

Konfigurieren von FMC mit Ansible zur Aktualisierung der FTD-Schnittstellen-IP

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Schritte zur Automatisierung von FirePOWER Management Center (FMC) beschrieben, um die FirePOWER Threat Defense (FTD)-Schnittstelle IP mit Ansible zu konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Ansible
- Ubuntu-Server
- Cisco FirePOWER Management Center (FMC) - Virtuell
- Cisco FirePOWER Threat Defense (FTD) - virtuell

Im Kontext dieser Laborsituation wird Ansible unter Ubuntu bereitgestellt.

Es ist wichtig sicherzustellen, dass Ansible erfolgreich auf jeder von Ansible unterstützten Plattform installiert wird, um die in diesem Artikel genannten Ansible-Befehle auszuführen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

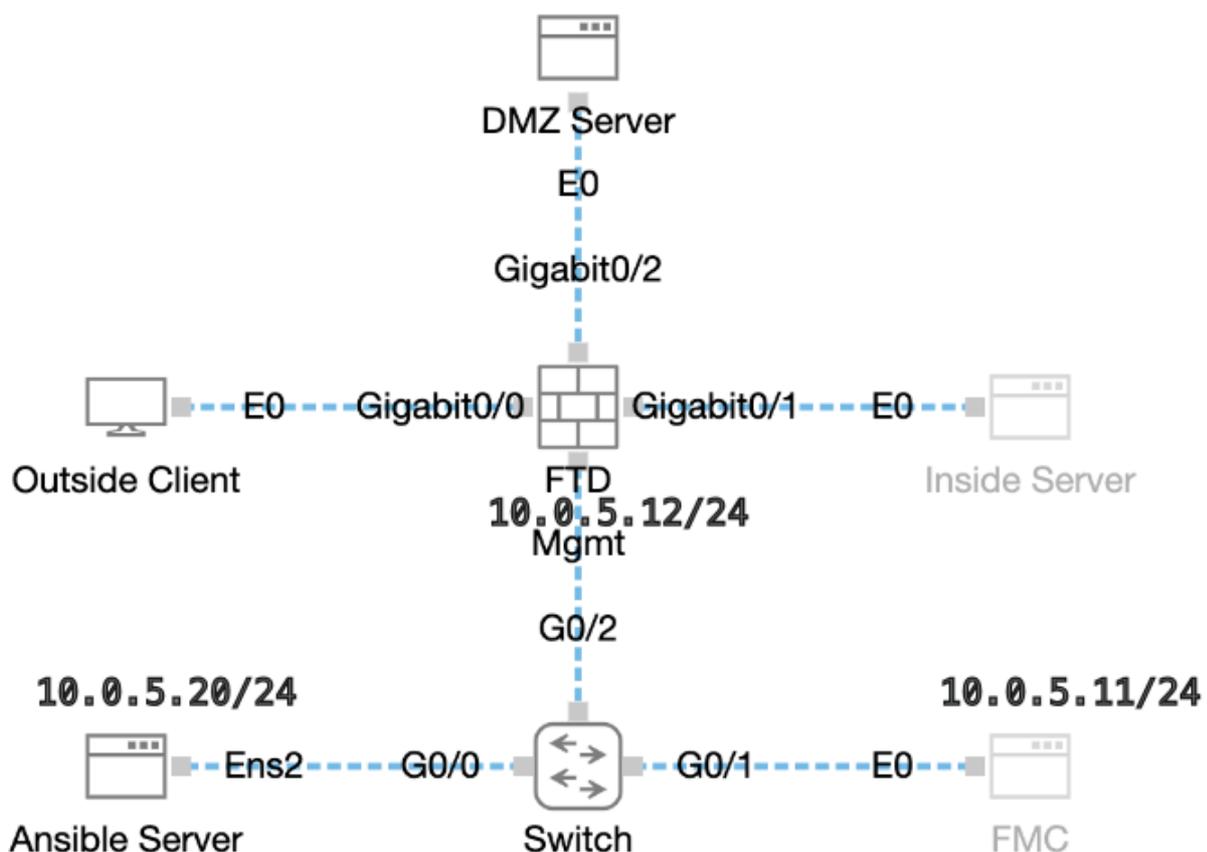
Hintergrundinformationen

Ansible ist ein äußerst vielseitiges Tool, das eine erhebliche Effizienz bei der Verwaltung von Netzwerkgeräten demonstriert. Für die Ausführung automatisierter Aufgaben mit Ansible können zahlreiche Methoden eingesetzt werden. Das in diesem Artikel verwendete Verfahren dient als Referenz für Testzwecke.

