

# 验证Firepower模式、实例、高可用性和可扩展性配置

## 目录

[简介](#)

[背景信息](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[验证高可用性和可扩展性配置](#)

[FMC高可用性](#)

[FMC UI](#)

[FMC CLI](#)

[FMC REST-API](#)

[FMC故障排除文件](#)

[FDM高可用性](#)

[FDM UI](#)

[FDM REST-API](#)

[FTD CLI](#)

[FTD SNMP轮询](#)

[FTD故障排除文件](#)

[FTD高可用性和可扩展性](#)

[FTD CLI](#)

[FTD SNMP](#)

[FTD故障排除文件](#)

[FMC UI](#)

[FMC REST API](#)

[FDM UI](#)

[FDM REST-API](#)

[FCM用户界面](#)

[FXOS CLI](#)

[FXOS REST API](#)

[FXOS机箱show-tech文件](#)

[ASA高可用性和可扩展性](#)

[ASA CLI](#)

[ASA SNMP](#)

[ASA show-tech文件](#)

[FCM用户界面](#)

[FXOS CLI](#)

[FXOS REST-API](#)

[FXOS机箱show-tech文件](#)

[验证防火墙模式](#)

[FTD防火墙模式](#)  
[FTD CLI](#)  
[FTD故障排除文件](#)  
[FMC UI](#)  
[FMC REST-API](#)  
[FCM用户界面](#)  
[FXOS CLI](#)  
[FXOS REST API](#)  
[FXOS机箱show-tech文件](#)  
[ASA防火墙模式](#)  
[ASA CLI](#)  
[ASA show-tech文件](#)  
[FCM用户界面](#)  
[FXOS CLI](#)  
[FXOS REST-API](#)  
[FXOS机箱show-tech文件](#)  
[验证实例部署类型](#)  
[FTD CLI](#)  
[FTD故障排除文件](#)  
[FMC UI](#)  
[FMC REST-API](#)  
[FCM用户界面](#)  
[FXOS CLI](#)  
[FXOS REST API](#)  
[FXOS机箱show-tech文件](#)  
[验证ASA情景模式](#)  
[ASA CLI](#)  
[ASA show-tech文件](#)  
[使用ASA验证Firepower 2100模式](#)  
[ASA CLI](#)  
[FXOS CLI](#)  
[FXOS show-tech文件](#)  
[已知问题](#)  
[相关信息](#)

## 简介

本文档介绍如何验证Firepower高可用性和可扩展性配置、防火墙模式和实例部署类型。

## 背景信息

高可用性和可扩展性配置、防火墙模式和实例部署类型的验证步骤通过REST-API查询、SNMP显示在用户界面(UI)、命令行界面(CLI)和故障排除文件中。

# 先决条件

## 要求

基本产品知识、REST-API、SNMP。

## 使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

本文档中的信息基于以下软件和硬件版本：

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower管理中心(FMC)版本7.1.x
- Firepower可扩展操作系统(FXOS)2.11.1.x
- Firepower设备管理器(FDM)7.1.x
- Firepower威胁防御7.1.x
- ASA 9.17.x

## 验证高可用性和可扩展性配置

高可用性是指故障切换配置。高可用性或故障切换设置会连接两台设备，以便在其中一台设备发生故障时，另一台设备可以接管。

可扩展性是指集群配置。集群配置允许您将多个FTD节点组合为单个逻辑设备。集群提供单个设备（管理、集成到网络）的所有便利性，以及多个设备增加的吞吐量和冗余。

在本文档中，这些表达式可互换使用：

- 高可用性或故障切换
- 可扩展性或群集

在某些情况下，无法验证高可用性和可扩展性配置或状态。例如，没有FTD独立配置的验证命令。独立、故障切换和集群配置模式是互斥的。如果设备没有故障切换和集群配置，则被视为在独立模式下运行。

