# 驗證Firepower模式、例項、高可用性和可擴充性 配置

## 目錄

簡介 <u>背景資訊</u> 必要條件 需求 採用元件 驗證高可用性和可擴充性配置 FMC高可用性 FMC UI FMC CLI **FMC REST-API** FMC故障排除檔案 FDM高可用性 FDM UI **FDM REST-API FTD CLI** FTD SNMP投票 FTD疑難排解檔案 FTD高可用性及可擴充性 FTD CLI **FTD SNMP** FTD疑難排解檔案 FMC UI **FMC REST API** FDM UI **FDM REST-API** FCM UI **FXOS CLI FXOS REST API** FXOS機箱show-tech檔案 ASA高可用性和可擴充性 **ASA CLI** ASA SNMP ASA show-tech檔案 FCM UI **FXOS CLI FXOS REST-API** FXOS機箱show-tech檔案 驗證防火牆模式

FTD防火牆模式 **FTD CLI** FTD疑難排解檔案 **FMC UI FMC REST-API** FCM UI **FXOS CLI FXOS REST API** FXOS機箱show-tech檔案 ASA防火牆模式 ASA CLI ASA show-tech檔案 FCM UI **FXOS CLI FXOS REST-API** FXOS機箱show-tech檔案 驗證例項部署型別 FTD CLI FTD疑難排解檔案 FMC UI **FMC REST-API** FCM UI **FXOS CLI FXOS REST API** FXOS機箱show-tech檔案 驗證ASA情景模式 ASA CLI ASA show-tech檔案 使用ASA驗證Firepower 2100模式 ASA CLI **FXOS CLI** FXOS show-tech檔案 已知的問題 相關資訊

## 簡介

本文檔介紹驗證Firepower高可用性和可擴充性配置、防火牆模式和例項部署型別。

## 背景資訊

高可用性和可擴充性配置、防火牆模式和例項部署型別的驗證步驟顯示在使用者介面(UI)、命令列 介面(CLI)、通過REST-API查詢、SNMP以及故障排除檔案中。

## 必要條件

#### 需求

基本產品知識、REST-API、SNMP。

### 採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本:

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower管理中心(FMC)版本7.1.x
- Firepower可擴充作業系統(FXOS)2.11.1.x
- Firepower裝置管理器(FDM)7.1.x
- Firepower威脅防禦7.1.x
- ASA 9.17.x

## 驗證高可用性和可擴充性配置

高可用性是指故障切換配置。高可用性或故障轉移設定將兩台裝置連線在一起,以便當其中一台裝 置發生故障時,另一台裝置可以接管。

可擴充性是指群集配置。使用群集配置,可以將多個FTD節點組合為一個邏輯裝置。集群提供單個 裝置(管理、整合到網路)的所有便利性,以及增加多個裝置的吞吐量和冗餘。

在本文檔中,這些表達式可互換使用:

- 高可用性或故障切換
- 可擴充性或群集

在某些情況下,無法驗證高可用性和可擴充性配置或狀態。例如,FTD獨立組態沒有驗證命令。獨 立、故障切換和群集配置模式相互排斥。如果裝置沒有故障切換和群集配置,則認為該裝置在獨立 模式下運行。

#### FMC高可用性

可以使用以下選項驗證FMC高可用性配置和狀態:

- FMC UI
- FMC CLI
- REST API請求

#### • FMC故障排除檔案

#### FMC UI

按照以下步驟驗證FMC UI上的FMC高可用性配置和狀態:

1.選擇System > Integration > High Availability:



2.檢查FMC的角色。在這種情況下,未配置高可用性,並且FMC在獨立配置中運行:

CISCO System /	wer Management Cent Integration / High Availability	er <sub>Overview</sub>	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	Q	6 <sup>00</sup> ¢	Ø Global \ admin ▼
Cloud Services	Realms Identity Sources	High Availability	eStreame	r Host Ir	put Client	Smart Softw	are Manage	er On-Prem				Peer Manager
Select a role for Role For This FMC Standalone (N Primary Secondary	r this Management Center ar ∷ Io High Availability)	nd specify peer det	ails to setup	high availa	bility.							

如果配置了高可用性,將顯示本地和遠端角色:

cisco	Firepower Man System / Integration /	agement Center High Availability	۹	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	¢ 🧠	🕜 Global \ adm	nin 🔻
Cloud S	Services Realms	Identity Sources	High Av	ailability	eStreamer	Host Input Cl	ient Sn	nart Software Sa	tellite				Peer Manager	
								(	🤹 Switch	Peer Roles 🖉 Break H	A	Pause S	ynchronization	
	Summary							System Statu	IS					
	Status		•	Synchroni	ization task is in	progress				Local Active - Primary	Rem Standby -	iote Secondi		
	Synchronization					🖉 ок				(10.122.148.122)	(10.122.	148.123	)	
	Active System		ropization	time : Mon	10.122	.148.122		Operating System Software Version		Fire Linux OS 7.1.0	Fire Linux	OS 7.1	.0	
		( HA Synch	ronizatio	n ume : Mon	10.100	30 2022 )				7.1.0-90	7.1.0	-90		
	Standby System	( HA synch	nronization	n time : Mon	May 23 15:25:	14 2022 )		Model		Cisco Firepower Management Center 4600	Cisco Fi Management	repower Center	4600	

#### **FMC CLI**

按照以下步驟驗證FMC CLI上的FMC高可用性配置和狀態:

1.通過SSH或控制檯連線訪問FMC。

2.運行expert命令,然後運行sudo su 命令:

#### > expert

admin@fmc1:~\$ **sudo su** Password: Last login: Sat May 21 21:18:52 UTC 2022 on pts/0 fmc1:/Volume/home/admin#

3.運行troubleshoot\_HADC.pl 命令,然後選擇選項1 顯示FMC的HA資訊。如果未配置高可用性,將 顯示以下輸出:

fmcl	/Volume/home/admin# troubleshoot_HADC.pl									
* * * * *	**************************************									
2	Execute Sybase DBPing									
3	3 Show Arbiter Status									
4	Check Peer Connectivity									
5	Print Messages of AQ Task									
6	Show FMC HA Operations History (ASC order)									
7	Dump To File: FMC HA Operations History (ASC order)									
8	Last Successful Periodic Sync Time (When it completed)									
9	Print HA Status Messages									
10	Compare active and standby device list									
11	11 Check manager status of standby missing devices									
12	Check critical PM processes details									
13	Help									
0	Exit									
* * * * *	***************************************									
Enter	choice: 1									
HA Enabled: No										
如果	如果配置了高可用性,將顯示以下輸出:									

fmc1:/Volume/home/admin# troubleshoot\_HADC.pl 1 Show HA Info Of FMC

2 Execute Sybase DBPing 3 Show Arbiter Status 4 Check Peer Connectivity 5 Print Messages of AQ Task 6 Show FMC HA Operations History (ASC order) 7 Dump To File: FMC HA Operations History (ASC order) 8 Help Enter choice: 1 HA Enabled: Yes This FMC Role In HA: Active - Primary Status out put: vmsDbEngine (system,gui) - Running 29061 In vmsDbEngineStatus(): vmsDbEngine process is running at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize/HADC.pm line 3471. Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running) Sybase Database Connectivity: Accepting DB Connections. Sybase Database Name: csm\_primary Sybase Role: Active

**附註**:在高可用性配置中,FMC角色可以具有**主**或**輔助**角色,以及active或standby狀態。

#### **FMC REST-API**

按照以下步驟通過FMC REST-API驗證FMC高可用性和可擴充性配置和狀態。使用REST-API客戶 端。在此範例中,使用**curl**:

1.請求身份驗證令牌:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
... < X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
2.使用此查詢中的令牌查詢全域性域的UUID:</pre>
```

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
```

```
"items": [
{
       {
           "name": "Global",
           "type": "Domain",
           "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
       },
       {
           "name": "Global/LAB2",
           "type": "Domain",
           "uuid": "84cc4afe-02bc-b80a-4b09-00000000000"
       },
       {
           "name": "Global/TEST1",
           "type": "Domain",
           "uuid": "ef0cf3e9-bb07-8f66-5c4e-00000000001"
       },
       {
           "name": "Global/TEST2",
           "type": "Domain",
           "uuid": "341a8f03-f831-c364-b751-00000000001"
       }
   ],
```

```
"links": {
    "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
},
    "paging": {
        "count": 4,
        "limit": 25,
        "offset": 0,
        "pages": 1
}
```

**附註**:命令字串的「**| python -m json.tool**」部分用於以JSON樣式設定輸出格式,並且是可選 的。

3.在此查詢中使用全域性域UUID:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/integration/fmchastatuses' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
如果未配置高可用性,將顯示以下輸出:
```

{
 "links": {},
 "paging": {
 "count": 0,
 "limit": 0,
 "offset": 0,
 "pages": 0
 }
}

如果配置了高可用性,將顯示以下輸出:

```
{
   "items": [
       {
           "fmcPrimary": {
               "ipAddress": "192.0.2.1",
               "role": "Active",
               "uuid": "de7bfc10-13b5-11ec-afaf-a0f8cf9ccb46"
           },
           "fmcSecondary": {
               "ipAddress": "192.0.2.2",
               "role": "Standby",
               "uuid": "a2de9750-4635-11ec-b56d-201c961a3600"
           },
           "haStatusMessages": [
               "Healthy"
           1.
           "id": "de7bfc10-13b5-11ec-afaf-a0f8cf9ccb46",
           "overallStatus": "GOOD",
           "syncStatus": "GOOD",
           "type": "FMCHAStatus"
       }
   1.
   "links": {
       "self": "https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/integration/fmchastatuses?offset=0&limit=25"
   },
```

```
"paging": {
    "count": 1,
    "limit": 25,
    "offset": 0,
    "pages": 1
}
```

#### FMC故障排除檔案

{

'stderr' => undef,

}

按照以下步驟驗證FMC高可用性配置和FMC故障排除檔案中的狀態:

1.開啟故障排除檔案,導航到資料夾<filename>.tar/results-<date>---xxxxxx/command-output

2. 開啟檔案usr-local-sf-bin-troubleshooting\_HADC.pl -a.output:

如果未配置高可用性,將顯示以下輸出:

# pwd
/var/tmp/results-05-06-2022--199172/command-outputs

