验证Firepower模式、实例、可用性、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用户界面
  - 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用户界面
  - FMC REST API
  - FDM UI
  - FDM REST-API
  - FCM UI
  - FXOS CLI
  - FXOS REST API
  - 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 UI
  - FXOS CLI
  - FXOS REST API
  - 机箱show-tech文件

检验防火墙模式

- FTD防火墙模式
  - FTD CLI
  - FTD故障排除文件
  - FMC用户界面

- FMC REST API
- FCM UI
- FXOS CLI
- FXOS REST API
- 机箱show-tech文件

ASA防火墙模式

- ASA CLI
- ASA show-tech文件
- FCM UI
- FXOS CLI
- FXOS REST API
- 机箱show-tech文件

验证实例部署类型

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

已知问题

相关信息

简介

本文档介绍对Firepower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。

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 1000、2100、Firepower 4100/9300
- 安全防火墙3100/4200
- Firepower管理中心(FMC)版本7.1.x
- Firepower可扩展操作系统(FXOS)2.11.1.x、2.16.x
- Firepower设备管理器(FDM)7.1.x
- Firepower威胁防御7.1.x、7.6.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，以便当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。通过集群配置，可以将多个FTD节点组合为一个逻辑设备。集群提供单个设备（管理、集成到网络）的所有便利性，以及增加多个设备的吞吐量和冗余。

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，FTD独立配置没有验证命令。独立、故障切换和集群配置模式互相排斥。如果设备没有故障切换和集群配置，则认为该设备在独立模式下运行。