## FMC高可用性

FMC高可用性配置和状态可通过以下选项进行验证：

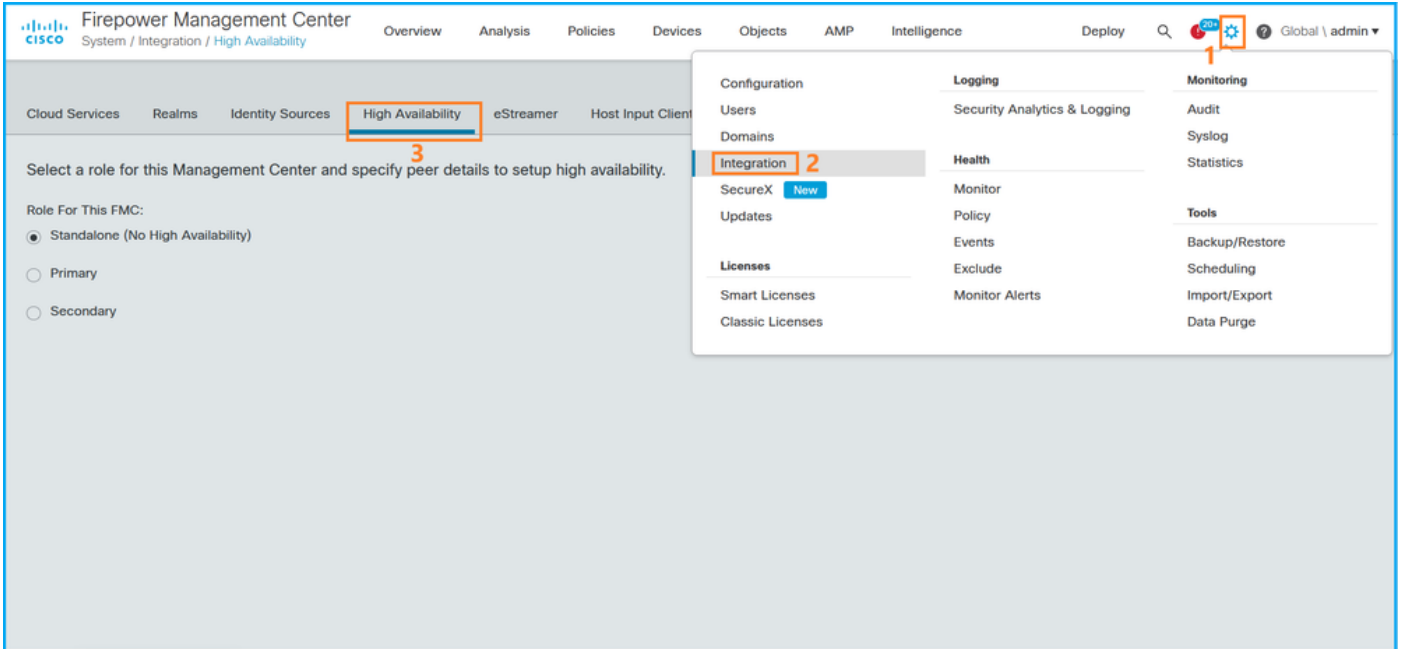
- FMC UI
- FMC CLI
- REST API请求

- FMC故障排除文件

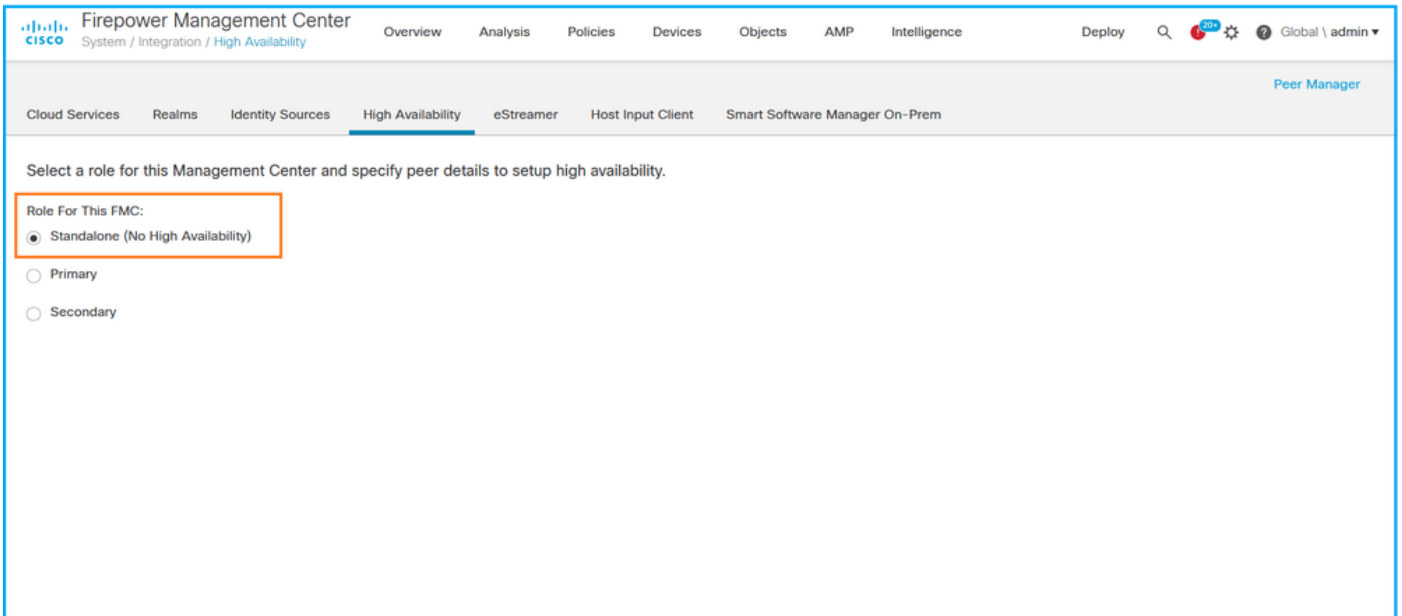
## FMC UI

按照以下步骤验证FMC UI上的FMC高可用性配置和状态：

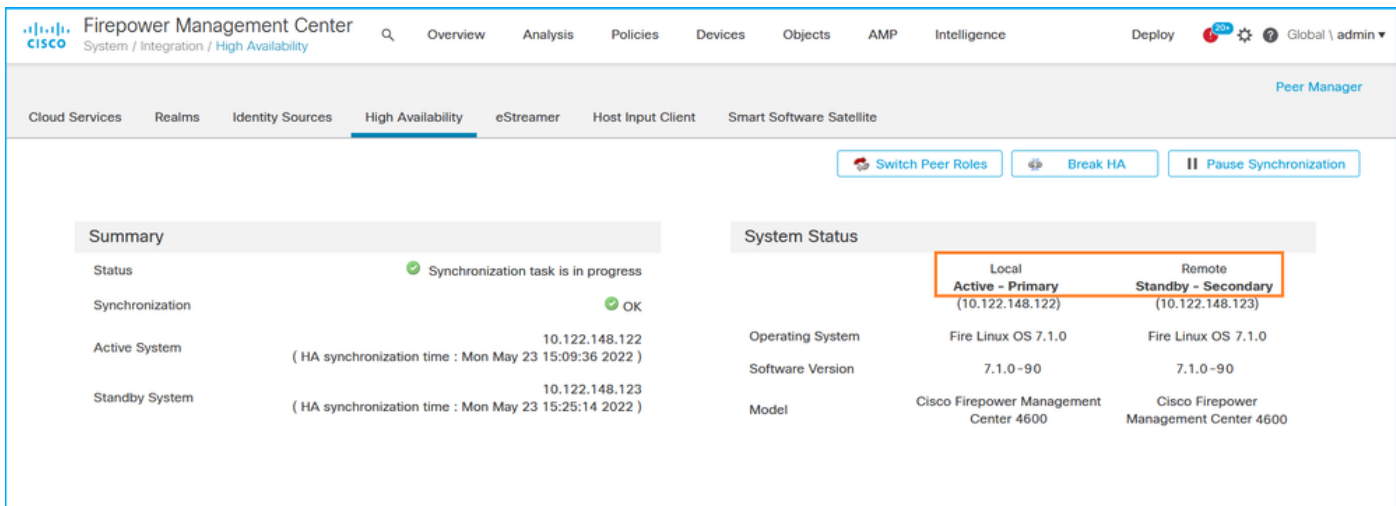
### 1.选择“系统”>“集成”>“高可用性”：



### 2.检查FMC的角色。在这种情况下，不配置高可用性，FMC在独立配置中运行：



如果配置了高可用性，则显示本地和远程角色：



## FMC CLI

按照以下步骤验证FMC CLI上的FMC高可用性配置和状态：

- 1.通过SSH或控制台连接访问FMC。
- 2.运行专家命令，然后运行**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.运行**troubleshoot\_HADC.pl**命令，并选择选项1显示FMC的HA信息。如果未配置高可用性，则显示以下输出：

```
fmc1:/Volume/home/admin# troubleshoot_HADC.pl
***** Troubleshooting Utility ***** 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 Last Successful Periodic Sync Time (When it completed)
9 Print HA Status Messages
10 Compare active and standby device list
11 Check manager status of standby missing devices
12 Check critical PM processes details
13 Help
0 Exit

*****
Enter choice: 1
HA Enabled: No
```

如果配置了高可用性，则显示以下输出：

```
fmc1:/Volume/home/admin# troubleshoot_HADC.pl
***** Troubleshooting Utility *****
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
0 Exit *****

```

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

```

**注意：在高可用性配置中，FMC角色可以具有主角色或辅助角色以及主用或备用状态。**

## FMC REST-API

按照以下步骤通过FMC REST-API验证FMC高可用性和可扩展性配置及状态。使用REST-API客户端。在本例中，curl被使用：

1.请求身份验证令牌：

```

# 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.使用此查询中的令牌查找全局域的UUID:

```

# 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-4b09-000000000000"
    },
    {
      "name": "Global/TEST1",
      "type": "Domain",
      "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
    },
    {
      "name": "Global/TEST2",
      "type": "Domain",
      "uuid": "341a8f03-f831-c364-b751-000000000001"
    }
  ]
},

```

```

"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
}
}

```

**注意：**命令字符串的“| python -m json.tool”部分用于以JSON样式格式化输出，是可选的。

### 3.在此查询中使用全局域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，则显示以下输出：

```

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

```

如果配置了高可用性，则显示以下输出：

```

{
  "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"
      ],
      "id": "de7bfc10-13b5-11ec-afaf-a0f8cf9ccb46",
      "overallStatus": "GOOD",
      "syncStatus": "GOOD",
      "type": "FMCHAStatus"
    }
  ],
  "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故障排除文件

按照以下步骤验证FMC高可用性配置和FMC故障排除文件中的状态：

- 1.打开故障排除文件并导航至文件夹<filename>.tar/results-<date>—xxxxxx/command-outputs
- 2.打开文件usr-local-sf-bin-troubleshoot\_HADC.pl -a.output:

如果未配置高可用性，则显示以下输出：

```

# 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
-----
Database  MirrorRole    NULL
Database  MirrorState   NULL
Database  PartnerState  NULL
Database  ArbiterState  NULL
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，则显示以下输出：

```

# 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',
    {
        'stderr' => undef,
        'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745

```



Type	Property	Value
Database	MirrorRole	primary
Database	MirrorState	synchronizing
Database	PartnerState	connected
Database	ArbiterState	connected
Server	ServerName	csn_primary

