Configurazione di FMC con FTD "andibile su bordo"

Sommario

Introduzione

In questo documento viene descritto come automatizzare la registrazione di Firepower Threat Defense (FTD) in Firepower Management Center (FMC) con Ansible.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Ansioso
- Server Ubuntu
- Virtual Cisco Firepower Management Center (FMC)
- Virtual Cisco Firepower Threat Defense (FTD)

Nel contesto di questa situazione di laboratorio, Ansible è schierato su Ubuntu.

È essenziale assicurarsi che Ansible sia installato correttamente su qualsiasi piattaforma supportata da Ansible per l'esecuzione dei comandi Ansible a cui si fa riferimento in questo articolo.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Ubuntu Server 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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

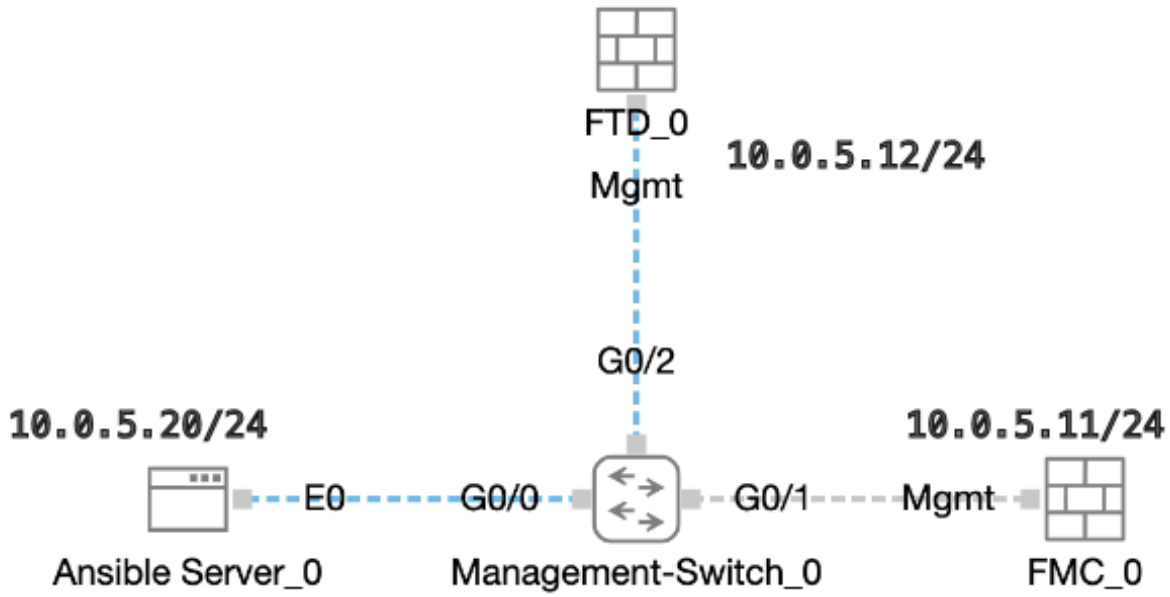
Premesse

Ansible è uno strumento estremamente versatile che dimostra una notevole efficacia nella gestione dei dispositivi di rete. Numerose metodologie possono essere impiegate per eseguire operazioni automatizzate con Ansible. Il metodo utilizzato in questo articolo serve da riferimento ai fini della prova.

In questo esempio, dopo aver caricato correttamente l'FTD virtuale è con licenza di base, modalità instradata, FTDv30 livello funzionalità e i criteri di controllo dell'accesso che sono con l'azione di permesso predefinita con log abilitato invio a FMC.

Configurazione

Esempio di rete



Topologia

Configurazioni

Poiché Cisco non supporta gli script di esempio o quelli scritti dal cliente, sono disponibili alcuni esempi che è possibile verificare in base alle esigenze.

È essenziale garantire che la verifica preliminare sia stata debitamente completata.

- Il server ansibile dispone di connettività Internet.
- Ansible Server è in grado di comunicare con la porta GUI FMC (la porta predefinita per l'interfaccia GUI FMC è 443).
- L'FTD è configurato con l'indirizzo IP corretto del manager, la chiave del registro e il nat-id.
- FMC è stato abilitato con la licenza intelligente.