In diesem Beispiel werden die IP-Adresse der Schnittstelle, die Maske und der Schnittstellename nach erfolgreicher Ausführung des strategischen Leitfadens auf FTD aktualisiert.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Da Cisco keine Beispiel-Skripte oder vom Kunden erstellte Skripte unterstützt, gibt es einige Beispiele, die Sie je nach Ihren Anforderungen testen können.

Es muss unbedingt sichergestellt werden, dass die vorläufige Überprüfung ordnungsgemäß abgeschlossen wurde.

- Ein möglicher Server verfügt über eine Internetverbindung.
- Ein möglicher Server kann erfolgreich mit dem FMC GUI-Port kommunizieren (der Standardport für die FMC GUI ist 443).
- Die FTD wurde erfolgreich bei FMC registriert.

Schritt 1: Stellen Sie über SSH oder die Konsole eine Verbindung mit der CLI des Ansible-Servers her.

Schritt 2: Führen Sie den Befehl `ansible-galaxy collection install cisco.fmcansible` aus, um die Ansible-Sammlung von FMC auf dem Ansible-Server zu installieren.

<#root>

```
cisco@inserthostname-here:~$
```

```
ansible-galaxy collection install cisco.fmcansible
```

Schritt 3: Führen Sie den Befehl aus, `mkdir /home/cisco/fmc_ansible` einen neuen Ordner zum Speichern der zugehörigen Dateien zu erstellen. In diesem Beispiel ist das Basisverzeichnis `/home/cisco/`, und der neue Ordnername lautet `fmc_ansible`.

<#root>

```
cisco@inserthostname-here:~$
```

```
mkdir /home/cisco/fmc_ansible
```

Schritt 4: Navigieren Sie zum Ordner `/home/cisco/fmc_ansible`, und erstellen Sie eine Inventardatei. In diesem Beispiel lautet der Name der Bestandsdatei `Inventory.ini`.

<#root>

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
inventory.ini
```

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **hervorgehobenen** Abschnitte mit genauen Parametern ändern.

```
<#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
```

Schritt 5: Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, erstellen Sie eine variable Datei. In diesem Beispiel lautet der Dateiname der Variablen `fmc-configure-interface-vars.yml`.

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-configure-interface-vars.yml
```

```
inventory.ini
```

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **hervorgehobenen** Abschnitte mit genauen Parametern

ändern.

```
<#root>
```

```
user: domain: 'Global' onboard: acp_name: 'TEMPACP' device_name: ftd1: 'FTDA' ftd_data: outside_name: '
```

```
Outside
```

```
' inside_name: '
```

```
Inside
```

```
' dmz_name: '
```

```
DMZ
```

```
' outside_ip: '
```

```
10.1.1.1
```

```
' inside_ip: '
```

```
10.1.2.1
```

```
' dmz_ip: '
```

```
10.1.3.1
```

```
' mask24: '
```

```
255.255.255.0
```

```
'
```

Schritt 6: Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, erstellen Sie eine Playbook-Datei. In diesem Beispiel lautet der Dateiname des strategischen Leitfadens `fmc-configure-interface-playbook.yaml`.

