FTD 고가용성을 생성하기 위해 Ansible로 FMC 구성

목차

소개

이 문서에서는 FMC(Firepower Management Center)를 자동화하여 Ansible을 통한 FTD(Firepower Threat Defense) High Availability를 생성하는 단계를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 앤서블
- Ubuntu 서버
- Cisco FMC(Firepower 관리 센터) 가상
- Cisco FTD(Firepower Threat Defense) 가상

이러한 실험실 상황에서 Ansible은 Ubuntu에 구축됩니다.

이 문서에서 참조하는 Ansible 명령을 실행하기 위해 Ansible이 지원하는 모든 플랫폼에 Ansible이 성공적으로 설치되도록 하는 것이 중요합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Ubuntu Server 22.04

- Ansible 2.10.8
- 파이썬 3.10
- Cisco Firepower Threat Defense Virtual 7.4.1
- Cisco Firepower Management Center Virtual 7.4.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

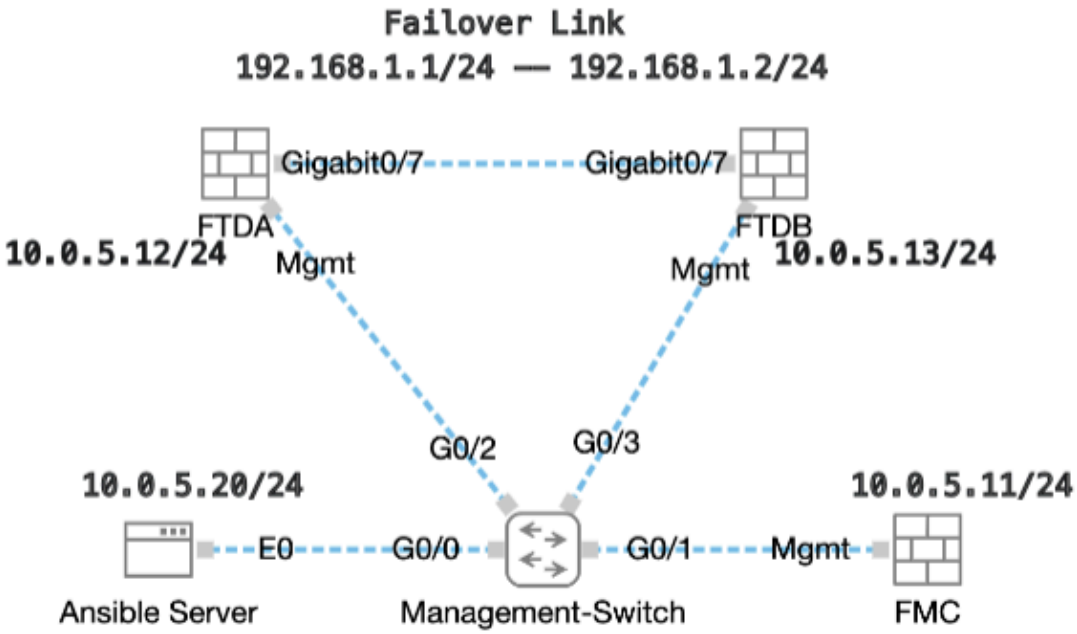
배경 정보

Ansible은 다양한 기능을 갖춘 툴로서 네트워크 디바이스 관리에 상당한 효율성을 입증했습니다. Ansible을 사용하여 자동화된 작업을 실행하기 위해 수많은 방법론이 사용될 수 있습니다. 이 글에 채용된 방법은 시험 목적의 참조로서 사용된다.

이 예에서는 플레이북 예제를 성공적으로 실행한 후 FTD 고가용성 및 대기 IP 주소가 생성됩니다.

구성

네트워크 다이어그램



토폴로지

설정

Cisco는 예제 스크립트나 고객 작성 스크립트를 지원하지 않으므로, 요구 사항에 따라 테스트할 수 있는 몇 가지 예제가 있습니다.

사전 검증이 적법하게 마무리되도록 하는 것이 필수적이다.