Ping database successful.

```

',
      '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

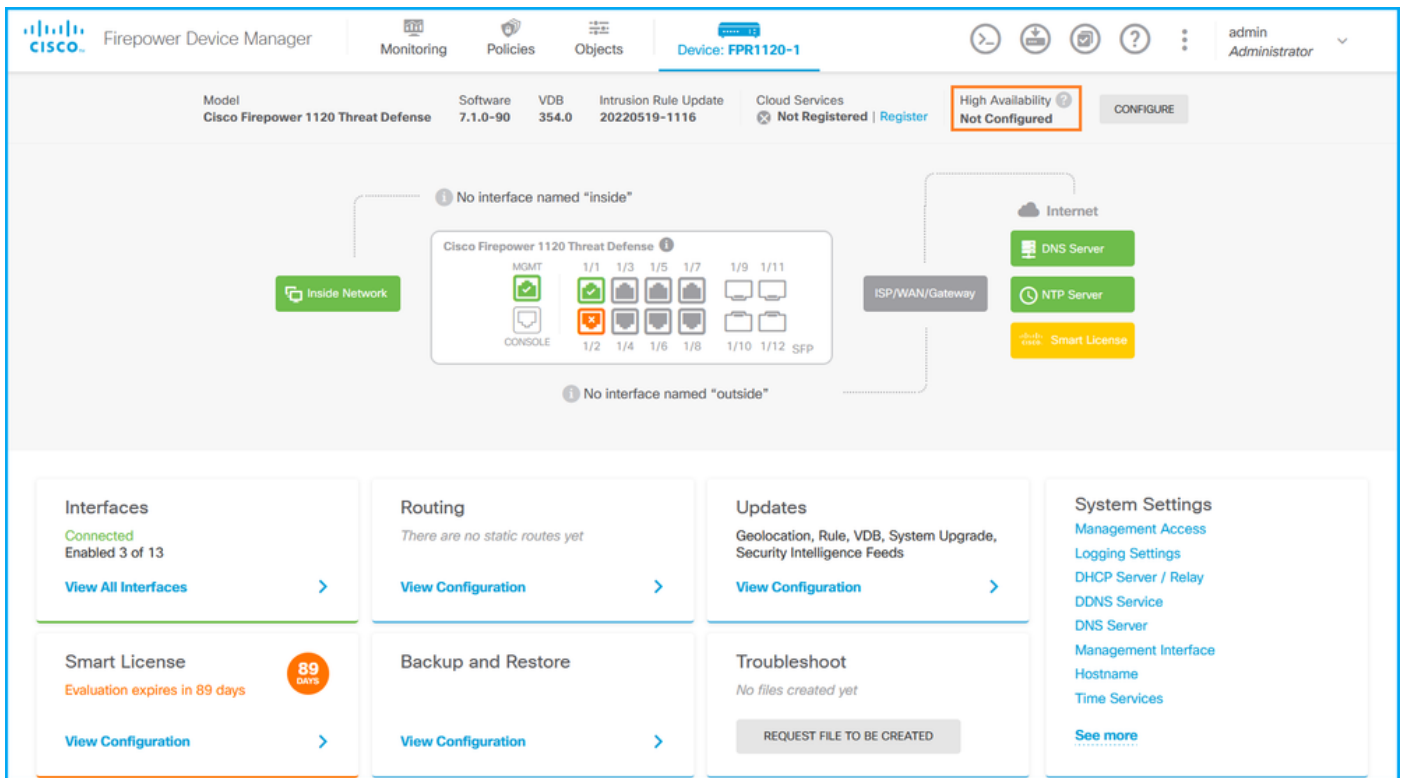
## FDM高可用性

可使用以下选项验证FDM高可用性配置和状态：

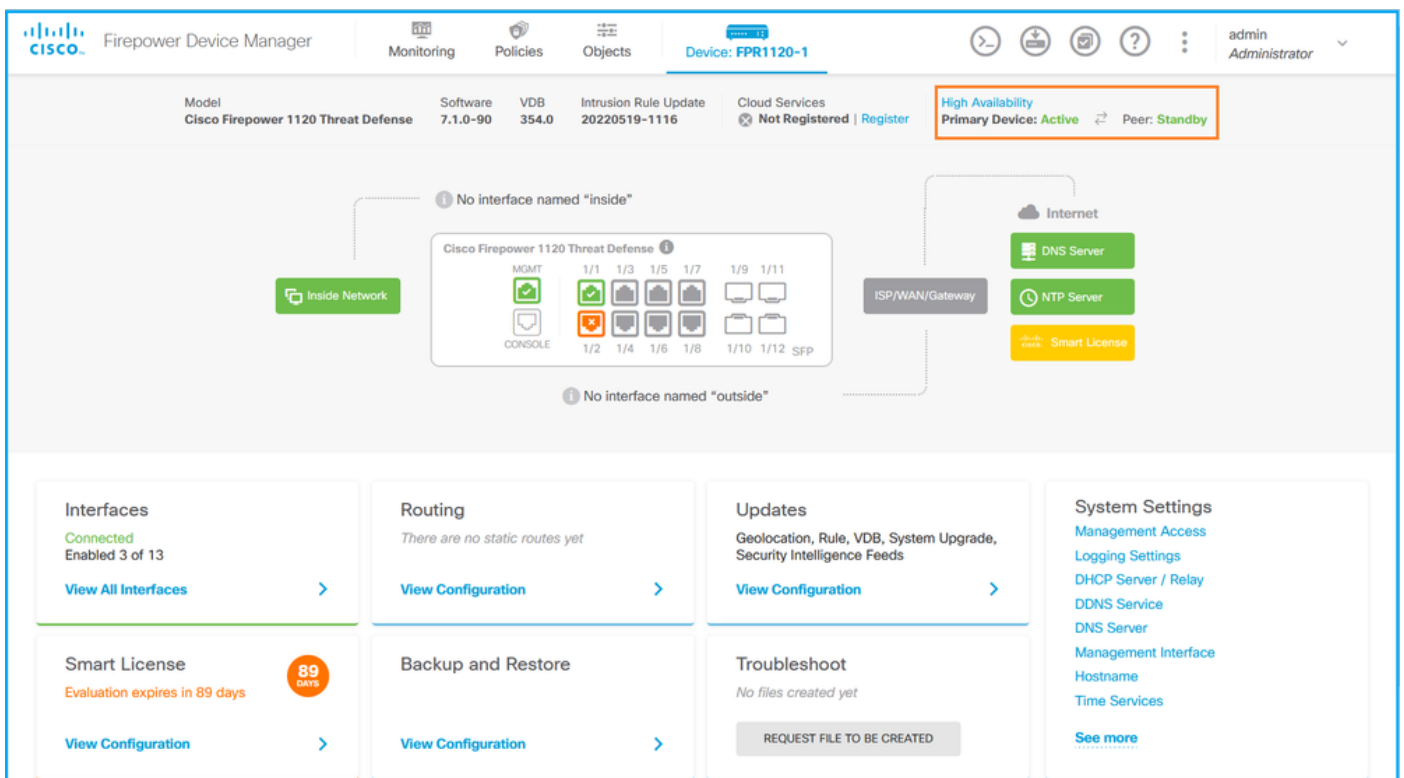
- FDM UI
- FDM REST API请求
- FTD CLI
- FTD SNMP轮询
- FTD故障排除文件

### FDM UI

要验证FDM UI上的FDM高可用性配置和状态，请在主页上选中“高可用性”。如果未配置高可用性，则“高可用性”值未配置：



如果配置了高可用性，则显示本地和远程对等设备故障切换配置和角色：



## FDM REST-API

按照以下步骤通过FDM REST-API请求验证FDM高可用性配置和状态。使用REST-API客户端。在本例中，curl被使用：

1.请求身份验证令牌：





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

## FTD CLI

按照部分中的步骤操作。

## FTD SNMP轮询

按照部分中的步骤操作。

## FTD故障排除文件

按照部分中的步骤操作。

## FTD高可用性和可扩展性

FTD高可用性、可扩展性配置和状态可通过以下选项进行验证：

- FTD CLI
- FTD SNMP
- FTD故障排除文件
- FMC UI
- FMC REST-API
- FDM UI
- FDM REST-API
- FCM用户界面
- FXOS CLI
- FXOS REST-API
- FXOS机箱show-tech文件

## FTD CLI

按照以下步骤验证FTD高可用性和可扩展性配置以及FTD CLI上的状态：

1.根据平台和部署模式使用以下选项访问FTD CLI:

- 直接SSH访问FTD — 所有平台
- 从FXOS控制台CLI(Firepower 1000/2100/3100)通过命令connect ftd访问
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
连接模块<x> [console|telnet],其中x是插槽ID，然后连接ftd [instance]，其中实例仅与多实例部署相关

- 对于虚拟FTD、直接SSH访问FTD或从虚拟机监控程序或云UI进行控制台访问

2.要验证FTD故障切换配置和状态，请在CLI上运行show running-config failover和show failover

state命令。

如果未配置故障切换，则显示以下输出：

```
> show running-config failover
no failover
>show failover state
                State          Last Failure Reason      Date/Time
This host -    Secondary
                Disabled      None
Other host -    Primary
                Not Detected  None
====Configuration State====
====Communication State==
```

如果配置了故障切换，则显示以下输出：

```
> 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 10.30.34.2 255.255.255.0 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.要验证FTD集群配置和状态，请在CLI上运行show running-config cluster和show cluster info命令。

如果未配置集群，则显示以下输出：

```
> show running-config cluster
>show cluster info
Clustering is not configured
```

如果配置了集群，则显示以下输出：

```
> 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
no unit join-acceleration
```

```
enable
```

```
> show cluster info
```

```
Cluster ftd_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.  : 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 members in the cluster:
```

```
Unit "unit-2-1" 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
```

**注意：主和控制角色相同。**

## FTD SNMP

按照以下步骤通过SNMP验证FTD高可用性和可扩展性配置及状态：

1. 确保已配置并启用SNMP。对于FDM管理的FTD，请参阅在Firepower FDM [上配置SNMP并对其进行故障排除](#)以了解配置步骤。有关FMC管理的FTD，请参阅在Firepower NGFW设备 [上配置SNMP以了解配置步骤](#)。

2. 要验证FTD故障切换配置和状态，请轮询OID.1.3.6.1.4.1.9.9.147.1.2.1.1。

如果未配置故障切换，则显示以下输出：

```
# snmpwalk -v2c -c cisco123 -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.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

如果配置了故障切换，则显示以下输出：

```
# snmpwalk -v2c -c cisco123 -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 (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.要验证集群配置和状态，请轮询OID 1.3.6.1.4.1.9.9.491.1.8.1。

如果未配置集群，则显示以下输出：

```

# 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

```

如果集群已配置但未启用，则显示以下输出：

```

# 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
...

```

如果集群已配置、启用且运行正常，则显示以下输出：

```

# 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
...

```

有关OID说明的详细信息，请[参阅CISCO-UNIFIED-FIREWALL-MIB](#)。

## FTD故障排除文件

按照以下步骤验证FTD高可用性和可扩展性配置以及FTD故障排除文件中的状态：

1.打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-<date>-xxxxxx/command-outputs。

2.打开文件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.要验证故障切换配置和状态，请选中**show failover**部分。

如果未配置故障切换，则显示以下输出：

```
----- 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
```

如果配置了故障切换，则显示以下输出：

```
----- 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.要验证FTD集群配置和状态，请检查**show cluster info**部分。

如果未配置集群，则显示以下输出：

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

**Clustering is not configured**

如果已配置并启用集群，则显示以下输出：

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

**Cluster ftd\_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.  : 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

