Het FMC configureren met aanpasbaar aan boord van het FTD

Inhoud

Inleiding

In dit document worden de stappen beschreven om de registratie van Firepower Threat Defence (FTD) bij Firepower Management Center (FMC) met Ansible te automatiseren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- anabel
- Ubuntu server
- Cisco Firepower Management Center (FMC) virtueel
- Cisco Firepower Threat Defence (FTD) virtueel

In de context van deze laboratoriumsituatie wordt Ansible ingezet op Ubuntu.

Het is van essentieel belang om ervoor te zorgen dat Ansible met succes wordt geïnstalleerd op elk platform dat wordt ondersteund door Ansible voor het uitvoeren van de Ansible commando's waarnaar in dit artikel wordt verwezen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Ubuntu server 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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

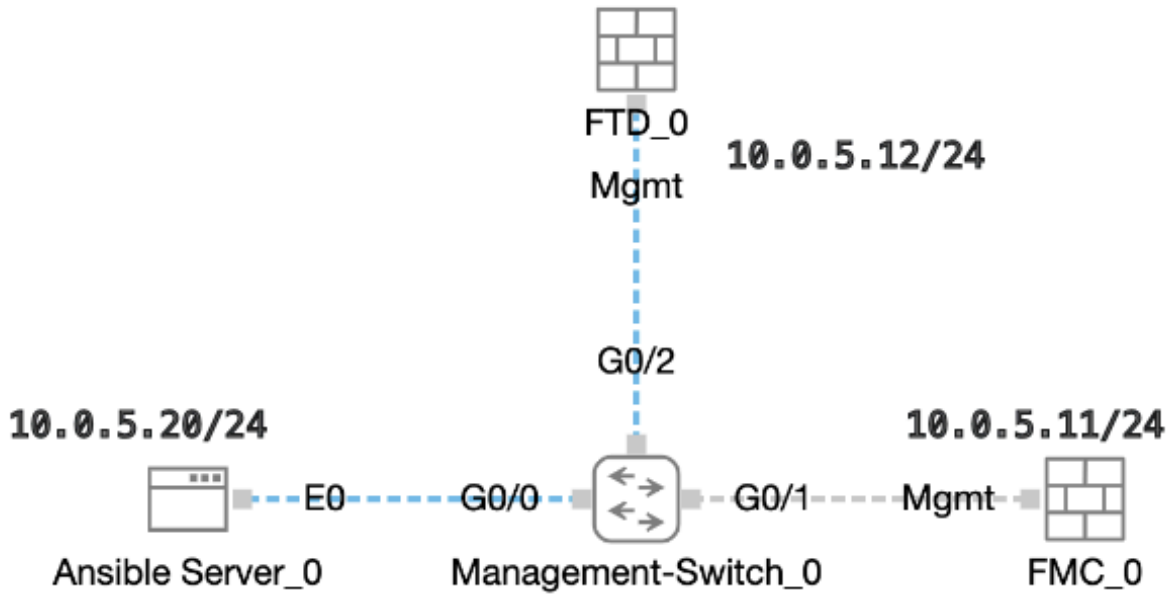
Achtergrondinformatie

Ansible is een zeer veelzijdig hulpmiddel, dat significante doeltreffendheid in het beheer van netwerkapparaten aantoont. Er kunnen tal van methodologieën worden gebruikt om geautomatiseerde taken uit te voeren met Ansible. De in dit artikel gebruikte methode dient als referentie voor testdoeleinden.

In dit voorbeeld, na het succesvol onboarden van de virtuele FTD is het met basisvergunning, gerouteerde wijze, functielaag FTDv30, en het toegangscontrolebeleid dat met standaard vergunningsactie met toegelaten logboek is die naar FMC verzenden.

Configureren

Netwerkdiagram



Topologie

Configuraties

Omdat Cisco voorbeeldscripts of door de klant geschreven scripts niet ondersteunt, hebben we enkele voorbeelden die u kunt testen afhankelijk van uw behoeften.

Het is van essentieel belang ervoor te zorgen dat de voorafgaande verificatie naar behoren is voltooid.

- Een omkeerbare server beschikt over internetverbinding.
- Een omkeerbare server kan met succes communiceren met de FMC GUI-poort (de standaardpoort voor FMC GUI is 443).
- De FTD is geconfigureerd met het juiste IP-adres van de beheerder, de registersleutel en de NAT-id.
- Het VCC wordt met succes ingeschakeld met slimme licentie.

