使用Ansible配置FMC到板載FTD

目錄

簡介

本文檔介紹向Ansible的Firepower管理中心(FMC)自動註冊Firepower威脅防禦(FTD)的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- 阿尼塞
- Ubuntu伺服器
- Cisco Firepower管理中心(FMC)虛擬
- Cisco Firepower威脅防禦(FTD)虛擬

在這種實驗室情況下，Ansible被部署在Ubuntu。

必須確保Ansible成功安裝在Ansible支援的任何平台上，以便運行本文中引用的Ansible命令。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Ubuntu伺服器22.04
- 阿尼塞2.10.8
- Python 3.10
- Cisco Firepower威脅防禦虛擬7.4.1
- Cisco Firepower管理中心虛擬7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

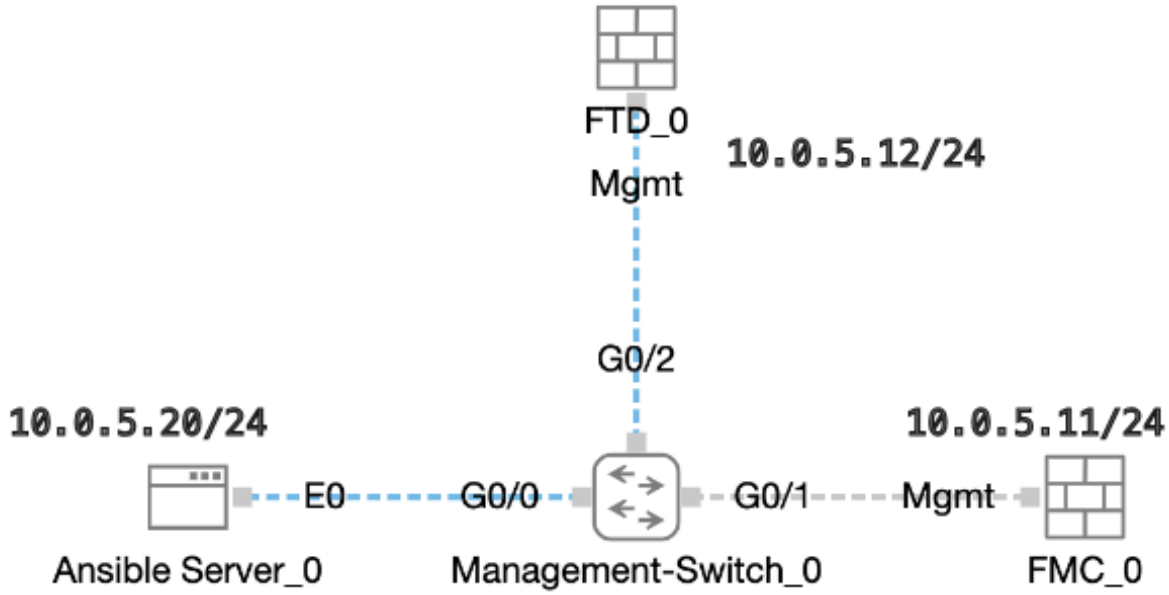
背景資訊

Ansible是一個功能非常豐富的工具，在管理網路裝置方面展現了極大的效率。使用Ansible可以採用多種方法來運行自動化任務。本文所採用的方法為試驗提供了參考。

在本範例中，成功載入虛擬FTD後，系統會使用基本授權、路由模式、功能層FTDv30，以及存取控制原則（具有預設的允許動作，且已啟用記錄傳送至FMC）。

設定

網路圖表



拓撲

組態

由於Cisco不支援示例指令碼或客戶編寫的指令碼，我們提供了一些可根據您的需求進行測試的示例。

必須確保適當完成初步核查。

- Ansible伺服器具有internet連線。
- Ansible伺服器能夠與FMC GUI埠成功通訊（FMC GUI的預設埠是443）。
- FTD設定有正確的管理員ip位址、註冊金鑰和nat-id。
- FMC已成功啟用智慧許可證。

步驟 1. 透過SSH或控制檯連線到Ansible伺服器的CLI。

步驟 2.運行命令ansible-galaxy collection install cisco.fmcansible以在Ansible伺服器上安裝FMC的Ansible集合。

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

步驟 3.運行命令mkdir /home/cisco/fmc_ansible以建立一個新資料夾來儲存相關檔案。在本示例中，主目錄是/home/cisco/ ，新資料夾名稱為fmc_ansible。

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

步驟 4. 導航到資料夾/home/cisco/fmc_ansible，建立資產檔案。在本示例中，資產檔名為inventory.ini。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

您可以複製以下內容並貼上以供使用，從而使用準確引數更改突出顯示的部分。

<#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

步驟 5. 導航到資料夾/home/cisco/fmc_ansible，建立變數檔案。在本示例中，變數檔名是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

您可以複製以下內容並貼上以供使用，從而使用準確引數更改突出顯示的部分。

<#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

'

第6步：導航到資料夾/home/cisco/fmc_ansible，建立攻略檔案。在本示例中，手冊檔名為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

