

فوتل ئاشن ئي زىن اكما مادختساب FTD

تاي وتحمل

[قىدمىلما](#)

[قىساس آلاتابل طتمىلما](#)

[تابل طتمىلما](#)

[قىمدختسەملىاتانوكمىلما](#)

[قىساس تامولىع](#)

[نىوكىتلما](#)

[كىلىشلىكىطى طختىلا مىسىلما](#)

[تائنىوكىتلما](#)

[قىحصلانم قىچىتلما](#)

[اھالىص او عاطخالا فاش كىتسىما](#)

[قلص تاذ تامولىع](#)

قىدمىلما

دض عافدىلا جمانرب ئاشنال (FirePOWER FMC) ۋ رادا زىرم ئاتىم تأ تاو طخ دىت سەملى اذە حضوى FirePOWER (FTD) نم ئينقت عم رفوتلار ئىامحلا تادىدەت ANSIBLE.

قىساس آلاتابل طتمىلما

تابل طتمىلما

قىيلاتلار ئىضاوەملاپ ئەفرۇم كېدىل نوکىت نأب Cisco يىصوت:

- لباقدىرىغ
- Ubuntu مىداخ
- Cisco FireSIGHT (FMC) ۋ رادا زىرم
- Cisco يرالى دىدەتلى دض يرەاظلا عافدىلا (FTD)

وتنوبوا يف Ansible رشن مىتى، يربىت خەملىا عضولىا اذە قايىس يف و.

نم موعىدم يىساساً ماظن يأ ئىلە حاجىب اهتىبىت مەدق نم دكأتلى يرورىمىلىا نم ئەلاقىملار ھەذە يف اھىلإ راشملىا رەققەنەلە رەمأوألا لىغشتلىق.

قىمدختسەملىاتانوكمىلما

قىيلاتلار ئىداملى تانوكمىلار جماربلى تارادىصا ئىلە دىت سەملى اذە يف ئەدرالى تامولىع سەمتى:

- Ubuntu Server 22.04 رادىصىلا

- 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 ةدوجملا 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.

