تكوين FMC باستخدام FTD مدمج قابل للتعديل

المحتويات

المقدمة

يوضح هذا المستند خطوات أتمتة تسجيل "الدفاع عن تهديد نظام التشغيل FirePOWER (FTD)" إلى مركز إدارة FirePOWER (FMC) باستخدام جهاز غير قابل للتعديل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- غير قابل
- خادم Ubuntu
- مركز إدارة FireSIGHT (FMC) الظاهري من Cisco
- الدفاع الظاهري ضد التهديد الناري (FTD) من Cisco

وفي سياق هذا الوضع المختبري، يتم نشر Ansible في أوبونتو.

من الضروري التأكد من أن Ansible قد تم تثبيتها بنجاح على أي نظام أساسي مدعوم من قبل Ansible لتشغيل الأوامر المنطقية المشار إليها في هذه المقالة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Ubuntu Server، الإصدار 22.04

- Ansible 2.10.8
- باي ثون 3,10
- Cisco Firepower Threat Defense Virtual 7.4.1
- Cisco Firepower Management Center Virtual 7.4.1

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

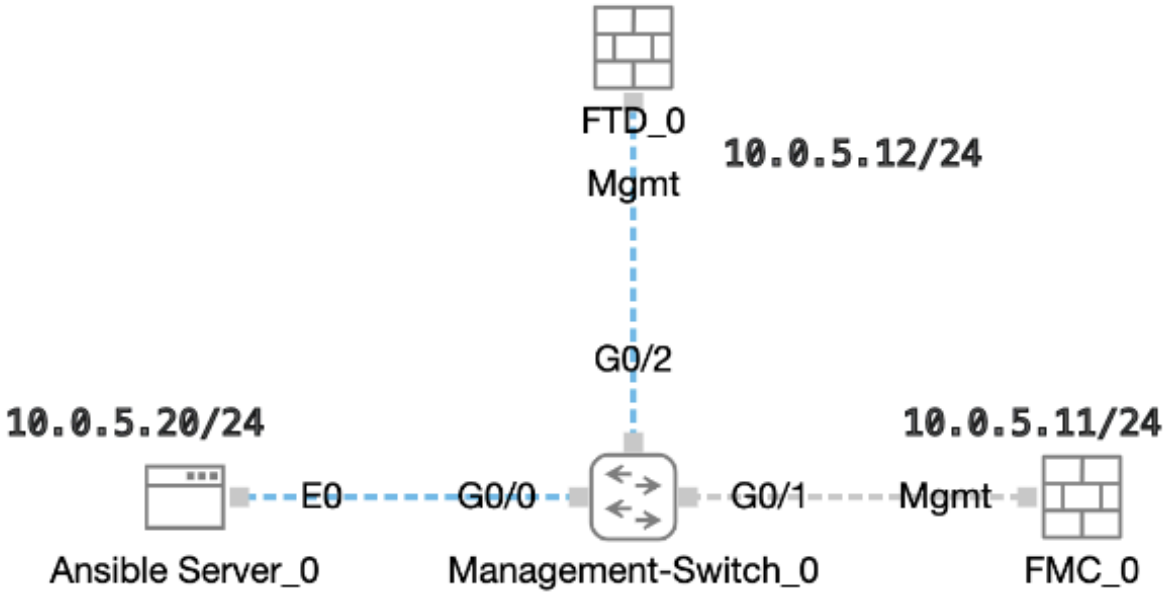
معلومات أساسية

Ansible عبارة عن أداة متعددة الاستخدامات بدرجة كبيرة، مما يظهر فعالية كبيرة في إدارة أجهزة الشبكة. يمكن إستخدام العديد من المنهجيات لتشغيل المهام المؤتمتة باستخدام برنامج Ansible. وتستخدم الطريقة المستخدمة في هذه المادة كمرجع لأغراض الاختبار.

في هذا المثال، بعد الانضمام بنجاح إلى برنامج FTD الظاهري، يكون مع الترخيص الأساسي والوضع الموجه وطبقة الميزات FTDv30 ونهج التحكم في الوصول الذي يكون مع إجراء السماح الافتراضي مع إرسال السجل الذي تم تمكينه إلى FMC.

التكوين

الرسم التخطيطي للشبكة



المخطط

التكوينات

نظرا لأن Cisco لا تدعم البرامج النصية للأمثلة أو البرامج النصية المكتوبة من قبل العميل، فلديانا بعض الأمثلة التي يمكنك إختبارها وفقا لاحتياجاتك.

ومن الضروري ضمان إنجاز التحقق الأولي على النحو الواجب.

