

# ثيـدـحـتـ ةـيـنـاـلـمـ إـعـمـ FMCـ نـيـوـكـتـ IPـ

## تاـيـوـتـ حـمـلـاـ

[ةـمـدـقـمـلـاـ](#)

[ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ](#)

[تـابـلـطـتـمـلـاـ](#)

[ةـمـدـخـتـسـمـلـاـتـانـوـكـمـلـاـ](#)

[ةـيـسـاسـأـتـامـوـلـعـمـ](#)

[نـيـوـكـتـلـاـ](#)

[ةـلـبـشـلـلـيـطـيـطـخـتـلـاـمـسـرـلـاـ](#)

[تـانـيـوـكـتـلـاـ](#)

[ةـحـصـلـلـاـنـمـقـقـحـتـلـاـ](#)

[اهـالـصـاوـعـاطـخـأـلـاـفـاشـكـتـسـاـ](#)

[ةـلـصـتـاذـتـامـوـلـعـمـ](#)

## ةـمـدـقـمـلـاـ

IPـ ةـهـجـاوـ نـيـوـكـتـلـ (FMC)ـ ةـرـادـاـ زـكـرـمـ ةـتـمـتـأـلـ ةـمـزـالـلـاـ تـاـوـطـخـلـاـ دـنـتـسـمـلـاـ اـذـهـ فـصـيـ لـيـدـعـتـلـلـ لـبـاـقـ رـيـغـ لـكـشـبـ IPـ ةـهـجـاوـ مـاـدـخـتـسـاـبـ (FTD)ـ دـيـدـهـتـ نـعـ عـافـدـلـاـبـ ةـصـاـخـلـاـ.

## ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ

### تابـلـطـتـمـلـاـ

ةـيـلـاتـلـاـ عـيـضـاـوـمـلـاـبـ ةـفـرـعـمـ كـيـدـلـ نـوـكـتـ نـأـبـ يـصـوـتـ:

- لـبـاـقـ رـيـغـ
- عـبـرـمـ دـاـخـ
- Ubuntu
- Cisco FireSIGHT (FMC)ـ ةـرـادـاـ زـكـرـمـ
- Cisco FTDـ يـرـانـلـاـ دـيـدـهـتـلـاـ دـضـ يـرـهـاـظـلـاـ عـافـدـلـاـ

وـتـنـوـبـوـأـ يـفـ Ansibleـ رـشـنـ مـتـيـ ،ـيـرـبـتـخـمـلـاـ عـضـوـلـاـ اـذـهـ قـاـيـسـ يـفـوـ.

نـمـ مـوـعـدـمـ يـسـاسـأـ مـاظـنـ يـأـ يـلـعـ حـاجـنـبـ اـهـتـيـبـثـتـ مـتـ دـقـ Ansibleـ نـأـ نـمـ دـكـأـتـلـاـ يـرـوـرـضـلـاـ نـمـ ةـلـاقـمـلـاـ هـذـهـ يـفـ اـهـيـلـاـ لـيـغـشـتـلـ Ansibleـ لـبـقـ.

### ةـمـدـخـتـسـمـلـاـ تـانـوـكـمـلـاـ

ةـيـلـاتـلـاـ ةـيـدـامـلـاـ تـانـوـكـمـلـاـوـجـمـارـبـلـاـ تـارـادـصـاـىـلـاـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ دـنـتـسـتـ:

- Ubuntu Server، 22.04

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

ةصالخ ةيلمعم ةئيب يف ةدوجموملا ةزهجألا نم دنتسملا اذه يف ةدراولي تامولعملا عاشنإ مت  
تناك اذا . (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجألا عيمج تأدب  
رمأ يأـل لمتحملـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـنـفـ ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـبـشـ.