```

```

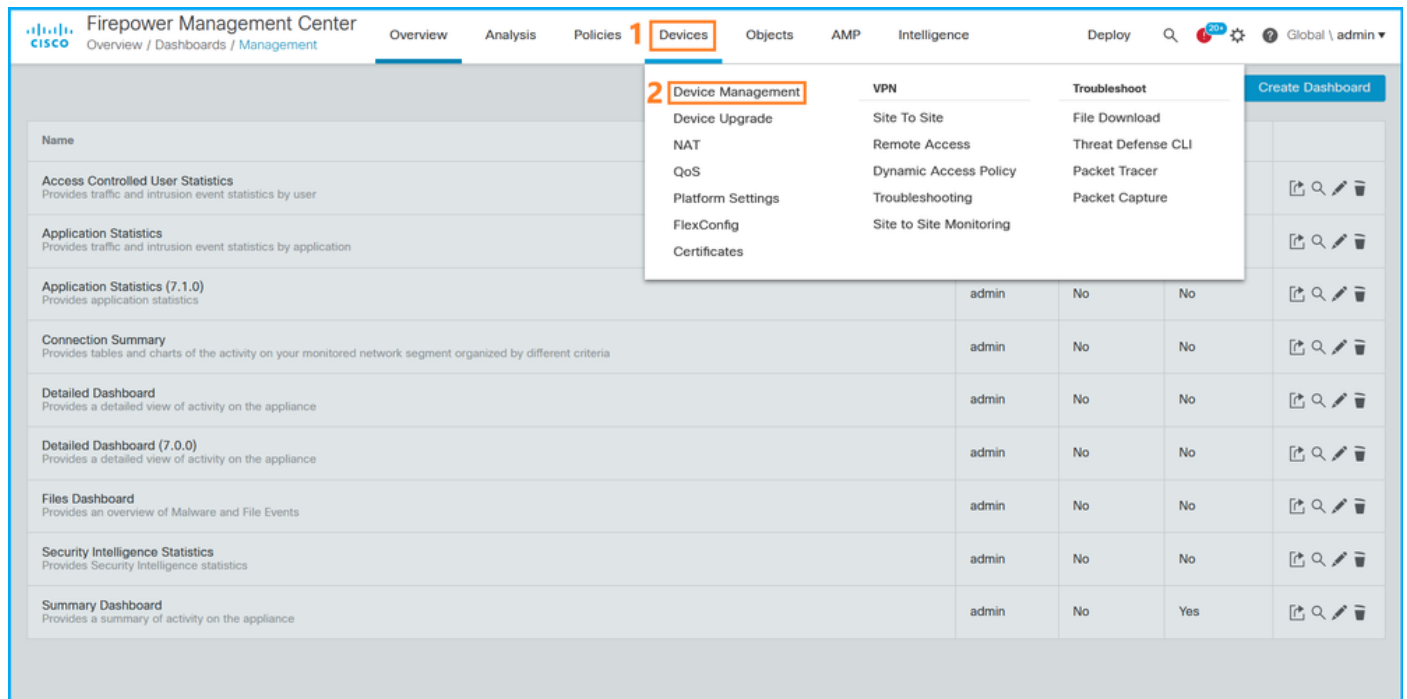
Other members in the cluster:
  Unit "unit-2-1" in state SLAVE
  ID          : 1
  Site ID     : 1
  Version     : 9.17(1)
  Serial No.  : FLM2108V9YG7S1
  CCL IP      : 10.173.2.1
  CCL MAC     : 0015.c500.028f
  Module      : FPR4K-SM-24
  Resource    : 20 cores / 44018 MB RAM
  Last join   : 14:02:46 UTC May 20 2022
  Last leave  : 14:02:31 UTC May 20 2022

```

## FMC UI

按照以下步骤验证FMC UI上的FTD高可用性和可扩展性配置及状态：

### 1.选择“设备”>“设备管理”：



2.要验证FTD高可用性和可扩展性配置，请检查标签“高可用性”或“集群”。如果两者都不存在，则FTD在独立配置中运行：

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB2 (3)						
ftd_cluster1 (2) Cluster						
10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5.443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha High Availability						
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	firepower-9300.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_standalone Snort 3 10.62.148.181 - Routed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1	

3.要验证FTD的高可用性和可扩展性状态，请在括号中检查设备角色。如果角色不存在且FTD不属于集群或故障转移，则FTD在独立配置中运行：

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB2 (3)						
ftd_cluster1 (2) Cluster						
10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5.443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha High Availability						
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	firepower-9300.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_standalone Snort 3 10.62.148.181 - Routed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1	

注意：在集群中，仅显示控制单元的角色。

## FMC REST API

在这些输出中，ftd\_ha\_1、ftd\_ha\_2、ftd\_standalone、ftd\_ha、ftc\_cluster1是用户可配置的设备名称。这些名称不指实际的高可用性和可扩展性配置或状态。

按照以下步骤通过FMC REST-API验证FTD高可用性和可扩展性配置及状态。使用REST-API客户端。在本例中，curl被使用：

## 1. 请求身份验证令牌：

```
# 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. 确定包含设备的域。在大多数REST API查询中，域参数是必填项。使用此查询中的令牌检索域列表：

```
# 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-4b09-000000000000"
    },
    ...
  ]
}
```

## 3. 使用域UUID查询特定设备记录和特定设备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-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
      },
      "name": "ftd_ha_1",
      "type": "Device"
    },
    ...
  ]
}
```

## 4. 要验证故障切换配置，请在此查询中使用第3步中的域UUID和设备/容器UUID:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'X-auth-access-
token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
"containerDetails": {
  "id": "eec3ddfc-d842-11ec-a15e-986001c83f2f",
  "name": "ftd_ha",
  "type": "DeviceHAPair"
},
...
```

## 5. 要验证故障切换状态，请在此查询中使用第4步中的域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/ftdddevicehapairs/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.要验证集群配置，请在此查询中使用第3步中的域UUID和设备/容器UUID:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devices/devicerecords/3344bc4a-d842-11ec-a995-817e361f7ea5' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
```

```
...
  "containerDetails": {
    "id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",
    "links": {
      "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/deviceclusters/ftdddevicecluster/8e6188c2-d844-11ec-bdd1-6e8d3e226370"
    },
    "name": "ftd_cluster1",
    "type": "DeviceCluster"
  },
  ...
```

7. 要验证集群状态，请在此查询中使用第6步中的域UUID和设备/容器UUID:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/deviceclusters/ftdddevicecluster/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"
      }
    }
  ],
  "id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",
```

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

## FDM UI

按照部分中的步骤操作。

## FDM REST-API

按照部分中的步骤操作。

## FCM用户界面

FCM UI在平台模式下的Firepower 4100/9300和Firepower 2100 (带ASA) 上可用。

按照以下步骤验证FCM用户界面上的FTD高可用性和可扩展性状态：

1.要验证FTD故障切换状态，请在“逻辑设备”页上检查“HA-ROLE”属性值：

The screenshot shows the FCM Logical Devices page for a standalone device named 'ftd1'. The device is in a 'Standalone' state with a status of 'ok'. The main table lists the application as 'FTD' with version '7.1.0.90' and resource profile 'RP20'. The management IP is '10.62.148.89' and the gateway is '10.62.148.1'. The management port is 'Ethernet1/1' and the status is 'Online'. The 'Attributes' section shows 'HA-ROLE' as 'active', which is highlighted with a red box. Other attributes include 'Cluster Operational Status: not applicable', 'FIREPOWER-MGMT-IP: 10.62.148.89', 'HA-LINK-INTF: Ethernet1/2', 'HA-LAN-INTF: Ethernet1/2', 'MGMT-URL: https://10.62.184.21/', and 'UUID: 7962088-d83b-11ec-941d-b9083eb612d8'.

**注意：**逻辑设备标识符旁边的独立标签是指机箱逻辑设备配置，而不是FTD故障切换配置。

2.要验证FTD集群配置和状态，请在“逻辑设备”页上检查“集群”标签和“CLUSTER-ROLE”属性值：

The screenshot shows the FCM Logical Devices page for a clustered device named 'ftd\_cluster1'. The device is in a 'Clustered' state with a status of 'ok'. The main table lists the application as 'FTD' with version '7.1.0.90' and resource profile 'RP20'. The management IP is '10.62.148.188' and the gateway is '10.62.148.129'. The management port is 'Ethernet1/1' and the status is 'Online'. The 'Attributes' section shows 'CLUSTER-ROLE' as 'control', which is highlighted with a red box. Other attributes include 'Cluster Operational Status: in-cluster', 'FIREPOWER-MGMT-IP: 10.62.148.188', 'CLUSTER-IP: 10.173.1.1', 'MGMT-URL: https://10.62.184.21/', and 'UUID: 3344bc4a-d842-11ec-a995-817e3617ea5'.

## FXOS CLI

FXOS CLI上的FTD高可用性和可扩展性配置以及状态验证在Firepower 4100/9300上可用。

按照以下步骤验证FTD高可用性和可扩展性配置以及FXOS CLI的状态：

1.建立到机箱的控制台或SSH连接。

2.要验证FTD高可用性状态，请运行**scope ssa**命令，然后运行**scope slot <x>**以切换到FTD运行的特定插槽并运行**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/
uuid              796eb8f8-d83b-11ec-941d-b9083eb612d8
```

...

3.要验证FTD集群配置和状态，请运行**scope ssa**命令，运行**show logical-device <name> detail expand**命令，其中name是逻辑设备名称，**show app-instance**命令。检查特定插槽的输出:

```
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
```

```
-----
```

ftd	<b>ftd_cluster1 1</b>	Enabled	Online	7.1.0.90	7.1.0.90
Container	No	RP20	<b>In Cluster</b>	<b>Master</b>	

## FXOS REST API

Firepower 4100/9300支持FXOS REST-API。

按照以下步骤通过FXOS REST-API请求验证FTD高可用性和可扩展性配置及状态。使用REST-API客户端。在本例中，curl被使用：

### 1.请求身份验证令牌：

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://192.0.2.100/api/login'
{
  "refreshPeriod": "0",
  "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d"
}
```

### 2.要验证FTD故障切换状态，请在此查询中使用令牌和插槽ID:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'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",
      "appName": "ftd",
      "clearLogData": "available",
      "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",
      "fsmRmtInvErrDescr": "",
      "fsmRmtInvRslt": "",
      "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-ftdl/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-ftdl/app/attribute-
ha-role",
    "value": "active"
  },
  {
    "key": "uuid",
    "rn": "app-attribute-uuid",
    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftdl/app/attribute-
uuid",
    "value": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
  }
],
...

