Configuration de FMC avec FTD Ansible to Onboard

Table des matières

Introduction

Ce document décrit les étapes permettant d'automatiser l'enregistrement de Firepower Threat Defense (FTD) auprès de Firepower Management Center (FMC) avec Ansible.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Ansible
- Serveur Ubuntu
- Cisco Firepower Management Center (FMC) virtuel
- Cisco Firepower Threat Defense (FTD) virtuel

Dans le cadre de cette situation de laboratoire, Ansible est déployé sur Ubuntu.

Il est essentiel de s'assurer que Ansible est correctement installé sur toute plate-forme prise en charge par Ansible pour exécuter les commandes Ansible mentionnées dans cet article.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur Ubuntu 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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

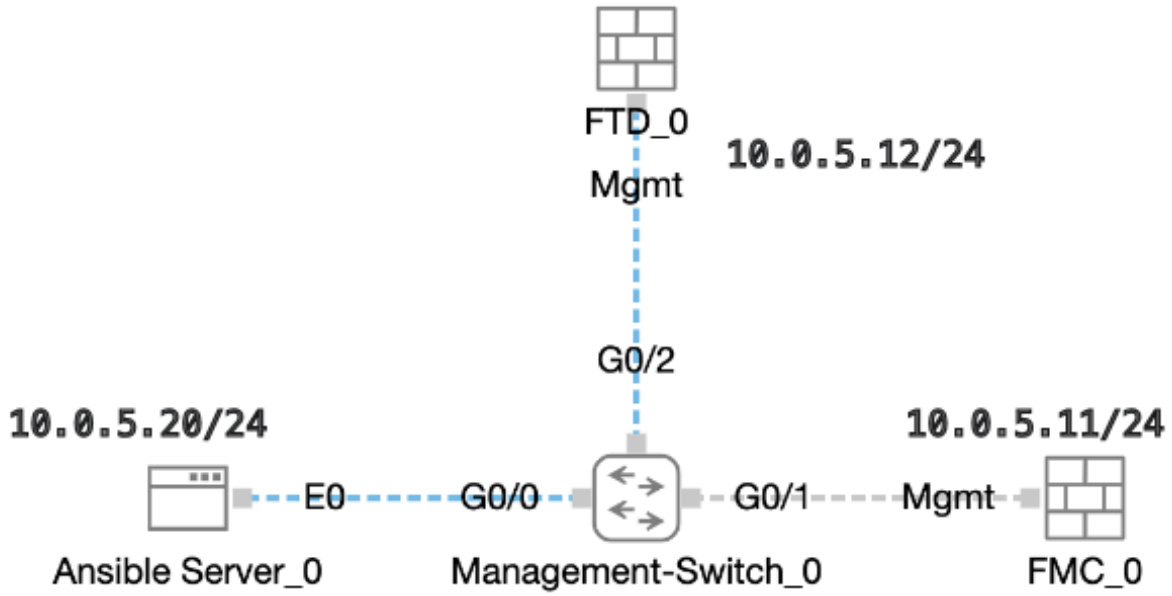
Informations générales

Ansible est un outil très polyvalent, qui démontre une efficacité significative dans la gestion des périphériques réseau. De nombreuses méthodologies peuvent être utilisées pour exécuter des tâches automatisées avec Ansible. La méthode utilisée dans cet article sert de référence aux fins de l'essai.

Dans cet exemple, après avoir intégré avec succès le FTD virtuel, c'est avec la licence de base, le mode routé, le niveau de fonctionnalité FTDv30 et la politique de contrôle d'accès qui est avec l'action d'autorisation par défaut avec l'envoi de journal activé au FMC.

Configurer

Diagramme du réseau



Topologie

Configurations

Étant donné que Cisco ne prend pas en charge les scripts d'exemple ou les scripts écrits par le client, nous avons quelques exemples que vous pouvez tester en fonction de vos besoins.

Il est essentiel de veiller à ce que la vérification préliminaire ait été dûment effectuée.