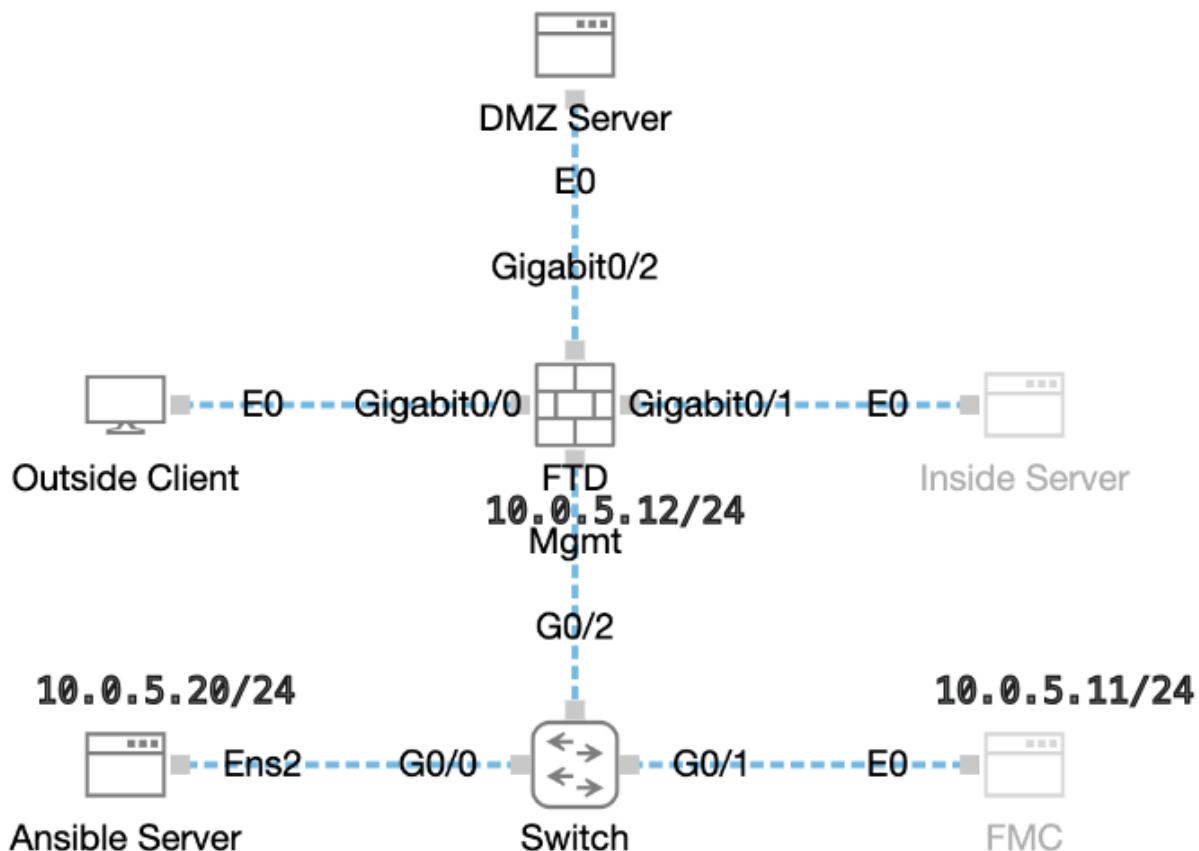
## ةيساسأ تامولعم

ةرادا يف ةريـبـكـ ةـيـلـاعـفـ رـهـظـيـ اـمـ ،ـرـيـبـكـ ةـجـرـدـبـ تـامـاـدـخـتـسـالـاـ ةـدـدـعـتـمـ ةـادـأـ نـعـ ةـرـابـعـ  
مـاـدـخـتـسـاـبـ ةـتـمـتـؤـمـلـاـ مـاـهـمـلـاـ لـيـغـشـتـلـاـ تـايـجـهـنـمـلـاـ نـمـ دـيـدـعـلـاـ مـاـدـخـتـسـاـ نـكـمـيـ .ـكـبـشـلـاـ ةـزـهـجـأـ  
جـمـانـرـبـ Ansibleـ .ـرـابـتـخـالـاـ ضـارـغـأـلـ عـجـرـمـكـ ةـدـاـمـلـاـ هـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـقـيـرـطـلـاـ مـدـخـتـسـتـوـ