```
# cat "usr-local-sf-bin-troubleshoot_HADC.pl -a.output"
Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:
$VAR1 = [
        'Mirror Server => csmEng',
        {
          'rcode' => 0,
          'stderr' => undef,
          'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745
Type
        Property
                                 Value
_____
                                  ------
        MirrorRole
Database
                                  NULL
         MirrorState
Database
                                  NULL
Database PartnerState
                                  NULL
                                 NULL
Database ArbiterState
Server
        ServerName
                                  csmEng
Ping database successful.
        }
      ];
 (system,gui) - Waiting
HA Enabled: No
Sybase Database Name: csmEng
Arbiter Not Running On This FMC.
Not In HA
如果配置了高可用性、將顯示以下輸出:
# pwd
/var/tmp/results-05-06-2022--199172/command-outputs
# cat "usr-local-sf-bin-troubleshoot_HADC.pl -a.output"
Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:
Status out put: vmsDbEngine (system,gui) - Running 9399
In vmsDbEngineStatus(): vmsDbEngine process is running at
/usr/local/sf/lib/perl/5.24.4/SF/Synchronize/HADC.pm line 3471.
$VAR1 = [
         'Mirror Server => csm_primary',
```

'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745 Туре Property Value -----\_\_\_\_\_ Database MirrorRole primary Database MirrorState synchronizing Database PartnerState connected Database ArbiterState connected Server ServerName csm\_primary Ping database successful. ۰, 'rcode' => 0 } ]; (system,gui) - Running 8185 . . . HA Enabled: Yes This FMC Role In HA: Active - Primary Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running) Sybase Database Connectivity: Accepting DB Connections. Sybase Database Name: csm\_primary Sybase Role: Active Sybase Database Name: csm\_primary Arbiter Running On This FMC.

Peer Is Connected

### FDM高可用性

可以使用以下選項驗證FDM高可用性配置和狀態:

- FDM UI
- FDM REST API請求
- FTD CLI
- FTD SNMP投票
- FTD疑難排解檔案

#### FDM UI

若要驗證FDM UI上的FDM高可用性配置和狀態,請在主**頁上檢**查「高可用性」**。如果未配置高可 用性,則High Availability**值為Not Configured:



如果配置了高可用性,將顯示本地和遠端對等裝置故障切換配置和角色:

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: FPR1120-1	admin (?) admin						
Model Cisco Firepower 1120 Threat I	Software VDB Intrusion Rule Upo Defense 7.1.0-90 354.0 20220519-1116	date Cloud Services High Availability R Not Registered   Register Primary Device	/ a: Active						
Image: State in the image: State i									
Interfaces Connected Enabled 3 of 13 View All Interfaces	Routing There are no static routes yet View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server / Relay DDNS Service						
Smart License Evaluation expires in 89 days View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname Time Services See more						

**FDM REST-API** 

按照以下步驟通過FDM REST-API請求驗證FDM高可用性配置和狀態。使用REST-API客戶端。在 此範例中,使用**curl**:

1.請求身份驗證令牌:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Cisco123" }'
'https://192.0.2.3/api/fdm/latest/fdm/token'
```

{

"access\_token":

"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0 xMWVjLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV 4cGlyZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDg xZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ 1c2VybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd\_1V6TbFe6M",

"expires\_in": 1800,

"refresh\_expires\_in": 2400,

"refresh\_token":

"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDIOMi0xMW VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2 luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw", "token\_type": "Bearer"

}

2.若要驗證高可用性配置,請在此查詢中使用訪問令牌值:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
```

eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0xMWV jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV4cGl yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyISInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDgxZS0 xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V ybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd\_1V6TbFe6M' 'https://192.0.2.3/api/fdm/v6/devices/default/ha/configurations'

如果未配置高可用性,將顯示以下輸出:

```
{
 "items": [
   {
     "version": "issgb3rw2lixf",
     "name": "HA",
     "nodeRole": null,
     "failoverInterface": null,
     "failoverName": null,
     "primaryFailoverIPv4": null,
     "secondaryFailoverIPv4": null,
     "primaryFailoverIPv6": null,
     "secondaryFailoverIPv6": null,
     "statefulFailoverInterface": null,
     "statefulFailoverName": null,
     "primaryStatefulFailoverIPv4": null,
     "secondaryStatefulFailoverIPv4": null,
     "primaryStatefulFailoverIPv6": null,
     "secondaryStatefulFailoverIPv6": null,
     "sharedKey": null,
     "id": "76ha83ga-c872-11f2-8be8-8e45bb1943c0",
     "type": "haconfiguration",
     "links": {
       "self": "https://192.0.2.2/api/fdm/v6/devices/default/ha/configurations/76ha83ga-c872-
11f2-8be8-8e45bb1943c0"
     }
   }
 ],
 "paging": {
   "prev": [],
```

```
"next": [],
"limit": 10,
"offset": 0,
"count": 1,
"pages": 0
}
如果配置了高可用性,將顯示以下輸出:
```

如未能直」向可用住,府顯小以下鞩山

```
{
   "items": [
    {
        "version": "issgb3rw2lixf",
        "name": "HA",
        "nodeRole": "HA_PRIMARY",
        "failoverInterface": {
            "version": "ezzafxo5ccti3",
            "name": "",
            "hardwareName": "Ethernet1/1",
            "id": "8d6c4ldf-3e5f-465b-8e5a-d336b282f93f",
            "type": "physicalinterface"
        },
    }
```

3.要驗證高可用性狀態,請使用以下查詢:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1Yi16ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0xMWV
jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDgxZS0
xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.ai3LUbnsL0JTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default'
如果未配置高可用性,將顯示以下輸出:
```

```
{
   "nodeRole" : null,
   "nodeState" : "SINGLE_NODE",
   "peerNodeState" : "HA_UNKNOWN_NODE",
   "configStatus" : "UNKNOWN",
   "haHealthStatus" : "HEALTHY",
   "disabledReason" : "",
   "disabledTimestamp" : null,
   "id" : "default",
   "type" : "hastatus",
   "links" : {
        "self" : "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
   }
}
```

如果配置了高可用性,將顯示以下輸出:

```
{
  "nodeRole": "HA_PRIMARY",
  "nodeState": "HA_ACTIVE_NODE",
  "peerNodeState": "HA_STANDBY_NODE",
  "configStatus": "IN_SYNC",
  "haHealthStatus": "HEALTHY",
  "disabledReason": "",
```

```
"disabledTimestamp": "",
"id": "default",
"type": "hastatus",
"links": {
    "self": "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
}
}
```

**FTD CLI** 

請按照一節中的步驟操作。

#### FTD SNMP投票

請按照一節中的步驟操作。

#### FTD疑難排解檔案

請按照一節中的步驟操作。

### FTD高可用性及可擴充性

FTD高可用性及可擴充性組態和狀態可以使用以下選項進行驗證:

- FTD CLI
- FTD SNMP
- FTD疑難排解檔案
- FMC UI
- FMC REST-API
- FDM UI
- FDM REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS機箱show-tech檔案

#### **FTD CLI**

請依照以下步驟操作,驗證FTD CLI上的FTD高可用性及可擴充性組態和狀態:

1.根據平台和部署模式,使用以下選項訪問FTD CLI:

- 直接通過SSH訪問FTD 所有平台
- 通過connect ftd指令,從FXOS主控台CLI(Firepower 1000/2100/3100)進行存取
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問:
   connect module <x> [console|telnet],其中x是插槽ID,然後connect ftd [instance],其中例項僅 與多例項部署相關
- 對於虛擬FTD,直接通過SSH訪問FTD,或透過虛擬機器監控程式或雲使用者介面進行主控台 訪問

2.為了驗證FTD容錯移轉組態和狀態,請在CLI上執行**show running-config failover**和**show failover** state命令。

如果未配置故障轉移,將顯示以下輸出:

> show running-config failover									
no failover									
>show failover state									
		State	Last H	ailure	Reason	Date/Time			
This host	-	Secondary							
		Disabled	None						
Other host	-	Primary							
		Not Detected	None						
====Configu	rati	lon State===							
====Communi	cati	lon State==							
如果配置了	故障	〕 轉移,將顯示」	以下輸出						
				-					
> show runn	ing-	-config failove	r						
failowar fa	+ 1	ron lan unit nri							

failover failover lan unit primary
failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 10.30.34.2 255.255.0 standby 10.30.34.3

>show failover state
State Last Failure Reason Date/Time
This host - Primary
Active None
Other host - Secondary
Standby Ready Comm Failure 09:21:50 UTC May 22 2022
====Configuration State===
Sync Done
====Communication State===
Mac set

3.為了驗證FTD集群配置和狀態,請在CLI上運行**show running-config cluster**和**show cluster info**命 令。

如果未配置集群,將顯示以下輸出:

> show running-config cluster
>show cluster info
Clustering is not configured
如果已配置集群,則顯示以下輸出:

```
> show running-config cluster
cluster group ftd_cluster1
key *****
local-unit unit-1-1
cluster-interface Port-channel48.204 ip 10.173.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
```

enable > show cluster info Cluster ftd\_cluster1: On Interface mode: spanned Cluster Member Limit : 16 This is "unit-1-1" in state MASTER : 0 ТD Site TD : 1 Version : 9.17(1) Serial No.: FLM1949C5RR6HE : 10.173.1.1 CCL TP CCL MAC : 0015.c500.018f : FPR4K-SM-24 Module Resource : 20 cores / 44018 MB RAM Last join : 13:53:52 UTC May 20 2022 Last leave: N/A Other members in the cluster: Unit "unit-2-1" in state SLAVE : 1 TD : 1 Site ID Version : 9.17(1) Serial No.: FLM2108V9YG7S1 CCL IP : 10.173.2.1 CCL MAC : 0015.c500.028f : FPR4K-SM-24 Module Resource : 20 cores / 44018 MB RAM Last join : 14:02:46 UTC May 20 2022 Last leave: 14:02:31 UTC May 20 2022

no unit join-acceleration

**附註**:master和control角色相同。

#### **FTD SNMP**

請依照以下步驟操作,透過SNMP驗證FTD高可用性及可擴充性組態和狀態:

 確保已配置並啟用SNMP。有關FDM管理的FTD的資訊,請參閱<u>在Firepower FDM上配置</u> <u>SNMP並對其</u>進行故障排除。有關FMC管理的FTD的資訊,請參閱<u>在Firepower NGFW裝置上</u> 配置SNMP以瞭解配置步驟。

2. 若要確認FTD容錯移轉組態和狀態,請輪詢OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1。** 如果未配置故障轉移,將顯示以下輸出:

# snmpwalk -v2c -c ciscol23 -On 192.0.2.5 .1.3.6.1.4.1.9.9.147.1.2.1.1.1 SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface" SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit" SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit (this device)" SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3 SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured" SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "Failover Off" SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off" M果配置了故障轉移. 將顯示以下輸出:

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit (this device)"
                                                                                  <-- This
device is primary
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 9
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 10
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "fover Ethernet1/2"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Active unit"
                                                                                   <--
Primary device is active
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Standby unit"
3.要驗證群集配置和狀態,請輪詢OID 1.3.6.1.4.1.9.9.491.1.8.1。
如果未配置集群,將顯示以下輸出:
# snmpwalk -v2c -c cisco123 192.0.2.5 .1.3.6.1.4.1.9.9.491.1.8.1
SNMPv2-SMI::enterprises.9.9.491.1.8.1.1.0 = INTEGER: 0
如果已配置但未啟用集群,則顯示以下輸出:
# snmpwalk -v2c -c cisco123 -On 192.0.2.7 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0
                                                            <-- Cluster status, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0
                                                           <-- Cluster unit state, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "ftd_cluster1"
                                                           <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"
                                                            <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0 <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1
                                                            <-- Cluster side ID
如果群集已配置、已啟用且運行正常,則顯示以下輸出:
# snmpwalk -v2c -c cisco123 -On 192.0.2.7 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 1
                                                           <-- Cluster status, enabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 16
                                                           <-- Cluster unit state, control
unit
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 10
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "ftd cluster1"
                                                         <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"
                                                            <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0
                                                            <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1
                                                            <-- Cluster side ID
. . .
```

有關OID描述的詳細資訊,請參閱<u>CISCO-UNIFIED-FIREWALL-MIB</u>。

#### FTD疑難排解檔案

請依照以下步驟操作,驗證FTD疑難排解檔案中的FTD高可用性及可擴充性組態和狀態:

1.開啟故障排除檔案,導航到資料夾<filename>-troubleshoot .tar/results-<date>---xxxxxx/command-output。

2. 開啟文件usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output:

/ngfw/var/common/results-05-22-2022--102758/command-outputs

# cat 'usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output' 3.要驗證故障切換配置和狀態. 請檢查show failover部分。

如果未配置故障轉移,將顯示以下輸出:

----- show failover -----

#### Failover Off

Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 1292 maximum MAC Address Move Notification Interval not set 如果配置了故障轉移,將顯示以下輸出:

----- show failover -----

#### Failover On

Failover unit Primary
Failover LAN Interface: fover Ethernet1/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.17(1), Mate 9.17(1)
Serial Number: Ours FLM2006EN9UR93, Mate FLM2006EQFWAGG
Last Failover at: 13:45:46 UTC May 20 2022

This host: Primary - Active

Active time: 161681 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Secondary - Standby Ready Active time: 0 (sec)

slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)
Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)...

4.為了驗證FTD集群配置和狀態,請檢查show cluster info部分。

如果未配置集群,將顯示以下輸出:

------ show cluster info -------Clustering is not configured 如果已配置並啟用集群,則顯示以下輸出:

----- show cluster info ------

Cluster	ftd_cluster	:1	: On					
Inte	erface mode:		spanned					
Cluster	Member Limi	.t	: 16					
This	s is "unit-1	-	1" in state MASTER					
	ID :		0					
	Site ID :		1					
	Version :		9.17(1)					
	Serial No.:		FLM1949C5RR6HE					
	CCL IP :		10.173.1.1					
	CCL MAC :		0015.c500.018f					
	Module :		FPR4K-SM-24					
	Resource :		20 cores / 44018 MB RAM					
	Last join :		13:53:52 UTC May 20 2022					
	Last leave:		N/A					
Other me	Other members in the cluster:							
Unit	"unit-2-1"	1	in state SLAVE					
	ID :		1					
	Site ID :		1					
	Version :		9.17(1)					
	Serial No.:		FLM2108V9YG7S1					
	CCL IP :		10.173.2.1					
	CCL MAC :		0015.c500.028f					
	Module :		FPR4K-SM-24					
	Resource :		20 cores / 44018 MB RAM					
	Last join :		14:02:46 UTC May 20 2022					
	Last leave:		14:02:31 UTC May 20 2022					

#### **FMC UI**

請按照以下步驟驗證FMC UI上的FTD高可用性和可擴充性配置和狀態:

### 1.選擇Devices > Device Management:

Firepower Management Center Overview / Dashboards / Management	w Analysis Policies	Devices Objects	AMP Intelliger	ice	Deploy	० 🊱	Ø Global \ admin ▼
Name           Access Controlled User Statistics Provides traffic and intrusion event statistics by user           Application Statistics Provides traffic and intrusion event statistics by application		2 Device Management Device Upgrade NAT QoS Platform Settings FlexConfig Certificates	VPN Site To Site Remote Accc Dynamic Acc Troubleshool Site to Site M	ess Policy ting tonitoring	Troubleshoot File Download Threat Defense Packet Tracer Packet Capture	e CLI e	Create Dashboard
Application Statistics (7.1.0) Provides application statistics Connection Summary Provides tables and charts of the activity on your monitored network segn	ent organized by different criteria			admin admin	No	No	
Detailed Dashboard Provides a detailed view of activity on the appliance				admin	No	No	12 Q / 1
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance				admin	No	No	₫٩≠₽
Files Dashboard Provides an overview of Malware and File Events				admin	No	No	╚९∕Т
Security Intelligence Statistics Provides Security Intelligence statistics				admin	No	No	╚९∕Т
Summary Dashboard Provides a summary of activity on the appliance				admin	No	Yes	╚९∕∎

2.為了驗證FTD高可用性和可擴充性配置,請檢查High Availability或Cluster標籤。如果兩者都不存 在,則FTD在獨立組態中執行:

View By: Domain   All (5) Error (0)   Warning (0) Offline (0)   Name Model   Version Chassis   Licenses Access Control Policy   Group	Add 🔻
Collapse All       Name       Model       Version       Chassis       Licenses       Access Control Policy       Group <ul> <li></li></ul>	
Name     Model     Version     Chassis     Licenses     Access Control Policy     Group       ↓ LAB2 (3)	
□ ∨ LAB2 (3) □ √ ftdcluster1 (2) [Cluster]	
ttd_cluster1 (2)	
	1:
10.62.148.188(Control) Short 3     10.62.148.188 - Routed     Firepower 4120 with FTD 7.1.0     III FP4120-5.443     Security Module - 1 (Container)     Base, Threat     acp1	:
Image: 10.62.148.191         Short 3         Firepower 4120 with FTD         7.1.0         KSEC-FPR4100-6 cisco com:443         Base, Threat         acp1	:
Tid_ha	/:
oftd_ha_1(Primary, Active)       Snort 3         10.62.148.89 - Transparent       Firepower 4150 with FTD       7.1.0       III KSEC-FPR4100-3:443 Security Module - 1 (Container)       Base, Threat       acp1	:
Image: Secondary, Standby)       Short 3         Firepower 4150 with FTD       7.1.0         Image: Security Module - 1 (Container)       Base, Threat         acp1	:
Image: bit d_standalone     Snort 3     Firepower 2120 with FTD     7.1.0     N/A     Base, Threat     acp1	1:

#### 3.為了驗證FTD高可用性和可擴充性狀態,請檢查括弧中的單位角色。如果角色不存在,且FTD不 屬於集群或故障轉移的一部分,則FTD在獨立配置中運行:

alialia cisco	Firepower Management Center Oven	riew Analysis Po	licies [	Devices Objects AMP		De	iploy Q 🍄 🌣 🔞 I	.AB2 \ admin 🔻
View By:	Domain						Deployn	nent History
All (5)	• Error (0) • Warning (0) • Offline (0)	Normal (5)     Dep	loyment Per	nding (0) • Upgrade (0) • Snor	rt 3 (5)		Q Search Device	Add 🔻
Collapse /								
•	lame	Model	Version	Chassis	Licenses	Access Control Policy	Group	
0 ~	LAB2 (3)							
	<ul> <li>ftd_cluster1 (2)</li> <li>Cluster</li> </ul>							1:
	10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	EP4120-5:443 Security Module - 1 (Container)	Base, Threat	acp1		:
	<ul> <li>10.62.148.191 Snort 3</li> <li>10.62.148.191 - Routed</li> </ul>	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1		:
	<ul> <li>√ ftd_ha High Availability</li> </ul>							1:
	ftd_ha_1(Primary, Active) Snort 3 10.62.148.89 - Transparent	Firepower 4150 with FTD	7.1.0	KSEC-FPR4100-3:443 Security Module - 1 (Container)	Base, Threat	acp1		:
	ftd_ha_2(Secondary, Standby) Snort 3 10.62.148.125 - Transparent	Firepower 4150 with FTD	7.1.0	Frepower-9300.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1		:
	td_standalone Snort 3     10.62.148.181 - Routed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1		1:

**附註**:在群集的情況下,僅顯示控制**單**元的角色。

#### **FMC REST API**

在這些輸出中, ftd\_ha\_1、ftd\_ha\_2、ftd\_standalone、ftd\_ha、ftc\_cluster1是使用者可配置的裝置 名。這些名稱不引用實際的高可用性和可擴充性配置或狀態。

請依照以下步驟操作,透過FMC REST-API驗證FTD高可用性及可擴充性組態和狀態。使用REST-API客戶端。在此範例中,使用**curl**:

#### 1. 請求身份驗證令牌:

# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc\_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
< X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
2.標識包含裝置的域。在大多數REST API查詢中, domain 引數是必需的。使用此查詢中的令牌檢 索域清單:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
ison.tool
{
  "items":
ſ
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-00000000000"
        },
```