```

3. 要验证FTD集群配置，请在此查询中使用逻辑设备标识符：

```

# 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",
          "gatewayv6": ":::",
          "key": "",
          "mode": "spanned-etherchannel",
          "name": "ftd_cluster1",
          "netmaskv4": "0.0.0.0",
          "poolEndv4": "0.0.0.0",
          "poolEndv6": ":::",
          "poolStartv4": "0.0.0.0",
          "poolStartv6": ":::",
          "prefixLength": "",
          "rn": "cluster-
bootstrap",
          "siteId": "1",
          "supportCclSubnet":
"supported",
          "updateTimestamp": "2022-05-20T13:38:21.872",
          "urllink": "https://192.0.2.101/api/ld/ftd_cluster1/cluster-bootstrap",
          "virtualIPv4": "0.0.0.0",
          "virtualIPv6": ":::"
        }
      ], ...
    }
  ]
}

```

#### 4.要验证FTD集群状态，请使用以下查询：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'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机箱show-tech文件

FTD高可用性和可扩展性配置及状态可在Firepower 4100/9300机箱show-tech文件中进行验证。

按照以下步骤验证FXOS机箱show-tech文件中的高可用性和可扩展性配置及状态：

1. 对于FXOS版本2.7及更高版本，请在

<name>\_BC1\_all.tar/FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中打开文件  
sam\_techsupportinfo

对于早期版本，请在FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中打开  
sam\_techsupportinfo文件。

2.要验证故障切换状态，请在“show slot expand detail”部分的特定插槽下检查ha-role属性值的值：

```
# 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: 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.要验证FTD集群配置，请在“show logical-device detail expand”部分中检查特定插槽下的Mode属性值的值:

``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:

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.要验证FTD集群状态，请在“show slot expand detail”部分的特定插槽下检查集群状态和集群角色属性值的值:

```
`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高可用性和可扩展性**

使用以下选项可验证ASA高可用性和可扩展性配置及状态：

- ASA CLI
- ASA SNMP轮询
- ASA show-tech文件
- FCM用户界面
- FXOS CLI
- FXOS REST-API
- FXOS机箱show-tech文件

## ASA CLI

按照以下步骤验证ASA CLI上的ASA高可用性和可扩展性配置：

1. 根据平台和部署模式，使用以下选项访问ASA CLI:

- 以设备模式直接telnet/SSH访问Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下从Firepower 2100上的FXOS控制台CLI访问，并通过connect asa命令连接到ASA
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
连接模块<x> [console|telnet],其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接SSH访问ASA，或从虚拟机监控程序或云UI进行控制台访问

2.要验证ASA故障切换配置和状态，请在ASA CLI上运行show running-config failover和show failover state命令。

如果未配置故障切换，则显示以下输出：

```
asa# show running-config failover
no failover
asa# show failover state
                State           Last Failure Reason      Date/Time
This host  -   Secondary
                Disabled       None
Other host -   Primary
                Not Detected   None
====Configuration State====
====Communication State====
```

如果配置了故障切换，则显示以下输出：

```
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 10.30.35.2 255.255.255.0 standby 10.30.35.3

# show failover state
                State           Last Failure Reason      Date/Time
This host  -   Primary
                Active         None
Other host -   Secondary
                Standby Ready   Comm Failure              19:42:22 UTC May 21 2022
====Configuration State====
```

```
Sync Done
====Communication State====
Mac set
```

3.要验证ASA集群配置和状态，请在CLI上运行show running-config cluster和show cluster info命令

。

如果未配置集群，则显示以下输出：

```
asa# show running-config cluster
asa# show cluster info
Clustering is not configured
```

如果配置了集群，则显示以下输出：

```
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

按照以下步骤通过SNMP验证ASA高可用性和可扩展性配置：

1. 确保已配置并启用SNMP。

2. 为了验证故障切换配置和状态轮询OID.1.3.6.1.4.1.9.147.1.2.1.1。1。

如果未配置故障切换，则显示以下输出：

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.10 .1.3.6.1.4.1.9.147.1.2.1.1.1
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.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

如果配置了故障切换，则显示以下输出：

```
# 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: "Active unit" <--
Primary device is active
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Standby unit"
```

3.要验证集群配置和状态，请轮询OID 1.3.6.1.4.1.9.9.491.1.8.1。

如果未配置集群，则显示以下输出：

```
# 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
```

如果集群已配置但未启用，则显示以下输出：

```
# 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
...
```

如果集群已配置、启用且运行正常，则显示以下输出：

```
# 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
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = 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: "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
...
```

有关OID说明的详细信息，请[参阅CISCO-UNIFIED-FIREWALL-MIB](#)。

## ASA show-tech文件

1. 要验证ASA故障切换配置和状态，请选中show failover部分。

如果未配置故障切换，则显示以下输出：

```
----- 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
```

如果配置了故障切换，则显示以下输出：

```
----- 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.要验证集群配置和状态，请检查show cluster info部分。

如果未配置集群，则显示以下输出：

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

Clustering is not configured

如果已配置并启用集群，则显示以下输出：

```
----- 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
```



...

## FCM用户界面

按照部分中的步骤操作。

## FXOS CLI

按照部分中的步骤操作。

## FXOS REST-API

按照部分中的步骤操作。

## FXOS机箱show-tech文件

按照部分中的步骤操作。

# 验证防火墙模式

## FTD防火墙模式

防火墙模式是指路由或透明防火墙配置。

可使用以下选项验证FTD防火墙模式：

- FTD CLI
- FTD show-tech
- FMC UI
- FMC REST-API
- FCM用户界面
- FXOS CLI
- FXOS REST-API
- FXOS机箱show-tech文件

**注意：**FDM不支持透明模式。

## FTD CLI

按照以下步骤在FTD CLI上验证FTD防火墙模式：

1.根据平台和部署模式使用以下选项访问FTD CLI:

- 直接SSH访问FTD — 所有平台
- 从FXOS控制台CLI(Firepower 1000/2100/3100)通过命令connect ftd访问
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
**connect module <x> [console|telnet]**,其中x是插槽ID，然后

connect ftd [instance] , 其中实例仅与多实例部署相关。

- 对于虚拟FTD、直接SSH访问FTD或从虚拟机监控程序或云UI进行控制台访问
- 2.要验证防火墙模式 , 请在CLI上运行show firewall 命令 :

```
> show firewall
Firewall mode: Transparent
```

## FTD故障排除文件

按照以下步骤验证FTD故障排除文件中的FTD防火墙模式 :

1.打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-<date>—xxxxxx/command-outputs.

2.打开文件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'
```

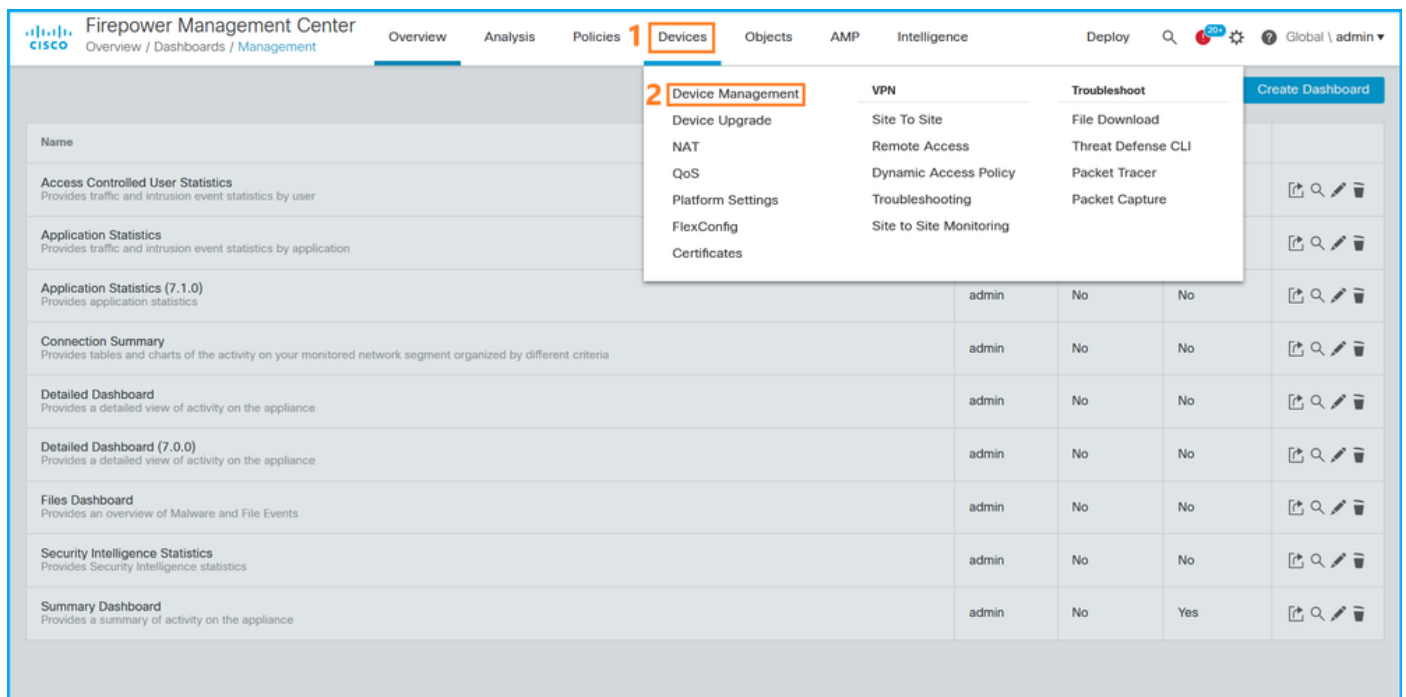
3.要验证FTD防火墙模式 , 请选中show firewall 部分 :