- Le serveur Ansible possède une connectivité Internet.
- Le serveur Ansible est capable de communiquer avec le port de l'interface graphique FMC (le port par défaut de l'interface graphique FMC est 443).
- Le FTD est configuré avec l'adresse IP du gestionnaire, la clé d'enregistrement et l'ID NAT corrects.
- Le FMC est activé avec la licence Smart.

Étape 1. Connectez-vous à la CLI du serveur Ansible via SSH ou la console.

Étape 2. Exécutez la commandeansible-galaxy collection install cisco.fmcansible afin d'installer la collection Ansible de FMC sur votre serveur Ansible.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Étape 3. Exécutez la commandemkdir /home/cisco/fmc_ansible afin de créer un nouveau dossier pour stocker les fichiers associés. Dans cet exemple, le répertoire de base est /home/cisco/, le nouveau nom de dossier est fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Étape 4. Accédez au dossier /home/cisco/fmc_ansible, create inventory file. Dans cet exemple, le nom du fichier d'inventaire est inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini
```

Vous pouvez dupliquer le contenu suivant et le coller pour l'utiliser, en modifiant les sections **mises en surbrillance** avec les paramètres précis.

<#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

Étape 5. Accédez au dossier /home/cisco/fmc_ansible, create variable file. Dans cet exemple, le nom de fichier de la variable est 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

Vous pouvez dupliquer le contenu suivant et le coller pour l'utiliser, en modifiant les sections **mises en surbrillance** avec les paramètres précis.

<#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

'

Étape 6. Accédez au dossier /home/cisco/fmc_ansible, créez un fichier de manuel. Dans cet exemple, le nom du fichier du playbook est 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

Vous pouvez dupliquer le contenu suivant et le coller pour l'utiliser, en modifiant les sections **mises en surbrillance** avec les paramètres précis.

<#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

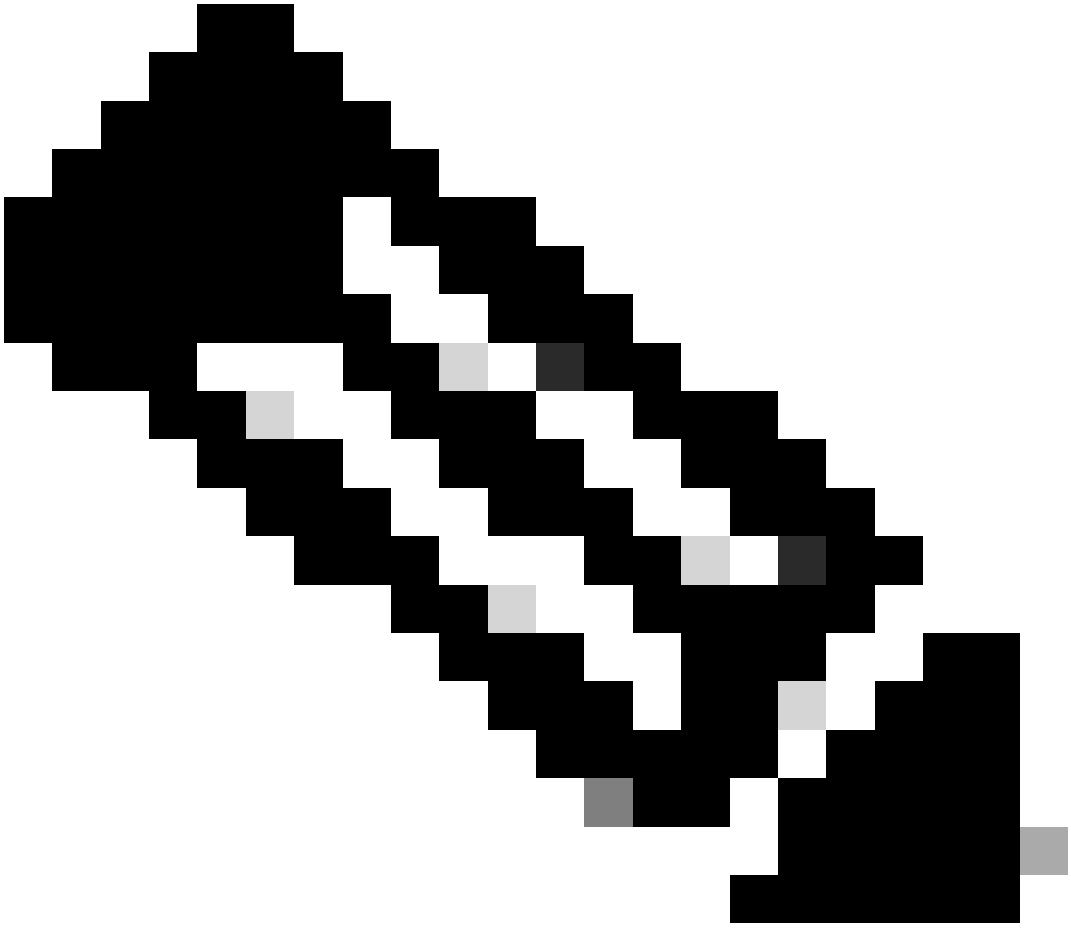
```
}}": "{{
```

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
```