3.使用域UUID查詢特定裝置記錄和特定裝置UUID:

4.為了驗證故障切換配置,請使用以下查詢中步驟3中的域UUID和裝置/容器UUID:

5.為了驗證故障切換狀態,請使用此查詢中步驟4中的域UUID和DeviceHAPair UUID:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devicehapairs/ftddevicehapairs/eec3ddfc-d842-11ec-a15e-986001c83f2f' -H 'X-auth-
access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
```

```
. . .
       "primaryStatus": {
            "currentStatus": "Active",
            "device": {
                "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
                "keepLocalEvents": false,
                "name": "ftd_ha_1"
            }
        },
        "secondaryStatus": {
            "currentStatus": "Standby",
            "device": {
                "id": "e60ca6d0-d83d-11ec-b407-cdc91a553663",
                "keepLocalEvents": false,
                "name": "ftd_ha_2"
            }
        }
```

6.為了驗證群集配置,請在此查詢中使用步驟3中的域UUID和裝置/容器UUID:

7. 要驗證群集狀態,請在此查詢中使用步驟6中的域UUID和裝置/容器UUID:

"id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
00000000000/deviceclusters/ftddevicecluster/8e6188c2-d844-11ec-bdd1-6e8d3e226370' -H 'X-auth-
access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
    "controlDevice": {
        "deviceDetails": {
            "id": "3344bc4a-d842-11ec-a995-817e361f7ea5",
            "name": "10.62.148.188",
            "type": "Device"
        }
    },
    "dataDevices": [
        {
            "deviceDetails": {
                "id": "a7ba63cc-d842-11ec-be51-f3efcd7cd5e5",
                "name": "10.62.148.191",
                "type": "Device"
            }
        }
    ],
```

```
"name": "ftd_cluster1",
"type": "DeviceCluster"
```

FDM UI

}

請按照一節中的步驟操作。

**FDM REST-API** 

請按照一節中的步驟操作。

FCM UI

FCM UI在Firepower 4100/9300和帶ASA的Firepower 2100平台模式下可用。

按照以下步驟驗證FCM UI上的FTD高可用性和可擴充性狀態:

1.若要確認FTD容錯移轉狀態,請檢查「邏輯裝置」頁面上的HA-ROLE屬性值:

Overview Interface	s Logical Devices	Security Engine	Platform Settings				System Tools Help admin
Logical Device List			(1 Container instance) 77% (66 of 86) Con	es Available			C Refresh Add •
ftd1	Sta	andalone	Status:ok				
Application	Version	Resource Pro	ofile Management IP	Gateway	Management Port	Status	
H FTD	7.1.0.90	RP20	10.62.148.89	10.62.148.1	Ethernet1/1	Online	💌 🎼 c 🗽 🔿
Interface N	ame 1/2 1/3		<b>Type</b> data data	Att C F M M K C	Initial Status: not-applicable           Duster Operational Status: not-applicable           InsErowers: not-applicable           InsErowers: not-applicable           InsErowers: not-applicable           InsErowers: not-applicable           Inservers: not	34.21/ -11ec-941d-b9083eb612d8	

**附註**:邏輯裝置識別符號旁邊的**Standalone**標籤是指機箱邏輯裝置配置,而不是FTD故障切換 配置。

2.要驗證FTD集群配置和狀態,請檢查「邏輯裝置」頁上的集群標籤和CLUSTER-ROLE屬性值:

Overview Inte	faces Logical Devices	Security Engine Platform	Settings				System Tools Help admin
Logical Device List		(1 Container	instance) 57% (26 of 46) Cores	: Available			C Refresh Add •
ftd_cluster1	a	ustered Status:ok					0 I
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
# FTD	7.1.0.90	RP20	10.62.148.188	10.62.148.129	Ethernet1/1	Online	💌 🎉 c 🔬 🖈
Interf	ice Name t-channel1 t-channel48.204		<b>Type</b> data cluster	Attribu Clust FIRE CLUS MCM UUID	tes or Operational Status : in-cluster owner.womr-IP : 10.62.148.188 TER-ROLE : control TER-IP : 10.173.11 TER-IP : 10.173.11 : control : control	1 184.21/ 2-11ec-a995-817e3617/ea5	

**FXOS CLI** 

Firepower 4100/9300上提供了FTD高可用性和可擴充性配置以及FXOS CLI上的狀態驗證。

按照以下步驟驗證FXOS CLI上的FTD高可用性及可擴充性組態和狀態:

1.建立到機箱的控制檯或SSH連線。

2.若要確認FTD高可用性狀態,請運行scope ssa 命令,然後運行scope slot <x>以切換到運行 FTD的特定插槽,並運行show app-instance expand 命令:

firepower # scope ssa firepower /ssa # scope slot 1 firepower /ssa/slot # show app-instance expand Application Instance: App Name: ftd Identifier: ftd1 Admin State: Enabled Oper State: Online Running Version: 7.1.0.90 Startup Version: 7.1.0.90 Deploy Type: Container Turbo Mode: No Profile Name: RP20 Cluster State: Not Applicable Cluster Role: None App Attribute: App Attribute Key Value ----- ----firepower-mgmt-ip 192.0.2.5 ha-lan-intf Ethernet1/2 ha-link-intf Ethernet1/2 ha-role active mgmt-url https://192.0.2.1/ 796eb8f8-d83b-11ec-941d-b9083eb612d8 uuid

3.若要驗證FTD叢集組態和狀態,請執行scope ssa 指令,執行show logical-device <name> detail expand 指令(其中名稱為邏輯裝置名稱),以及show app-instance 指令。檢查特定插槽的輸出:

```
firepower # scope ssa
firepower /ssa # show logical-device ftd_cluster1 detail expand
Logical Device:
  Name: ftd_cluster1
  Description:
  Slot ID: 1
  Mode: Clustered
  Oper State: Ok
  Template Name: ftd
  Error Msg:
  Switch Configuration Status: Ok
  Sync Data External Port Link State with FTD: Disabled
  Current Task:
firepower /ssa # show app-instance
App Name Identifier Slot ID Admin State Oper State Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State Cluster Role
----- -----
```

#### **FXOS REST API**

Firepower 4100/9300支援FXOS REST-API。

按照以下步驟通過FXOS REST-API請求驗證FTD高可用性和可擴充性配置和狀態。使用REST-API客戶端。在此範例中,使用curl:

1.請求身份驗證令牌:

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
{
        "refreshPeriod": "0",
         "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb8888816c94d"
}
2.若要確認FTD容錯移轉狀態,請使用以下查詢中的權杖和插槽ID:
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb8888816c94d'
'https://192.0.2.100/api/slot/1/app-inst'
. . .
{ "smAppInstance"
"sec-svc/app-ftd-7.1.0.90", "appinstance"
"clearLogData": "available",
"clearLogData": "clearLogData": "clearLogData"; 
                                                                                                "adminState": "enabled",
                                                                                                                                                                                  "appDn":
                                                                                  "appInstId": "ftd_001_JAD201200R43VLP1G3",
"clusterOperationalState": "not-applicable",
                                                                                                                         "clusterRole": "none",
"currentJobProgress": "100",
                                                                                     "currentJobState": "succeeded",
"currentJobType": "start",
                                                                                "deployType": "container",
                                                                                                                                                                     "dn": "slot/1/app-
inst/ftd-ftd1",
                                                          "errorMsg": "",
                                                                                                                      "eventMsg": "",
"executeCmd": "ok",
                                                               "externallyUpgraded": "no",
                                                                                                                                                        "fsmDescr": "",
                         "fsmProgr": "100",
                                                                         "fsmRmtInvErrCode": "none",
                                                                              "fsmRmtInvRslt": "",
"fsmRmtInvErrDescr": "",
                                                                                                                                                    "fsmStageDescr": "",
                         "fsmStatus": "nop",
                                                                               "fsmTry": "0",
                                                                                                                                                      "hotfix": "",
  "identifier": "ftd1",
                         "operationalState": "online",
                         "reasonForDebundle": "",
                         "resourceProfileName": "RP20",
                         "runningVersion": "7.1.0.90",
                          "smAppAttribute": [
                                  {
                                          "key": "firepower-mgmt-ip",
                                          "rn": "app-attribute-firepower-mgmt-ip",
                                          "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
firepower-mgmt-ip",
                                          "value": "192.0.2.5"
                                  },
                                  {
                                          "key": "ha-link-intf",
                                          "rn": "app-attribute-ha-link-intf",
                                          "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-link-intf",
                                          "value": "Ethernet1/2"
                                  },
                                  {
                                          "key": "ha-lan-intf",
                                          "rn": "app-attribute-ha-lan-intf",
                                          "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
```

