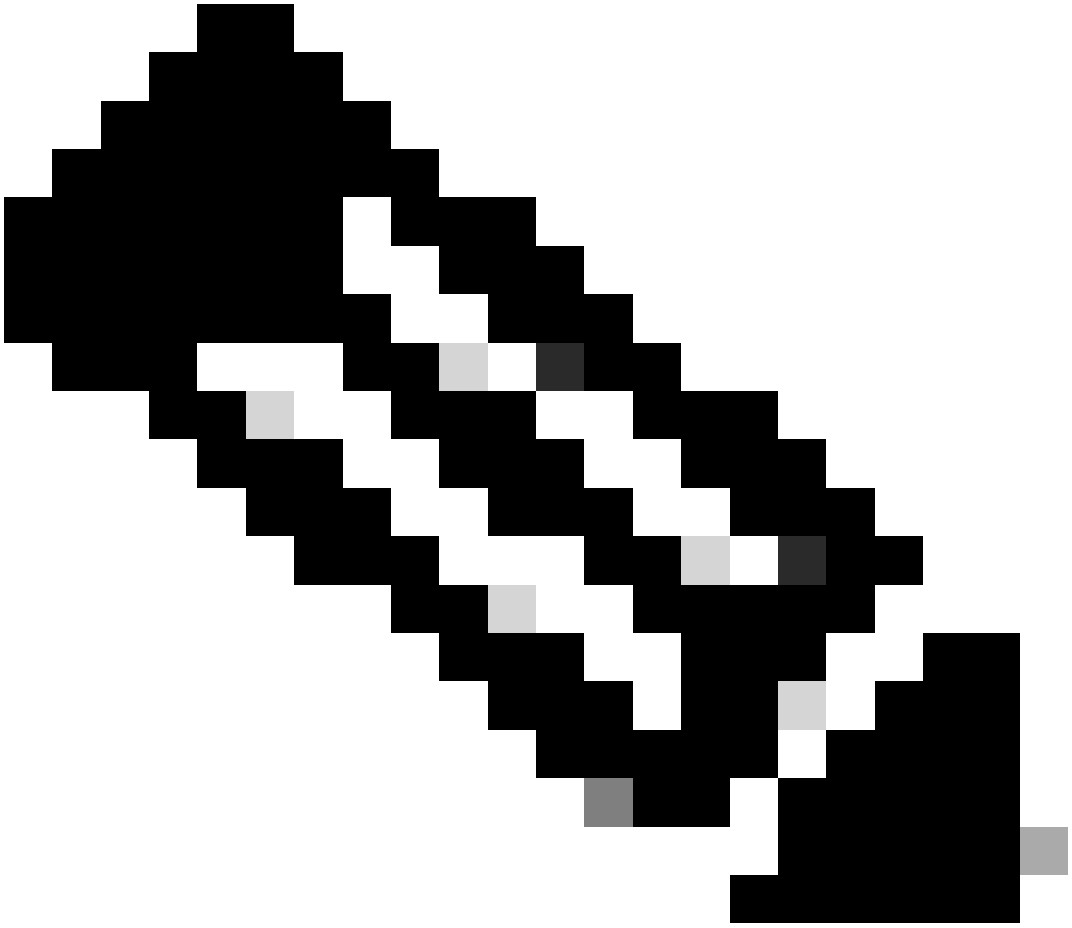
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



Nota: Los nombres en negrita de este cuaderno de campaña de ejemplo sirven como variables. Los valores correspondientes de estas variables se conservan en el archivo de variables.

Paso 7. Navegue hasta la carpeta **/home/cisco/fmc_ansible**, ejecute el comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"para reproducir la tarea ansible.

En este ejemplo, el comando es 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] **

Paso 8. Navegue hasta la carpeta /home/cisco/fmc_ansible, cree un archivo de variable para actualizar la dirección IP standby de FTD HA. En este ejemplo, el nombre de archivo de la variable es 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

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones en **negrita** con los parámetros 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

'

Paso 9. Vaya a la carpeta **/home/cisco/fmc_ansible**, crear archivo de cuaderno para actualizar la dirección IP de reserva de FTD HA. En este ejemplo, el nombre del archivo del cuaderno es 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

Puede duplicar este contenido y pegarlo para su uso, alterando las secciones en **negrita** con los parámetros 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

