使用Ansible配置FMC以板载FTD

目录

简介

本文档介绍使用Ansible自动向Firepower管理中心(FMC)注册Firepower威胁防御(FTD)的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Ansible
- Ubuntu服务器
- Cisco Firepower管理中心(FMC)虚拟
- Cisco Firepower威胁防御(FTD)虚拟

在这种实验室情况下，Ansible被部署在Ubuntu上。

必须确保Ansible成功安装在Ansible支持的任何平台上，才能运行本文中引用的Ansible命令。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Ubuntu服务器22.04
- Ansible 2.10.8
- Python 3.10
- 思科Firepower威胁防御虚拟7.4.1
- 思科Firepower管理中心虚拟7.4.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

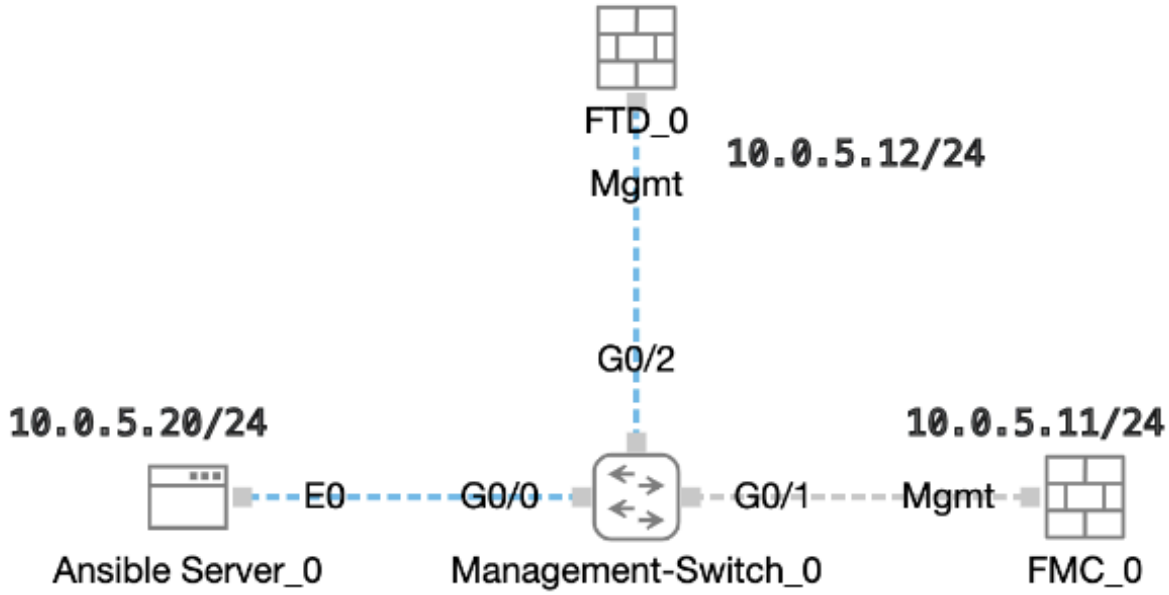
背景信息

Ansible是一个功能非常全面的工具，在管理网络设备时显示了显著的功效。通过Ansible，可以采用多种方法运行自动化任务。本文所采用的方法为试验提供了参考。

在本示例中，在成功加入虚拟FTD后，它使用基本许可证、路由模式、功能层FTDv30，以及访问控制策略，该策略使用默认允许操作，并且已启用日志发送到FMC。

配置

网络图



拓扑

配置

由于思科不支持示例脚本或客户编写的脚本，我们提供了一些您可以根据需要进行测试的示例。

必须确保适当完成初步核查。

- Ansible服务器具有Internet连接。
- Ansible服务器能够与FMC GUI端口成功通信（FMC GUI的默认端口为443）。
- FTD配置了正确的管理器ip地址、注册密钥和nat-id。
- FMC已成功启用智能许可证。

步骤1: 通过SSH或控制台连接到Ansible服务器的CLI。

第二步：运行命令ansible-galaxy collection install cisco.fmcansible以在Ansible服务器上安装FMC的Ansible集合。

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

第三步：运行命令mkdir /home/cisco/fmc_ansible以创建一个新文件夹来存储相关文件。在本示例中，主目录为/home/cisco/，新文件夹名称为fmc_ansible。