- يتميز الخادم غير القابل للتوصيل بإمكانية الاتصال بالإنترنت.
- يتميز الخادم القابل للتشغيل بإمكانية الاتصال بنجاح بمنفذ واجهة المستخدم الرسومية (GUI) لـ FMC (المنفذ الافتراضي لواجهة المستخدم الرسومية (GUI) لـ FMC وهو 443).
- يتم تكوين FTD باستخدام عنوان IP للمدير الصحيح ومفتاح التسجيل ومعرف nat.
- يتم تمكين FMC مع الترخيص الذكي بنجاح.

الخطوة 1. قم بالاتصال بواجهة سطر الأوامر (CLI) الخاصة بالخادم الافتراضي عبر بروتوكول SSH أو وحدة التحكم.

الخطوة 2. قم بتشغيل الأمرansible-galaxy collection install cisco.fmcansible من أجل تثبيت مجموعة غير معقولة من المجموعات للتشغيل على الخادم غير القابل للتشغيل FMC.

<#root>

cisco@inserthostname-here:~$

ansible-galaxy collection install cisco.fmcansible

الخطوة 3. قم بتشغيل الأمر mkdir /home/cisco/fmc_ansibleلإنشاء مجلد جديد لتخزين الملفات ذات الصلة. في هذا المثال، الدليل الرئيسي هو /home/cisco/، واسم المجلد الجديد هو fmc_ansible.

<#root>

cisco@inserthostname-here:~$

mkdir /home/cisco/fmc_ansible

الخطوة 4. انتقل إلى المجلد /home/cisco/fmc_ansible، وقم بإنشاء ملف مخزون. في هذا المثال، اسم ملف المخزون هو inventory.ini.

<#root>

cisco@inserthostname-here:~$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible$

ls

inventory.ini

يمكنك مضاعفة المحتوى التالي وصقه للاستخدام، تعديل المقاطع المميزة بالمحددات الدقيقة.

<#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
```

الخطوة 5. انتقل إلى المجلد /home/cisco/fmc_ansible، وقم بإنشاء ملف متغير. في هذا المثال، اسم الملف المتغير هو 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

يمكنك مضاعفة المحتوى التالي وصقه للاستخدام، تعديل المقاطع المميزة بالمحددات الدقيقة.

<#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

'

الخطوة 6.انتقل إلى المجلد /home/cisco/fmc_ansible، قم بإنشاء ملف كتاب التشغيل. في هذا المثال، اسم ملف دفتر التشغيل هو 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

يمكنك مضاعفة المحتوى التالي ولصقه للاستخدام، تعديل المقاطع المميزة بالمحددات الدقيقة.

<#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

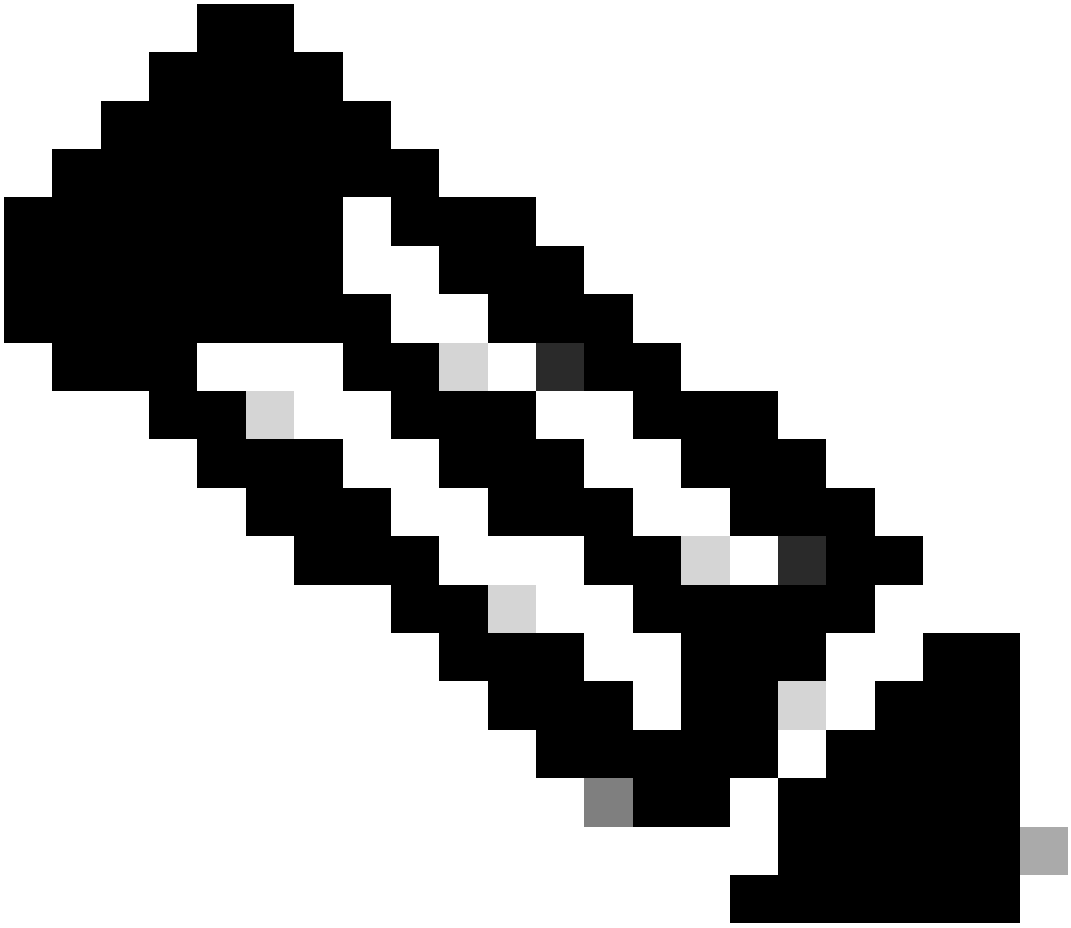
```
}}": "{{
```

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
```