您可以複製以下內容並貼上以供使用，從而使用準確引數更改突出顯示的部分。

<#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

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

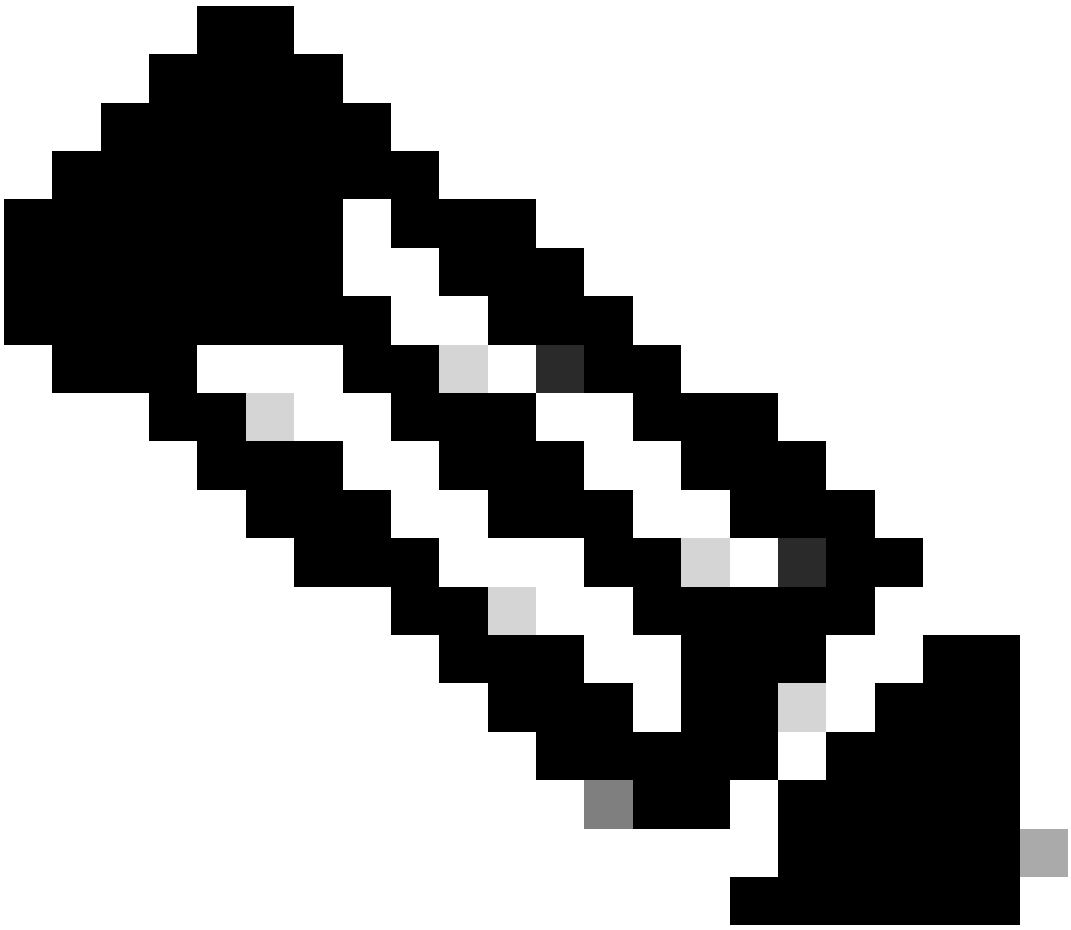
device_name.ftd1

```
}}"

 - 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
```



注意：在此範例手冊中反白的名稱會作為變數。這些變數的對應值會保留在變數檔案中。

步驟 7. 導航到資料夾/home/cisco/fmc_ansible，運行命令 **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** 以播放ansible任務。在本示例中，命令是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"

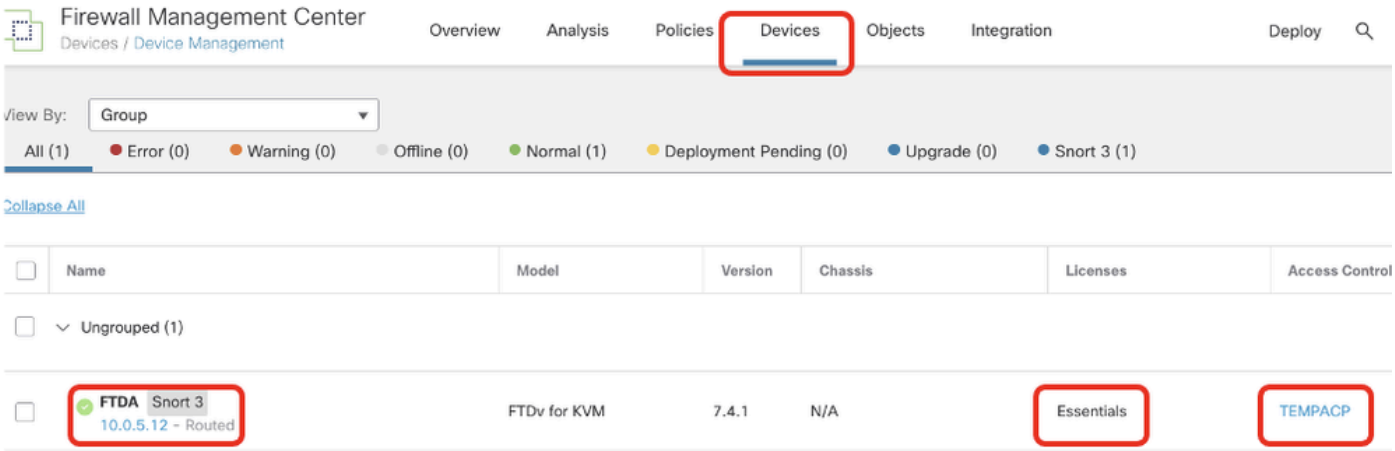
```
PLAY [FMC Onboard FTD] *********************************************************************************

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
```

驗證

使用本節內容，確認您的組態是否正常運作。

登入FMC GUI。導覽至**Devices** > **Device Management**，FTD已在FMC上成功註冊，且已設定存取控制原則。



裝置管理頁面

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

若要檢視更多有關ansible實戰手冊的記錄，您可以使用-vvv執行ansible實戰手冊。

<#root>

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

-vvv

相關資訊

[Cisco Devnet FMC Ansible]

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。