```
ha-lan-intf",
                    "value": "Ethernet1/2"
                },
                {
                    "key": "mgmt-url",
                    "rn": "app-attribute-mgmt-url",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
mgmt-url",
                    "value": "https://192.0.2.1/"
                },
                {
                    "key": "ha-role",
                    "rn": "app-attribute-ha-role",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-role",
                    "value": "active"
                },
                {
                    "key": "uuid",
                    "rn": "app-attribute-uuid",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
uuid",
                    "value": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
                }
            ],
```

3. 要驗證FTD集群配置,請在此查詢中使用邏輯裝置識別符號:

. . .

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.102/api/ld/ftd_cluster1'
```

```
{
    "smLogicalDevice": [
        {
            "description": "",
            "dn": "ld/ftd_cluster1",
            "errorMsg": "",
            "fsmDescr": "",
            "fsmProgr": "100",
            "fsmRmtInvErrCode": "none",
            "fsmRmtInvErrDescr": "",
            "fsmRmtInvRslt": "",
            "fsmStageDescr": "",
            "fsmStatus": "nop",
            "fsmTaskBits": "",
            "fsmTry": "0",
            "ldMode": "clustered",
            "linkStateSync": "disabled",
            "name": "ftd_cluster1",
            "operationalState": "ok",
   "slotId": "1",
                               "smClusterBootstrap": [
                                                                        {
"cclNetwork": "10.173.0.0",
                                                 "chassisId": "1",
"gatewayv4": "0.0.0.0",
                                                                                     "key": "",
                                             "gatewayvб": "::",
                    "mode": "spanned-etherchannel",
                                                                          "name": "ftd_cluster1",
                    "netmaskv4": "0.0.0.0",
                                                                  "poolEndv4": "0.0.0.0",
           "poolEndv6": "::",
                                                   "poolStartv4": "0.0.0.0",
                                                                                   "rn": "cluster-
"poolStartv6": ":::",
                                          "prefixLength": "",
bootstrap",
                                 "siteId": "1",
                                                                     "supportCclSubnet":
                                  "updateTimestamp": "2022-05-20T13:38:21.872",
"supported",
                    "urllink": "https://192.0.2.101/api/ld/ftd_cluster1/cluster-bootstrap",
                    "virtualIPv4": "0.0.0.0",
                                                                   "virtualIPv6": "::"
                }
                              ], ...
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb8888816c94d'
'https://192.0.2.102/api/slot/1/app-inst'
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_JAD19500BABIYA30058",
            "appName": "ftd",
            "clearLogData": "available",
            "clusterOperationalState": "in-cluster",
            "clusterRole": "master",
            "currentJobProgress": "100",
            "currentJobState": "succeeded",
            "currentJobType": "start",
            "deployType": "container",
            "dn": "slot/1/app-inst/ftd-ftd_cluster1",
            "errorMsg": "",
            "eventMsg": "",
            "executeCmd": "ok",
            "externallyUpgraded": "no",
            "fsmDescr": "",
            "fsmProgr": "100",
            "fsmRmtInvErrCode": "none",
            "fsmRmtInvErrDescr": "",
            "fsmRmtInvRslt": "",
            "fsmStageDescr": "",
            "fsmStatus": "nop",
            "fsmTry": "0",
            "hotfix": "",
            "identifier": "ftd_cluster1",
            "operationalState": "online",
            "reasonForDebundle": "",
            "resourceProfileName": "RP20",
            "runningVersion": "7.1.0.90",
```

. . .

#### FXOS機箱show-tech檔案

FTD高可用性及可擴充性組態和狀態可在Firepower 4100/9300機箱show-tech檔案中驗證。

按照以下步驟驗證FXOS機箱show-tech檔案中的高可用性和可擴充性配置和狀態:

1. 對於FXOS 2.7及更高版本,請在

<name>\_BC1\_all.tar/FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中開啟 sam\_techsupportinfo 檔案

對於早期版本,請在FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中開啟 sam\_techsupportinfo 文**件。** 

2.為了驗證故障轉移狀態,請檢查「show slot expand detail」一節中特定插槽下的ha-role屬性值:

```
. . .
`show slot expand detail`
Slot:
   Slot ID: 1
   Log Level: Info
   Admin State: Ok
   Oper State: Online
   Disk Format State: Ok
   Disk Format Status: 100%
   Clear Log Data: Available
   Error Msg:
   Application Instance:
       App Name: ftd
       Identifier: ftd1
       Admin State: Enabled
       Oper State: Online
       Running Version: 7.1.0.90
       Startup Version: 7.1.0.90
       Deploy Type: Container
       Turbo Mode: No
       Profile Name: RP20
       Hotfixes:
       Externally Upgraded: No
       Cluster State: Not Applicable
       Cluster Role: None
       Current Job Type: Start
       Current Job Progress: 100
       Current Job State: Succeeded
       Clear Log Data: Available
       Error Msg:
       Current Task:
       App Attribute:
           App Attribute Key: firepower-mgmt-ip
           Value: 10.62.148.89
           App Attribute Key: ha-lan-intf
           Value: Ethernet1/2
           App Attribute Key: ha-link-intf
           Value: Ethernet1/2
           App Attribute Key: ha-role
           Value: active
           App Attribute Key: mgmt-url
           Value: https://10.62.184.21/
3.為了驗證FTD叢集組態,請檢查「show logical-device detail expand」一節中特定插槽下的
Mode屬性值:
`show logical-device detail expand`
Logical Device:
   Name: ftd_cluster1
   Description:
   Slot ID: 1
   Mode: Clustered
```

```
Error Msg:
Switch Configuration Status: Ok
```

Oper State: Ok Template Name: ftd Sync Data External Port Link State with FTD: Disabled Current Task: Cluster Bootstrap: Name of the cluster: ftd\_cluster1 Mode: Spanned Etherchannel Chassis Id: 1 Site Id: 1 Key: Cluster Virtual IP: 0.0.0.0 IPv4 Netmask: 0.0.0.0 IPv4 Gateway: 0.0.0.0 Pool Start IPv4 Address: 0.0.0.0 Pool End IPv4 Address: 0.0.0.0 Cluster Virtual IPv6 Address: :: IPv6 Prefix Length: IPv6 Gateway: :: Pool Start IPv6 Address: :: Pool End IPv6 Address: :: Last Updated Timestamp: 2022-05-20T13:38:21.872 Cluster Control Link Network: 10.173.0.0

#### 4.為了驗證FTD集群狀態,請檢查「**show slot expand detail」**部分中特定插槽下的**集群狀態**和**集群** 角色屬性值:

```
`show slot expand detail`
Slot:
   Slot ID: 1
   Log Level: Info
   Admin State: Ok
   Oper State: Online
   Disk Format State: Ok
   Disk Format Status:
   Clear Log Data: Available
   Error Msg:
   Application Instance:
       App Name: ftd
        Identifier: ftd_cluster1
       Admin State: Enabled
        Oper State: Online
       Running Version: 7.1.0.90
       Startup Version: 7.1.0.90
       Deploy Type: Native
       Turbo Mode: No
       Profile Name:
       Hotfixes:
       Externally Upgraded: No
        Cluster State: In Cluster
       Cluster Role: Master
       Current Job Type: Start
       Current Job Progress: 100
        Current Job State: Succeeded
       Clear Log Data: Available
       Error Msg:
        Current Task:
```

### ASA高可用性和可擴充性

可以使用以下選項驗證ASA高可用性和可擴充性配置和狀態:

- ASA CLI
- ASA SNMP輪詢
- ASA show-tech檔案
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS機箱show-tech檔案

#### ASA CLI

按照以下步驟驗證ASA CLI上的ASA高可用性和可擴充性配置:

- 1. 根據平台和部署模式,使用以下選項訪問ASA CLI:
- 在裝置模式下直接通過telnet/SSH訪問Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下從Firepower 2100上的FXOS控制檯CLI訪問,並使用**connect asa** 命令連線到 ASA
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問:
   connect module <x> [console]telnet],其中x是插槽ID,然後連接asa

•對於虛擬ASA,直接通過SSH訪問ASA,或者通過虛擬機器監控程式或雲UI進行控制檯訪問 2.為了驗證ASA故障切換配置和狀態,請在ASA CLI上運行show running-config failover和show failover state命令。

如果未配置故障轉移,將顯示以下輸出:

asa# show running-config failover no failover asa# show failover state Last Failure Reason Date/Time State This host -Secondary Disabled None Other host -Primary Not Detected None ====Configuration State=== ====Communication State== 如果配置了故障轉移,將顯示以下輸出:

asa# show running-config failover
failover failover lan unit primary
failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 10.30.35.2 255.255.0 standby 10.30.35.3
# show failover state

11 10			
	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		

====Communication State===

Mac set

3.為了驗證ASA群集配置和狀態,請在CLI上運行**show running-config cluster**和**show cluster info**命 令。

如果未配置集群,將顯示以下輸出:

asa# show running-config cluster asa# show cluster info Clustering is not configured 如果已配置集群,則顯示以下輸出:

```
asa# show running-config cluster
cluster group asa_cluster1
key *****
local-unit unit-1-1
cluster-interface Port-channel48.205 ip 10.174.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
no unit join-acceleration
enable
```

```
asa# show cluster info

Cluster asa_cluster1: On

Interface mode: spanned

Cluster Member Limit : 16

This is "unit-1-1" in state MASTER

ID : 0

Site ID : 1

Version : 9.17(1)

Serial No.: FLM2949C5232IT

CCL IP : 10.174.1.1

CCL MAC : 0015.c500.018f

Module : FPR4K-SM-24
```

ASA SNMP

按照以下步驟通過SNMP驗證ASA高可用性和可擴充性配置:

1. 確保已配置並啟用SNMP。

2. 為了驗證故障切換配置和狀態輪詢OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1。** 如果未配置故障轉移,將顯示以下輸出:

19:42:22 UTC May 21 2022

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
如果配置了故障轉移,將顯示以下輸出:
```

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.10 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit (this device)" <--
This device is primary
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 9
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 10
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "fover Ethernet1/2"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "fover Unit" <--
Primary device is active
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Standby unit"
3.為了驗證群集配置和狀態,請輪詢OID 1.3.6.1.4.1.9.9.491.1.8.1。</pre>
```

如果未配置集群,將顯示以下輸出:

```
# snmpwalk -v2c -c cisco123 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
SNMPv2-SMI::enterprises.9.9.491.1.8.1.1.0 = INTEGER: 0
如果已配置但未啟用集群,則顯示以下輸出:
```

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0 <-- Cluster status, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0 <-- Cluster unit state, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "asa_cluster1" <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1" <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0 <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1 <-- Cluster side ID</pre>
```

如果群集已配置、已啟用且運行正常,則顯示以下輸出:

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 1 <-- Cluster status, enabled
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 16 <-- Cluster unit state, control unit
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "asa_cluster1" <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1" <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0 <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1 <-- Cluster side ID
...</pre>
```

有關OID描述的詳細資訊,請參閱<u>CISCO-UNIFIED-FIREWALL-MIB</u>。

ASA show-tech檔案

. . .