- Ansible 서버는 인터넷 연결을 보유하고 있습니다.
- Ansible 서버는 FMC GUI 포트와 성공적으로 통신할 수 있습니다(FMC GUI의 기본 포트는 443).
- 두 개의 FTD 디바이스가 FMC에 성공적으로 등록되었습니다.
- 기본 FTD는 인터페이스 IP 주소로 구성됩니다.

1단계. SSH 또는 콘솔을 통해 Ansible 서버의 CLI에 연결합니다.

2단계. Ansible 서버ansible-galaxy collection install cisco.fmcansible에 FMC의 Ansible 컬렉션을 설치하려면 명령을 실행합니다.

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

3단계. 관련 파일mkdir /home/cisco/fmc_ansible을 저장할 새 폴더를 만들려면 명령을 실행합니다. 이 예에서 홈 디렉토리는 /home/cisco/이고 새 폴더 이름은 fmc_ansible입니다.

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

4단계. /home/cisco/fmc_ansible 폴더로 이동하여 인벤토리 파일을 생성합니다. 이 예에서 인벤토리 파일 이름은 inventory.ini입니다.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

이 내용을 복제하여 활용을 위해 붙여 넣을 수 있으며, 정확한 매개변수로 **굵은** 섹션을 변경할 수 있습니다.

<#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

5단계. /home/cisco/fmc_ansible 폴더로 이동하여 FTD HA 생성을 위한 변수 파일을 생성합니다. 이 예에서 변수 파일 이름은 fmc-create-ftd-ha-vars.yml입니다.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-create-ftd-ha-vars.yml

inventory.ini

이 내용을 복제하여 활용을 위해 붙여 넣을 수 있으며, 정확한 매개변수로 **굵은** 섹션을 변경할 수 있습니다.

<#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

'

6단계. /home/cisco/fmc_ansible 폴더로 이동하여 FTD HA 생성을 위한 플레이북 파일을 생성합니다. 이 예에서 플레이북 파일 이름은 fmc-create-ftd-ha-playbook.yaml입니다.

<#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

이 내용을 복제하여 활용을 위해 붙여 넣을 수 있으며, 정확한 매개변수로 **굵은** 섹션을 변경할 수 있습니다.

<#root>

--- - name: FMC Create FTD HA hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configuration: operation: g

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

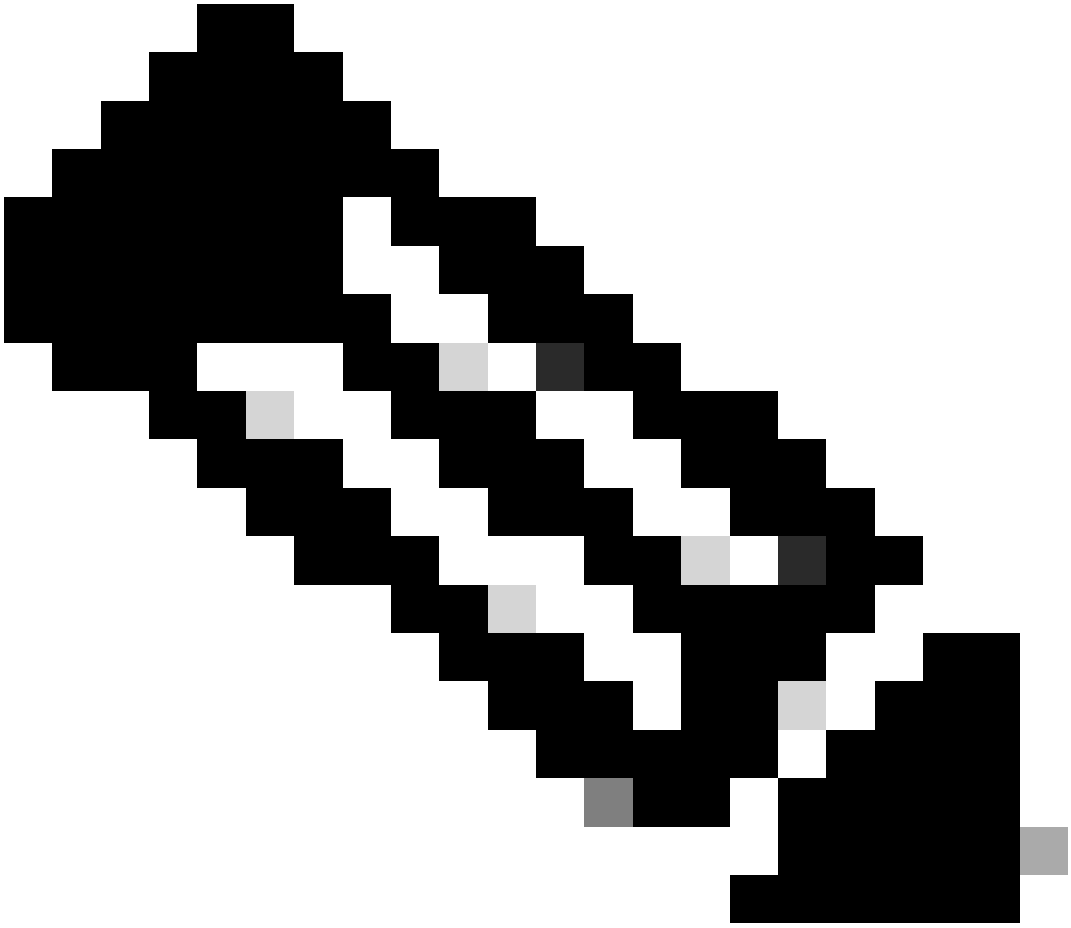
}}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'