Remarque : les noms mis en surbrillance dans cet exemple de guide de vente servent de variables. Les valeurs correspondantes de ces variables sont conservées dans le fichier de variables.

Étape 7. Accédez au dossier /home/cisco/fmc_ansible, run command **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** afin de lire la tâche ansible. Dans cet exemple, la commande est ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

<#root>

cisco@inserthostname-here:~$

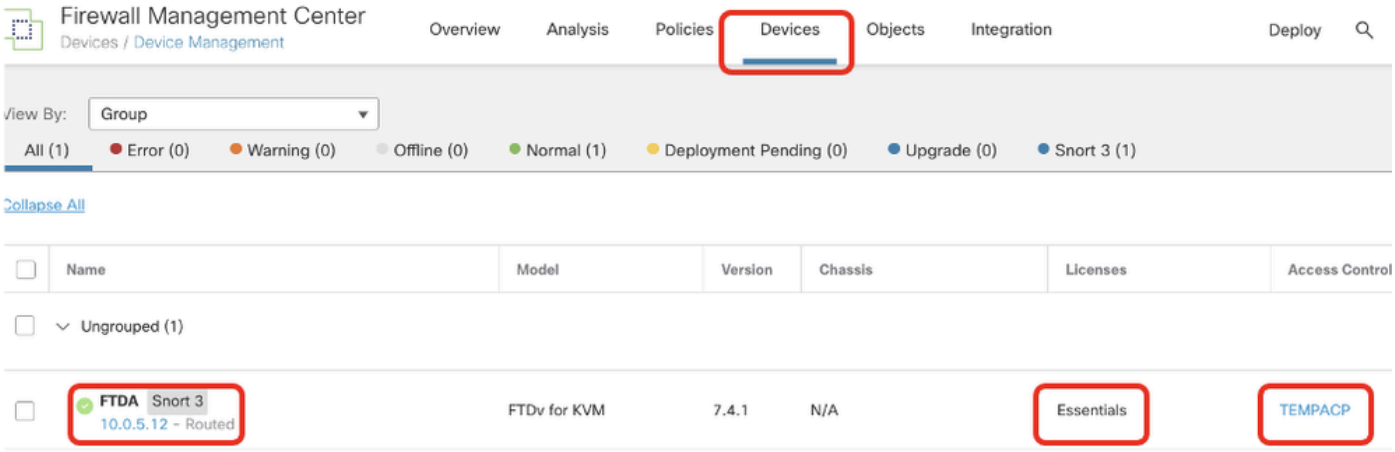
cd /home/cisco/fmc_ansible/

```
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
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Connectez-vous à FMC GUI. Accédez à **Périphériques > Gestion des périphériques,** le FTD enregistré avec succès sur FMC avec la stratégie de contrôle d'accès configurée.



Page Device Management

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de voir plus de journaux de playbook ansible, vous pouvez exécuter le playbook ansible avec -vvv.

<#root>

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

-vvv

Informations connexes

[Cisco Devnet FMC Ansible]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.