ليـغـشـتـ دـعـبـ FTDـ يـلـاـ ةـهـجـاـوـلـاـ مـسـاوـعـاـنـقـلـاـوـ ةـهـجـاـوـلـلـ IPـ نـاـوـنـعـ ثـيـدـحـتـ مـتـيـ ،ـلـاـثـمـلـاـ اـذـهـ يـفـ  
جـاـجـنـبـ لـيـغـشـتـلـاـ رـتـفـدـ لـاـثـمـ

## نيـوكـتـلـاـ

### ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



## تاني يوكتل

لبق نم ٰبوقتكملا ٰيصنلا جماربلأا ٰيصنلا جماربلأا مععدت ال Cisco نأ ارظن كتاجايتحال اقفو اهرابتخا كنكمي يتلأا ٰلثملأا ضعب انيدلف ،ليمعلا

بجاولأا وحنلا ىلع يلولأا ققحتلا لامكأ نامض يرورصلأا نمو.

- تـنـرـتـنـإـلـاـبـ لـاـصـتـاـلـاـ ٰـيـنـاـكـمـاـبـ لـيـصـوـتـلـلـ لـبـاـقـلـاـ رـيـغـ مـدـاـخـلـاـ زـيـمـتـيـ .
- مدختسملا ٰهـجـاوـ ذـفـنـمـبـ حـاجـنـبـ لـاـصـتـاـلـاـ ٰـيـنـاـكـمـاـبـ لـيـغـشـتـلـلـ لـبـاـقـلـاـ مـدـاـخـلـاـ زـيـمـتـيـ .
- (GUI) FMC ٰـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ٰـهـجـاـوـلـ يـضـاـرـتـفـاـلـاـ ٰـذـفـنـمـلـاـ (GUI) FMC ٰـيـمـوـسـرـلـاـ ٰـهـجـاـوـلـ 443).
- يـفـ حـاجـنـبـ FTD لـيـجـسـتـ مـتـ .

لوكوتورب رباع يضارتفالا مداخلاب ٰصاخلا (CLI) رمأولأا رطس ٰهـجـاـوـبـ لـاـصـتـاـلـاـبـ مـقـ . 1. ٰـوـطـخـلـاـ مـكـحـتـلـاـ ٰـهـجـوـ وـأـ SSH.

نم ٰـلـوـقـعـمـ رـيـغـ ٰـعـوـمـجـ تـيـبـثـتـ لـجـأـ نـمـ لـيـغـشـتـبـ مـقـ . 2. ٰـوـطـخـلـاـ

لـيـغـشـتـلـلـ لـبـاـقـلـاـ رـيـغـ مـدـاـخـلـاـ ىـلـعـ FMC.

<#root>

```
cisco@inserthostname-here:~$  
ansible-galaxy collection install cisco.fmcansible
```

لـاـثـمـلـاـ اـذـهـ يـفـ . ٰـلـصـلـاـ تـاذـ تـافـلـمـلـاـ نـيـزـخـتـلـ دـيـدـجـ دـلـجـمـ ءـاـشـنـإـلـ ئـلـيـغـشـتـبـ مـقـ . 3. ٰـوـطـخـلـاـ

رمـأـوـلـاـ لـيـغـشـتـبـ مـقـ .mkdir /home/cisco/fmc\_ansible

وهـ دـيـدـجـلـاـ دـلـجـمـلـاـ مـسـاـ ،ـ وـهـ يـسـيـئـرـلـاـ لـيـلـدـلـاـ

<#root>

```
cisco@inserthostname-here:~$  
mkdir /home/cisco/fmc ansible
```

وهـ نـوـزـخـمـلـاـ فـلـمـ مـسـاـ ،ـ لـاـثـمـلـاـ اـذـهـ يـفـ . نـوـزـخـمـ فـلـمـ ءـاـشـنـإـبـ مـقـ وـ ،ـ دـلـجـمـلـاـ ىـلـاـ لـقـتـنـاـ . 4. ٰـوـطـخـلـاـ

inventory.ini.