Stap 1. Maak verbinding met de CLI van de Ansible server via SSH of console.

Stap 2. Voer de opdracht ansible-galaxy collection install cisco.fmcansible uit om de Ansible Collection van FMC op uw Ansible Server te installeren.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Stap 3. Start de opdracht mkdir /home/cisco/fmc_ansible om een nieuwe map te maken voor het opslaan van de bijbehorende bestanden. In dit voorbeeld is de home directory /home/cisco/, de nieuwe mapnaam is fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Stap 4. Navigeer naar de map /home/cisco/fmc_ansible en maak een voorraadbestand. In dit voorbeeld, de inventaris bestandsnaam is inventaris.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/


ccisco@inserthostname-here:~/fmc_ansible$

ls
```

inventory.ini

U kunt de volgende inhoud dupliceren en plakken voor gebruik, door de **gemarkeerde** secties te veranderen met de nauwkeurige parameters.

<#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

Stap 5. Navigeer naar de map /home/cisco/fmc_ansible en maak een variabele bestand. In dit voorbeeld is de variabele bestandsnaam fmc-onboard-ftd-vars.yml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-onboard-ftd-vars.yml

inventory.ini

U kunt de volgende inhoud dupliceren en plakken voor gebruik, door de **gemarkeerde** secties te veranderen met de nauwkeurige parameters.

<#root>

user:
 domain: 'Global'
onboard:
 acp_name: '

TEMPACP

'
device_name:
 ftd1: '

FTDA

'
 ftd1_reg_key: '

cisco

'
 ftd1_nat_id: '

natcisco

'
mgmt:
 ftd1: '

10.0.5.12

'

Stap 6.Navigeer naar de map /home/cisco/fmc_ansible en maak een afspeelboekbestand. In dit voorbeeld is de bestandsnaam van het afspeelboek fmc-onboard-ftd-playbook.yaml.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

fmc-onboard-ftd-playbook.yaml

fmc-onboard-ftd-vars.yml inventory.ini

U kunt de volgende inhoud dupliceren en plakken voor gebruik, door de **gemarkeerde** secties te veranderen met de nauwkeurige parameters.

<#root>

- name: FMC Onboard FTD

```
hosts: fmc
connection: httpapi

tasks:

- name: Task01 - Get User Domain
cisco.fmcansible.fmc_configuration:
operation: getAllDomain
filters:
name: "{{
```

user.domain

```
 }}"
 register_as: domain

 - name: Task02 - Create ACP TEMP_ACP
 cisco.fmcansible.fmc_configuration:
 operation: "createAccessPolicy"
 data:
 type: "AccessPolicy"
 name: "{{accesspolicy_name | default(
```

onboard.acp_name

```
) }}"
 defaultAction: {
 'action': 'PERMIT',
 'logEnd': True,
 'logBegin': False,
 'sendEventsToFMC': True
 }
 path_params:
 domainUUID: "{{ domain[0].uuid }}"

 - name: Task03 - Get Access Policy
 cisco.fmcansible.fmc_configuration:
 operation: getAllAccessPolicy
 path_params:
 domainUUID: "{{ domain[0].uuid }}"
 filters:
 name: "{{
```

onboard.acp_name

```
 }}"
 register_as: access_policy

 - name: Task04 - Add New FTD1
 cisco.fmcansible.fmc_configuration:
 operation: createMultipleDevice
 data:
 hostName: "{{ ftd_ip | default(item.key) }}"
 license_caps:
 - 'BASE'
 ftdMode: 'ROUTED'
 type: Device
 regKey: "{{ reg_key | default(
```

device_name.ftd1_reg_key

```
) }}"
 performanceTier: "FTDv30"
 name: "{{ ftd_name | default(item.value) }}"
```

```
 accessPolicy:
 id: '{{ access_policy[0].id }}'
 type: 'AccessPolicy'
 natID: "{{ nat_id | default(
```

device_name.ftd1_nat_id