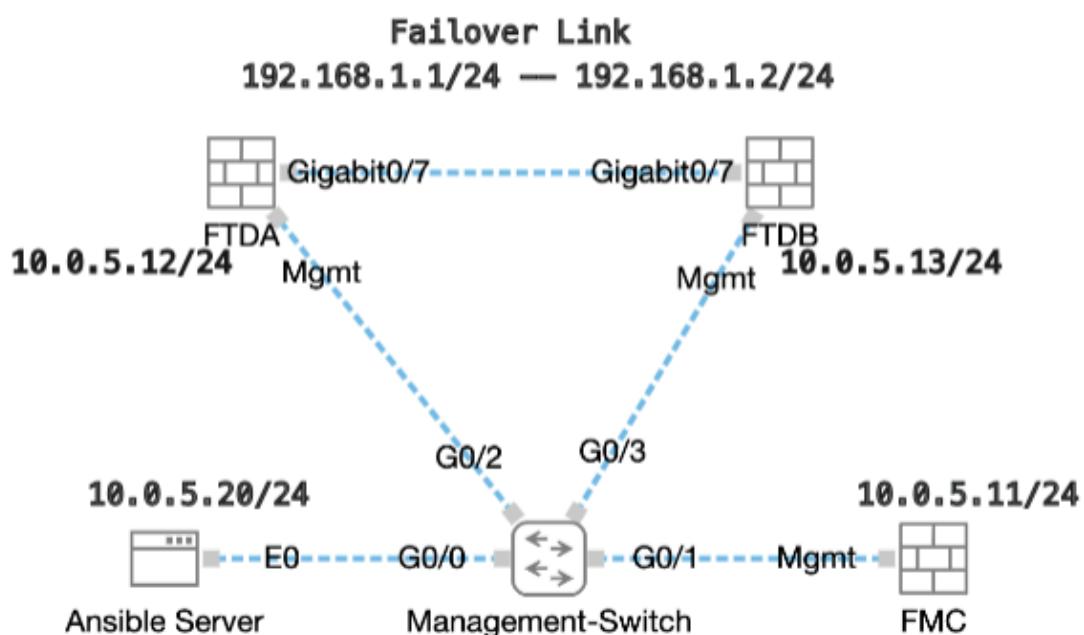
ةيساسأ تامولعم

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

صـاخـلـاـ يـطـايـتـحـالـاـ IPـ نـاـونـعـ وـرـفـوتـلـاـ يـلـاعـ FTDـ بـ صـاخـلـاـ IPـ نـاـونـعـ عـاـشـنـإـ مـتـيـ ،ـلـاـثـمـلـاـ اـذـهـ يـفـ
حـاجـنـبـ لـيـغـشـتـلـاـ رـتـفـدـ لـاـثـمـ لـيـغـشـتـ دـعـبـ ٥ـ.

نـيـوـكـتـلـاـ

ةـكـبـشـلـلـ يـطـيـطـخـتـلـاـ مـسـرـلـاـ



طـطـخـمـلـاـ

تـانـيـوـكـتـلـاـ

لـبـقـ نـمـ ةـبـوـتـكـمـلـاـ ةـيـصـنـلـاـ جـمـارـبـلـاـ وـأـ ةـلـثـمـأـلـلـ ةـيـصـنـلـاـ جـمـارـبـلـاـ مـعـدـتـ الـ Ciscoـ نـأـلـ اـرـظـنـ
كـتـاجـاـيـتـحـالـاـ اـقـفـوـاهـرـابـتـخـاـ كـنـكـمـيـ يـتـلـاـ ةـلـثـمـأـلـاـ ضـعـبـ اـنـيـدـلـفـ ،ـلـيـمـعـلـاـ

بجاوألا وحنلا ىلع يلؤألا ققحتلا لامك انامض يرورصلانمو.

- تبرتن إلاب لاصتا لـ FMC (GUI) لـ FMC (CLI) زيمتي.
- مدخلتسملاءه جاوزفونم ب حاجن ب لاصتا لـ FMC (GUI) لـ FMC (CLI) زيمتي.
- مدخلتسملاءه جاوزفونم ب حاجن ب لـ FTD (CLI) زيمتسملاءه جاوزفونم ب حاجن ب لـ FTD (CLI).
- يف حاجن ب FTD (CLI) زيمتسملاءه جاوزفونم ب حاجن ب لـ FTD (CLI).
- ةهجاولل IP ناوئع مادختسا ب يسأسا نيوكت مت.

لوكوتورب رباع يضارتفالا مدخلاب ةصاخلا (CLI) رمأولا رطس ةهجاوب لاصتا لـ FTD (CLI) 1. ةوطخلانم كمحتلابا ةدحو وأ SSH.

نم ةلوقعم رieg ةعومجم تيبيثت لجأ نم ansible-galaxy collection install cisco.fmcansible 2. ةوطخلانم كمحتلابا ةدحو وأ SSH.

<#root>

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

لاثملاءه يف .ةلصلاتاذ تافلمملانيزختل ديدج دلجم عاشنإل رمأولا لـ FMC (CLI) 3. ةوطخلانم كمحتلابا ديدجلا دلجملا مسا، fmc_ansible وه يسيئرلا ليلدلا.

<#root>

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

وه نوزخملاءه فلم مسا، لاثملاءه يف .نوزخم فلم عاشناب مق و /home/cisco/fmc_ansible، دلجملا ىلإ لقتنا 4. ةوطخلانم كمحتلابا ديدجلا دلجملا مسا، inventory.ini.