<#root>

```
cisco@inserthostname-here:~$  
cd /home/cisco/fmc ansible/  
ccisco@inserthostname-here:~/fmc ansible$  
ls
```

**inventory.ini**

ة. قيقدلا تاددحملاب قربملا عطاقملارىيغتو، مادختسسالل هقصلىو وتحمل اذاه ئفعاضم كنكمي.

<#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

وه رىغتملا فلملا مسا، لاثملا اذاه يف. رىغتم فلم عاشناب مقو، دلجملا ىلإ لقتنا 5. ئوطخل fmc-configure-interface-vars.yml.

<#root>

cisco@inserthostname-here:~\$

cd /home/cisco/fmc\_ansible/

ccisco@inserthostname-here:~/fmc\_ansible\$

ls

**fmc-configure-interface-vars.yml**

**inventory.ini**

ة. قيقدلا تاددحملاب قربملا عطاقملارىيغت عم، مادختسسالل هقصلىو وتحمل اذاه ئفعاضم كنكمي.

<#root>

```

user: domain: 'Global' onboard: acp_name: 'TEMPACP' device_name: ftd1: 'FTDA' ftd_data: outside_name: 'outside
' inside_name: '
inside
' dmz_name: '
DMZ
' outside_ip: '
10.1.1.1
' inside_ip: '
10.1.2.1
' dmz_ip: '
10.1.3.1
' mask24: '
255.255.255.0
'

```

رتفذ فلم مسا ،لاثمل اذه يف .ليغشت باتك فلم عاشناب مق ،/home/cisco/fmc\_ansible دلجملا ىلإ لقتنا.6. ووطخلا  
fmc-configure-interface-playbook.yaml.

```

<#root>
cisco@inserthostname-here:~$ cd /home/cisco/fmc_ansible/
ccisco@inserthostname-here:~/fmc_ansible$ ls
fmc-configure-interface-playbook.yaml
fmc-configure-interface-vars.yml inventory.ini

```

ةـقـيـقـدـلـا تـادـدـحـمـلـا بـقـرـبـهـلـا عـطـاقـمـلـا رـيـيـغـتـوـ ،مـاـدـخـتـسـالـلـ هـقـصـلـوـيـوـتـجـمـلـا اـذـهـ ةـفـعـاضـمـ لـكـنـكـمـيـ.

<#root>

```

--- - name: Update FTD Interface IP Address hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configure
user.domain
}]" register_as: domain - name: Task02 - Get Devices cisco.fmcansible.fmc_configuration: operation: ge

