Configurar o FMC com Ansible para FTD a bordo

Contents

Introdução

Este documento descreve as etapas para automatizar o registro do Firepower Threat Defense (FTD) no Firepower Management Center (FMC) com o Ansible.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ansible
- Servidor Ubuntu
- Cisco Firepower Management Center (FMC) Virtual
- Cisco Firepower Threat Defense (FTD) Virtual

No contexto desta situação de laboratório, Ansible é implantado no Ubuntu.

É essencial garantir que o Ansible seja instalado com êxito em qualquer plataforma suportada pelo Ansible para executar os comandos Ansible referenciados neste artigo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor 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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

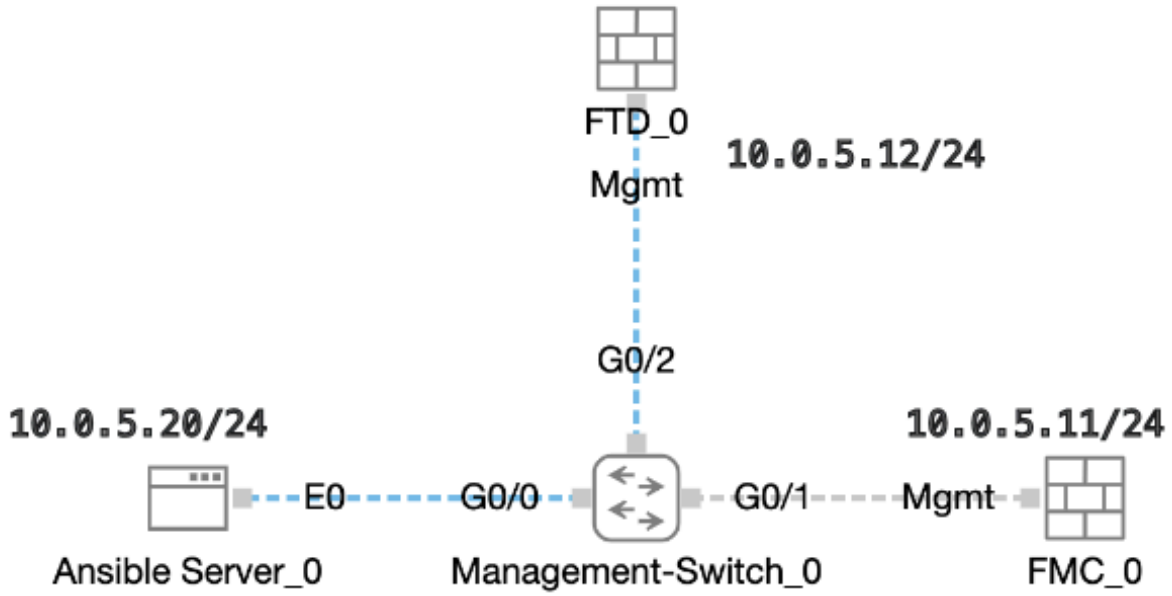
Informações de Apoio

O Ansible é uma ferramenta altamente versátil que demonstra uma eficiência significativa no gerenciamento de dispositivos de rede. Várias metodologias podem ser empregadas para executar tarefas automatizadas com a Ansible. O método utilizado neste artigo serve de referência para fins de teste.

Neste exemplo, após a integração bem-sucedida do FTD virtual, ele é com a licença básica, o modo roteado, o FTDv30 de camada de recursos e a política de controle de acesso, que é com a ação de permissão padrão com o envio de log habilitado para o FMC.

Configurar

Diagrama de Rede



Topologia

Configurações

Como a Cisco não oferece suporte a scripts de exemplo ou scripts escritos por clientes, temos alguns exemplos que você pode testar de acordo com suas necessidades.

É essencial assegurar que a verificação preliminar foi devidamente concluída.