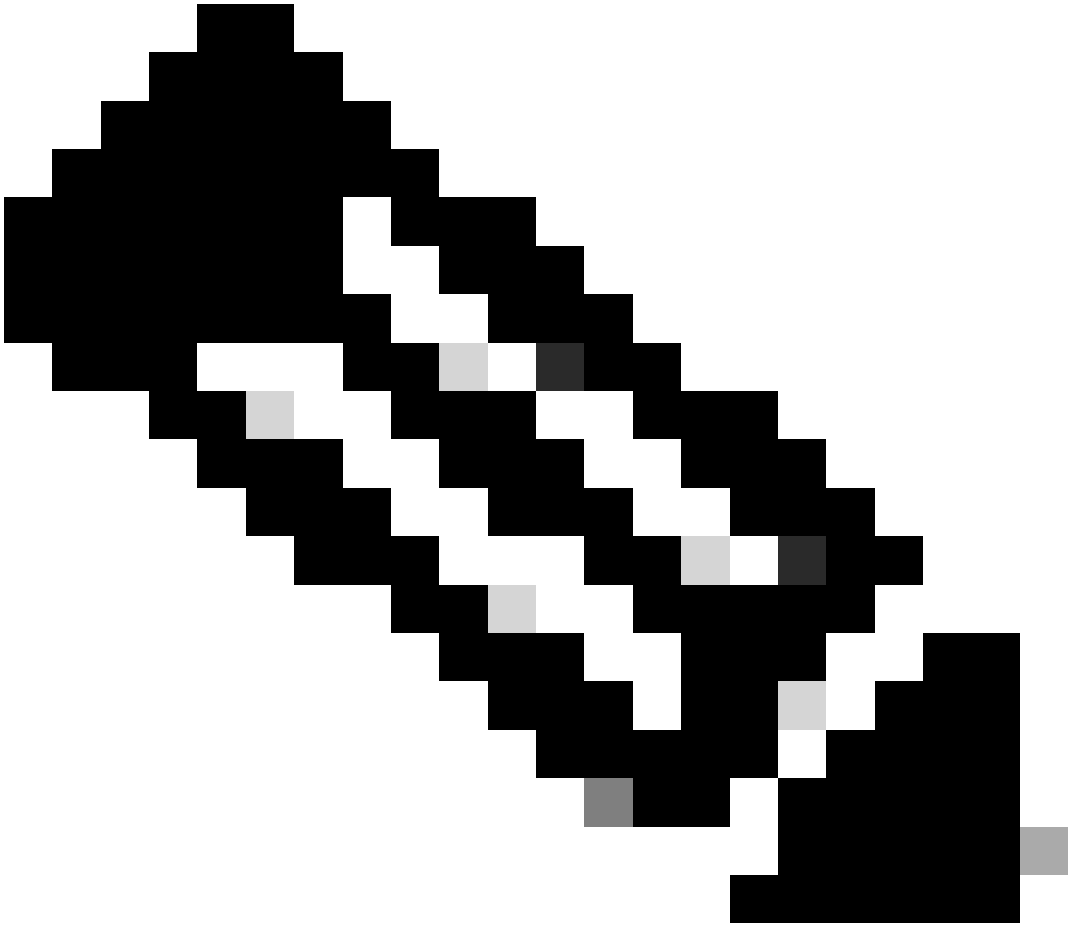
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



Nota: Los nombres en negrita de este cuaderno de campaña de ejemplo sirven como variables. Los valores correspondientes de estas variables se conservan en el archivo de variables.

Paso 10. Navegue hasta la carpeta **/home/cisco/fmc_ansible**, ejecute el comando ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"para reproducir la tarea ansible.

En este ejemplo, el comando es ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml" .