Passaggio 1. Connettersi alla CLI del server Ansible tramite SSH o console.

Passaggio 2. Eseguire il comando ansible-galaxy collection install cisco.fmcansible per installare la raccolta Ansible di FMC nel server Ansible.

```
<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible
```

Passaggio 3. Eseguire il comando mkdir /home/cisco/fmc_ansible per creare una nuova cartella in cui archiviare i file correlati. In questo esempio, la home directory è /home/cisco/, il nome della nuova cartella è fmc_ansible.

```
<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible
```

Passaggio 4. Passare alla cartella /home/cisco/fmc_ansible, Crea file di inventario. In questo esempio, il nome del file di inventario è inventory.ini.

```
<#root>

cisco@inserthostname-here:~$

 cd /home/cisco/fmc_ansible/


ccisco@inserthostname-here:~/fmc_ansible$

ls
```

inventory.ini

Potete duplicare il seguente contenuto e incollarlo per l'utilizzo, modificando le sezioni **evidenziate** con i parametri accurati.

<#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

Passaggio 5. Passare alla cartella /home/cisco/fmc_ansible, create variable file. In questo esempio, il nome del file della variabile è 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

Potete duplicare il seguente contenuto e incollarlo per l'utilizzo, modificando le sezioni **evidenziate** con i parametri accurati.

<#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

'

Passaggio 6.Passare alla cartella /home/cisco/fmc_ansible, creare il file della playbook. In questo esempio, il nome del file del playbook è 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

Potete duplicare il seguente contenuto e incollarlo per l'utilizzo, modificando le sezioni **evidenziate** con i parametri accurati.