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



참고: 이 예제 플레이북에서 굵게 표시된 이름은 변수 역할을 합니다. 이러한 변수에 대한 해당 값은 변수 파일 내에 보존됩니다.

7단계. 폴더/**홈/cisco/fmc_ansible**로 이동하여 명령ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"을 실행하여 ansible 작업을 재생합니다.

이 예에서 명령은 입니다ansible-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:~/fm

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

PLAY [FMC Create FTD HA] **

8단계. /home/cisco/fmc_ansible 폴더로 이동하여 FTD HA 대기 IP 주소 업데이트를 위한 변수 파일을 생성합니다. 이 예에서 변수 파일 이름은 fmc-create-ftd-ha-standby-ip-vars.yml입니다.

<#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

이 내용을 복제한 다음 사용을 위해 붙여 넣어 정확한 매개변수로 **굵게** 섹션을 변경할 수 있습니다.

<#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

'

9단계. 폴더/**홈/cisco/fmc_ansible로 이동하여 FTD** HA 대기 IP 주소 업데이트를 위한 플레이북 파일을 생성합니다. 이 예에서 플레이북 파일 이름은 fmc-create-ftd-ha-standby-ip-playbook.yaml입니다.

<#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

이 내용을 복제하여 활용을 위해 붙여 넣을 수 있으며, 정확한 매개변수로 **굵은** 섹션을 변경할 수 있습니다.