FMC高可用性

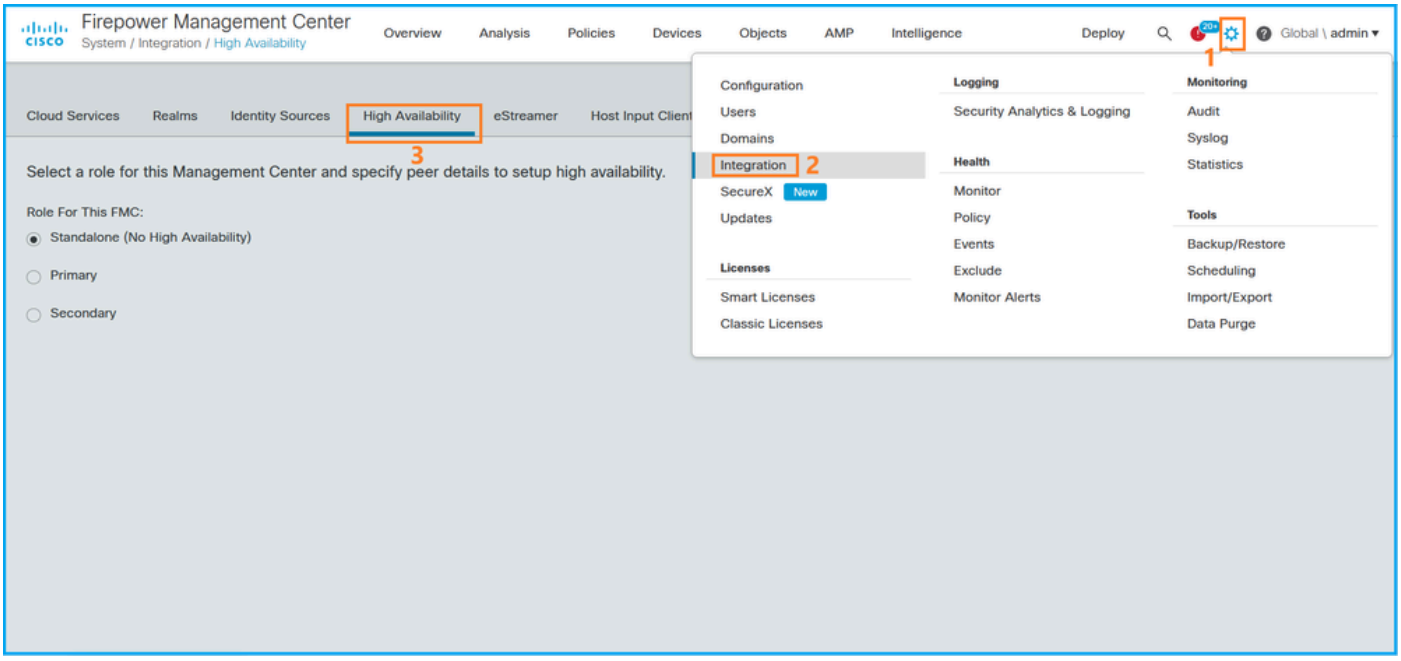
FMC高可用性配置和状态可通过使用以下选项进行验证：

- FMC用户界面
- FMC CLI
- REST API请求
- FMC故障排除文件

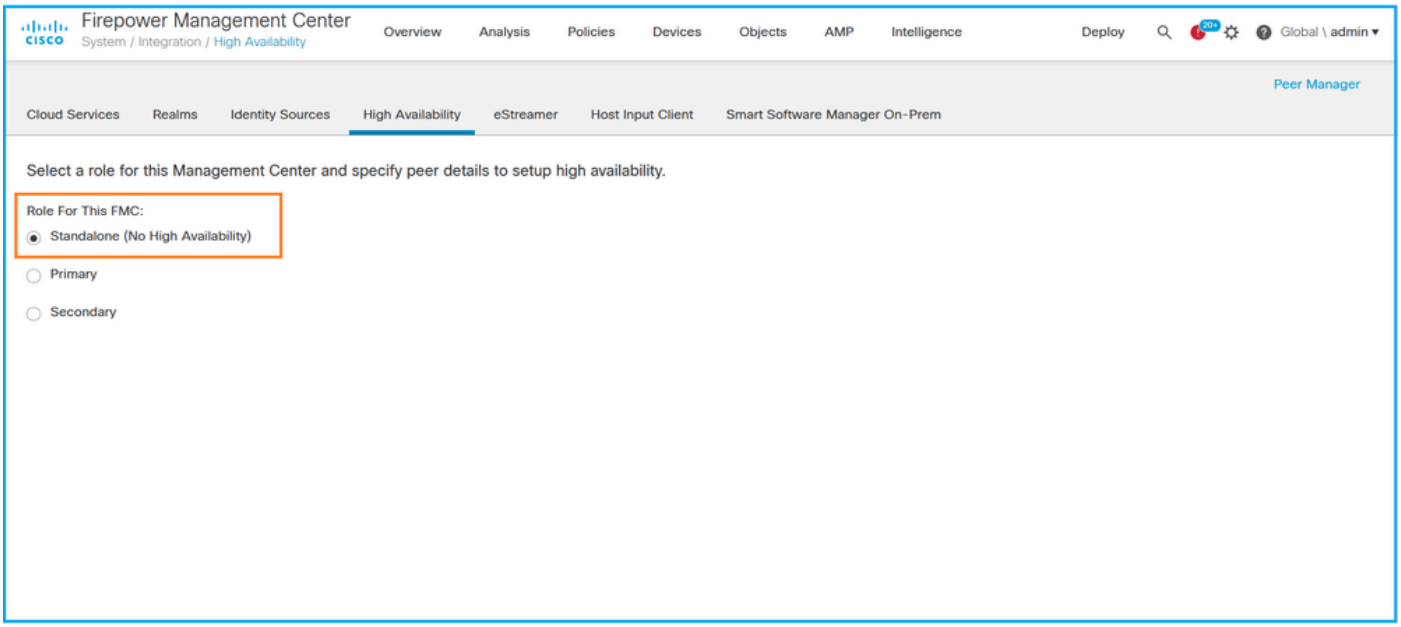
FMC用户界面

按照以下步骤验证FMC UI上的FMC高可用性配置和状态：

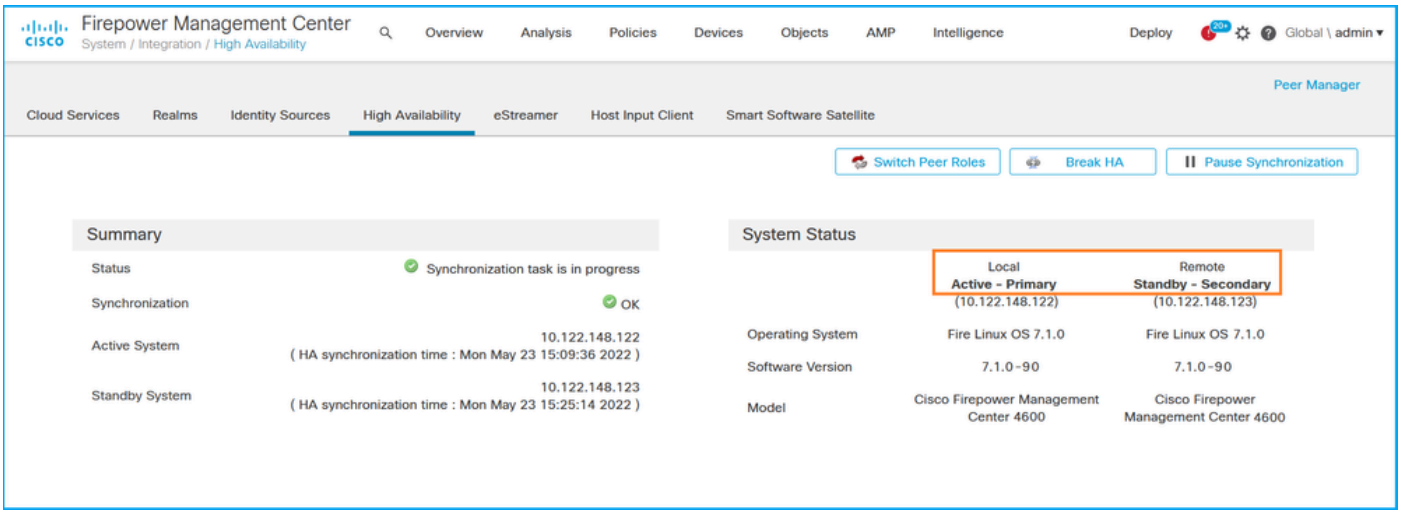
1.选择System > Integration > High Availability:



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



如果配置了高可用性，则会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expert命令，然后运行sudo su命令：

```
<#root>

>

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 Show HA Info Of FMC。如果未配置高可用性，将显示以下输出：

```
<#root>

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，将显示以下输出：

<#root>

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/
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active或standby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。在本示例中，使用curl:

1.请求身份验证令牌：

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B

...
< 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:

<#root>

```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'

{    "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：部件 命令字符串的| python -m json.tool用于以JSON样式设置输出格式，并且是可选的。

3.在此查询中使用全局域UUID:

<#root>

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/i
```

如果未配置高可用性，将显示以下输出：

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

如果配置了高可用性，将显示以下输出：

<#root>

```
{
    "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/integr
    },
    "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，然后导航到文件夹<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，将显示以下输出：

<#root>