1. 要驗證ASA故障切換配置和狀態,請檢查show failover 部分。

如果未配置故障轉移,將顯示以下輸出:

----- show failover ------

#### Failover Off

Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 1292 maximum MAC Address Move Notification Interval not set 如果配置了故障轉移.將顯示以下輸出:

----- show failover -----

Failover On Failover unit Primary Failover LAN Interface: fover Ethernet1/2 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 1 of 1291 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.17(1), Mate 9.17(1) Serial Number: Ours FLM2006EN9AB11, Mate FLM2006EQZY02 Last Failover at: 13:45:46 UTC May 20 2022 This host: Primary - Active Active time: 161681 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys) Other host: Secondary - Standby Ready

Active time: 0 (sec)

slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)

•••

2.若要驗證群集配置和狀態,請檢查show cluster info 部分。

如果未配置集群,將顯示以下輸出:

------ show cluster info -------Clustering is not configured 如果已配置並啟用集群,則顯示以下輸出:

------ show cluster info ------Cluster asa\_cluster1: On Interface mode: spanned Cluster Member Limit : 16 This is "unit-1-1" in state MASTER ID : 0 Site ID : 1 Version : 9.17(1) Serial No.: FLM2949C5232IT

CCL IP	:	10.174.1.1
CCL MAC	:	0015.c500.018f
Module	:	FPR4K-SM-24

#### FCM UI

. . .

請按照一節中的步驟操作。

**FXOS CLI** 

請按照一節中的步驟操作。

**FXOS REST-API** 

請按照一節中的步驟操作。

#### FXOS機箱show-tech檔案

請按照一節中的步驟操作。

## 驗證防火牆模式

#### FTD防火牆模式

防火牆模式是指路由或透明防火牆配置。

可以使用以下選項驗證FTD防火牆模式:

- FTD CLI
- FTD show-tech
- FMC UI
- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS機箱show-tech檔案

附註:FDM不支援透明模式。

FTD CLI

執行以下步驟驗證FTD CLI上的FTD防火牆模式:

1.根據平台和部署模式,使用以下選項訪問FTD CLI:

- 直接通過SSH訪問FTD 所有平台
- 通過connect ftd指令,從FXOS主控台CLI(Firepower 1000/2100/3100)進行存取
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問:

connect module <x> [console]telnet],其中x是插槽ID,然後

連線ftd [例項],其中例項僅與多例項部署相關。

 對於虛擬FTD,直接通過SSH訪問FTD,或透過虛擬機器監控程式或雲使用者介面進行主控台 訪問

2.若要驗證防火牆模式,請在CLI上執行show firewall命令:

> show firewall
Firewall mode: Transparent

#### FTD疑難排解檔案

執行以下步驟驗證FTD疑難排解檔案中的FTD防火牆模式:

1.開啟故障排除檔案,導航到資料夾<filename>-troubleshoot .tar/results-<date>---xxxxxx/command-output。

2. 開啟文件usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output:

# pwd /ngfw/var/common/results-05-22-2022--102758/command-outputs # cat 'usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output' 3.若要確認FTD防火牆模式,請檢查show firewall 一節:

----- show firewall -----

Firewall mode: Transparent

FMC UI

按照以下步驟驗證FMC UI上的FTD防火牆模式:

1.選擇Devices > Device Management:

Firepower Management Center Overview / Dashboards / Management Overview / Dashboards / Management	lligence	Deploy	० 🌮🌣 ।	Ø Global \ admin ▼
Name     VPN       Name     Device Management     VPN       NAT     Remote       Access Controlled User Statistics     QoS     Dynamic       Provides traffic and intrusion event statistics by user     Platform Settings     Troubles       Application Statistics     FlexConfig     Site to statistics       Provides traffic and intrusion event statistics by application     Certificates     Certificates	Site Access c Access Policy shooting Site Monitoring	Troubleshoot File Download Threat Defense Packet Tracer Packet Capture	e CLI	reate Dashboard
Application Statistics (7.1.0) Provides application statistics	admin	No	No	12 Q / 1
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	C < / 🕯
Detailed Dashboard Provides a detailed view of activity on the appliance	admin	No	No	₫ Q 🖊 🗑
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance	admin	No	No	₫ Q 🖊 🗑
Files Dashboard Provides an overview of Malware and File Events	admin	No	No	12 Q / 1
Security Intelligence Statistics Provides Security Intelligence statistics	admin	No	No	C < / 7
Summary Dashboard Provides a summary of activity on the appliance	admin	No	Yes	CQ/T

### 2.檢查Routed或Transparent標籤:

Firepower Manage	ement Center Overvie	ew Analysis Po	licies D	evices Objects AMP		De	ploy Q 🍄 🌣 🔞 l	.AB2 ∖ admin ▼		
View By: Domain All (5) • Error (0) • W	Varning (0) Offline (0)	<ul> <li>Normal (5)</li> </ul>	oloyment Pen	ding (0) • Upgrade (0) • Sno	rt 3 (5)		Deployn	Add 🔻		
Collapse All										
Name		Model	Version	Chassis	Licenses	Access Control Policy	Group			
🗌 🗸 LAB2 (3)										
Cluster (2)								1:		
10.62.148.188(Con 10.62.148.188 - Ro	short 3 buted	Firepower 4120 with FTD	7.1.0	EP4120-5:443 Security Module - 1 (Container)	Base, Threat	acp1		:		
10.62.148.191 Sn 10.62.148.191 - 10.62.148.191 - 10.62.148.191	ort 3	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1		:		
<pre>ftd_ha High Availability</pre>								1:		
ftd_ha_1(Primary, / 10.62.148.89 - Trans	Active) Snort 3	Firepower 4150 with FTD	7.1.0	EXEC-FPR4100-3:443 Security Module - 1 (Container)	Base, Threat	acp1		:		
ftd_ha_2(Secondar 10.62.148.125 - Irr	ry, Standby) Snort 3 ansparent	Firepower 4150 with FTD	7.1.0	Frepower-9300.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1		:		
ftd_standalone Snort 10.62.148.181 - Route	t 3 ed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1		1:		

#### **FMC REST-API**

請依照以下步驟操作,透過FMC REST-API驗證FTD防火牆模式。使用REST-API客戶端。在此範 例中,使用**curl**:

1. 請求身份驗證令牌:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
< X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb</pre>
```

```
2.標識包含裝置的域。在大多數REST API查詢中,domain 引數是必需的。使用此查詢中的令牌檢
索域清單:
```

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
  "items":
[
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-00000000000"
        },
. . .
```

3.使用域UUID查詢特定裝置記錄和特定裝置UUID:

4.在此查詢中使用步驟3中的域UUID和裝置/容器UUID,並檢查ftdMode的值:

```
# curl -s -k -X 'GET' 'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
00000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
...
```

```
{
    "accessPolicy": {
        "id": "00505691-3a23-0ed3-0006-536940224514",
        "name": "acp1",
        "type": "AccessPolicy"
    },
    "advanced": {
        "enableOGS": false
    },
    "description": "NOT SUPPORTED",
    "ftdMode": "ROUTED",
```

#### FCM UI

. . .

您可以在Firepower 4100/9300上驗證FTD的防火牆模式。

按照以下步驟驗證FCM UI上的FTD防火牆模式:

1.在Logical Devices(邏輯裝置)頁面上編輯邏輯裝置:

Overv	iew Interface	s Logical Devices	Security Engine	Platform Settings				System Tools Help admin
Logical	Device List	1		(1 Container instance) 77% (66 of 86	i) Cores Available			C Refresh Add •
ftd	ι		Standalone	Status:ok				2 🖉
A	plication	Version	Resource Pr	ofile Management IP	Gateway	Managen	nent Port Status	
⊕ F	O	7.1.0.90	RP20	10.62.148.89	10.62.148.1	Ethernet1	/1 Online	🚾 🎘 C 🚈 🖈
	Interface N	ame		Туре		Attributes		
	Ethernet	1/2		data		Cluster Operational Statu	s: not-applicable	
	Ethernet	1/3		data		FIREPOWER-MGMT-IP HA-LINK-INTF HA-LAN-INTF MGMT-URL HA-ROLE UUID	: 10.62.148.89 : Ethernet1/2 : Ethernet1/2 : https://10.62.184.21/ : active : 796eb8f8-d83b-11ec-941d-b9083eb612d8	

### 2.按一下應用程式圖示,然後在「設定」頁籤中選中**防火牆**模式:

Ove	erview Interface	s Logio	cal Devices Security E	ngine Platform Settings					System Tools Help admin
Edit Sta	ting - ftd1 ndalone   Cisco Fire	epower Ti	hreat Defense   7.1.0.90	Cisco Firepower Threat Defense - I	Bootstrap Configuration		×		Save Cancel
Data	a Ports			General Information Settings Agree	ement	^	<u> </u>		
	Ethernet1/2 Ethernet1/3			Permit Expert mode for FTD SSH sessions:	yes	•			
	Ethernet1/4			Search domains:	cisco com				
_	Ethernet1/5			Firmer Noday	Terroret				_
+	Ethernet1/6			Firewaii Mode:	Transparent		1		
	Ethernet1/8			DNS Servers:	8.8.8.8		- ·		
				Fully Qualified Hostname:					
				Password:		Set: Yes	FTD - 7.1.0	.90	
				Confirm Password:			Click to config	jure	
				Registration Key:		Set: Yes			
				Confirm Registration Key:					
				Firepower Management Center IP:	10.62.184.21				
				Firepower Management Center NAT ID					
				Freeboo Telefore					
				Eventing Interface:					
	Application	Version	Resou	Hardware Crypto:	Enabled	·	danagement Port	Status	
	FTD	7.1.0.90	RP20			~	themet1/1	online	
	Interface Nan	e		1700	ОК	Cancel	-		
	Ethernet1/	2		data					
	Ethernet1/	3		data					

### **FXOS CLI**

您可以在Firepower 4100/9300上驗證FTD的防火牆模式。

請依照以下步驟在FXOS CLI上驗證FTD防火牆模式:

- 1. 建立到機箱的控制檯或SSH連線。
- 切換到作用域sa,然後切換到特定的**邏輯裝置,**運行show mgmt-bootstrap expand 命令,並 檢查FIREWALL\_MODE屬性值:

firepower# scope ssa
firepower /ssa # scope logical-device ftd\_cluster1
firepower /ssa/logical-device # show mgmt-bootstrap expand

Management Configuration: App Name: ftd

Secret Bootstrap Key: Kev Value ----- -----PASSWORD REGISTRATION\_KEY IP v4: Slot ID Management Sub Type IP Address Netmask Gateway Last Updated Timestamp \_\_\_\_\_ 1 Firepower 10.62.148.188 255.255.255.128 10.62.148.129 2022-05-20T13:50:06.238 Bootstrap Key: Kev Value ----- -----DNS\_SERVERS 192.0.2.250 FIREPOWER\_MANAGER\_IP 10.62.184.21 FIREWALL MODE routed PERMIT\_EXPERT\_MODE yes SEARCH\_DOMAINS cisco.com . . .