```
----- show firewall -----
Firewall mode: Transparent
```

## FMC UI

按照以下步骤验证FMC UI上的FTD防火墙模式 :

1.选择“设备”>“设备管理” :



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. The 'Devices' menu is expanded, showing 'Device Management' (highlighted with a red box and a '2'), 'VPN', and 'Troubleshoot'. Below the menu, there is a table of dashboards with columns for Name, Description, and actions (Share, Search, Edit, Delete). The table lists various dashboards such as 'Access Controlled User Statistics', 'Application Statistics', 'Connection Summary', 'Detailed Dashboard', 'Files Dashboard', 'Security Intelligence Statistics', and 'Summary Dashboard'.

Name	Description	admin	No	No	Share Search Edit Delete
Access Controlled User Statistics	Provides traffic and intrusion event statistics by user				Share Search Edit Delete
Application Statistics	Provides traffic and intrusion event statistics by application				Share Search Edit Delete
Application Statistics (7.1.0)	Provides application statistics	admin	No	No	Share Search Edit Delete
Connection Summary	Provides tables and charts of the activity on your monitored network segment organized by different criteria	admin	No	No	Share Search Edit Delete
Detailed Dashboard	Provides a detailed view of activity on the appliance	admin	No	No	Share Search Edit Delete
Detailed Dashboard (7.0.0)	Provides a detailed view of activity on the appliance	admin	No	No	Share Search Edit Delete
Files Dashboard	Provides an overview of Malware and File Events	admin	No	No	Share Search Edit Delete
Security Intelligence Statistics	Provides Security Intelligence statistics	admin	No	No	Share Search Edit Delete
Summary Dashboard	Provides a summary of activity on the appliance	admin	No	Yes	Share Search Edit Delete

2.检查“已路由”或“透明”标签:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB2 (3)						
ftd_cluster1 (2)						
Cluster						
10.62.148.188 (Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - Snort3	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com:443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha High Availability						
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 firepower-9300.cisco.com:443 Security Module - 1 (Container) Base, Threat acp1						
ftd_standalone Snort 3 10.62.148.181 - Routed						
Firepower 2120 with FTD 7.1.0 N/A Base, Threat acp1						

## FMC REST-API

按照以下步骤通过FMC REST-API验证FTD防火墙模式。使用REST-API客户端。在本例中，curl被使用：

### 1. 请求身份验证令牌：

```
# 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. 确定包含设备的域。在大多数REST API查询中，域参数是必填项。使用此查询中的令牌检索域列表：

```
# 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-4b09-000000000000"
    }
  ],
  ...
}
```

3. 使用域UUID查询特定设备记录和特定设备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-4b09-000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
      },
      "name": "ftd_ha_1",
      "type": "Device"
    },
    ...
  ]
}
```

4.在此查询中使用第3步中的域UUID和设备/容器UUID，并检查ftdMode的值:

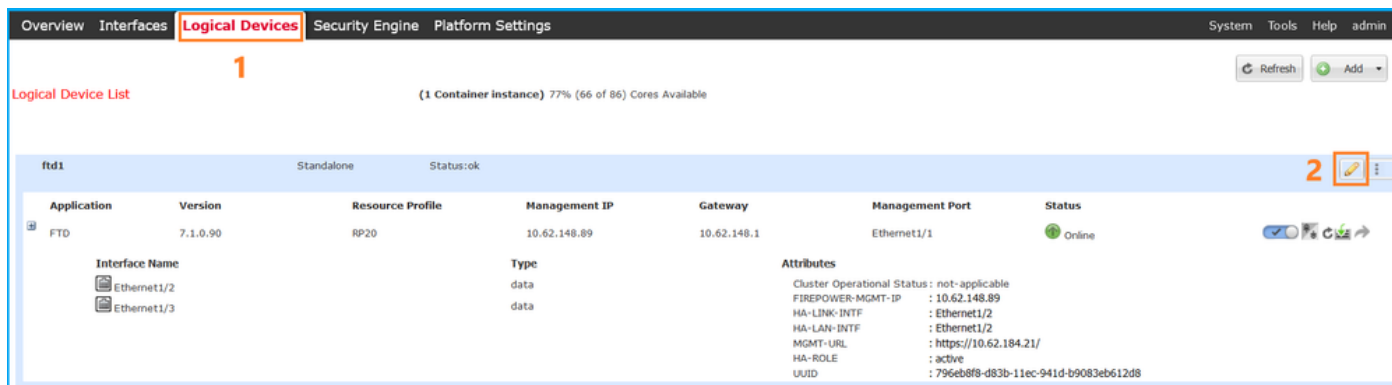
```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept: application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
{
  "accessPolicy": {
    "id": "00505691-3a23-0ed3-0006-536940224514",
    "name": "acpl",
    "type": "AccessPolicy"
  },
  "advanced": {
    "enableOGS": false
  },
  "description": "NOT SUPPORTED",
  "ftdMode": "ROUTED",
  ...
}
```

## FCM用户界面

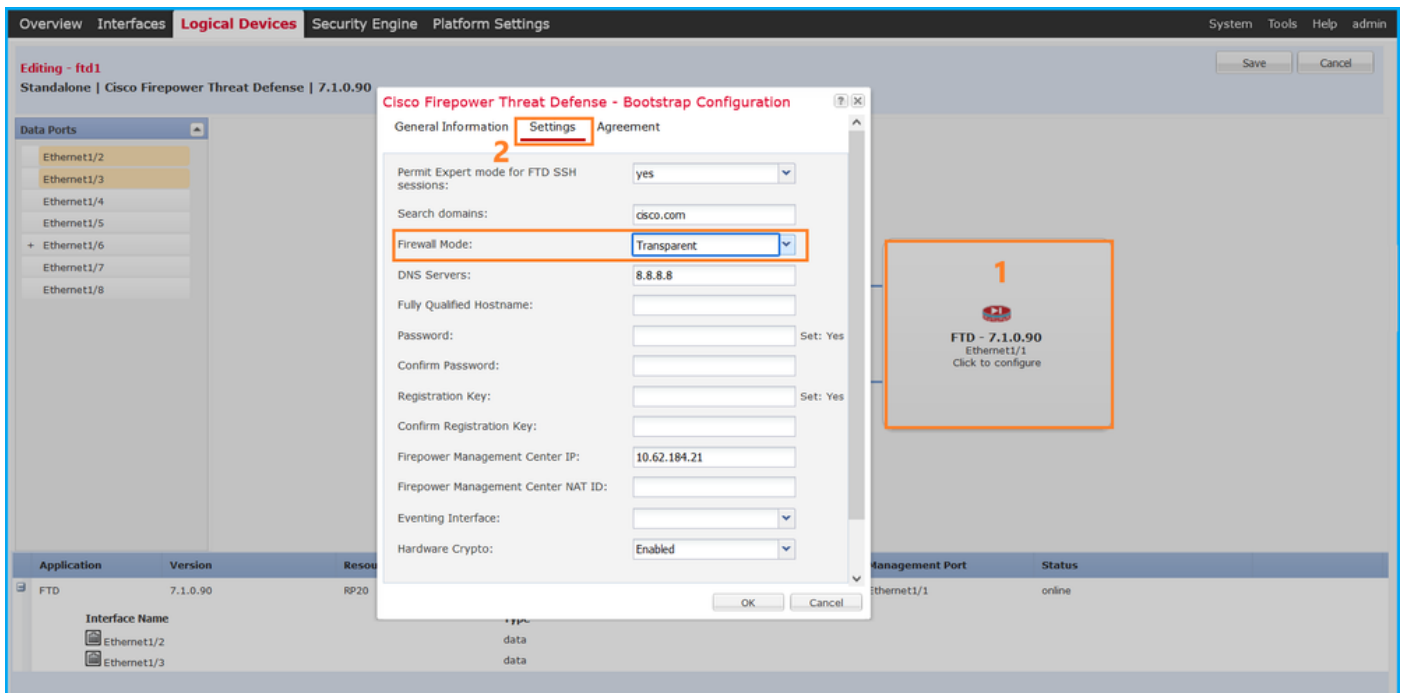
可在Firepower 4100/9300上验证FTD的防火墙模式。

按照以下步骤验证FCM UI上的FTD防火墙模式：

1.在“逻辑设备”页上编辑逻辑设备：



2.单击应用程序图标，然后在“设置”选项卡中选中“防火墙模式”：



## FXOS CLI

可在Firepower 4100/9300上验证FTD的防火墙模式。

按照以下步骤在FXOS CLI上验证FTD防火墙模式：

1. 与机箱建立控制台或SSH连接。
2. 切换到范围ssa，然后切换到特定逻辑设备，运行show mgmt-bootstrap expand 命令，并检查 FIREWALL\_MODE属性值：

```
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:

Key	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:

Key	Value
DNS_SERVERS	192.0.2.250
FIREPOWER_MANAGER_IP	10.62.184.21
<b>FIREWALL_MODE</b>	<b>routed</b>

```
PERMIT_EXPERT_MODE      yes
SEARCH_DOMAINS          cisco.com
```

...