- Um servidor possível possui conectividade com a Internet.
- Um servidor Ansible pode se comunicar com êxito com a porta GUI do FMC (a porta padrão da GUI do FMC é 443).
- O FTD é configurado com o endereço ip correto do gerente, a chave de registro e o nat-id.
- O FMC foi habilitado com êxito com a Smart License.

Etapa 1. Conecte-se ao CLI do servidor Ansible via SSH ou console.

Etapa 2. Execute o comandoansible-galaxy collection install cisco.fmcansible para instalar a coleção Ansible do FMC em seu servidor Ansible.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Etapa 3. Execute o comandomkdir /home/cisco/fmc_ansible para criar uma nova pasta para armazenar os arquivos relacionados. Neste exemplo, o diretório inicial é /home/cisco/, o nome da nova pasta é fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Etapa 4. Navegue até a pasta /home/cisco/fmc_ansible, crie o arquivo de inventário. Neste exemplo, o nome do arquivo de inventário é inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini
```

Você pode duplicar o conteúdo a seguir e colá-lo para utilização, alterando as seções **destacadas** com os parâmetros precisos.

<#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
```

Etapa 5. Navegue até a pasta /home/cisco/fmc_ansible, criar arquivo de variável. Neste exemplo, o nome do arquivo de variável é 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
```

Você pode duplicar o conteúdo a seguir e colá-lo para utilização, alterando as seções **destacadas** com os parâmetros precisos.

<#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

'

Etapa 6.Navegue até a pasta /home/cisco/fmc_ansible, crie o arquivo de manual de atividades. Neste exemplo, o nome do arquivo de playbook é 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

Você pode duplicar o conteúdo a seguir e colá-lo para utilização, alterando as seções **destacadas** com os parâmetros precisos.

<#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

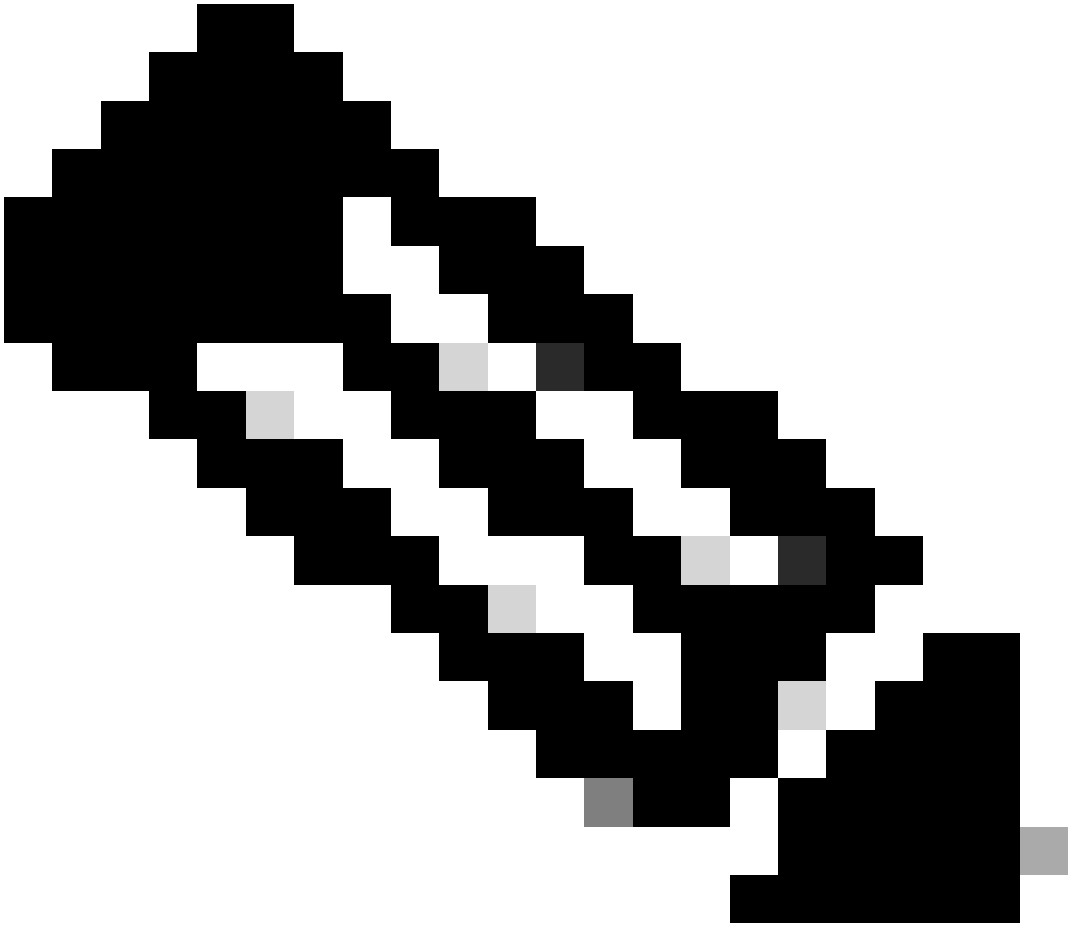
```
}}": "{{
```

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
```