#### **FXOS REST API**

Firepower 4100/9300支援FXOS REST-API。

請依照以下步驟操作,透過FXOS REST-API要求驗證FTD防火牆模式。使用REST-API客戶端。在 此範例中,使用**curl**:

1. 請求身份驗證令牌:

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123'
https://192.0.2.100/api/ld/ftd_cluster1
{
    "refreshPeriod": "0",
    "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d"
}
2.使用此查詢中的邏輯裝置識別符號並檢查FIREWALL_MODE鍵的值:
```

#### FXOS機箱show-tech檔案

FTD的防火牆模式可在Firepower 4100/9300的show-tech檔案中驗證。

按照以下步驟驗證FXOS機箱show-tech檔案中的FTD防火牆模式:

1. 對於FXOS 2.7及更高版本,請在<name>\_BC1\_all.tar/

FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中開啟sam\_techsupportinfo 檔案 對於早期版本,請在FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar中開啟 sam\_techsupportinfo 檔案。

2. 檢查特定識別符號和插槽下的show logical-device detail expand部分:

# pwd /var/tmp/20220313201802\_F241-01-11-FPR-2\_BC1\_all/FPRM\_A\_TechSupport/ # cat sam\_techsupportinfo . . . `show logical-device detail expand` Logical Device: Name: ftd\_cluster1 Description: Slot ID: 1 Mode: Clustered Oper State: Ok Template Name: ftd Error Msg: Switch Configuration Status: Ok Sync Data External Port Link State with FTD: Disabled Current Task: . . . Bootstrap Key: Key: DNS\_SERVERS Value: 192.0.2.250 Last Updated Timestamp: 2022-05-20T13:28:37.093 Key: FIREPOWER\_MANAGER\_IP Value: 10.62.184.21 Last Updated Timestamp: 2022-05-20T13:28:37.093 Key: FIREWALL\_MODE Value: routed Last Updated Timestamp: 2022-05-20T13:28:37.093

#### • • •

### ASA防火牆模式

可以使用以下選項驗證ASA防火牆模式:

- ASA CLI
- ASA show-tech
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS機箱show-tech檔案

#### ASA CLI

按照以下步驟驗證ASA CLI上的ASA防火牆模式:

1. 根據平台和部署模式,使用以下選項訪問ASA CLI:

- 在裝置模式下直接通過telnet/SSH訪問Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下從Firepower 2100上的FXOS控制檯CLI訪問,並使用**connect asa** 命令連線到 ASA
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問: connect module <x> [console|telnet],其中x是插槽ID,然後連接asa

•對於虛擬ASA,直接通過SSH訪問ASA,或者通過虛擬機器監控程式或雲UI進行控制檯訪問 2.在CLI上執行**show firewall**命令:

asa# show firewall Firewall mode: Routed

ASA show-tech檔案

要驗證ASA防火牆模式,請檢查show firewall 部分:

----- show firewall ------ Firewall mode: Routed

#### FCM UI

請按照一節中的步驟操作。

**FXOS CLI** 

請按照一節中的步驟操作。

**FXOS REST-API** 

請按照一節中的步驟操作。

#### FXOS機箱show-tech檔案

請按照一節中的步驟操作。

## 驗證例項部署型別

有兩種應用程式例項部署型別:

- 本機例項 本機例項使用安全模組/引擎的所有資源(CPU、RAM和磁碟空間),因此您只能 安裝一個本機例項。
- 容器例項 容器例項使用安全模組/引擎的資源子集。只有FMC管理的FTD支援多例項功能
   ; asa或由FDM管理的FTD不支援此功能。

只有Firepower 4100/9300上的FTD支援容器模式例項組態。

可以使用以下選項驗證例項部署型別:

- FTD CLI
- FTD顯示技術
- FMC UI
- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS機箱show-tech檔案

### FTD CLI

請依照以下步驟操作,驗證FTD CLI上的FTD執行個體部署型別:

- 1. 根據平台和部署模式,使用以下選項訪問FTD CLI:
- 直接通過SSH訪問FTD 所有平台
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問:

connect module <x> [console|telnet],其中x是插槽ID,然後connect ftd [instance],其中例項僅與多例項部署相關。

2. 運行show version system命令,並檢查包含字串SSP Slot Number的行。如果此行存在 Container,則FTD會在容器模式下執行:

> show version system

 ------ [ firepower ]----- 

 Model
 : Cisco Firepower 4120 Threat Defense (76) Version 7.1.0 (Build 90)

 UUID
 : 3344bc4a-d842-11ec-a995-817e361f7ea5

 VDB version
 : 346

Cisco Adaptive Security Appliance Software Version 9.17(1) SSP Operating System Version 2.11(1.154)

Compiled on Tue 30-Nov-21 18:38 GMT by builders System image file is "disk0:/fxos-lfbff-k8.2.11.1.154.SPA" Config file at boot was "startup-config"

firepower up 2 days 19 hours Start-up time 3 secs

SSP Slot Number: 1 (Container)

#### FTD疑難排解檔案

請依照以下步驟操作,驗證FTD疑難排解檔案中的FTD例項部署型別:

- 1. 開啟疑難排解檔案並導覽至<filename>-troubleshoot .tar/results-<date>-xxxxxx/commandoutput資料夾。
- 2. 開啟文件usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output:

/ngfw/var/common/results-05-22-2022--102758/command-outputs

# cat 'usr-local-sf-bin-sfcli.pl show\_tech\_support asa\_lina\_cli\_util.output'

#### 3. 檢查包含字串SSP Slot Number的行。如果此行存在Container,則FTD會在容器模式下執行:

[	firepower ]
Model	: Cisco Firepower 4120 Threat Defense (76) Version 7.1.0 (Build 90)
UUID	: 3344bc4a-d842-11ec-a995-817e361f7ea5
VDB version	: 346

Cisco Adaptive Security Appliance Software Version 9.17(1) SSP Operating System Version 2.11(1.154)

Compiled on Tue 30-Nov-21 18:38 GMT by builders System image file is "disk0:/fxos-lfbff-k8.2.11.1.154.SPA" Config file at boot was "startup-config"

```
firepower up 2 days 19 hours
Start-up time 3 secs
```

```
SSP Slot Number: 1 (Container)
```

### **FMC UI**

按照以下步驟驗證FMC UI上的FTD例項部署型別:

#### 1. 選擇Devices > Device Management:

Firepower Management Center     Overview / Dashboards / Management     Overview     Analysis     Policies	Devices Objects AMP Intellig	ence	Deploy	० 🌮🌣	Ø Global \ admin ▼
Name           Access Controlled User Statistics           Provides traffic and intrusion event statistics by user           Application Statistics           Provides traffic and intrusion event statistics by application	2         Device Management         VPN           Device Upgrade         Site To Site           NAT         Remote Ac           QoS         Dynamic A           Platform Settings         Troublesho           FlexConfig         Site to Site           Certificates         Site to Site	cess ccess Policy oting Monitoring	Troubleshoot File Download Threat Defens Packet Tracer Packet Captur	e CLI	Create Dashboard
Application Statistics (7.1.0) Provides application statistics		admin	No	No	C < / T
Connection Summary Provides tables and charts of the activity on your monitored network segment organized by different criteria		admin	No	No	╚़⊲∕≆
Detailed Dashboard Provides a detailed view of activity on the appliance		admin	No	No	C < / T
Detailed Dashboard (7.0.0) Provides a detailed view of activity on the appliance		admin	No	No	C < / 7
Files Dashboard Provides an overview of Malware and File Events		admin	No	No	C < / 7
Security Intelligence Statistics Provides Security Intelligence statistics		admin	No	No	C < / 7
Summary Dashboard Provides a summary of activity on the appliance		admin	No	Yes	C < / T

2. 檢查Chassis列。如果行中存在Container,則FTD會在容器模式下運行。

Firepower Management Center Ove	rview Analysis P	olicies	Devices Objects AMP		De	ploy Q 🍄🌣 🍘 L	.AB2 \ admin ▼
View By: Domain 🔹						Deploym	nent History
All (5) • Error (0) • Warning (0) • Offline (0)	Normal (5)	eployment P	ending (0) • Upgrade (0) • Sn	ort 3 (5)		Q, Search Device	Add 🔻
Collapse_All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Group	
□ ∨ LAB2 (3)							^
Cluster (2)							1
10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	EP4120-5:443 Security Module - 1 (Container)	Base, Threat	acp1		:
<ul> <li>10.62.148.191 Snort 3</li> <li>10.62.148.191 - Routed</li> </ul>	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1		:
□ ∨ <mark>ftd_ha</mark> High Availability							1
ftd_ha_1(Primary, Active) Snort 3 10.62.148.89 - Transparent	Firepower 4150 with FTD	7.1.0	間 KSEC-FPR4100-3:443 Security Module - 1 (Container)	Base, Threat	acp1		:
ftd_ha_2(Secondary, Standby) Snort 3 10.62.148.125 - Transparent	Firepower 4150 with FTD	7.1.0	Frepower-9300 cisco.com/443 Security Module - 1 (Container)	Base, Threat	acp1		:

#### **FMC REST-API**

請按照以下步驟通過FMC REST-API驗證FTD例項部署型別。使用REST-API客戶端。在此範例中 ,使用**curl**:

1. 請求身份驗證令牌:

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H
'Authentication: Basic' -u 'admin:Cisco123' | grep -i X-auth-access-token
< X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
2.標識包含裝置的域。在大多數REST API查詢中, domain 引數是必需的。使用此查詢中的令牌檢
索域清單:
```

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
  "items":
[
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-00000000000"
        },
```

3.使用域UUID查詢特定裝置記錄和特定裝置UUID:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
```

```
"items": [
```

```
{
    "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
    "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
0000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
        },
        "name": "ftd_ha_1",
        "type": "Device"
     },
...
```

4.使用此查詢中步驟3中的域UUID和裝置/容器UUID,並檢查isMultiInstance的值:

```
# curl -s -k -X 'GET' 'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
00000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept:
application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
...
"name": "ftd_cluster1",
"isMultiInstance": true,
```

## **FCM UI**

. . .