```
#
```

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，将显示以下输出：

```
<#root>

#

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/
$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                csm_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
```

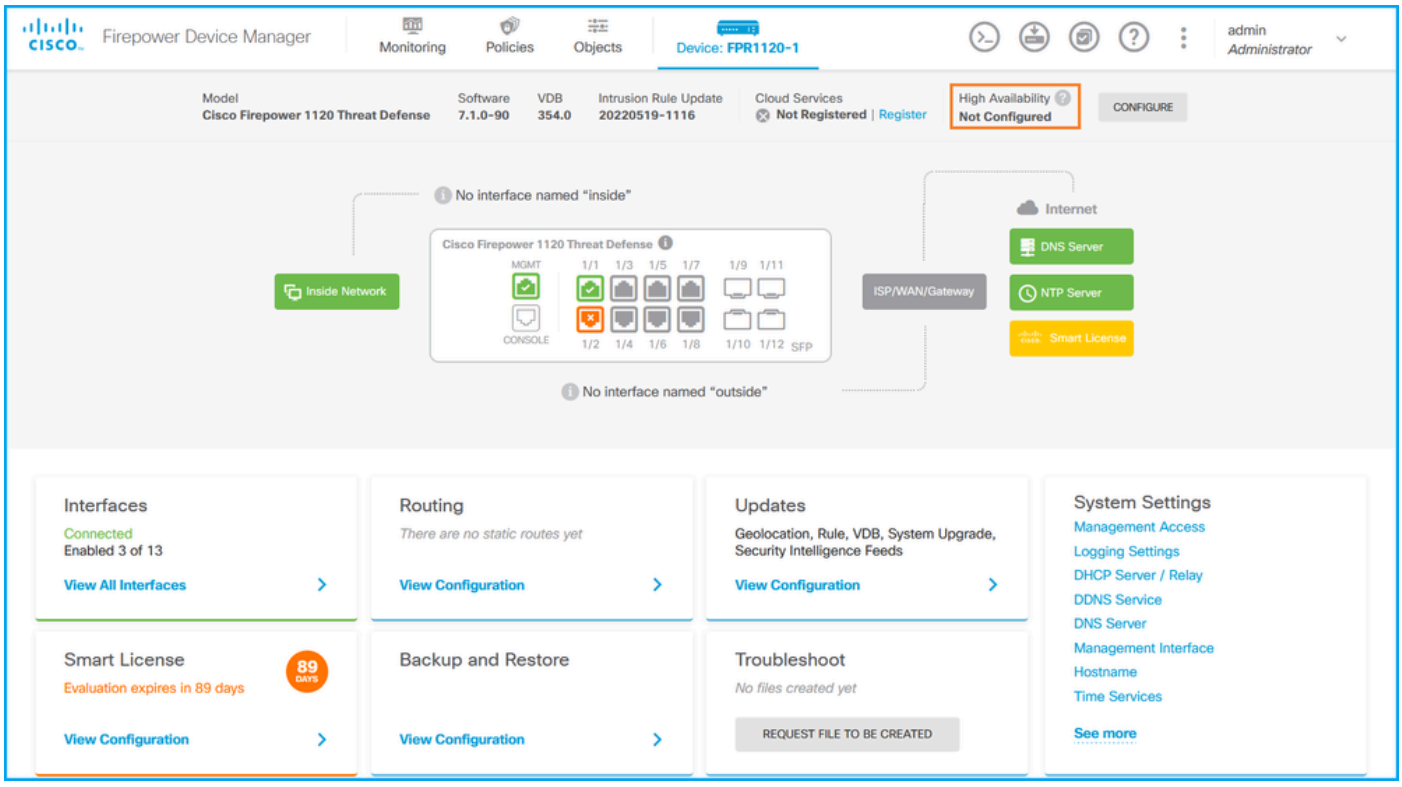
FDM高可用性

可以使用以下选项验证FDM高可用性配置和状态：

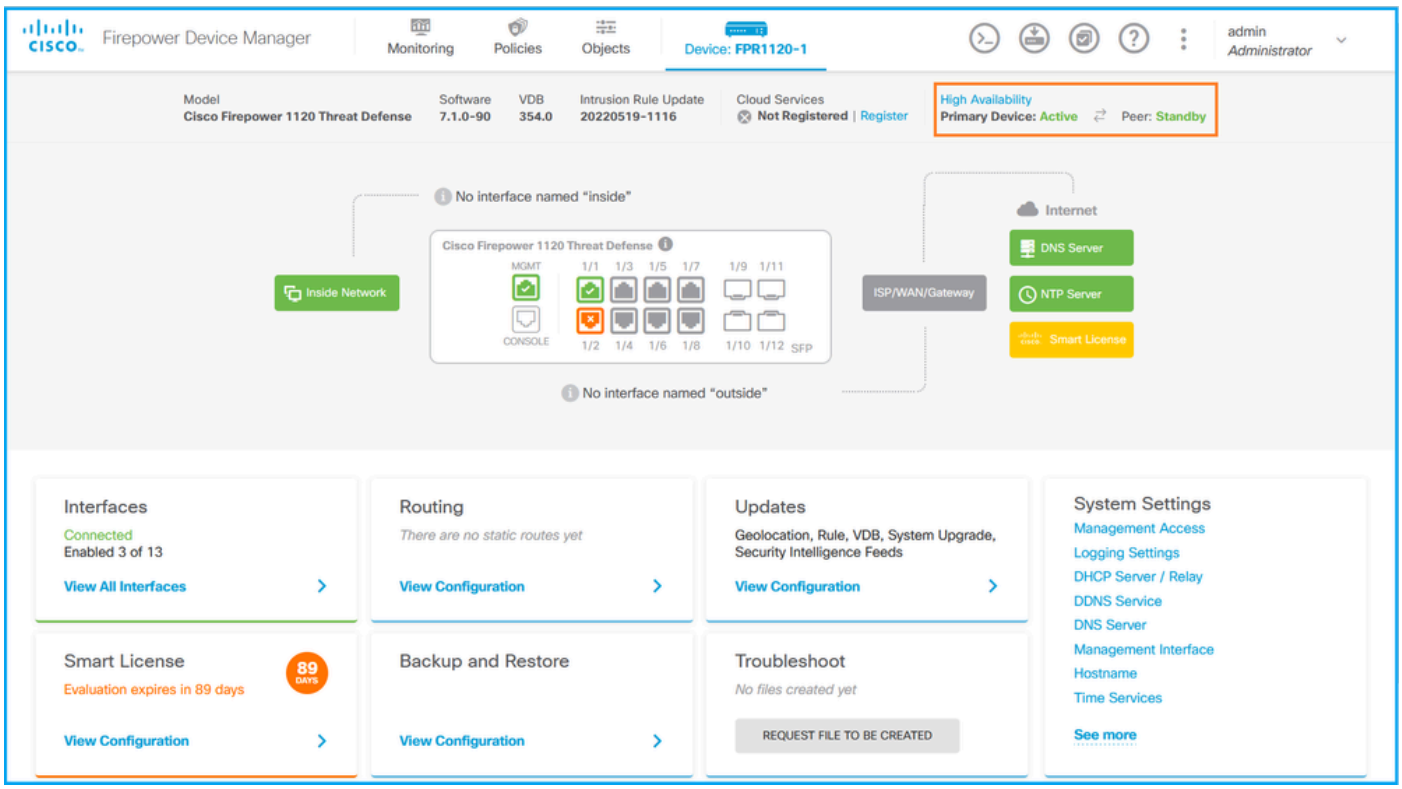
- FDM UI
- FDM REST API请求
- FTD CLI
- FTD SNMP轮询
- FTD故障排除文件

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High Availability。如果未配置高可用性，则High Availability值为Not Configured:



如果配置了高可用性，则会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。在本示例中，使用curl:

1.请求身份验证令牌：

<#root>

#

curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ "gra

{
    "

access_token

":
    "

eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0xMWVjLWE5MmE

",
    "expires_in": 1800,
    "refresh_expires_in": 2400,
    "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIx
    "token_type": "Bearer"
}

2.要验证高可用性配置，请使用此查询中的访问令牌值：

<#root>

#

curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiO

如果未配置高可用性，将显示以下输出：

<#root>