<#root>

```
cisco@inserthostname-here:~$  
cd /home/cisco/fmc_ansible/  
  
ccisco@inserthostname-here:~/fmc_ansible$  
ls  
  
inventory.ini
```

ةقيق دلا تاملا عطا قملا رئيغتو، مادختسالل هقصل وىوتحمل اذه راركت 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

فلمل امسا ، لاثمل اذه يف FTD HA. عاشنال ريغتم فلم عاشناب مق و /home/cisco/fmc_ansible دلجملا ىلا لقتنا 5. ۋوطخلما fmc-create-ftd-ha-vars.yml.

<#root>

cisco@inserthostname-here:~\$

cd /home/cisco/fmc_ansible/

ccisco@inserthostname-here:~/fmc_ansible\$

ls

fmc-create-ftd-ha-vars.yml

inventory.ini

ةقيق دلا تاملا عطا قملا رئيغتو، مادختسالل هقصل وىوتحمل اذه راركت كنكمي.

<#root>

user: domain: 'Global' device_name: ftd1: '

FTDA

' ftd2: '

```

FTDB

' ftd_ha: name: '


FTD_HA

' active_ip: ' 192.168.1.1
' standby_ip: ' 192.168.1.2
' key: cisco
mask24: ' 255.255.255.0
'

```

مسا لاثمل ا اذه يف FTD HA. عاشن اال ليغشتلا باتك فلم عاشناب مق و دلجملا ىلا لقتنا 6. ٥وطخل ا و ه ليغشتلا رتفد فلم fmc-create-ftd-ha-playbook.yaml.

```

<#root>

cisco@inserthostname-here:~$ cd /home/cisco/fmc_ansible/
ccisco@inserthostname-here:~/fmc_ansible$ ls
fmc-create-ftd-ha-playbook.yaml
fmc-create-ftd-ha-vars.yml inventory.ini

```

ةقيق دلا تاملاع مل ا مادختس اب ققماغل ا عطا قمل ا رئيغت و مادختس اال هقص ل و ىوتح مل ا اذه راركت كنكمي.

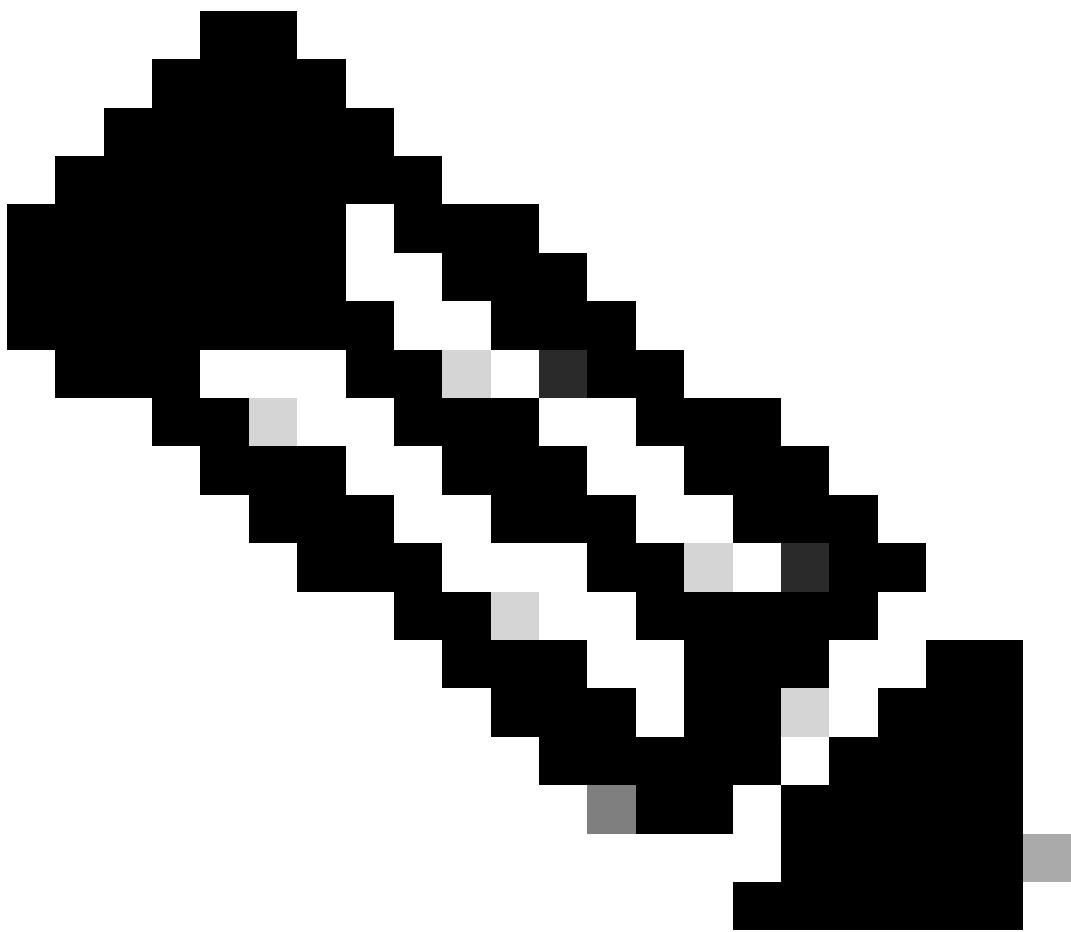
```

<#root>

--- - name: FMC Create FTD HA hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_configuration: operation: get
user.domain
}]" register_as: domain - name: Task02 - Get FTD1 cisco.fmcansible.fmc_configuration: operation: getAll
device_name.ftd1
}]" register_as: ftd1_list - name: Task03 - Get FTD2 cisco.fmcansible.fmc_configuration: operation: get
device_name.ftd2