若要驗證FTD執行個體部署型別,請檢查「邏輯裝置」中**「資源設**定檔」屬性的值。如果值不為空 ,則FTD在容器模式下執行:

Overv	iew Interfaces	Logical Devices	Security Engine	Platform Sett	ings				System Tools Help admin
Logical	Device List	(1 Container instance) 57% (26 of 46) Cores Available							
ftd	duster1	c	lustered	Status:ok					0 I
Al B FT	plication	Version 7.1.0.90	Resource Prof	ile	Management IP 10.62.148.188	Gateway 10.62.148.129	Management Port Ethernet1/1	Status	🚾 🌠 c 🚈 み

## **FXOS CLI**

按照以下步驟驗證FXOS CLI上的FTD例項部署型別:

- 1. 建立到機箱的控制檯或SSH連線。
- 切換到scope ssa, 然後運行show app-instance命令, 然後根據插槽和識別符號檢查特定 FTD的Deploy Type列:

firepower # scope ssa firepower /ssa # show app-instance App Name Identifier Slot ID Admin State Oper State Running Version Startup Version Deploy Type Turbo Mode Profile Name Cluster State Cluster Role \_\_\_\_ \_\_ \_\_\_\_\_ \_ Enabled Online 7.1.0.90 7.1.0.90 ftd\_cluster1 1 ftd Container No RP20 In Cluster Master

### **FXOS REST API**

按照以下步驟通過FXOS REST-API請求驗證FTD例項部署型別。使用REST-API客戶端。在此範例

```
中,使用curl:
```

1. 請求身份驗證令牌:

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://10.62.148.88/api/login'
{
    "refreshPeriod": "0",
    "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d"
}
2.在此查詢中指定令牌、插槽ID,並檢查deployType的值:
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb8888816c94d'
https://192.0.2.100/api/slot/1/app-inst
... {
      "smAppInstance": [
                                  {
                                                 "adminState": "enabled",
                                                                                      "appDn":
"sec-svc/app-ftd-7.1.0.90",
                                        "appInstId": "ftd_001_JAD201200R43VLP1G3",
                            "clearLogData": "available",
"appName": "ftd",
"clusterOperationalState": "not-applicable",
                                                         "clusterRole": "none",
"currentJobProgress": "100",
                                        "currentJobState": "succeeded",
                                     "deployType": "container",
"currentJobType": "start",
. . .
```

#### FXOS機箱show-tech檔案

按照以下步驟驗證FXOS機箱show-tech檔案中的FTD防火牆模式:

1. 對於FXOS 2.7及更高版本,請在<name>\_BC1\_all.tar/

FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中開啟sam\_techsupportinfo 檔案 對於早期版本,請在FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar中開啟 sam\_techsupportinfo 檔案。

2. 檢查特定插槽的「show slot expand detail」部分和識別符號:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
# cat sam_techsupportinfo
`show slot expand detail`
Slot:
   Slot ID: 1
   Log Level: Info
   Admin State: Ok
   Oper State: Online
   Disk Format State: Ok
   Disk Format Status: 100%
   Clear Log Data: Available
   Error Msg:
   Application Instance:
       App Name: ftd
        Identifier: ftd_cluster1
       Admin State: Enabled
        Oper State: Online
```

Running Version: 7.1.0.90 Startup Version: 7.1.0.90 Deploy Type: Container

# 驗證ASA情景模式

ASA支援單情景和多情景模式。FTD不支援多內容模式。

可以使用以下選項驗證上下文型別:

- ASA CLI
- ASA show-tech

#### ASA CLI

按照以下步驟驗證ASA CLI上的ASA情景模式:

- 1. 根據平台和部署模式,使用以下選項訪問ASA CLI:
- 在裝置模式下直接通過telnet/SSH訪問Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下從Firepower 2100上的FXOS控制檯CLI訪問,並使用**connect asa** 命令連線到 ASA
- 通過命令(Firepower 4100/9300)從FXOS CLI訪問:
   connect module <x> [console]telnet],其中x是插槽ID,然後連接asa

•對於虛擬ASA,直接通過SSH訪問ASA,或者通過虛擬機器監控程式或雲UI進行控制檯訪問 2.在CLI上執行**show mode**命令:

ASA# show mode Security context mode: multiple

ASA# **show mode** Security context mode: **single** 

#### ASA show-tech檔案

按照以下步驟驗證ASA show-tech檔案中的ASA情景模式:

1. 檢查show-tech檔案中的**show context detail**部分。在這種情況下,由於存在多個上下文,因此情 景模式是多情景模式:

----- show context detail -----

```
Context "system", is a system resource
Config URL: startup-config
Real Interfaces:
Mapped Interfaces: Ethernet1/1, Ethernet1/10, Ethernet1/11,
Ethernet1/12, Ethernet1/13, Ethernet1/14, Ethernet1/15,
Ethernet1/16, Ethernet1/2, Ethernet1/3, Ethernet1/4, Ethernet1/5,
Ethernet1/6, Ethernet1/7, Ethernet1/8, Ethernet1/9, Ethernet2/1,
Ethernet2/2, Ethernet2/3, Ethernet2/4, Ethernet2/5, Ethernet2/6,
Ethernet2/7, Ethernet2/8, Internal-Data0/1, Internal-Data1/1,
```

Management1/1 Class: default, Flags: 0x00000819, ID: 0

```
Context "admin", has been created
Config URL: disk0:/admin.cfg
Real Interfaces: Ethernet1/1, Ethernet1/2, Management1/1
Mapped Interfaces: Ethernet1/1, Ethernet1/2, Management1/1
Real IPS Sensors:
Mapped IPS Sensors:
Class: default, Flags: 0x00000813, ID: 1
Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Real IPS Sensors:
Mapped IPS Sensors:
Class: default, Flags: 0x00000809, ID: 507
```

# 使用ASA驗證Firepower 2100模式

具備ASA的Firepower 2100可以在以下模式之一運行:

- 平台模式 在FXOS中配置基本操作引數和硬體介面設定。這些設定包括介面管理狀態更改、 EtherChannel配置、NTP、映像管理等。FCM Web介面或FXOS CLI可用於FXOS配置。
- •裝置模式(預設) 裝置模式允許使用者配置ASA中的所有策略。FXOS CLI僅提供高級命令。

使用以下選項驗證採用ASA的Firepower 2100模式:

- ASA CLI
- FXOS CLI
- FXOS show-tech

### ASA CLI

按照以下步驟驗證在ASA CLI上使用ASA的Firepower 2100模式:

1.使用telnet/SSH訪問Firepower 2100上的ASA。

2.在CLI上執行show fxos mode命令:

```
ciscoasa(config)# show fxos mode
Mode is currently set to plaftorm
```

裝置模式:

ciscoasa(config)# show fxos mode
Mode is currently set to appliance

**附註**:在多情景模式下,system或admin 情景中提供show fxos mode命令。

### **FXOS CLI**

按照以下步驟在FXOS CLI上使用ASA驗證Firepower 2100模式:

1.使用telnet/SSH訪問Firepower 2100上的ASA。

#### 2.運行**connect fxos**命令:

ciscoasa/admin(config)# connect fxos Configuring session. . Connecting to FXOS. ... Connected to FXOS. Escape character sequence is 'CTRL-^X'.

**附註**:在多情景模式下,connect fxos命令在admin情景中可用。

3.運行show fxos-mode命令:

firepower-2140# show fxos mode
Mode is currently set to plaftorm

#### 裝置模式:

firepower-2140#show fxos mode Mode is currently set to appliance

#### FXOS show-tech檔案

按照以下步驟驗證FXOS機箱show-tech檔案中的ASA的Firepower 2100模式:

1. 開啟<name>\_FPRM.tar.gz/<name>\_FPRM.tar中的tech\_support\_brief檔案

2.檢查「show fxos-mode」部分:

```
# pwd
/var/tmp/fp2k-1_FPRM/
# cat tech_support_brief
...
`show fxos-mode`
Mode is currently set to platform
裝置模式:
```

# pwd
/var/tmp/fp2k-1\_FPRM/
# cat tech\_support\_brief
...
`show fxos-mode`
Mode is currently set to appliance



思科錯誤ID CSCwb94424 ENH:新增CLISH命令以驗證FMC HA配置

思科錯誤ID CSCvn31622 ENH:新增FXOS SNMP OID以輪詢邏輯裝置和應用例項配置

思科錯誤ID CSCwb97767 ENH:新增OID以驗證FTD例項部署型別

思科錯誤ID <u>CSCwb97772</u> ENH:在Firepower 2100上的ASA的show-tech中包括「show fxos mode」輸出

思科錯誤ID CSCwb97751 無法使用OID 1.3.6.1.4.1.9.9.491.1.6.1.1進行透明防火牆模式驗證

# 相關資訊

- 安全防火牆管理中心REST API快速入門手冊7.1版
- <u>在Firepower NGFW裝置上配置SNMP</u>
- <u>Cisco Firepower威脅防禦REST API指南</u>
- Cisco FXOS REST API參考
- <u>Cisco ASA相容性</u>
- Firepower 1000/2100和安全防火牆3100 ASA和FXOS捆綁版本
- <u>捆綁元件</u>
- Firepower檔案生成故障排除過程
- Cisco Firepower 2100入門指南
- <u>思科Firepower威脅防禦相容性指南</u>