# FTDをオンボードするためのAnsibleを使用したFMCの設定

## 内容



## はじめに

このドキュメントでは、Ansibleを使用してFirepower Management Center(FMC)へのFirepower Threat Defense(FTD)の登録を自動化する手順について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- アンサブル
- Ubuntuサーバ
- Cisco Firepower Management Center(FMC)仮想
- Cisco Firepower Threat Defense(FTD)仮想

このラボ環境では、AnsibleはUbuntuに導入されています。

この記事で参照されているAnsibleコマンドを実行するために、Ansibleがサポートするすべてのプラットフォームに Ansibleが正常にインストールされていることを確認する必要があります。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Ubuntuサーバ22.04

- Ansible 2.10.8
- Python 3.10
- Cisco Firepower Threat Defense(FTD)仮想7.4.1
- Cisco Firepower Management Center(FMC)仮想7.4.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

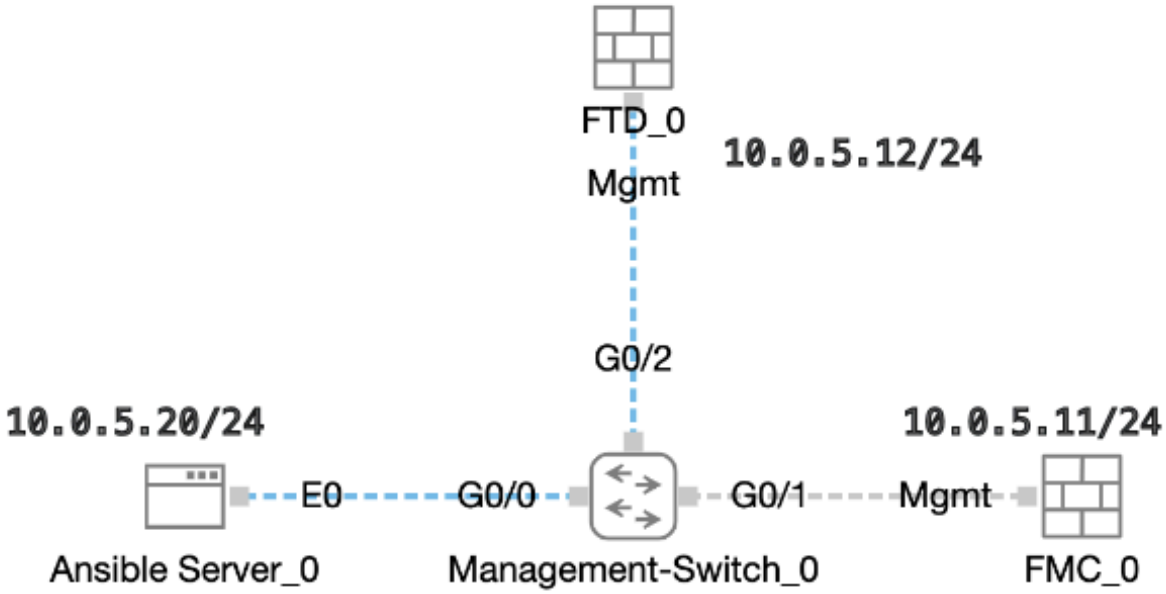
# 背景説明

Ansibleは汎用性の高いツールで、ネットワークデバイスの管理において大きな効果を発揮します。Ansibleを使用して自動化されたタスクを実行するには、さまざまな方法を使用できます。この文書で使用されている方法は、テスト目的の参照用として使用できます。

この例では、仮想FTDのオンボーディングに成功した後、基本ライセンス、ルーテッドモード、機能階層FTDv30、およびFMCに送信するログが有効なデフォルトのpermitアクションがあるアクセスコントロールポリシーが使用されます。

# 設定

## ネットワーク図




トポロジ

## コンフィギュレーション

シスコはサンプルスクリプトまたはお客様が作成したスクリプトをサポートしていないため、お

客様の二ーズに応じてテストできる例がいくつかあります。

予備検証が正式に完了したことを確認することが不可欠です。

- Ansibleサーバはインターネット接続を備えています。
- Ansibleサーバは、FMC GUIポート（FMC GUIのデフォルトポートは443）と正常に通信できます。
- FTDに正しいマネージャIPアドレス、登録キー、およびnat-idが設定されている。
- スマートライセンスでFMCが正常に有効化されます。