<#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

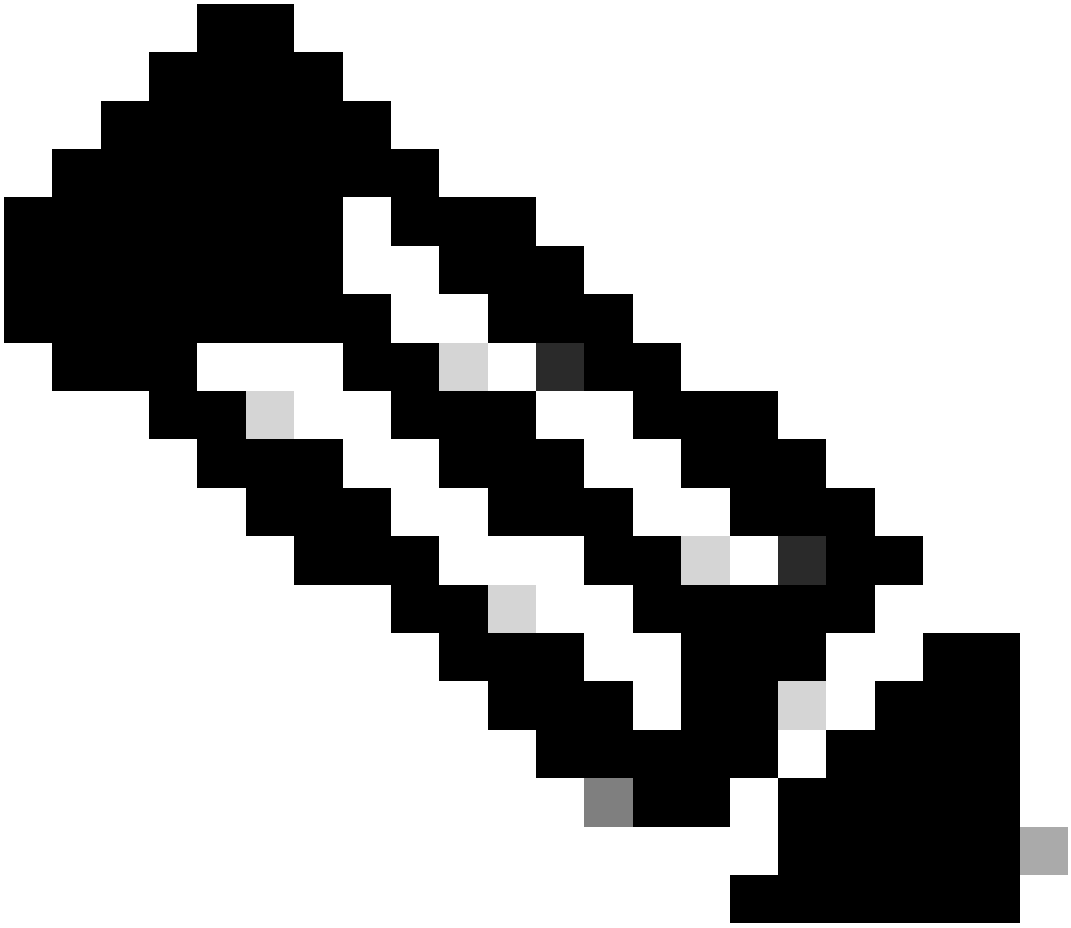
}}" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c

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: "{{



참고: 이 예제 플레이북에서 굵게 표시된 이름은 변수 역할을 합니다. 이러한 변수에 대한 해당 값은 변수 파일 내에 보존됩니다.

10단계. 폴더/**홈/cisco/fmc_ansible**로 이동하여 명령ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"을 실행하여 ansible 작업을 재생합니다.

이 예에서 명령은 입니다ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml".