```
{
  "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
      }
    }
  ],
  "paging": {
    "prev": [],
    "next": [],
    "limit": 10,
    "offset": 0,
    "count": 1,
    "pages": 0
  }
}
```


如果配置了高可用性，将显示以下输出：

<#root>


```
{
  "items": [
    {
      "version": "issgb3rw2lixf",


 "name": "HA",



      "nodeRole": "HA_PRIMARY",


      "failoverInterface": {
        "version": "ezzafxo5ccti3",
        "name": "",
        "hardwareName": "Ethernet1/1",
        "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
        "type": "physicalinterface"
      },
...
```


3.要验证高可用性状态，请使用以下查询：

<#root>

```
#

curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiO
```

如果未配置高可用性，将显示以下输出：

<#root>

```
{
  "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，将显示以下输出：

<#root>

```
{
 "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

按照FTD CLI部分中的步骤进行操作。

FTD SNMP轮询

按照FTD SNMP部分中的步骤操作。

FTD故障排除文件

按照FTD故障排除文件部分中的步骤进行操作。

FTD高可用性和可扩展性

可使用以下选项验证FTD高可用性和可扩展性配置和状态：

- FTD CLI
- FTD SNMP
- FTD故障排除文件
- FMC用户界面
- FMC REST-API
- FDM UI
- FDM REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- 机箱显示技术文件

FTD CLI

按照以下步骤验证FTD CLI上的FTD高可用性和可扩展性配置及状态：

1.根据平台和部署模式，使用以下选项访问FTD CLI:

- 通过SSH直接访问FTD — 所有平台
- 通过connect ftd命令从FXOS控制台CLI(Firepower 1000/2100/3100/4200)进行访问
- 从FXOS CLI通过命令(Firepower 4100/9300)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，直接通过SSH访问FTD，或者从虚拟机监控程序或云用户界面访问控制台

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。

如果未配置故障转移，将显示以下输出：

```
<#root>

>

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，将显示以下输出：

```
<#root>

>

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，将显示以下输出：

```
<#root>

>

show running-config cluster


>

show cluster info


Clustering is not configured
```

如果配置了集群，将显示以下输出：

```
<#root>

>

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：源角色和控制角色相同。

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. 确保配置并启用了SNMP。对于FDM管理的FTD，有关配置步骤，请参阅在Firepower FDM上配置并排除SNMP故障。对于FMC管理的FTD，请参阅在Firepower NGFW设备上配置SNMP，了解配置步骤。
2. 要验证FTD故障切换配置和状态，请轮询OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1。

如果未配置故障转移，将显示以下输出：

```
<#root>

#

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，将显示以下输出：

<#root>

#

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，将显示以下输出：

<#root>

 # 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：

<#root>

#

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、已启用且运行正常，则显示以下输出：

```
<#root>

#

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描述的详细信息，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到文件夹<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:

<#root>

```
# 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。

如果未配置故障转移，将显示以下输出：

<#root>

```
----------------- 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，将显示以下输出：

<#root>

```
------------------ 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，将显示以下输出：

<#root>

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


Clustering is not configured
```