```

```
 }}" register_as: ftd2_list - name: Task04 - Get Physical Interfaces cisco.fmcansible.fmc_configuration  
ftd_ha.name  
 }}" type: "DeviceHAPair" ftdHABootstrap: { 'isEncryptionEnabled': false, 'encKeyGenerationScheme': 'CU  
ftd_ha.key  
 }", 'useSameLinkForFailovers': true, 'lanFailover': { 'useIPv6Address': false, 'subnetMask': "{{  
ftd_ha.mask24  
 }}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'  
ftd_ha.standby_ip  
 }", 'logicalName': 'LAN-INTERFACE', 'activeIP': "{{  
ftd_ha.active_ip  
 }}" }, 'statefulFailover': { 'useIPv6Address': false, 'subnetMask': "{{  
ftd_ha.mask24  
 }}", 'interfaceObject': { 'id': '{{ primary_physical_interfaces[7].id }}', 'type': 'PhysicalInterface'  
ftd_ha.standby_ip  
 }", 'logicalName': 'STATEFUL-INTERFACE', 'activeIP': "{{  
ftd_ha.active_ip  
 }}" } } path_params: domainUUID: "{{ domain[0].uuid }}" - name: Task06 - Wait for FTD HA Ready ansible
```



هذهل ةفدارملالا ميقلالا ىلع ظافحلا متى .تاريغتم ئاب اثملالا اذه يف ضيرعلالا طخلاب ئامسألا دعت :ةظحالم
ريغتملا فلم نمض تاريغتملا.

لارجعكم لىلا دلجملا لىلا لقتنلا 7. ئوطخلالا /home/cisco/fmc_ansible/ رمألا ليغشتبا مق، ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@<playbook_vars>.yml

فه رمألا ،لاثملالا اذه يف ansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yaml" .

```
<#root>
```

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

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

```

ccisco@inserthostname-here:~/fmc_ansible$ ls
fmc-create-ftd-ha-playbook.yaml fmc-create-ftd-ha-vars.yml inventory.ini cisco@inserthostname-here:~/f
ansible-playbook -i inventory.ini fmc-create-ftd-ha-playbook.yaml -e@"fmc-create-ftd-ha-vars.yml"
PLAY [FMC Create FTD HA] ****

```

دادعتسالا عضو يف IP ناونع ثي دحتل ريغتم فلم عاشناب مق و /home/cisco/fmc_ansible دلجملا لقا لقتنا 8. ۋوطخلا fmc-create-ftd-ha-standby-ip-vars.yml.