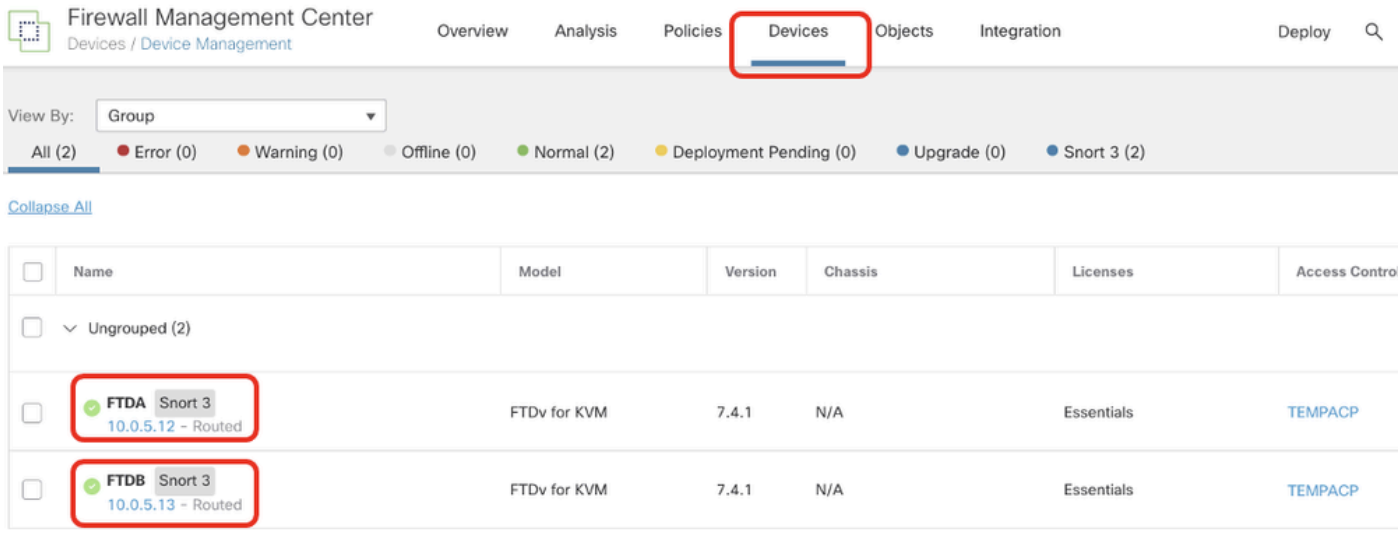
<#root>

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

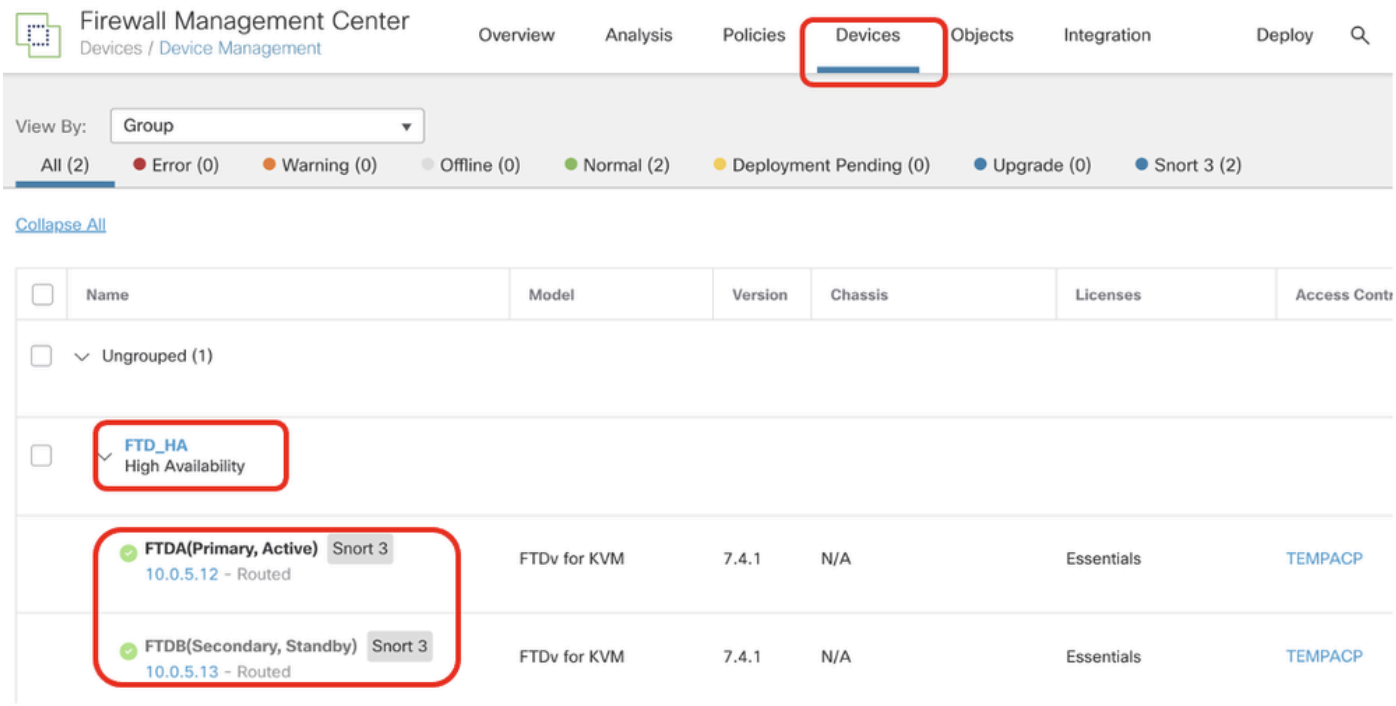
다음을 확인합니다.