如果已配置并启用集群，则显示以下输出：

<#root>

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

Cluster ftd_cluster1: On
```

```
    Interface mode: spanned
Cluster Member Limit : 16

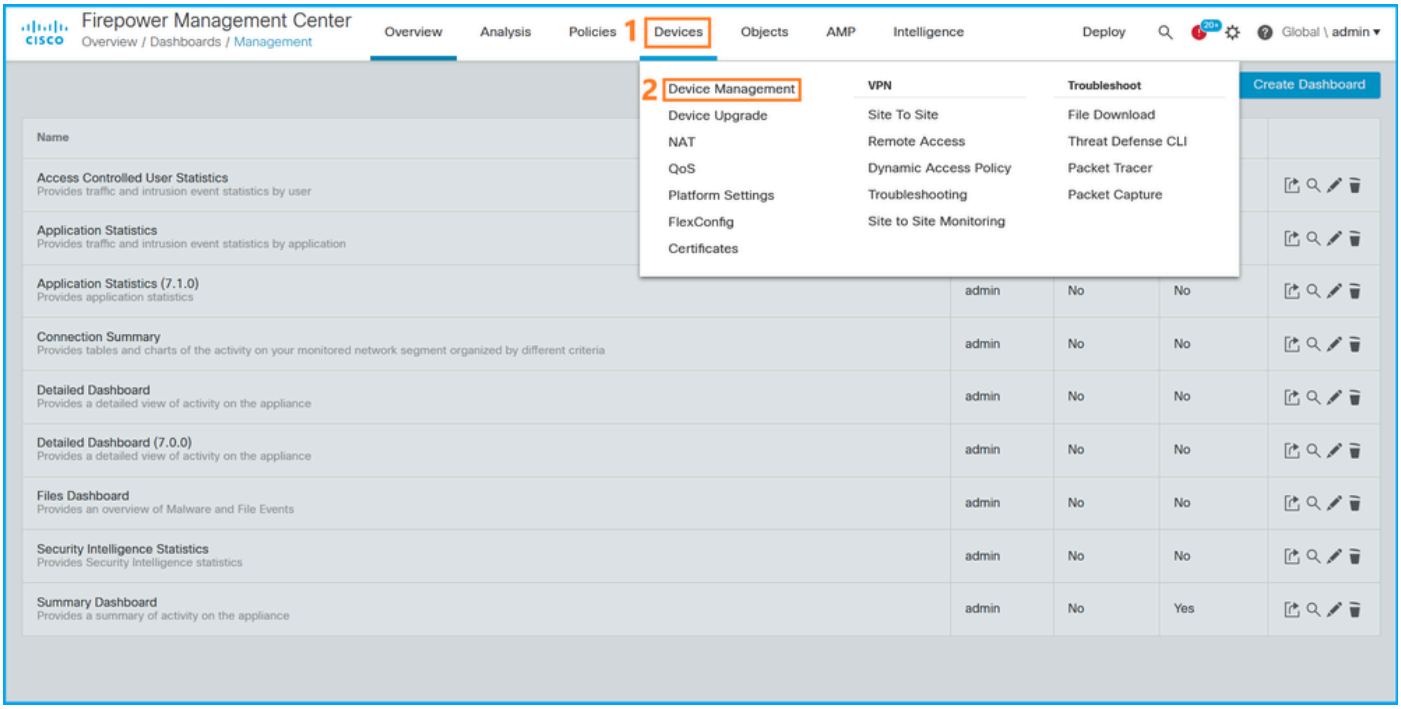

This is "unit-1-1" in state MASTER

        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
```

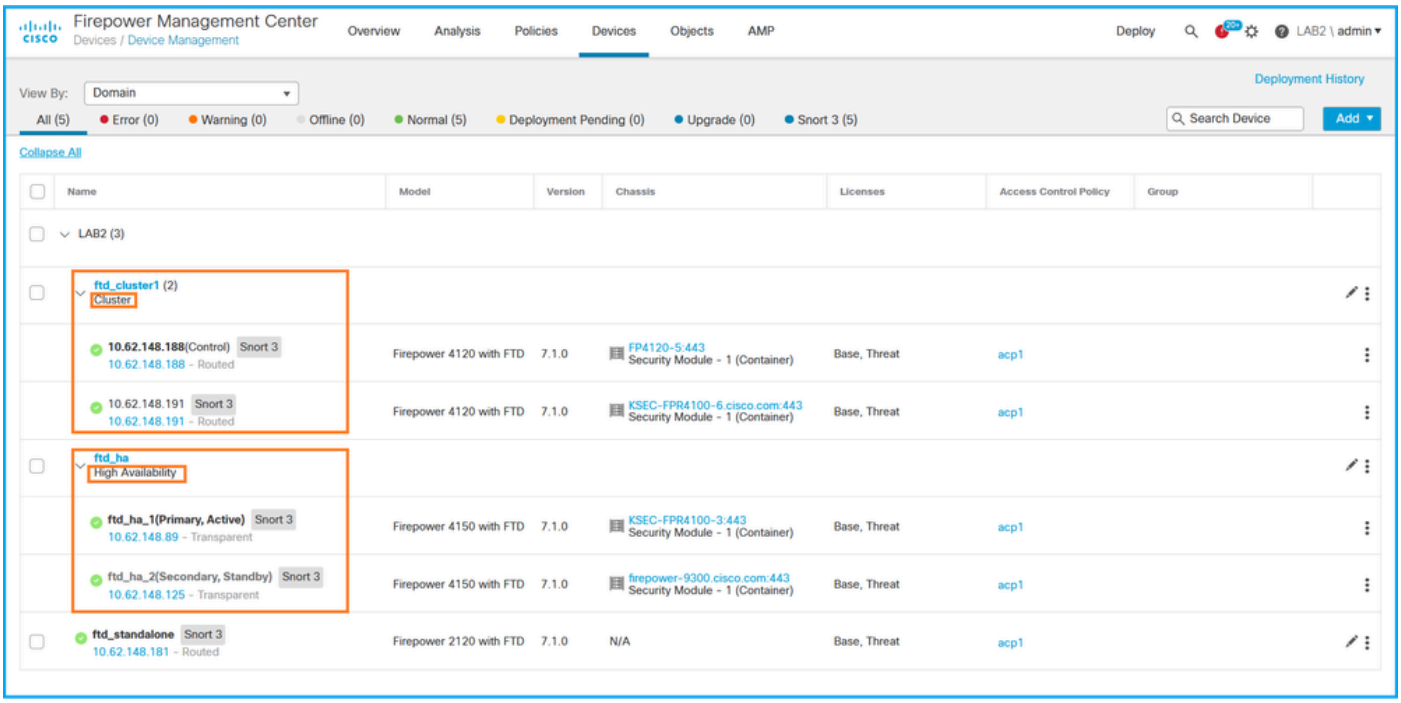
FMC用户界面

按照以下步骤在FMC UI上验证FTD高可用性和可扩展性配置及状态：

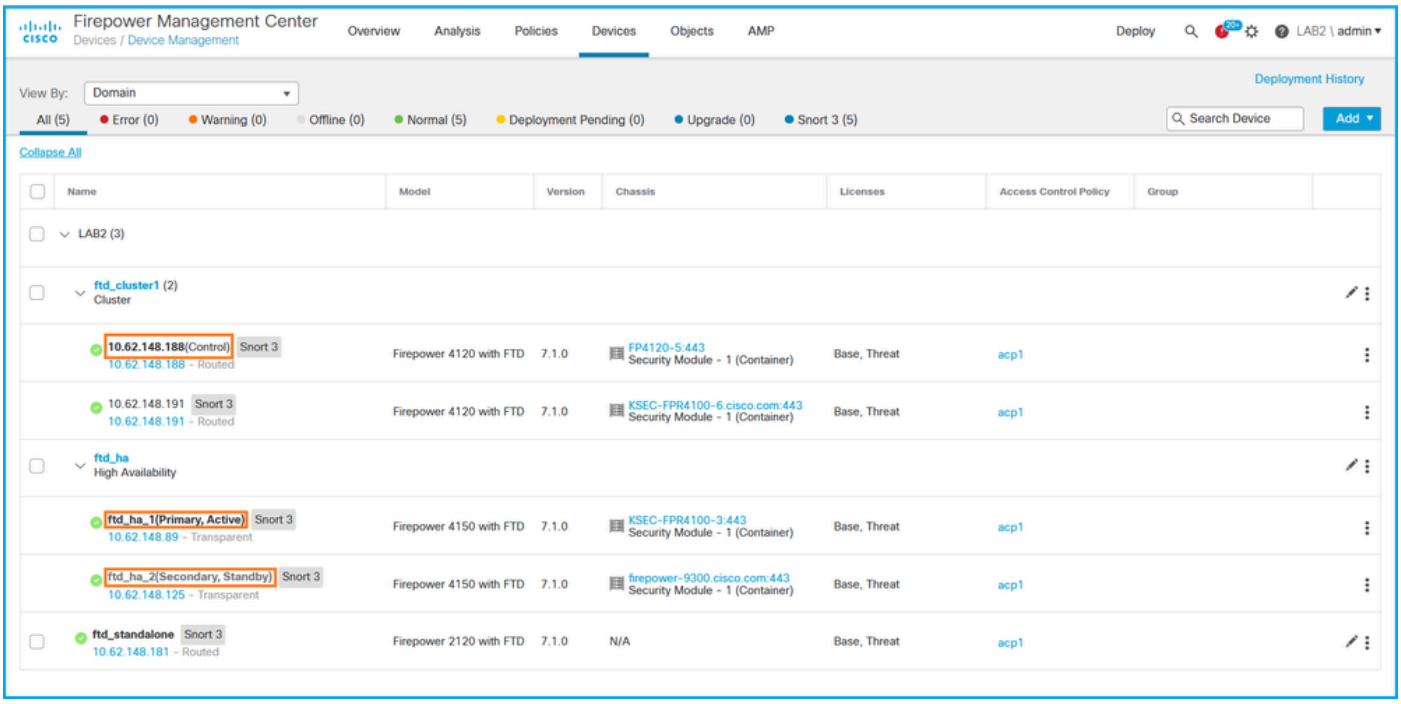
1.选择Devices > Device Management:



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：



3.为了验证FTD高可用性和可扩展性状态，请检查括号中的设备角色。如果角色不存在，并且FTD不是集群或故障转移的一部分，则FTD在独立配置中运行：



注意：在集群的情况下，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和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。在本示例中，使用curl:

1. 请求身份验证令牌：

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B
```

```
< X-auth-access-token:
```

```
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

2.标识包含设备的域。在大多数REST API查询中，domain参数是必需的。使用此查询中的令牌检索域列表：

<#root>

```
#
```

```
curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
   "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:

<#root>

#

curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/de

```
{
    "items": [
        {
```

"id": "796eb8f8-d83b-11ec-941d-b9083eb612d8"

```
,
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-00000000000
            },
```

"name": "ftd_ha_1",

```
            "type": "Device"
        },
       ...
```

4.要验证故障转移配置，请使用此查询第3步中的域UUID和设备/容器UUID:

<#root>

#

curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devic

```
...
        "containerDetails": {
```

"id": "eec3ddfc-d842-11ec-a15e-986001c83f2f",

"name": "ftd_ha",

"type": "DeviceHAPair"

```
        },
...
```

5.要验证故障切换状态，请使用此查询第4步中的域UUID和DeviceHAPair UUID:

<#root>

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

...

"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，请使用此查询第3步中的域UUID和设备/容器UUID:

<#root>

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/dev
...
        "containerDetails": {
            "id": "
8e6188c2-d844-11ec-bdd1-6e8d3e226370
",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-00000000000
            },
"name": "ftd_cluster1",
            "type": "DeviceCluster"
        },
...
```

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

<#root>

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/dev
{
    "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FDM UI部分中的步骤操作。

FDM REST-API

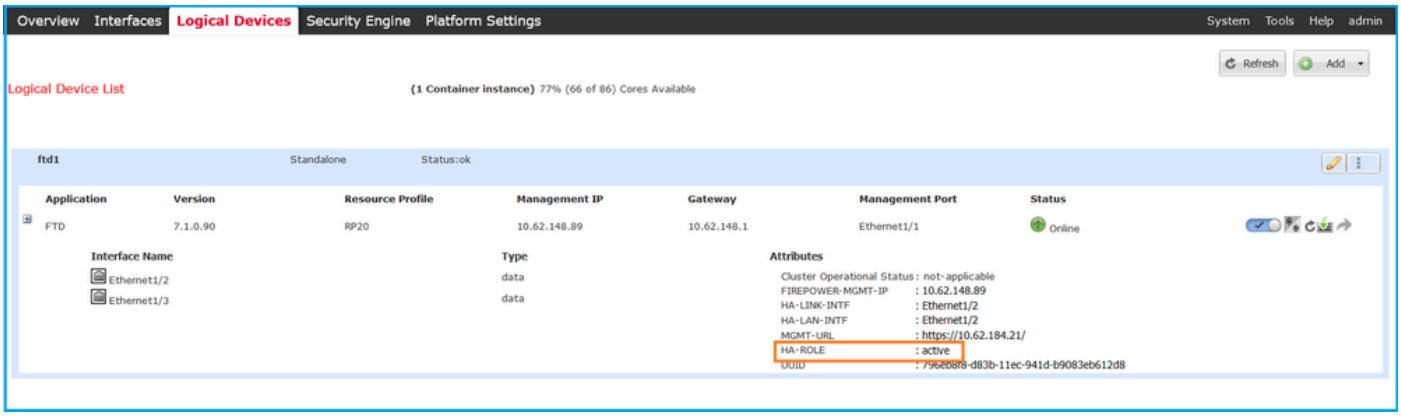
按照REST-API部分中的步骤进行操作。

FCM UI

FCM UI在带有ASA的Firepower 4100/9300和Firepower 2100平台模式下可用。

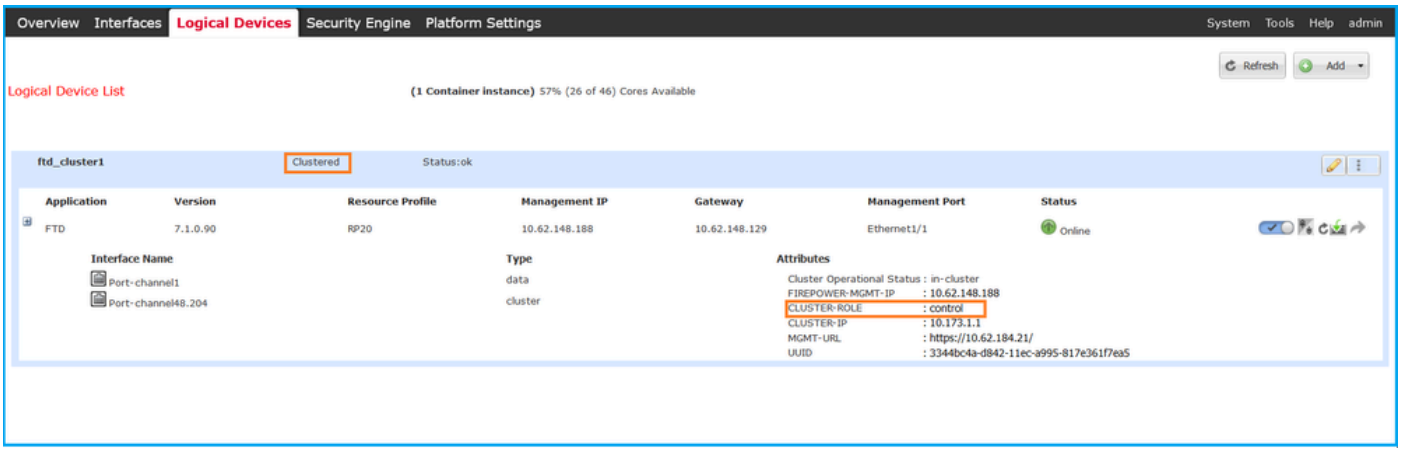
按照以下步骤验证FCM UI上的FTD高可用性和可扩展性状态：

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



注意：逻辑设备标识符旁边的Standalone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，请检查“逻辑设备”页上的集群标签和集群角色属性值：



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或安全防火墙3100/4200上可用。

按照以下步骤在FXOS CLI上验证FTD高可用性和可扩展性配置及状态：

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：

<#root>

```
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）和show app-instance命令。检查特定插槽的输出:

<#root>

```
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 Ty
---------- ---------- ---------- ----------- --------------- --------------- --------------- ---------
ftd
```

ftd_cluster1

1

```
          Enabled     Online           7.1.0.90        7.1.0.90        Container   No         RP20
```

In Cluster

Master

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。在本示例中，使用curl:

1.请求身份验证令牌：

<#root>

 # 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，请使用此查询中的令牌和插槽ID:

<#root>

#

curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453c

...

```
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_JAD20120OR43VLP1G3",
            "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-firepowe
                    "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-
                    "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-i
                    "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. 要验证FTD集群配置，请在此查询中使用逻辑设备标识符：

<#root>

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da445

{
    "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，请使用此查询：

<#root>

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da445
```


```
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_JAD19500BABIYA3OO58",
            "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",
...
```

机箱show-tech文件

可以在Firepower 1000/2100/4100/9300或安全防火墙3100/4200机箱show-tech文件中验证FTD高可用性和可扩展性配置和状态。

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

1. 在Firepower 4100/9300上，对于FXOS版本2.7及更高版本，请打开<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中的sam_techsupportinfo文件

对于早期版本，请打开FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中的sam_techsupportinfo文件。

2.在Firepower 1000/2100和安全防火墙3100/4200上打开文件tech_support_brief。

2.为了验证故障切换状态，请检查“show slot expand detail”部分中特定插槽下的ha-role属性值:

<#root>

```
# 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.为了验证FTD集群配置，请检查“show logical-device detail expand”部分中特定插槽下的Mode属性值:

<#root>

`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.为了验证FTD集群状态，请在show slot expand detail部分中检查特定插槽下的集群状态和集群角色属性值:

<#root>

`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

可以使用以下选项验证ASA高可用性和可扩展性配置和状态：

- ASA CLI
- ASA SNMP轮询
- ASA show-tech file
- FCM UI
- FXOS CLI
- FXOS REST-API
- 机箱显示技术文件

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:

- 在设备模式下直接通过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
- 从FXOS CLI通过命令(Firepower 4100/9300)访问：

  connect module <x> [console|telnet]，其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接通过SSH访问ASA，或者从虚拟机监控程序或云UI访问控制台

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。

如果未配置故障转移，将显示以下输出：