<#root>

```

cisco@inserthostname-here:~$ cd /home/cisco/fmc_ansible/
ccisco@inserthostname-here:~/fmc_ansible$ ls
fmc-create-ftd-ha-playbook.yaml
fmc-create-ftd-ha-standby-ip-vars.yml
fmc-create-ftd-ha-vars.yml inventory.ini

```

قىقدلا تامىلۇملا مادختساپ قىماغلا عطا قىملا رىيغتو، مادختساپلۇمۇتەنەن كەنگەمى.

<#root>

```

user: domain: 'Global' ftd_data: outside_name: ''
outside
' inside_name: '
inside
' outside_ip: '10.1.1.1' inside_ip: '10.1.2.1' mask24: '255.255.255.0' ftd_ha: name: '
FTD_HA
' outside_standby: '
10.1.1.2
' inside_standby: '
10.1.2.2
'

```

عوضوي IP ناونع ثيدحت لليغشتلا باتك فلم عاشناب مقو، دلجملا لقا لقتنا 9. ووطخلا fmc-create-ftd-ha-standby-ip-playbook.yaml. وه ليغشتلا رتفد فلم مسا، لاثملها اذه يف FTD HA.

<#root>

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

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

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-create-ftd-ha-playbook.yaml
```

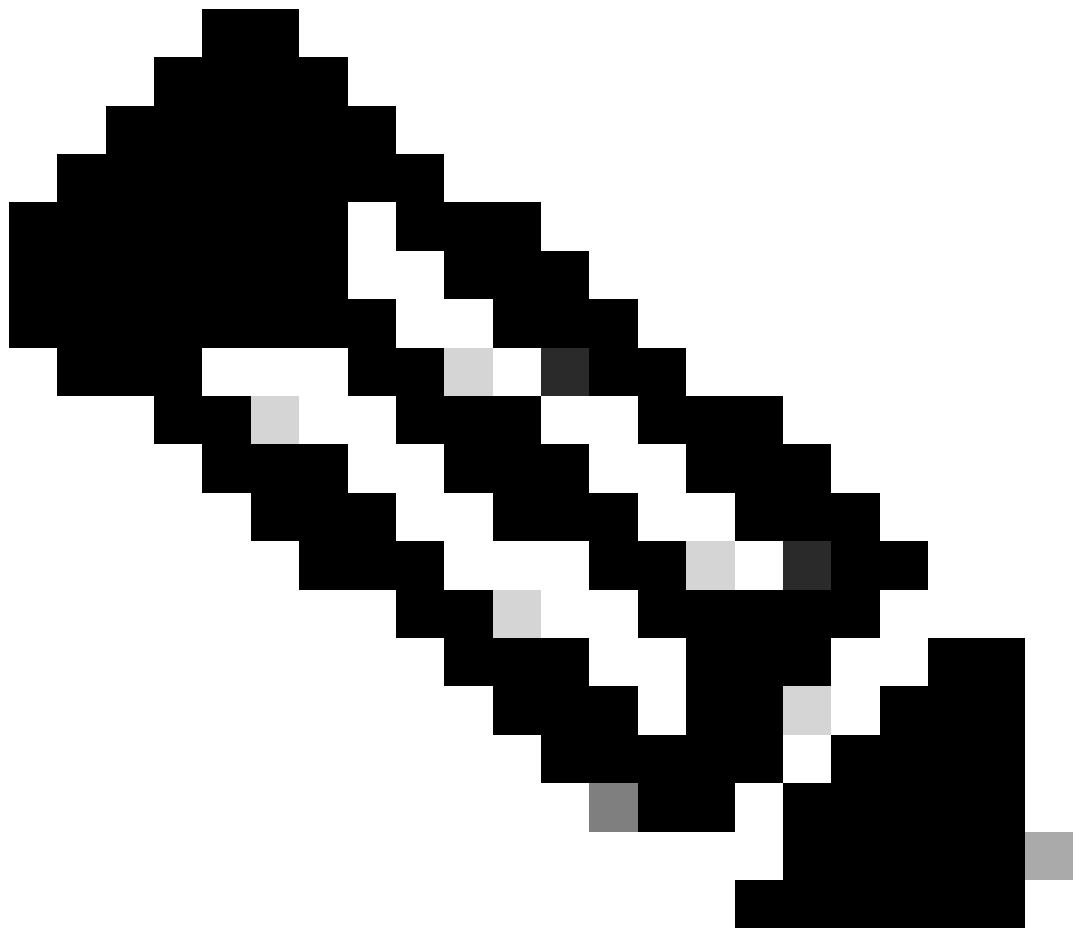
```
fmc-create-ftd-ha-standby-ip-playbook.yaml
```