```

```
device_name.ftd1

}]" register_as: device_list - name: Task03 - Get Physical Interfaces cisco.fmcansible.fmc_configuration

ftd_data.outside_name

}]" ipv4: static: address: "{{ Outside_ip | default(
ftd_data.outside_ip

) }}" netmask: "{{ Outside_netmask | default(
ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:
GigabitEthernet0/0

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

ftd_data.inside_name

}]" ipv4: static: address: "{{ Inside_ip | default(
ftd_data.inside_ip

) }}" netmask: "{{ Inside_netmask | default(
ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:
GigabitEthernet0/1

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{

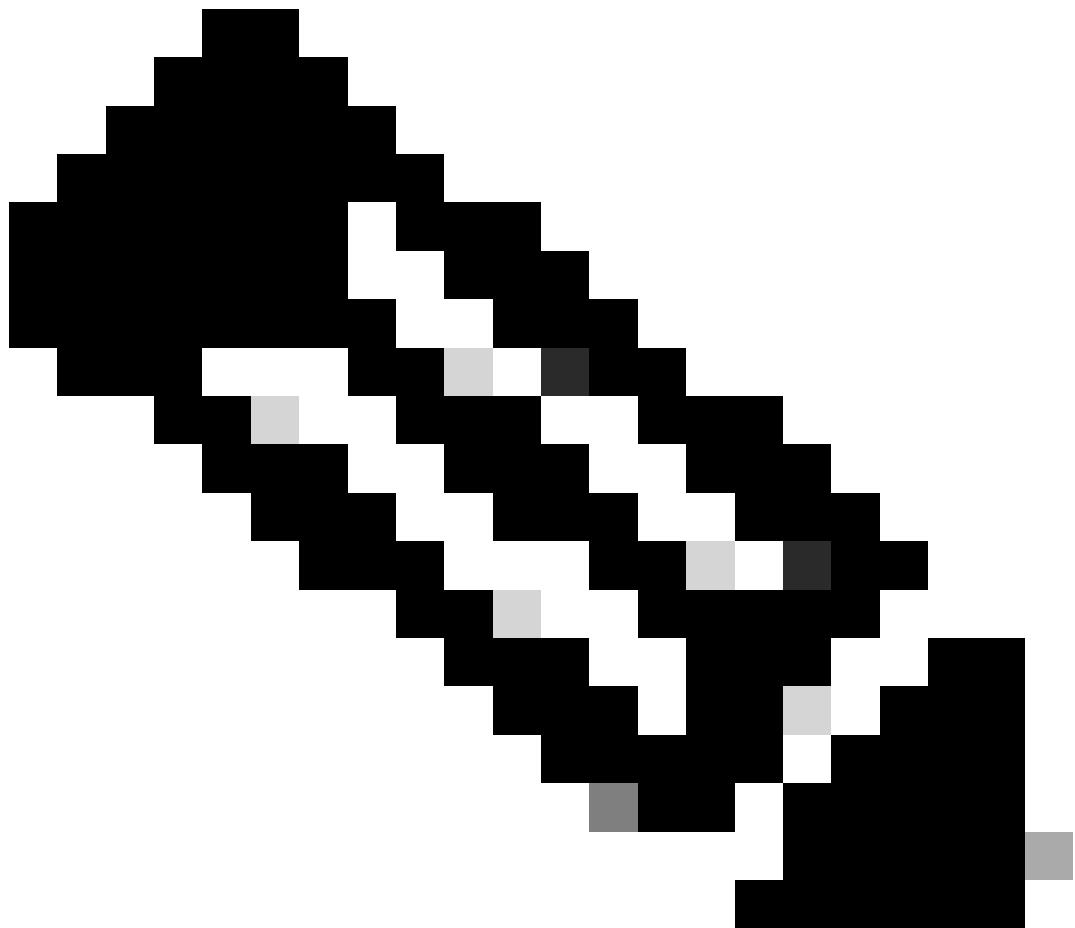
ftd_data.dmz_name

}]" ipv4: static: address: "{{ DMZ_ip | default(
ftd_data.dmz_ip

) }}" netmask: "{{ DMZ_netmask | default(
ftd_data.mask24

) }}" MTU: 1500 enabled: True mode: NONE type: physicalinterface name:
GigabitEthernet0/2

path_params: domainUUID: '{{ domain[0].uuid }}' containerUUID: '{{ device_list[0].id }}' objectId: '{{
```



نمض تاريغتملا هذهل ةفدارملما ميقالا ىلع ظافحلا متي .تاريغتمك لاثملما اذه يف ۋزربملا عامسألا مدخلت :ظفالىم ريغتملا فلم.