ملاحظة: تخدم الأسماء المبرزة في هذا المثال كمتغيرات. يتم الحفاظ على القيم المرادفة لهذه المتغيرات ضمن ملف المتغير.

الخطوة 7. انتقل إلى المجلد /home/cisco/fmc_ansible، قم بتشغيل الأمر **ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@"<playbook_vars>.yml"** لتشغيل المهمة غير المحتملة. في هذا المثال، الأمر هو ansible-playbook -i inventory.ini fmc-onboard-ftd-playbook.yaml -e @"fmc-onboard-ftd-vars.yml" .

<#root>

cisco@inserthostname-here:~$

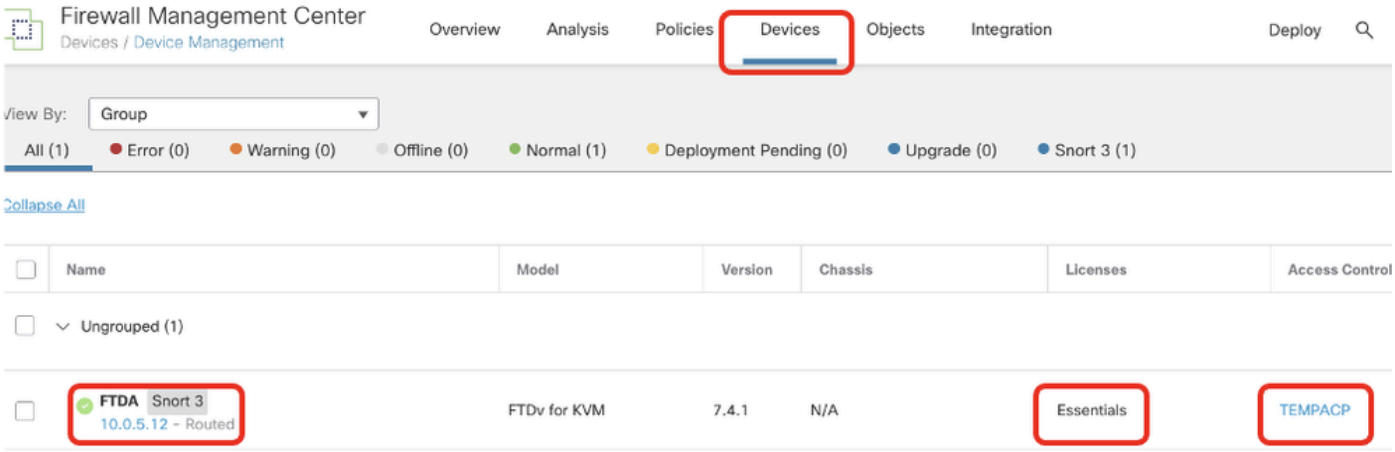
cd /home/cisco/fmc_ansible/

```
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
```

التحقق من الصحة

استخدم هذه القسم لتأكيد عمل التكوين بشكل صحيح.

سجل الدخول إلى واجهة المستخدم الرسومية (GUI) لوحدة التحكم FMC. انتقل إلى الأجهزة > إدارة الأجهزة، تم تسجيل FTD بنجاح على FMC باستخدام نهج التحكم في الوصول الذي تم تكوينه.



صفحة إدارة الأجهزة

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

لمشاهدة المزيد من سجلات كتاب التشغيل غير القابل للتشغيل، يمكنك تشغيل كتاب التشغيل غير القابل للتشغيل باستخدام -vvv.

<#root>

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

-vvv

معلومات ذات صلة

Cisco Devnet FMC Ansible

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).