```
fmc-create-ftd-ha-standby-ip-vars.yml fmc-create-ftd-ha-vars.yml inventory.ini
```

وقيق دلا تاملعملاء مدخلت سباب قماغلا عطاقملاء رئيغتو، مدخلتسا لـ هـ قـ صـ لـ وـ يـ وـ حـ جـ مـ لـ اـ اـ ذـ رـ اـ رـ اـ كـ نـ كـ مـ يـ.

<#root>

```
--- - name: FMC Update FTD HA Interface Standby IP hosts: fmc connection: httpapi tasks: - name: Task01 - Get User Domain cisco.fmcansible.fmc_config:  
user.domain  
        }" register_as: domain - name: Task02 - Get FTD HA Object cisco.fmcansible.fmc_configuration: operational  
ftd_data.outside_name  
        }" register_as: outside_interface - name: Task04 - Get Inside Interface cisco.fmcansible.fmc_configuration:  
ftd_data.inside_name  
        }" register_as: inside_interface - name: Task05 - Configure Standby IP-Outside cisco.fmcansible.fmc_c  
ftd_ha.outside_standby  
        }"} monitorForFailures: true path_params: objectId: "{{ outside_interface[0].id }}" containerUUID: "{{  
ftd_ha.inside_standby  
        }"} monitorForFailures: true path_params: objectId: "{{ inside_interface[0].id }}" containerUUID: "{{
```



هذهل ةفدارملا ميقلالا ىلع ظافحلا متني .تاريغتم قباثمب لاثملالا اذه يف ضيرعلاب ئامسألا دعت :ةظحالم ريغتملا فلم نمض تاريغتملا.

رملأا ليغشت بمق، دلجملا ىلا لقتنا 10. ووطخلأ /home/cisco/fmc_ansible/ رمألا ليغشت بمق، ansible-playbook -i <inventory_name>.ini <playbook_name>.yaml -e@<playbook_vars>.yml .

رمألا، لاثملالا اذه يف ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@<fmc-create-ftd-ha-standby-ip-vars>.yml .

<#root>

cisco@inserhostname-here:~\$

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