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

第四步： 导航到文件夹/home/cisco/fmc_ansible，创建资产文件。在本示例中，资产文件名为inventory.ini。

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

您可以复制以下内容并粘贴以供使用，以使用准确参数更改**突出**显示的部分。

<#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
```

第五步： 导航到文件夹/home/cisco/fmc_ansible，创建变量文件。在本示例中，变量文件名为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

您可以复制以下内容并粘贴以供使用，以使用准确参数更改**突出**显示的部分。

<#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：导航到文件夹/home/cisco/fmc_ansible，创建攻略文件。在本示例中，手册文件名为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

您可以复制以下内容并粘贴以供使用，以使用准确参数更改**突出**显示的部分。

<#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

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

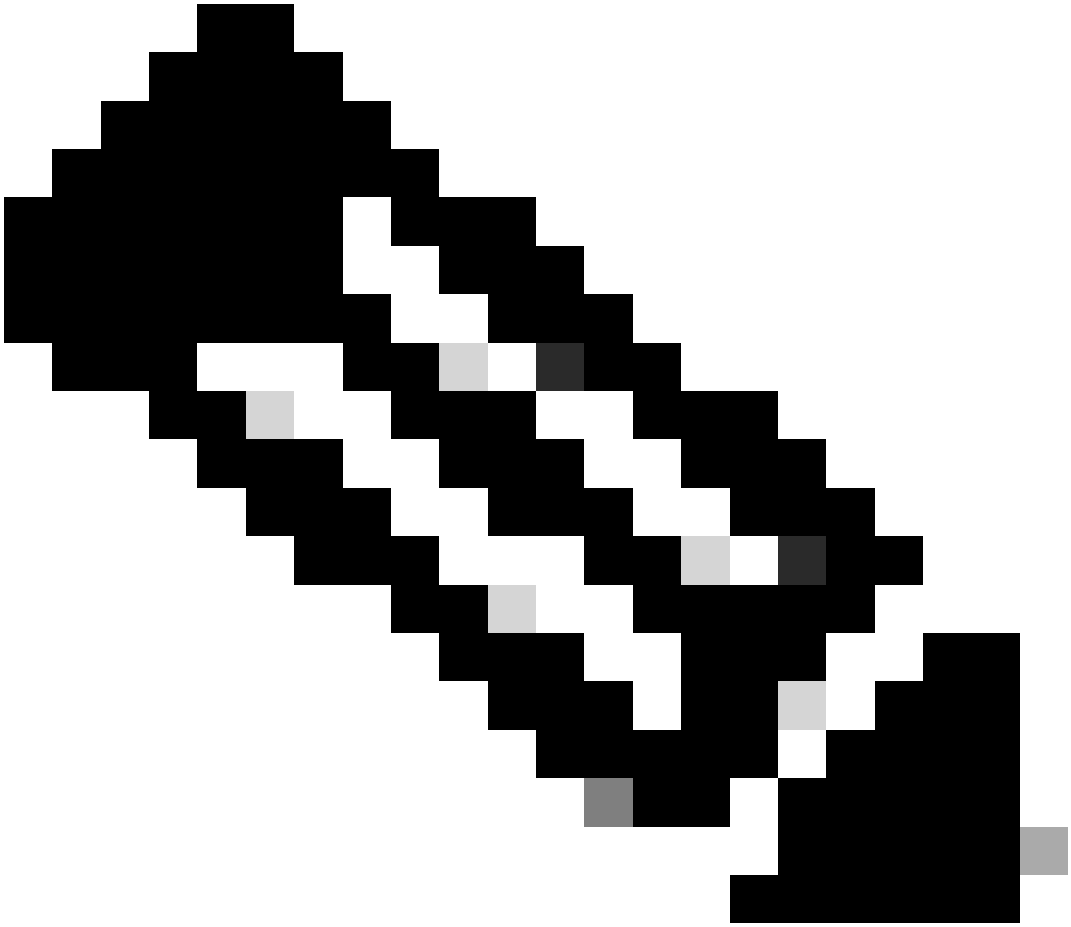
device_name.ftd1

```
}}"

 - 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：本示例手册中突出显示的名称用作变量。这些变量的对应值保留在变量文件中。

步骤 7. 导航到文件夹/home/cisco/fmc_ansible，run command **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** 以播放ansible任务。在本示例中，该命令是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"

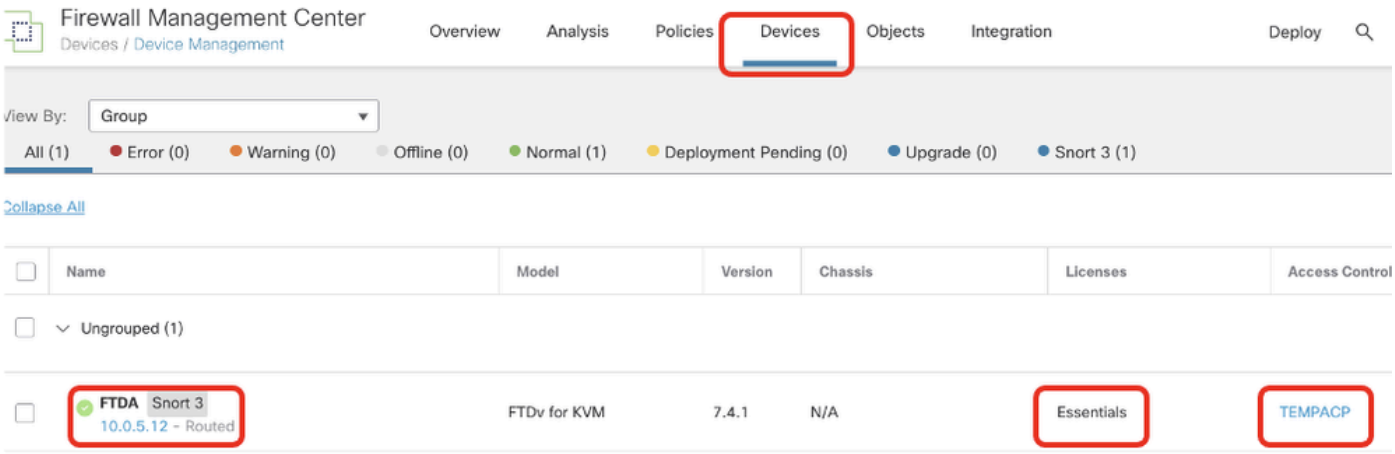
```
PLAY [FMC Onboard FTD] *********************************************************************************

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
```

验证

使用本部分可确认配置能否正常运行。

登录FMC GUI。导航到设备>设备管理，该FTD已使用配置的访问控制策略在FMC上成功注册。



“设备管理”(*Device Management*)页面

故障排除

本部分提供的信息可用于对配置进行故障排除。

要查看ansible攻略的更多日志，您可以使用-vvv运行ansible攻略。

<#root>

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

-vvv

相关信息

[Cisco Devnet FMC Ansible]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。