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-configure-interface-playbook.yaml
```

```
fmc-configure-interface-vars.yml inventory.ini
```

Sie können diesen Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **hervorgehobenen** Abschnitte mit genauen Parametern ändern.

<#root>

--- - name: Update FTD Interface IP Address hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configu

user.domain

}}" register_as: domain - name: Task02 - Get Devices cisco.fmcansible.fmc_configuration: operation: ge

device_name.ftd1

}}" register_as: device_list - name: Task03 - Get Physical Interfaces cisco.fmcansible.fmc_configurati

ftd_data.outside_name

}}" ipv4: static: address: "{{ Outside_ip | default(

ftd_data.outside_ip

) }}" netmask: "{{ Outside_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/0

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

ftd_data.inside_name

}}" ipv4: static: address: "{{ Inside_ip | default(

ftd_data.inside_ip

}}" netmask: "{{ Inside_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/1

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

ftd_data.dmz_name

}}" ipv4: static: address: "{{ DMZ_ip | default(

ftd_data.dmz_ip

) }}" netmask: "{{ DMZ_netmask | default(

ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:

GigabitEthernet0/2

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{



Hinweis: Die in diesem strategischen Leitfaden hervorgehobenen Namen dienen als Variablen. Die entsprechenden Werte für diese Variablen werden innerhalb der Variablendatei beibehalten.

Schritt 7. Navigieren Sie zum Ordner **/home/cisco/fmc_ansible**, führen Sie den Befehl `ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e"<playbook_vars>.yaml"` aus, um die ansible Aufgabe abzuspielden.

In diesem Beispiel lautet der Befehl `ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e"fmcconfigureinterfacevars.yaml"` .

<#root>

cisco@inserthostname-here:~\$

```
cd /home/cisco/fmc_ansible/
```

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

```
ls
```

```
fmc-configure-interface-playbook.yaml fmc-configure-interface-vars.yaml inventory.ini
```

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

```
ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars"
```

```
PLAY [Update FTD Interface IP Address] *****
```

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

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

```
TASK [Task02 - Get Devices] *****  
ok: [10.0.5.11]
```

```
TASK [Task03 - Get Physical Interfaces] *****  
ok: [10.0.5.11]
```

```
TASK [Task04 - Setup Outside Interface with static IP] *****  
changed: [10.0.5.11]
```

```
TASK [Task05 - Setup Inside Interface with static IP] *****  
changed: [10.0.5.11]
```

```
TASK [Task06 - Setup DMZ Interface with static] *****  
changed: [10.0.5.11]
```

```
TASK [Task07 - Get Deployable Devices] *****  
ok: [10.0.5.11]
```

```
TASK [Task08 - Start Deployment] *****  
changed: [10.0.5.11]
```

```
TASK [Wait for Deployment Complete] *****  
ok: [10.0.5.11]
```

```
TASK [Task09 - Poll Deployment Status Until Deployment Successful] *****  
ok: [10.0.5.11]
```

```
TASK [Task10 - Stop The Playbook If The Deployment Failed] *****  
skipping: [10.0.5.11]
```

```
PLAY RECAP *****  
10.0.5.11 : ok=11 changed=4 unreachable=0 failed=0 skipped=1 rescued=0 ignored=0
```

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Stellen Sie über SSH oder die Konsole eine Verbindung zur CLI des FTD her, und führen Sie die Befehle `show interface ip brief` und `show running-config interface GigabitEthernet 0/X` aus.

Schnittstellename, IP-Adresse und Maske wurden erfolgreich konfiguriert.

```
<#root>
```

```
> show interface ip brief
```

```
Interface IP-Address OK? Method Status Protocol
```

```
GigabitEthernet0/0 10.1.1.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/1 10.1.2.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/2 10.1.3.1
```

```
YES manual
```

```
up up
```

```
>
```

```
show running-config interface GigabitEthernet 0/0
```

```
!  
interface GigabitEthernet0/0  
nameif
```

```
Outside
```

```
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```

```
ip address 10.1.1.1 255.255.255.0
```

```
>
```

```
show running-config interface GigabitEthernet 0/1
```

```
!
```

```
interface GigabitEthernet0/1
nameif

Inside

cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

ip address 10.1.2.1 255.255.255.0
```

>

```
show running-config interface GigabitEthernet 0/2
```

```
!
interface GigabitEthernet0/2
nameif

DMZ
```

```
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 10.1.3.1 255.255.255.0
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Um mehr Logs von ansible playbook zu sehen, können Sie ansible playbook mit -vvv ausführen

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

Zugehörige Informationen

[Cisco DevNet FMC-fähig](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.