```
) }}"
 path_params:
 domainUUID: '{{ domain[0].uuid }}'
 loop: "{{ ftd_ip_name | dict2items }}"
 vars:
 ftd_ip_name:
 "{{
```

mgmt.ftd1

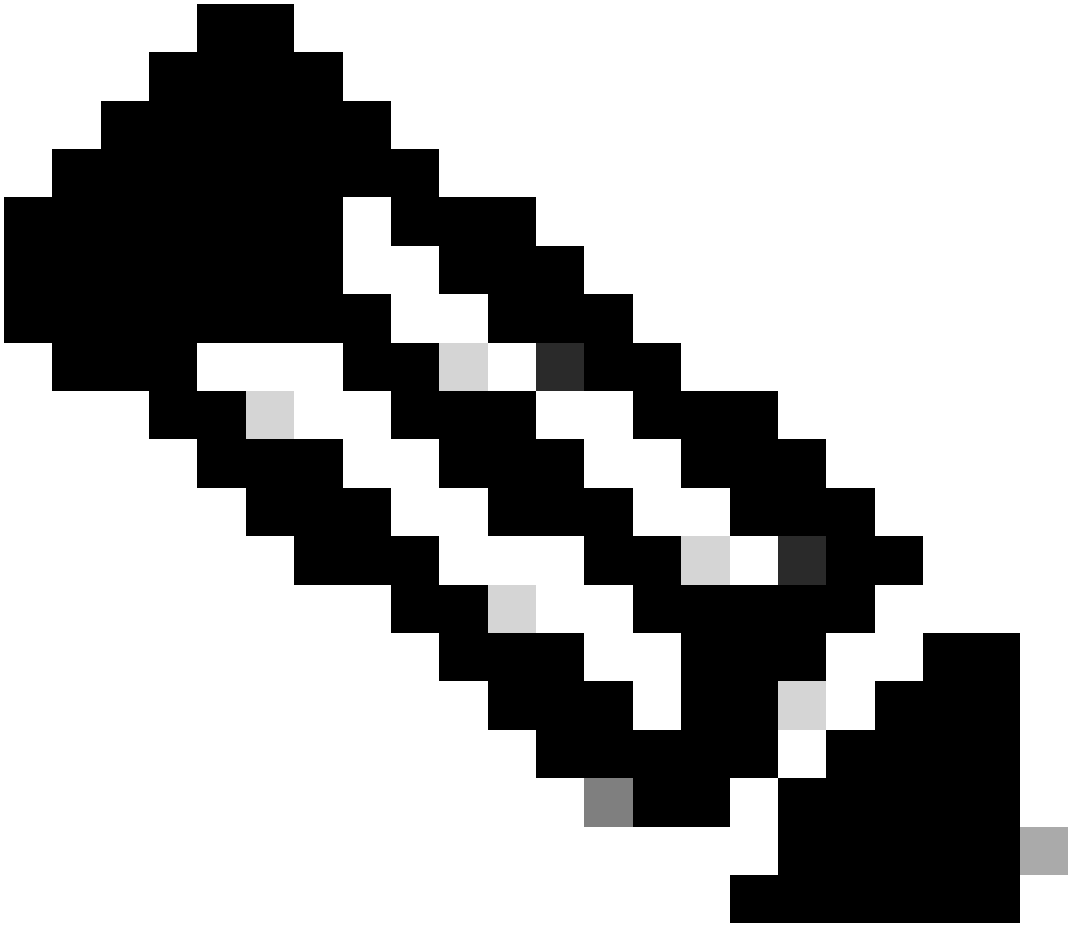
```
}}": "{{
```

device_name.ftd1

```
}}"

 - name: Task05 - Wait For FTD Registration Completion
 ansible.builtin.wait_for:
 timeout: 120
 delegate_to: localhost


 - name: Task06 - Confirm FTD Init Deploy Complete
 cisco.fmcansible.fmc_configuration:
 operation: getAllDevice
 path_params:
 domainUUID: '{{ domain[0].uuid }}'
 query_params:
 expanded: true
 filters:
 name: "{{
```

device_name.ftd1