## FXOS REST API

Firepower 4100/9300支持FXOS REST-API。

按照以下步骤通过FXOS REST-API请求验证FTD防火墙模式。使用REST-API客户端。在本例中，curl被使用：

1. 请求身份验证令牌：

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123'
https://192.0.2.100/api/1d/ftd_cluster1
{
  "refreshPeriod": "0",
  "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d"
}
```

2. 在此查询中使用逻辑设备标识符并检查FIREWALL\_MODE键的值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
https://192.0.2.100/api/1d/ftd_cluster1
...
      {
        "key": "FIREWALL_MODE",
        "rn": "key-FIREWALL_MODE",
        "updateTimestamp": "2022-05-20T13:28:37.093",
        "urllink": "https://192.0.2.100/api/1d/ftd_cluster1/mgmt-
bootstrap/ftd/key/FIREWALL_MODE",
        "value": "routed"
      },
...

```

## FXOS机箱show-tech文件

FTD的防火墙模式可在Firepower 4100/9300的show-tech文件中进行验证。

按照以下步骤验证FXOS机箱show-tech文件中的FTD防火墙模式：

1. 对于FXOS版本2.7及更高版本，请在<name>\_BC1\_all.tar/  
FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中打开文件sam\_techsupportinfo  
对于早期版本，请在FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar中打开  
sam\_techsupportinfo文件。

2. 检查特定标识符和插槽下的“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防火墙模式

可使用以下选项验证ASA防火墙模式：

- ASA CLI
- ASA show-tech
- FCM用户界面
- FXOS CLI
- FXOS REST-API
- FXOS机箱show-tech文件

## ASA CLI

按照以下步骤在ASA CLI上验证ASA防火墙模式：

1. 根据平台和部署模式，使用以下选项访问ASA CLI:

- 以设备模式直接telnet/SSH访问Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下从Firepower 2100上的FXOS控制台CLI访问，并通过connect asa命令连接到ASA
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
连接模块<x> [console|telnet],其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接SSH访问ASA，或从虚拟机监控程序或云UI进行控制台访问

2. 在CLI上运行show firewall命令：

```
asa# show firewall
Firewall mode: Routed
```

## ASA show-tech文件

要验证ASA防火墙模式，请选中show firewall 部分：

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

## FCM用户界面

按照部分中的步骤操作。

## FXOS CLI

按照部分中的步骤操作。

## FXOS REST-API

按照部分中的步骤操作。

## FXOS机箱show-tech文件

按照部分中的步骤操作。

# 验证实例部署类型

有2种应用实例部署类型：

- 本地实例 — 本地实例使用安全模块/引擎的所有资源（CPU、RAM和磁盘空间），因此只能安装一个本地实例。
- 容器实例 — 容器实例使用安全模块/引擎的资源子集。仅FMC管理的FTD支持多实例功能；ASA或FDM管理的FTD不支持它。

仅Firepower 4100/9300上的FTD支持容器模式实例配置。

可使用以下选项验证实例部署类型：

- FTD CLI
- FTD Show-tech
- FMC UI
- FMC REST-API
- FCM用户界面
- FXOS CLI
- FXOS REST-API
- FXOS机箱show-tech文件

## FTD CLI

按照以下步骤验证实例部署类型：

1. 根据平台和部署模式，使用以下选项访问FTD CLI:
  - 直接SSH访问FTD — 所有平台



• 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
连接模块<x> [console|telnet]，其中x是插槽ID，然后连接ftd [instance]，其中实例仅与多实例部署相关。

2. 运行show version system命令，并检查带有字符串SSP插槽编号的行。如果此行中存在容器，则FTD在容器模式下运行：

```
> 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故障排除文件

按照以下步骤验证FTD故障排除文件中的FTD实例部署类型：

1. 打开故障排除文件并导航至文件夹<filename>-troubleshoot .tar/results-<date>-xxxxxx/command-outputs。
2. 打开文件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. 使用字符串SSP插槽编号检查行。如果此行中存在容器，则FTD在容器模式下运行：

```
-----[ 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
```

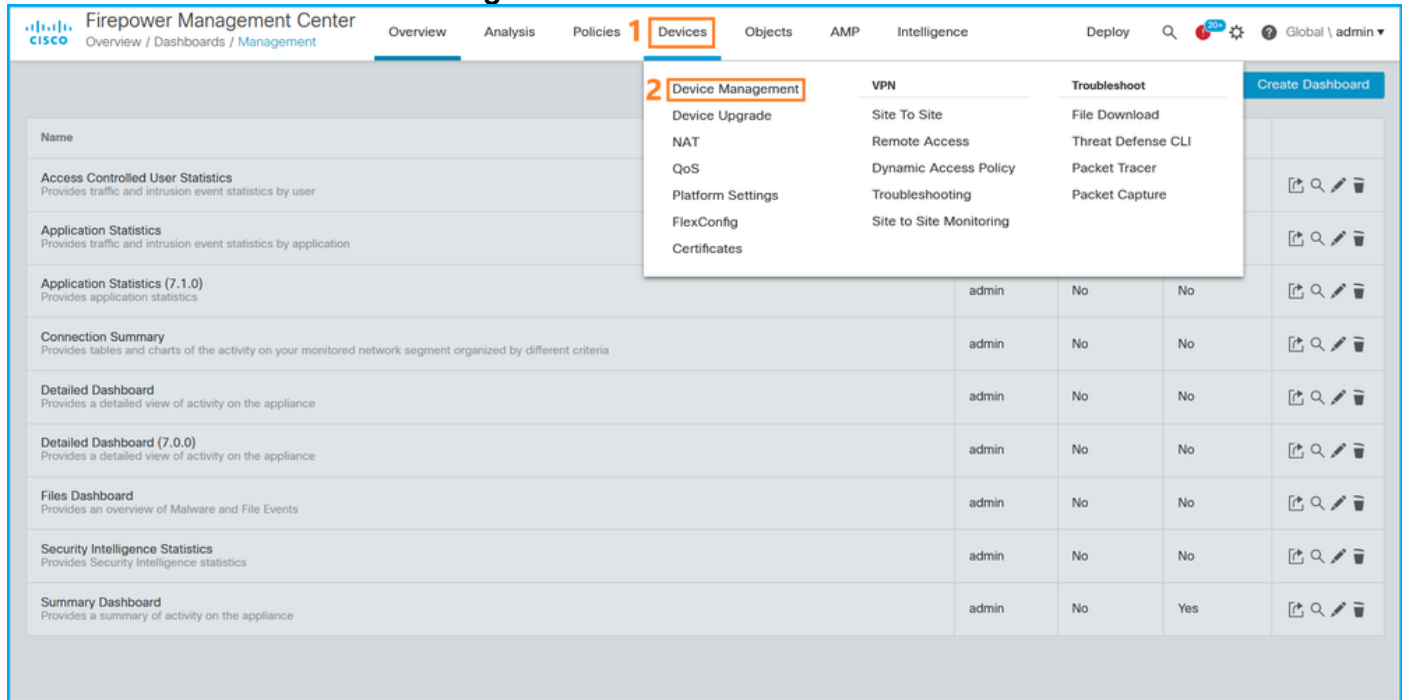
SSP Slot Number: 1 (Container)

...

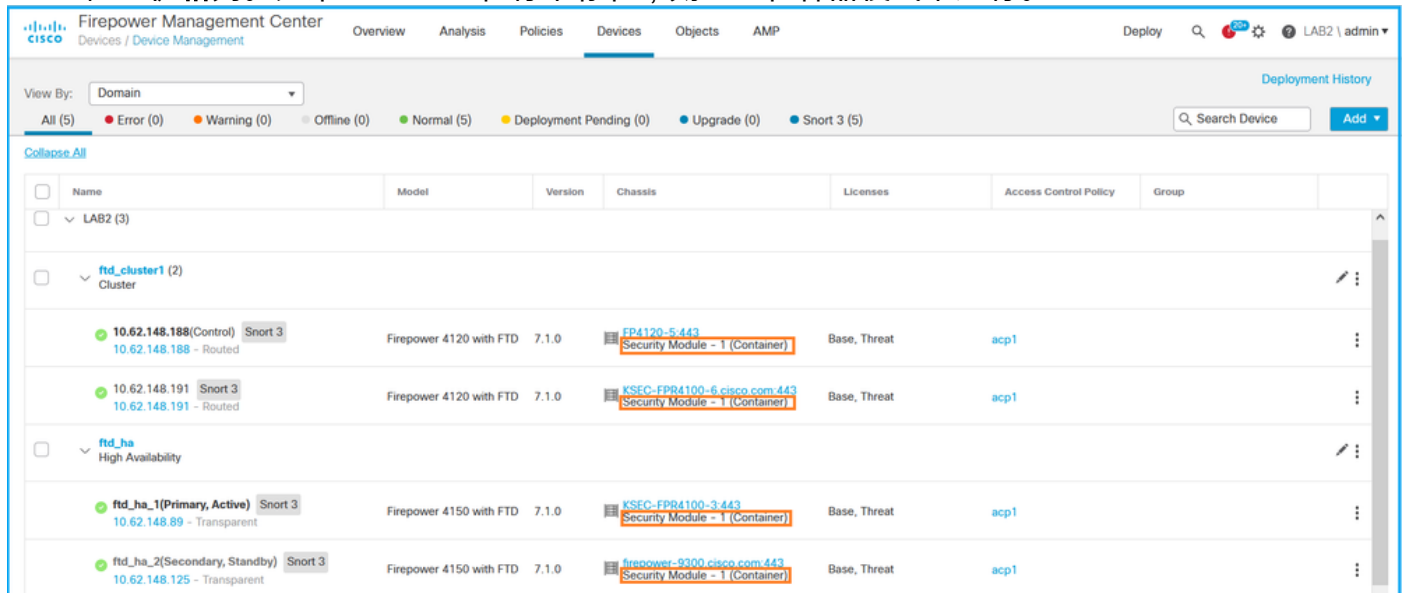
## FMC UI

按照以下步骤验证FMC UI上的FTD实例部署类型：

### 1. 选择Devices > Device Management:



### 2. 检查机箱列。如果Container在行中存在，则FTD在容器模式下运行。



## FMC REST-API

按照以下步骤通过FMC REST-API验证FTD实例部署类型。使用REST-API客户端。在本例中，curl被使用：

### 1. 请求身份验证令牌：