ステップ 1： SSHまたはコンソールを使用してAnsibleサーバのCLIに接続します。

ステップ 2：コマンドansible-galaxy collection install cisco.fmcansibleを実行して、AnsibleサーバにFMCのAnsibleコレクションをインストールします。

<#root>

cisco@inserthostname-here:~$

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

ステップ 3：コマンドmkdir /home/cisco/fmc_ansibleを実行して、関連ファイルを保存する新しいフォルダを作成します。この例では、ホームディレクトリは/home/cisco/で、新しいフォルダ名はfmc_ansibleです。

<#root>

cisco@inserthostname-here:~$

**mkdir /home/cisco/fmc_ansible**

ステップ 4： /home/cisco/fmc_ansibleフォルダに移動し、インベントリファイルを作成します。この例では、インベントリファイルの名前はinventory.iniです。

<#root>

cisco@inserthostname-here:~$

**cd /home/cisco/fmc_ansible/**

ccisco@inserthostname-here:~/fmc_ansible$

**ls**

**inventory.ini**

次の内容を複製して利用できるように貼り付け、正確なパラメータで**強調表示**されたセクションを変更できます。

<#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

ステップ 5： /home/cisco/fmc_ansibleフォルダに移動し、変数ファイルを作成します。この例では、変数のファイル名はfmc-onboard-ftd-vars.ymlです。

<#root>

cisco@inserthostname-here:~$

**cd /home/cisco/fmc_ansible/**

ccisco@inserthostname-here:~/fmc_ansible$

**ls**

**fmc-onboard-ftd-vars.yml**

inventory.ini

次の内容を複製して利用できるように貼り付け、正確なパラメータで**強調表示**されたセクションを変更できます。

<#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**

'

ステップ6:/home/cisco/fmc_ansibleフォルダに移動し、プレイブックファイルを作成します。この例では、プレイブックのファイル名はfmc-onboard-ftd-playbook.yamlです。