```
 }}"
 register_as: device_list
 until: device_list[0].deploymentStatus is match("DEPLOYED")
 retries: 1000
 delay: 3
```



Opmerking: de namen die in dit voorbeeldafspeelboek worden gemarkeerd, dienen als variabelen. De corresponderende waarden voor deze variabelen blijven in het variabele bestand bewaard.

Stap 7. Navigeer naar de map /home/cisco/fmc_ansible, voer de opdracht uit **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** om de taak met de hand af te spelen. In dit voorbeeld is de opdracht ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

<#root>

cisco@inserthostname-here:~$

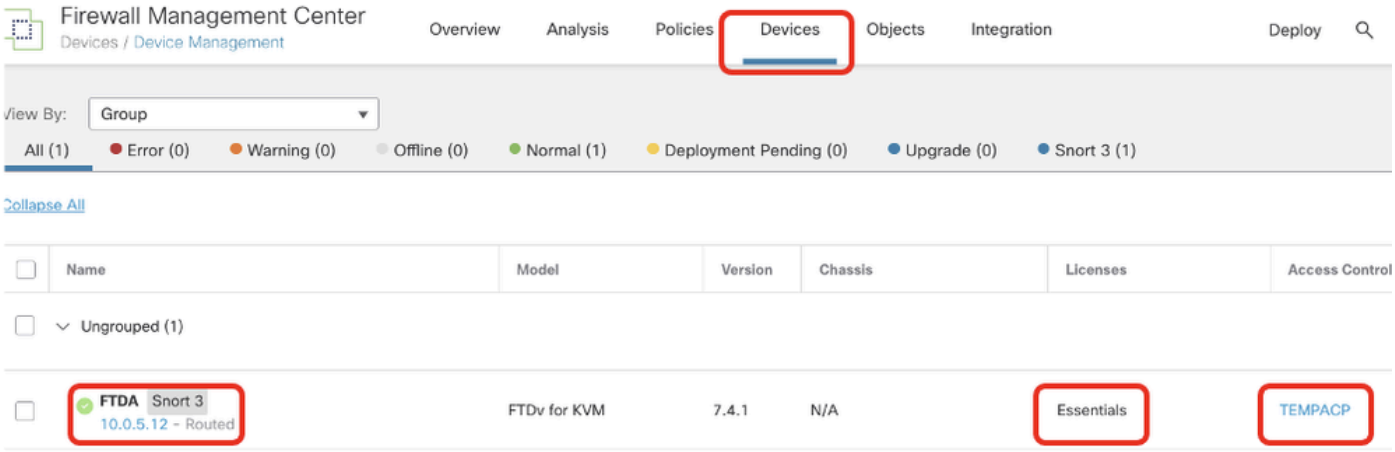
cd /home/cisco/fmc_ansible/

```
cisco@inserthostname-here:~/fmc_ansible$
ls

fmc-onboard-ftd-playbook.yaml fmc-onboard-ftd-vars.yml inventory.ini

cisco@inserthostname-here:~/fmc_ansible$
ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml"



PLAY [FMC Onboard FTD] *********************************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [10.0.5.11]

TASK [Task01 - Get User Domain] ************************************************************************
ok: [10.0.5.11]

TASK [Task02 - Create ACP TEMP_ACP] ********************************************************************
changed: [10.0.5.11]

TASK [Task03 - Get Access Policy] **********************************************************************
ok: [10.0.5.11]

TASK [Task04 - Add New FTD1] ***************************************************************************
changed: [10.0.5.11] => (item={'key': '10.0.5.12', 'value': 'FTDA'})

TASK [Task05 - Wait For FTD Registration Completion] ***************************************************
ok: [10.0.5.11]

TASK [Task06 - Confirm FTD Init Deploy Complete] *******************************************************
FAILED - RETRYING: Task06 - Confirm FTD Init Deploy Complete (1000 retries left).
FAILED - RETRYING: Task06 - Confirm FTD Init Deploy Complete (999 retries left).
FAILED - RETRYING: Task06 - Confirm FTD Init Deploy Complete (998 retries left).
FAILED - RETRYING: Task06 - Confirm FTD Init Deploy Complete (997 retries left).
FAILED - RETRYING: Task06 - Confirm FTD Init Deploy Complete (996 retries left).
ok: [10.0.5.11]

PLAY RECAP *********************************************************************************************
10.0.5.11 : ok=7 changed=2 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
```

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Inloggen bij FMC GUI. Navigeren naar **Apparaten > Apparaatbeheer,** de FTD met succes geregistreerd op FMC met geconfigureerd toegangscontrolebeleid.



Pagina voor apparaatbeheer

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Om meer logboeken van ansible playbook te zien, kunt u ansible playbook uitvoeren met -vv.

<#root>

cisco@inserthostname-here:~/fmc_ansible$ ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml"

-vvv

Gerelateerde informatie

[Cisco Devnet FMC Ansible]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.