Observação: os nomes destacados neste manual de atividades de exemplo servem como variáveis. Os valores correspondentes para essas variáveis são preservados no arquivo de variáveis.

Passo 7. Navegue até a pasta /home/cisco/fmc_ansible, execute o comando **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** para reproduzir a tarefa analisável. Neste exemplo, o comando é ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

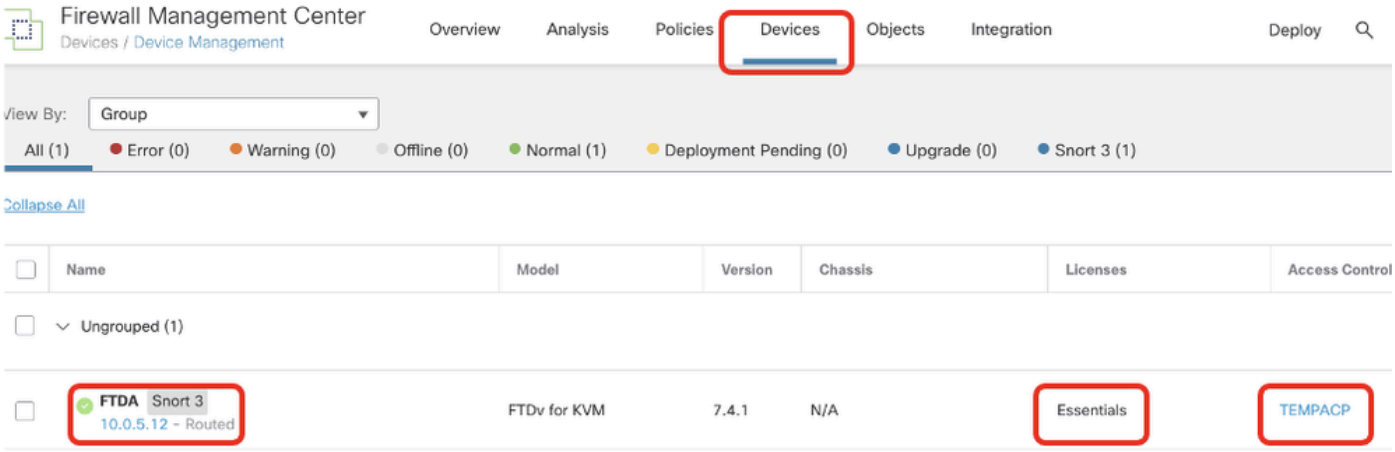
```
<#root>

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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Faça login na GUI do FMC. Navegue até **Devices > Device Management,** o FTD foi registrado com êxito no FMC com a política de controle de acesso configurada.



Página Gerenciamento de Dispositivos

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para ver mais registros de um manual de atividades possível, você pode executar um manual de atividades com o - vvv.

<#root>

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

-vvv

Informações Relacionadas

[Cisco Devnet FMC Ansible]

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.