<#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

次の内容を複製して利用できるように貼り付け、正確なパラメータで**強調表示**されたセクションを変更できます。

<#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**

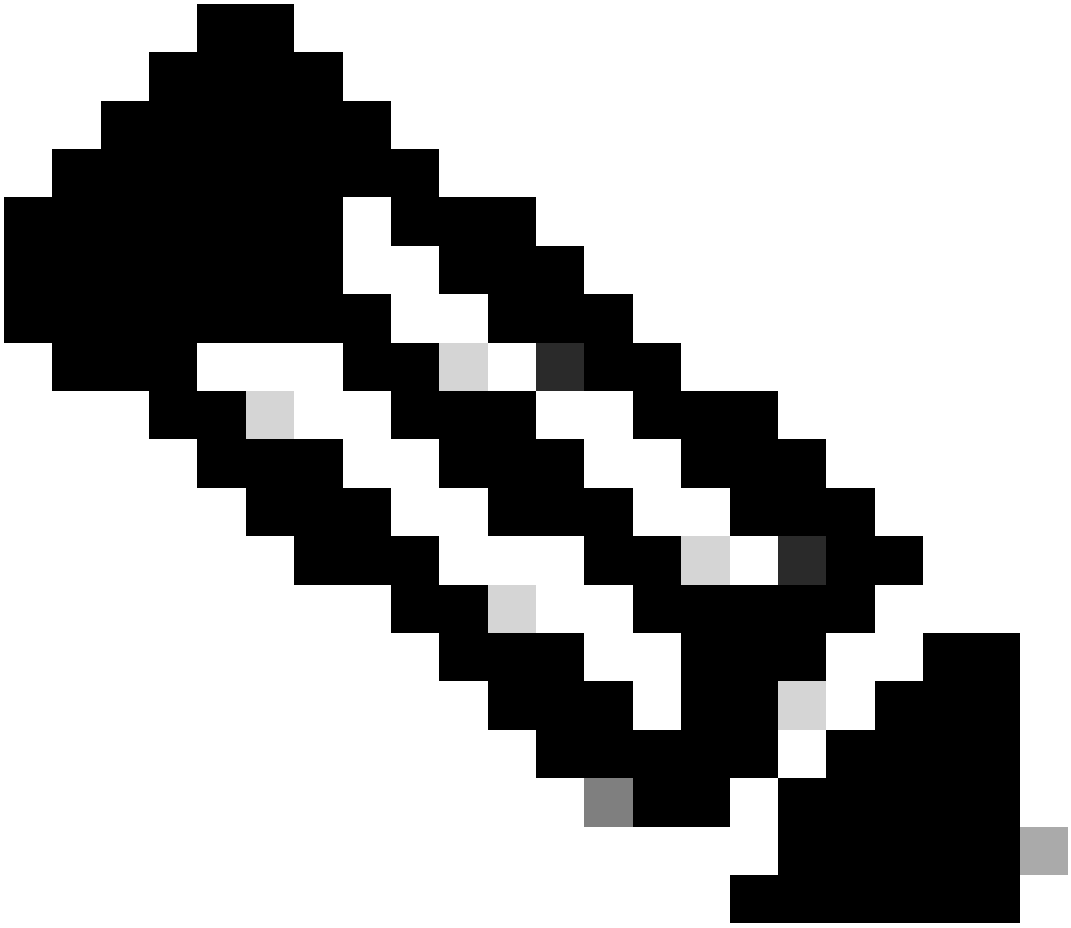
```
}}": "{{
```

**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
```



**注**：このプレイブック例で強調表示されている名前は、変数として機能します。これらの変数に対応する値は、変数ファイル内に保存されます。

---

手順 7： /home/cisco/fmc_ansibleフォルダに移動し、ansibleタスクを再生する **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** ためにコマンドを実行します。この例では、コマンドはansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" です。

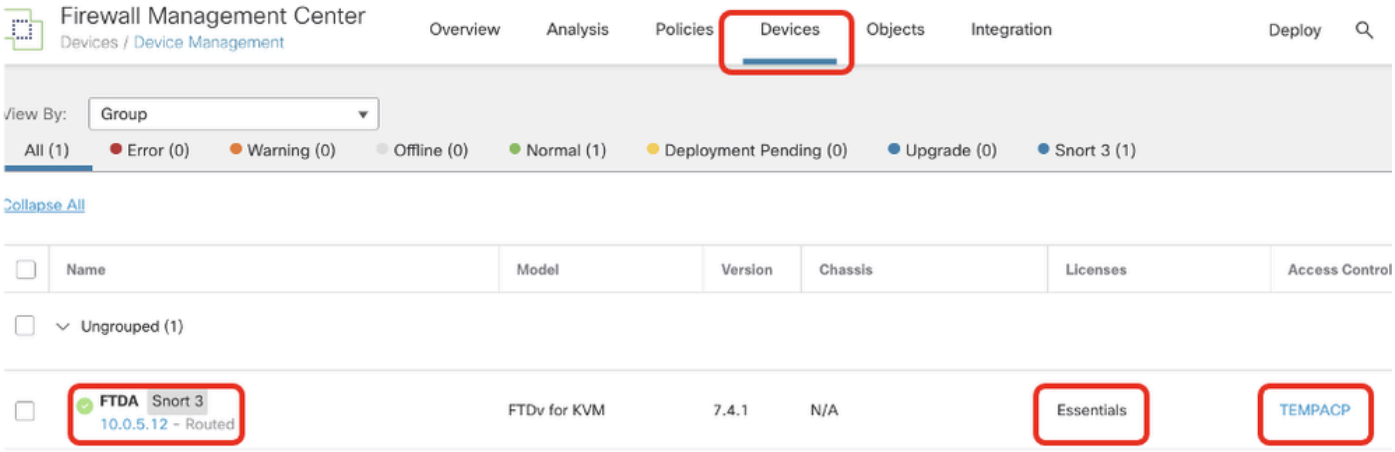
```
<#root>

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
```

## 確認

このセクションでは、設定が正常に動作していることを確認します。

FMC GUIにログインします。**Devices > Device Management, the FTD registered successfully on FMC with configured access control policy**の順に移動します。




デバイス管理ページ

## トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

Ansible Playbookのログをさらに表示するには、-vvvを使用してAnsible Playbookを実行します。

**<#root>**

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

**-vvv**

## 関連情報

[Cisco Devnet FMCアンサブル]

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。