```
# 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.确定包含设备的域。在大多数REST API查询中，域参数是必填项。使用此查询中的令牌检索域列表：

```
# 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-4b09-000000000000"
    },
    ...
  ]
}
```

3.使用域UUID查询特定设备记录和特定设备UUID:

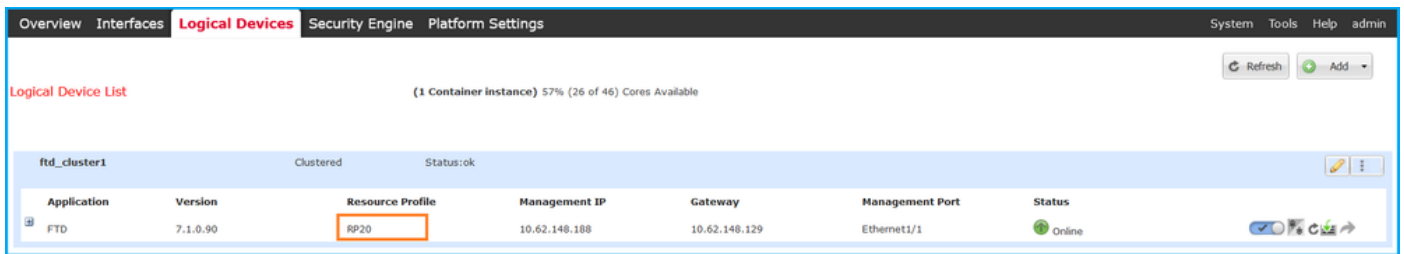
```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
  "items": [
    {
      "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
      },
      "name": "ftd_ha_1",
      "type": "Device"
    },
    ...
  ]
}
```

4.使用此查询中步骤3中的域UUID和设备/容器UUID，并检查isMultiInstance的值:

```
# curl -s -k -X 'GET' 'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/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用户界面

要验证FTD实例部署类型，请检查逻辑设备中的资源配置文件属性的值。如果值不为空，则FTD在容器模式下运行：



## FXOS CLI

按照以下步骤在FXOS CLI上验证FTD实例部署类型：

1. 与机箱建立控制台或SSH连接。
2. 切换到scope ssa并运行show app-instance 命令，然后根据插槽和标识符检查特定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
-----
ftd          ftd_cluster1 1          Enabled      Online          7.1.0.90      7.1.0.90
Container    No            RP20          In Cluster   Master
```

## FXOS REST API

按照以下步骤通过FXOS REST-API请求验证FTD实例部署类型。使用REST-API客户端。在本例中，curl被使用：

1. 请求身份验证令牌：

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' 'https://10.62.148.88/api/login'
{
  "refreshPeriod": "0",
  "token": "3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d"
}
```

2. 指定令牌、此查询中的插槽ID，并检查deployType的值：

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
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",
"appName": "ftd",      "clearLogData": "available",
"clusterOperationalState": "not-applicable",      "clusterRole": "none",
"currentJobProgress": "100",      "currentJobState": "succeeded",
"currentJobType": "start",      "deployType": "container",
...
}
```

## FXOS机箱show-tech文件

按照以下步骤验证FXOS机箱show-tech文件中的FTD防火墙模式：

1. 对于FXOS版本2.7及更高版本，请在<name>\_BC1\_all.tar/  
FPRM\_A\_TechSupport.tar.gz/FPRM\_A\_TechSupport.tar中打开文件sam\_techsupportinfo  
对于早期版本，请在FPRM\_A\_TechSupport.tar.gz/ FPRM\_A\_TechSupport.tar中打开  
sam\_techsupportinfo文件。

2. 检查特定插槽的“show slot expand detail”部分和标识符:

```
# 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
```

## 验证ASA情景模式

ASA支持单情景和多情景模式。FTD不支持多情景模式。

可以使用以下选项验证情景类型：

- ASA CLI
- ASA show-tech

## ASA CLI

按照以下步骤在ASA CLI上验证ASA情景模式：

1. 根据平台和部署模式，使用以下选项访问ASA CLI:

- 以设备模式直接telnet/SSH访问Firepower 1000/3100和Firepower 2100上的ASA
- 在平台模式下从Firepower 2100上的FXOS控制台CLI访问，并通过connect asa命令连接到ASA
- 通过命令(Firepower 4100/9300)从FXOS CLI访问：  
连接模块<x> [console|telnet],其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接SSH访问ASA，或从虚拟机监控程序或云UI进行控制台访问
- 2.在CLI上运行show mode命令：

```
ASA# show mode
Security context mode: multiple
```

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

## ASA show-tech文件

按照以下步骤在ASA show-tech文件中验证ASA情景模式：

1. 检查show-tech文件中的show context detail部分。在这种情况下，情景模式是多情景，因为存在多个情景：

```
----- 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验证Firepower 2100模式

带ASA的Firepower 2100可以在以下模式之一下运行：

- 平台模式 — 基本操作参数和硬件接口设置在FXOS中配置。这些设置包括接口管理状态更改、EtherChannel配置、NTP、映像管理等。FCM Web界面或FXOS CLI可用于FXOS配置。
- 设备模式（默认） — 设备模式允许用户在ASA中配置所有策略。FXOS CLI中仅提供高级命令

使用以下选项验证带ASA的Firepower 2100模式：

- ASA CLI
- FXOS CLI
- FXOS show-tech

## ASA CLI

按照以下步骤在ASA CLI上使用ASA验证Firepower 2100模式：

- 1.使用telnet/SSH访问Firepower 2100上的ASA。
- 2.在CLI上运行show fxos mode命令：

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

设备模式：

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

**注意：**在多情景模式下，show fxos mode命令在系统或管理情景中可用。

## FXOS CLI

按照以下步骤在FXOS CLI上使用ASA验证Firepower 2100模式：

- 1.使用telnet/SSH访问Firepower 2100上的ASA。
- 2.运行connect fxos命令：

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

**注意：**在多情景模式下，connect fxos命令在管理情景中可用。

- 3.运行show fxos-mode命令：

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

设备模式：

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

## FXOS show-tech文件

按照以下步骤在FXOS机箱show-tech文件中使用ASA验证Firepower 2100模式：

1.在<name>\_FPRM.tar.gz/<name>\_FPRM.tar中打开文件tech\_support\_brief

2.选中“show fxos-mode”部分：

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

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

## 已知问题

思科漏洞ID [CSCwb94424](#) 增强：为FMC HA配置验证添加CLISH命令

思科漏洞ID [CSCvn31622](#) 增强：添加FXOS SNMP OID以轮询逻辑设备和应用实例配置

思科漏洞ID [CSCwb97767](#) 增强：添加OID以验证FTD实例部署类型

思科漏洞ID [CSCwb97772](#) 增强：在Firepower 2100上的ASA的show-tech中包含“show fxos mode”的输出

思科漏洞ID [CSCwb97751](#) 用于透明防火墙模式验证的OID 1.3.6.1.4.1.9.9.491.1.6.1.1不可用

## 相关信息

- [安全防火墙管理中心REST API快速入门指南，版本7.1](#)
- [在Firepower NGFW设备上配置SNMP](#)
- [思科Firepower威胁防御REST API指南](#)
- [思科FXOS REST API参考](#)
- [思科ASA兼容性](#)
- [Firepower 1000/2100和安全防火墙3100 ASA和FXOS捆绑包版本](#)
- [捆绑组件](#)
- [Firepower文件生成过程故障排除](#)
- [Cisco Firepower 2100入门指南](#)
- [思科Firepower威胁防御兼容性指南](#)