```
ccisco@inserthostname-here:~/fmc_ansible$
```

```
ls
```

```
fmc-create-ftd-ha-playbook.yaml
```

```
fmc-create-ftd-ha-standby-ip-playbook.yaml
```

```
fmc-create-ftd-ha-standby-ip-vars.yml
```

```
fmc-create-ftd-ha-vars.yml
```

```
inventory.ini
```

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

```
ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-ip-vars.yml"
```

```
PLAY [FMC Update FTD HA Interface Standby IP] ****
```

ڦڻا نم قچھ تلا

، ڦڻا ڦرادي > ڦڻا ىلإ لقتننا (GUI) ڦيموسرلا مدخلت سملاء ڦوچ او ىلإ لودلا لجس ، ڦلمتحمل ریغ ڦمممل ليغشت لبوق
اهنيوكت مت يتلا لوصولاي ف مکحتلا ڦس اي اس مدخلتساب FMC ىلع حاجن ب تافلم نم نينثا ليجست مت.

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control
<input type="checkbox"/>	Ungrouped (2)					
<input type="checkbox"/>	FTDA Snort 3 10.0.5.12 - Routed	FTDv for KVM	7.4.1	N/A	Essentials	TEMPACP
<input type="checkbox"/>	FTDB Snort 3 10.0.5.13 - Routed	FTDv for KVM	7.4.1	N/A	Essentials	TEMPACP

ڦلمتحم ریغ ڦمممل ليغشت لبوق

، ڦڻا ڦرادي > ڦڻا ىلإ لقتننا (GUI) ڦيموسرلا مدخلت سملاء ڦوچ او ىلإ لودلا لجس ، ڦلمتحمل ریغ ڦمممل ليغشت دعب
حاجن ب FTD HA عاشن ا مت

Firewall Management Center

Devices / Device Management

Overview Analysis Policies Devices Objects Integration Deploy

Devices tab is highlighted with a red box.

View By: Group

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

[Collapse All](#)

Name	Model	Version	Chassis	Licenses	Access Contr
FTD_HA	FTDv for KVM	7.4.1	N/A	Essentials	TEMPACP
FTDA(Primary, Active) Snort 3 10.0.5.12 - Routed	FTDv for KVM	7.4.1	N/A	Essentials	TEMPACP
FTDB(Secondary, Standby) Snort 3 10.0.5.13 - Routed					

جاجنب ۋەلمىتەمەنلا رىغ ۋەمىملا لىيغىشەت دىب

اھىيوكىت مەت دادعتىسىلا ۋەچاوب صاخلىا IP ناونۇن و لىشلىلا زواجىتپ صاخلىا IP ناونۇن رىپرەت قوف رقنا جاجنب.

Firewall Management Center

Devices / High Availability

Overview Analysis Policies Devices Objects Integration Deploy admin SECURE

FTD_HA

Cisco Firepower Threat Defense for KVM

Save Cancel

High Availability Link

Interface	GigabitEthernet0/7
Logical Name	LAN-INTERFACE
Primary IP	192.168.1.1
Secondary IP	192.168.1.2
Subnet Mask	255.255.255.0
IPsec Encryption	Disabled

State Link

Interface	GigabitEthernet0/7
Logical Name	LAN-INTERFACE
Primary IP	192.168.1.1
Secondary IP	192.168.1.2
Subnet Mask	255.255.255.0
Statistics	

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
management						
Inside	10.1.2.1	10.1.2.2				
Outside	10.1.1.1	10.1.1.2				

رەفوتلىا ۋېلائىع FTD لىيصاكتى

اھىالىص او ئاطخىڭلا فاشكىتسا

اھىالىص او ئىيوكىتلار ئاطخىڭلا فاشكىتسا اھىم ادختىسىلا كىنكمى تامولۇم مىسىقلار اذە رەفوى.

لېباقلار رىغ لىيغىشتىلا باتك لىيغىشتى كىنكمى، لىيغىشتىللى لېباقلار رىغ لىيغىشتىلا باتك تالجىس نىم دىزمەل ۋەدەاشمىل

لیغشتلل مادختس اب -vvv.

<#root>

```
cisco@inserthostname-here:~/fmc_ansible$ ansible-playbook -i inventory.ini fmc-create-ftd-ha-standby-ip-playbook.yaml -e@"fmc-create-ftd-ha-standby-  
-vvv
```

موليما تام تاذ صلقل

[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).