<#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

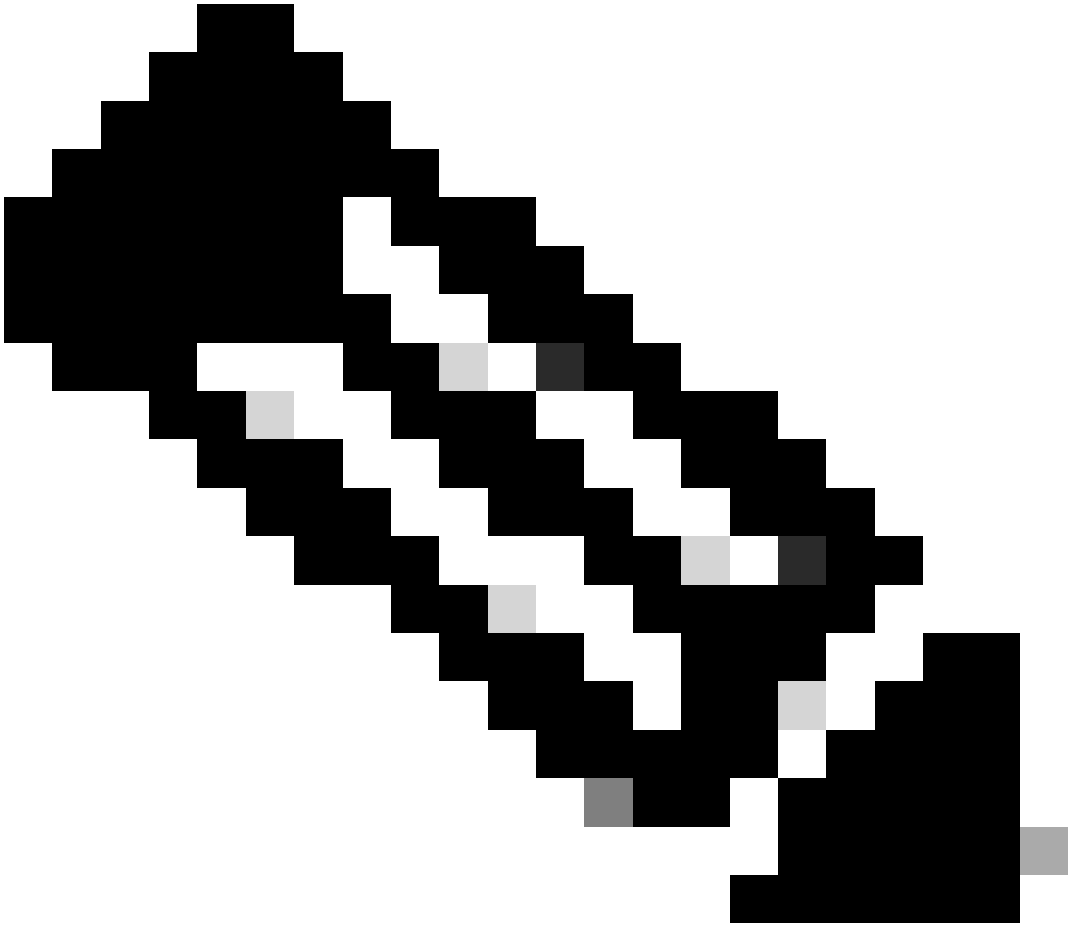
```
}}": "{{
```

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
```



Nota: i nomi evidenziati in questo esempio di playbook fungono da variabili. I valori corrispondenti per queste variabili vengono mantenuti nel file delle variabili.

Passaggio 7. Passare alla cartella /home/cisco/fmc_ansible, eseguire il comando **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** per eseguire l'attività andibile. Nell'esempio, il comando è ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

<#root>

cisco@inserthostname-here:~$

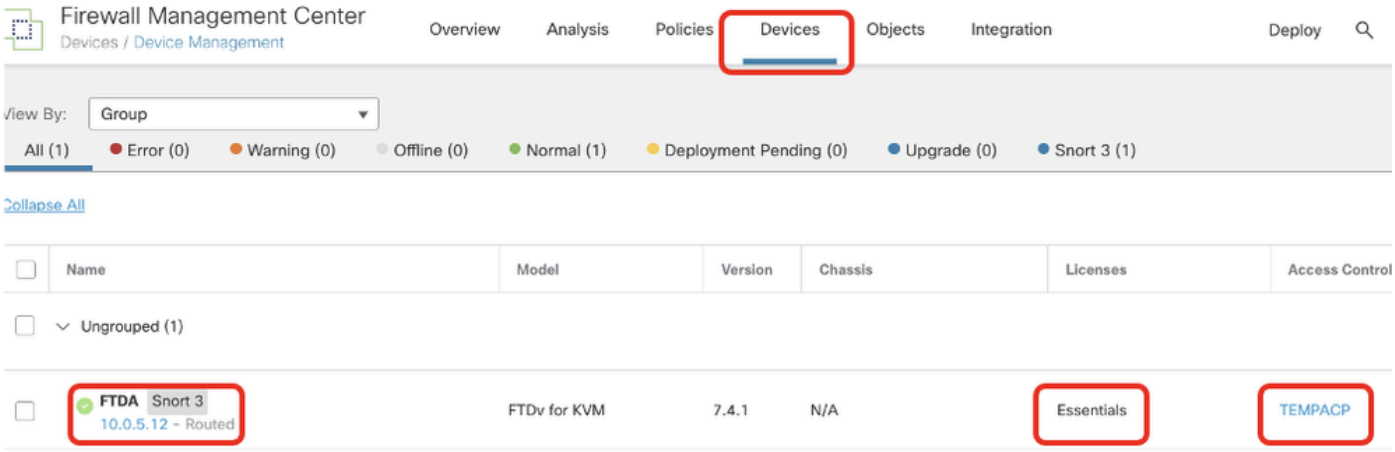
cd /home/cisco/fmc_ansible/

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Accedere all'interfaccia utente di FMC. Passare a **Dispositivi > Gestione dispositivi,** il FTD è stato registrato correttamente sul FMC con i criteri di controllo di accesso configurati.



Pagina Gestione dispositivi

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

Per visualizzare più registri di un playbook andibile, è possibile eseguire un playbook ansibile con -vv.

<#root>

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

-vvv

Informazioni correlate

[Cisco Devent FMC Ansible]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).