Konfigurieren von FMC mit Ansible für Onboard-FTD

Inhalt

Einleitung

Dieses Dokument beschreibt die Schritte zur Automatisierung der Registrierung von Firepower Threat Defense (FTD) beim Firepower Management Center (FMC) mit Ansible.

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.

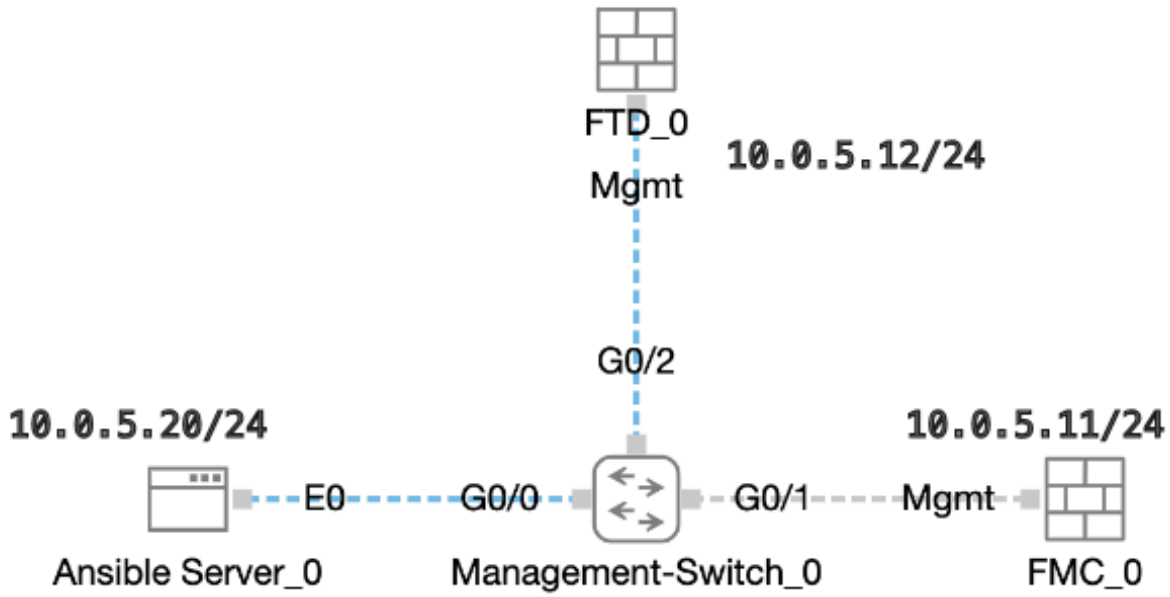
Hintergrundinformationen

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 nach dem erfolgreichen Onboarding des virtuellen FTD die Basislizenz, der Routing-Modus, die FTDv30-Funktionsebene und die Zugriffskontrollrichtlinie verwendet, die bei aktiviertem Protokoll die standardmäßige Genehmigungsaktion beim Senden an FMC enthält.

Konfigurieren

Netzwerkdiagramm



Topologie

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 ist unbedingt sicherzustellen, dass die Vorprüfung 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).
- Das FTD ist mit der richtigen Manager-IP-Adresse, dem richtigen Registrierungsschlüssel und der richtigen NAT-ID konfiguriert.
- Das FMC wurde mit der Smart-Lizenz aktiviert.

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 Befehlmkdir /home/cisco/fmc_ansible aus, um 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 den folgenden Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **markierten** Abschnitte mit den 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, und erstellen Sie eine variable Datei. In diesem Beispiel lautet der Dateiname der Variablen 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

Sie können den folgenden Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **markierten** Abschnitte mit den genauen Parametern ändern.

<#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

'

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-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

Sie können den folgenden Inhalt duplizieren und zur Verwendung einfügen, indem Sie die **markierten** Abschnitte mit den genauen Parametern ändern.