확인 가능한 작업을 실행하기 전에 FMC GUI에 로그인합니다. Devices(디바이스) > **Device Management(디바이스 관리)로 이동합니다.** 두 개의 FTD가 구성된 액세스 제어 정책을 사용하여 FMC에 성공적으로 등록되었습니다.



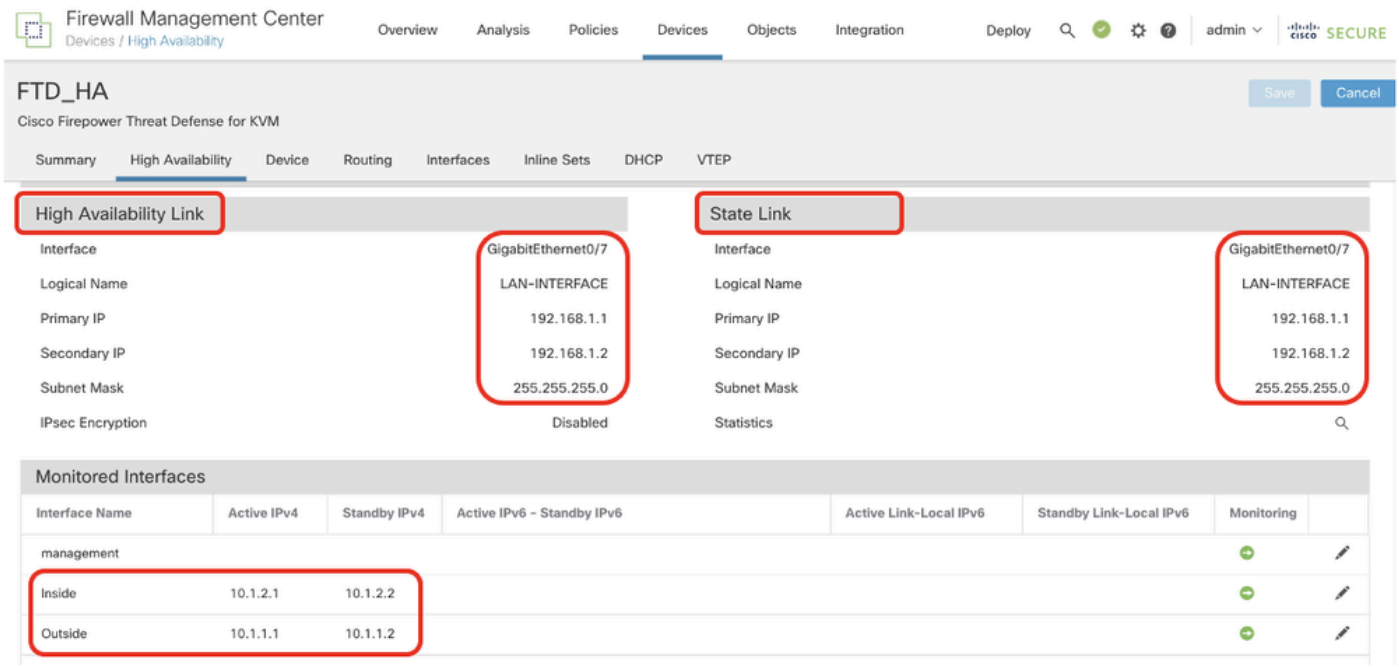
실행 가능한 작업을 실행하기 전

확인 가능한 작업을 실행한 후 FMC GUI에 로그인합니다. Devices(**디바이스**) > **Device Management(디바이스 관리), FTD** HA가 성공적으로 생성됨으로 이동합니다.



실행 가능한 작업을 성공적으로 실행한 후

Edit **of FTD** HA, failover ip address 및 interface standby ip address is successfully를 클릭합니다.



FTD 고가용성 세부 정보

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

Ansible 플레이북의 로그를 더 보려면 -vv로 ansible 플레이북을 실행할 수 있습니다.

<#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

관련 정보

Cisco Devnet FMC Ansible

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.