---

لامتحنلا رىغ ئەممەملە لىغىشتلىقتنىدا 7. دلجملا ىلا لىقتنىدا رمألا لىغىشتلىقنى دلجملا /home/cisco/fmc\_ansible/، مۇنىشنى ئىلىنى ئېرىدىمىز. ansible-playbook -i <inventory\_name>.ini <playbook\_name>.yaml -e@<playbook\_vars>.yml

وھ رمألا، لاثملما اذه يف ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@fmc-configure-interface-vars.yaml .

```
<#root>
```

```
cisco@inserthostname-here:~$
```

```
cd /home/cisco/fmc_ansible/
```

```
cisco@inserthostname-here:~/fmc_ansible$  
ls  
  
fmc-configure-interface-playbook.yaml fmc-configure-interface-vars.yml inventory.ini  
  
cisco@inserthostname-here:~/fmc_ansible$  
ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yml"  
  
PLAY [Update FTD Interface IP Address] ****  
  
TASK [Gathering Facts] ****  
ok: [10.0.5.11]  
  
TASK [Task01 - Get User Domain] ****  
ok: [10.0.5.11]  
  
TASK [Task02 - Get Devices] ****  
ok: [10.0.5.11]  
  
TASK [Task03 - Get Physical Interfaces] ****  
ok: [10.0.5.11]  
  
TASK [Task04 - Setup Outside Interface with static IP] ****  
changed: [10.0.5.11]  
  
TASK [Task05 - Setup Inside Interface with static IP] ****  
changed: [10.0.5.11]  
  
TASK [Task06 - Setup DMZ Interface with static] ****  
changed: [10.0.5.11]  
  
TASK [Task07 - Get Deployable Devices] ****  
ok: [10.0.5.11]  
  
TASK [Task08 - Start Deployment] ****  
changed: [10.0.5.11]  
  
TASK [Wait for Deployment Complete] ****  
ok: [10.0.5.11]  
  
TASK [Task09 - Poll Deployment Status Until Deployment Successful] ****  
ok: [10.0.5.11]  
  
TASK [Task10 - Stop The Playbook If The Deployment Failed] ****  
skipping: [10.0.5.11]  
  
PLAY RECAP ****  
10.0.5.11 : ok=11 changed=4 unreachable=0 failed=0 skipped=1 rescued=0 ignored=0
```

حیحص لکشب نیوکتل ا لمع دیکأتل مسقل ا اذه مدخلتسا

رمألا تلغش و مكحتلل ئيفرط ئدحو وأ SSH قىرط نع FTD لىا نم CLI لىا ئىلا تطبر interface GigabitEthernet 0/X . show interface ip brief و show running-config

جاجنب عانقل او ip ناونع و ئەج اول ا مسا نیوكت مت.

<#root>

```
> show interface ip brief  
Interface IP-Address OK? Method Status Protocol
```

```
GigabitEthernet0/0 10.1.1.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/1 10.1.2.1
```

```
YES manual
```

```
up up
```

```
GigabitEthernet0/2 10.1.3.1
```

```
YES manual
```

```
up up
```

>

```
show running-config interface GigabitEthernet 0/0
```

```
!  
interface GigabitEthernet0/0  
nameif
```

```
outside
```

```
cts manual  
propagate sgt preserve-untag  
policy static sgt disabled trusted  
security-level 0
```

```
ip address 10.1.1.1 255.255.255.0
```

>

```
show running-config interface GigabitEthernet 0/1
```

!

```
interface GigabitEthernet0/1
nameif

Inside

cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0

ip address 10.1.2.1 255.255.255.0
```

>

```
show running-config interface GigabitEthernet 0/2
```

```
!
interface GigabitEthernet0/2
nameif
```

**DMZ**

```
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 10.1.3.1 255.255.255.0
```

اوهالص او نويوكتل اهالص اوهالص او نويوكتل

اهالص او نويوكتل اهالص اوهالص او نويوكتل

لباقل ریغ لیغشتلا باتک لیغشت كنكمي ، لیغشتلل لباقل ریغ لیغشتلا باتک تالجس نم ديزمل اذه اش مل  
- مادختسس اب لیغشتلل

```
cisco@inserthostname-here:~/fmc_ansible$ ansible-playbook -i inventory.ini fmc-configure-interface-playbook.yaml -e@"fmc-configure-interface-vars.yaml"
```

ةلص تاذ تامولع

[Cisco Devnet FMC Ansible](#)

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).