<#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

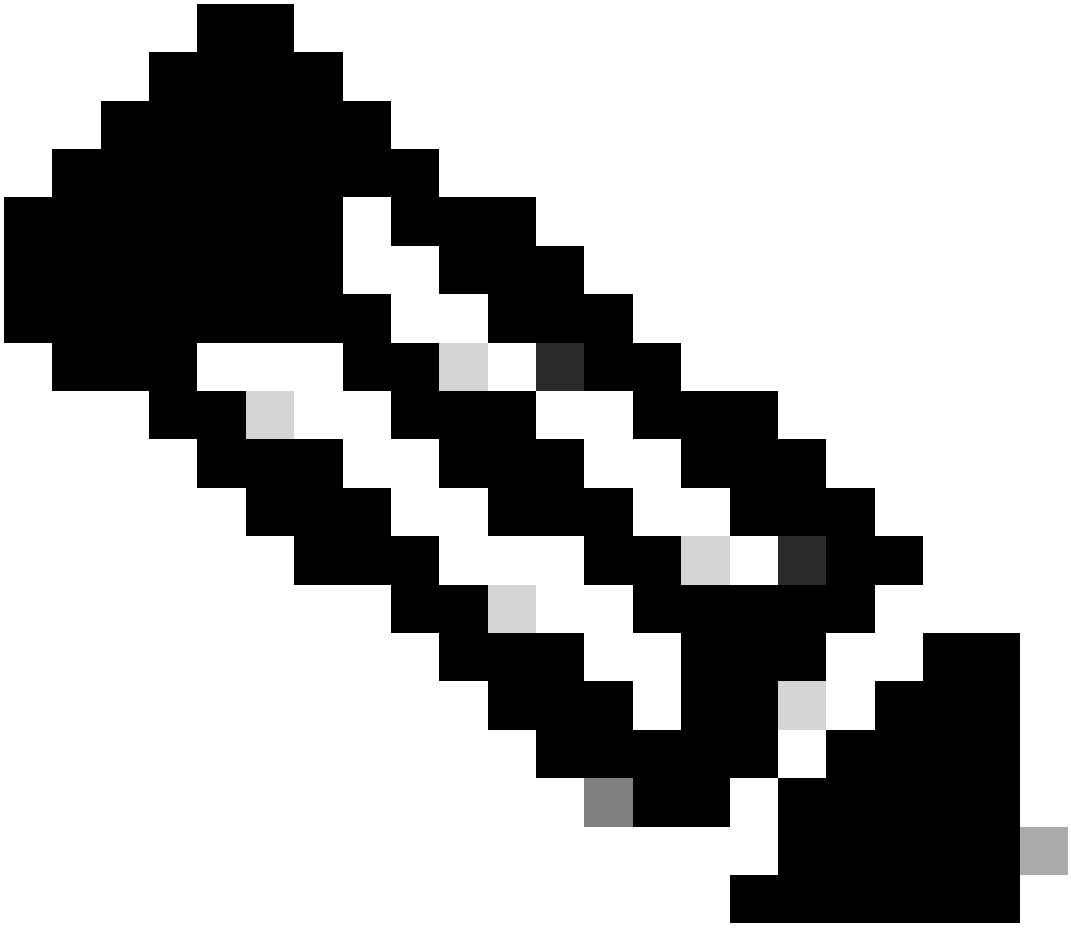
```
}}": "{{
```

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
```



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 aus, **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** um die ansible Aufgabe abzuspielen. In diesem Beispiel lautet der Befehl ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

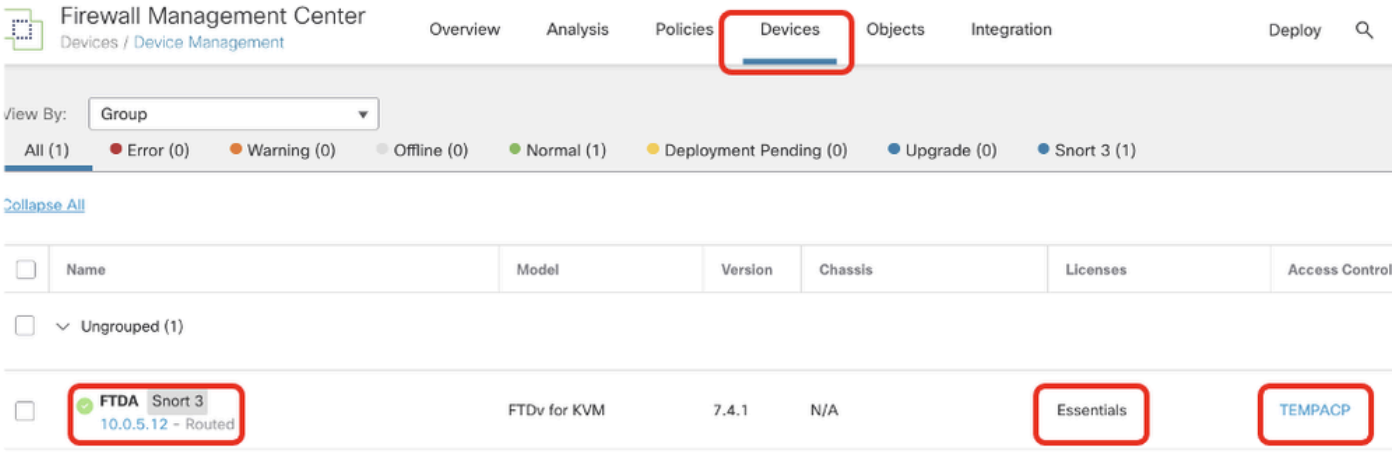
```
<#root>

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
```

Überprüfung

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

FMC-GUI anmelden Navigieren Sie zu **Devices (Geräte) > Device Management (Geräteverwaltung),** das FTD wurde erfolgreich auf dem FMC mit konfigurierter Zugriffskontrollrichtlinie registriert.



Seite für Gerätemanagement

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.

<#root>

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

-vvv

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.