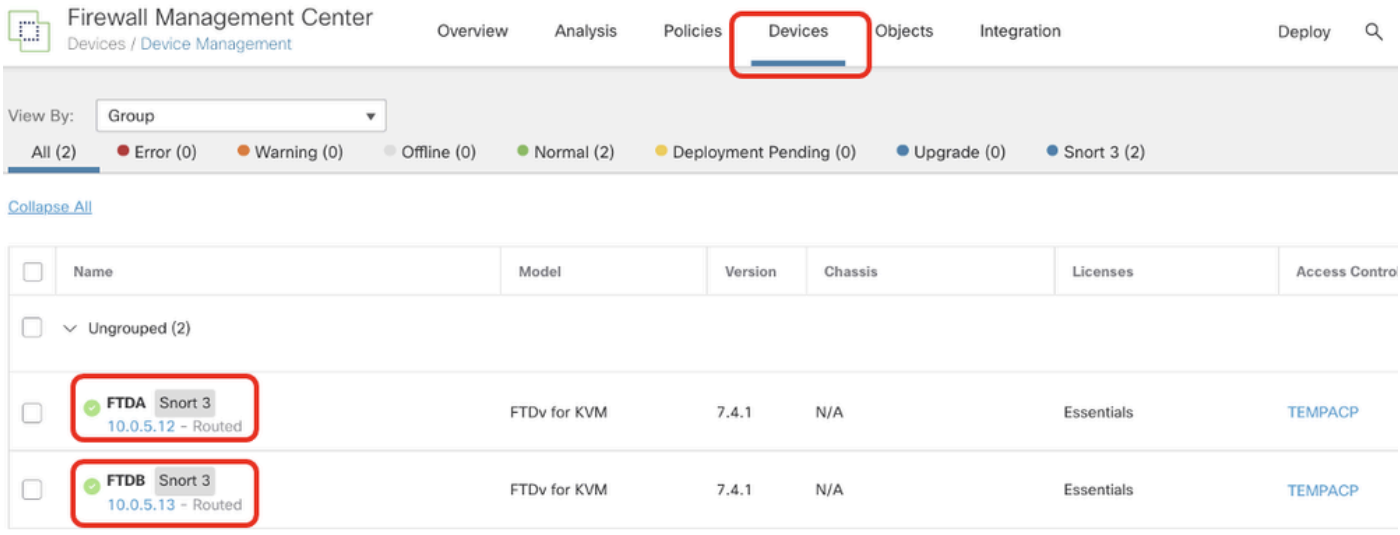
<#root>

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

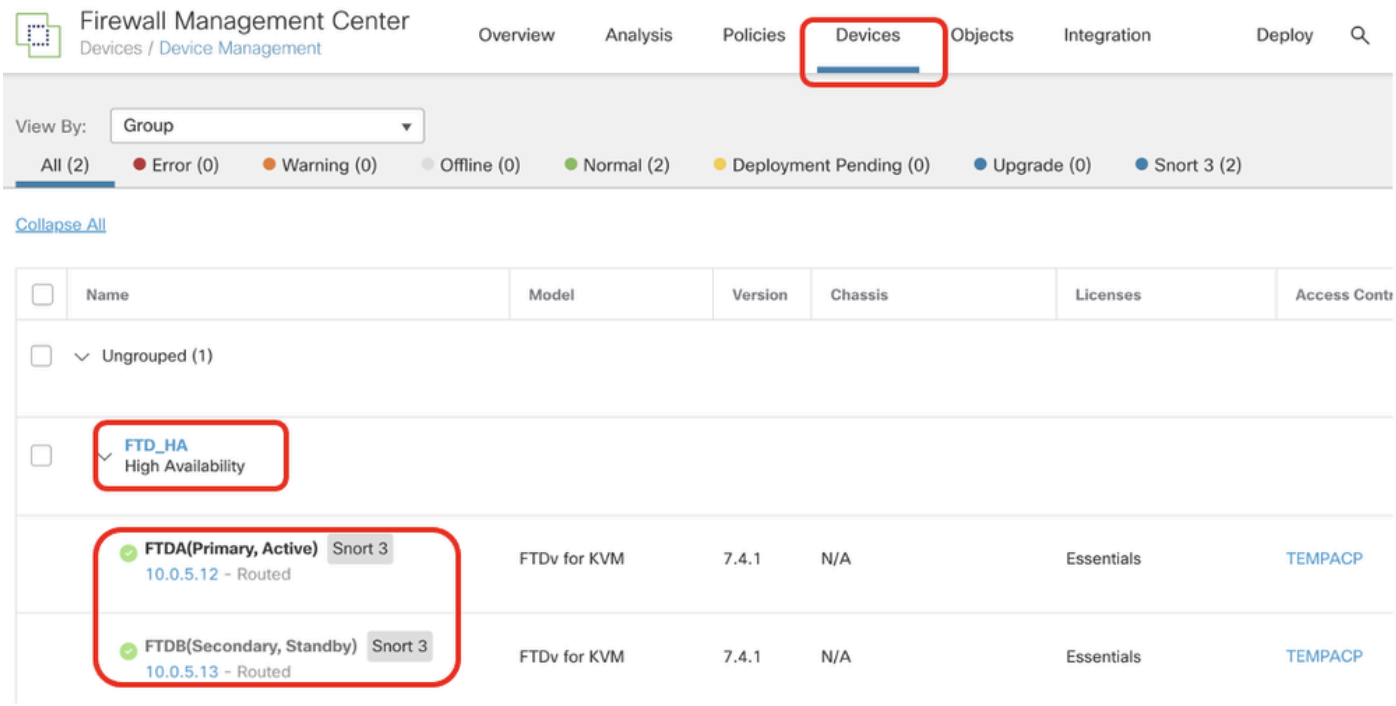
Verificación

Antes de ejecutar la tarea de análisis, inicie sesión en la GUI de FMC. Vaya a **Devices > Device Management,** dos FTD registrados correctamente en FMC con la política de control de acceso configurada.



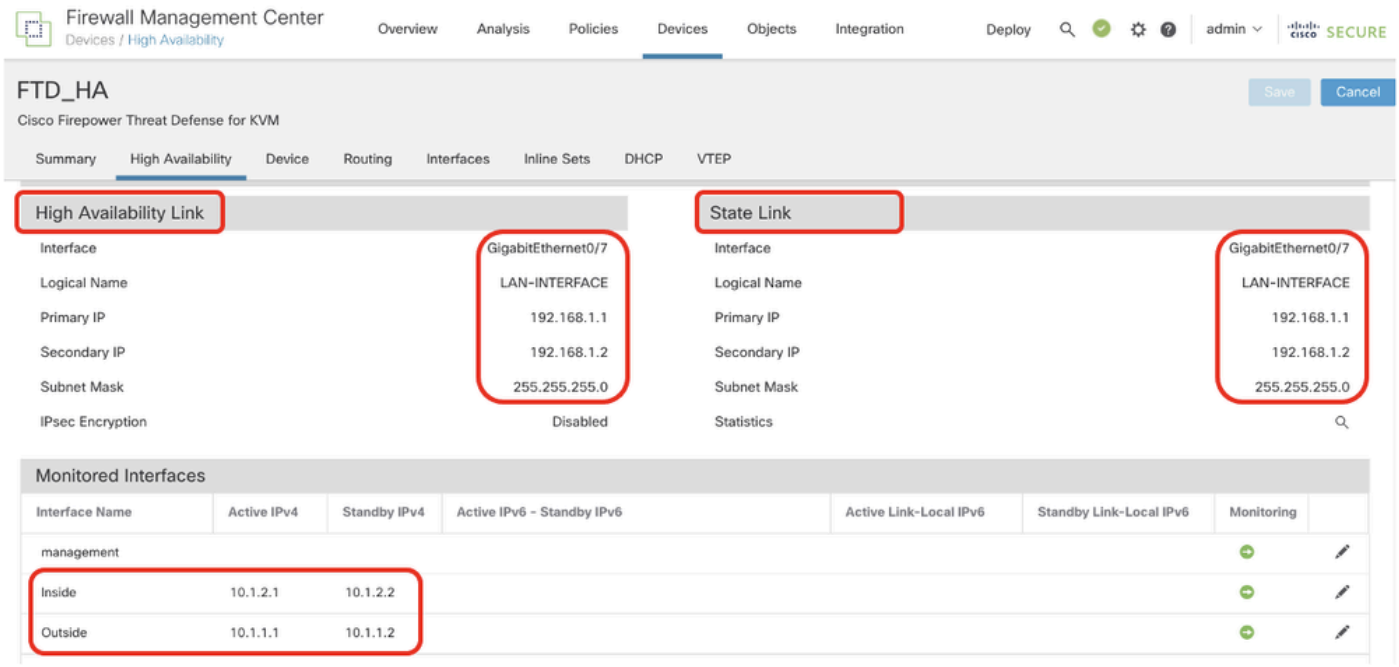
Antes de ejecutar la tarea Ansible

Después de ejecutar la tarea de análisis, inicie sesión en la GUI de FMC. Vaya a **Devices > Device Management,** FTD HA se ha creado correctamente.



Después de ejecutar correctamente la tarea Ansible

Haga clic en **Editar** de FTD HA, la dirección IP de failover y la dirección IP standby de la interfaz se configuran correctamente.



FTD High Availability Detail

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para ver más registros del cuaderno de campaña de Ansible, puede ejecutar el cuaderno de campaña de Ansible 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

Información Relacionada

Cisco Devnet FMC Ansible

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).