```
<#root>

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，将显示以下输出：

```
<#root>

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，将显示以下输出：

```
<#root>

asa#

show running-config cluster
```

```
asa#
show cluster info


Clustering is not configured
```

如果配置了集群，将显示以下输出：

```
<#root>
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. 确保配置并启用了SNMP。

2. 要验证故障切换配置和状态轮询OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1。

如果未配置故障转移，将显示以下输出：

```
<#root>

#

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"
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，将显示以下输出：

```
<#root>

#

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.为了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，将显示以下输出：

```
<#root>
```

```
# 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：

```
<#root>
#
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、已启用且运行正常，则显示以下输出：

```
<#root>
#
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描述的详细信息，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。

如果未配置故障转移，将显示以下输出：

```
<#root>
------------------ 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，将显示以下输出：

```
<#root>
```

```
------------------ 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，将显示以下输出：

<#root>

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


Clustering is not configured
```

如果已配置并启用集群，则显示以下输出：

<#root>

```
------------------ 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

按照FCM UI部分中的步骤操作。

FXOS CLI

按照FXOS CLI部分中的步骤进行操作。

FXOS REST API

按照FXOS REST-API部分中的步骤进行操作。

机箱show-tech文件

按照机箱show-tech文件部分中的步骤进行操作。

检验防火墙模式

FTD防火墙模式

防火墙模式是指路由或透明防火墙配置。

可以使用以下选项验证FTD防火墙模式：

- FTD CLI
- FTD show-tech
- FMC用户界面
- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- 机箱显示技术文件

注意：FDM不支持透明模式。

FTD CLI

按照以下步骤验证FTD CLI上的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:

- 通过SSH直接访问FTD — 所有平台
- 通过connect ftd命令从FXOS控制台CLI(Firepower 1000/2100/3100)进行访问
- 从FXOS CLI通过命令(Firepower 4100/9300)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，直接通过SSH访问FTD，或者从虚拟机监控程序或云用户界面访问控制台

2.要验证防火墙模式，请在CLI上运行show firewall命令：

```
<#root>

>

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到文件夹<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:

```
<#root>

# 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：

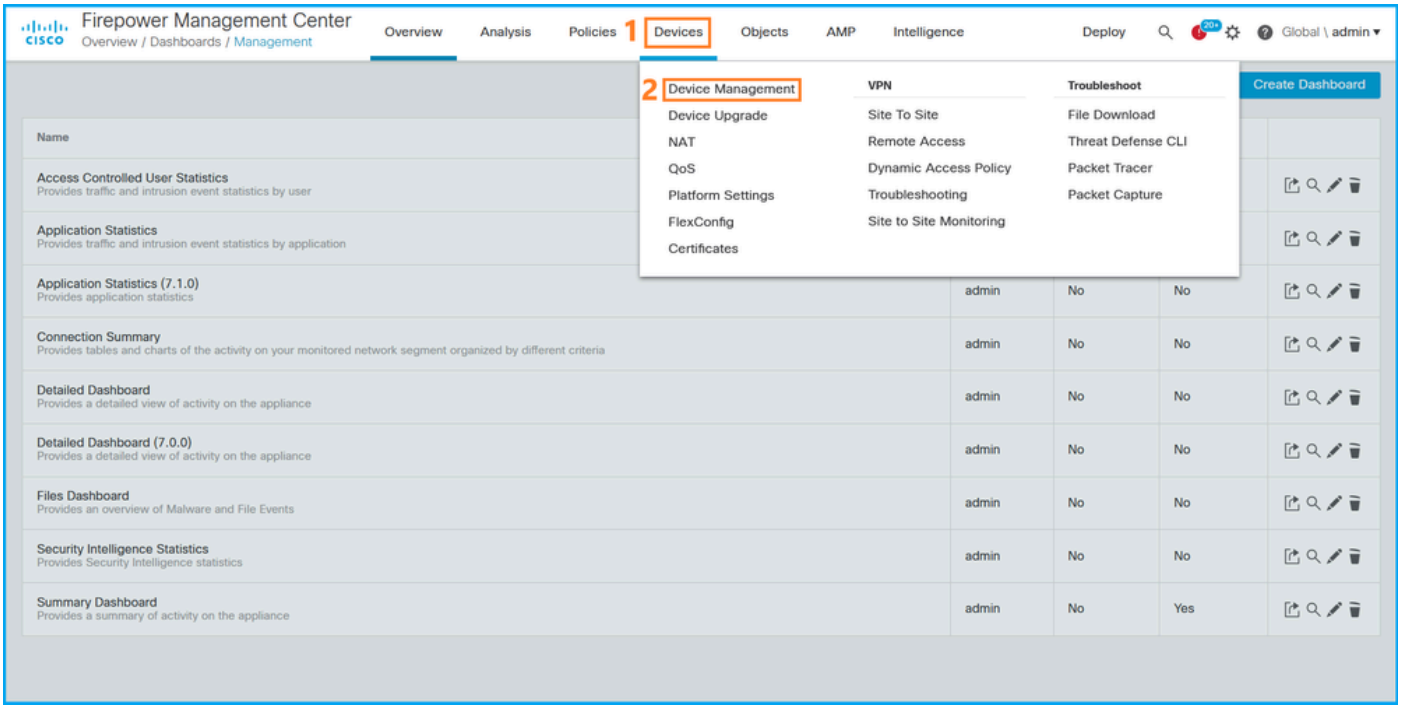
```
<#root>
```

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

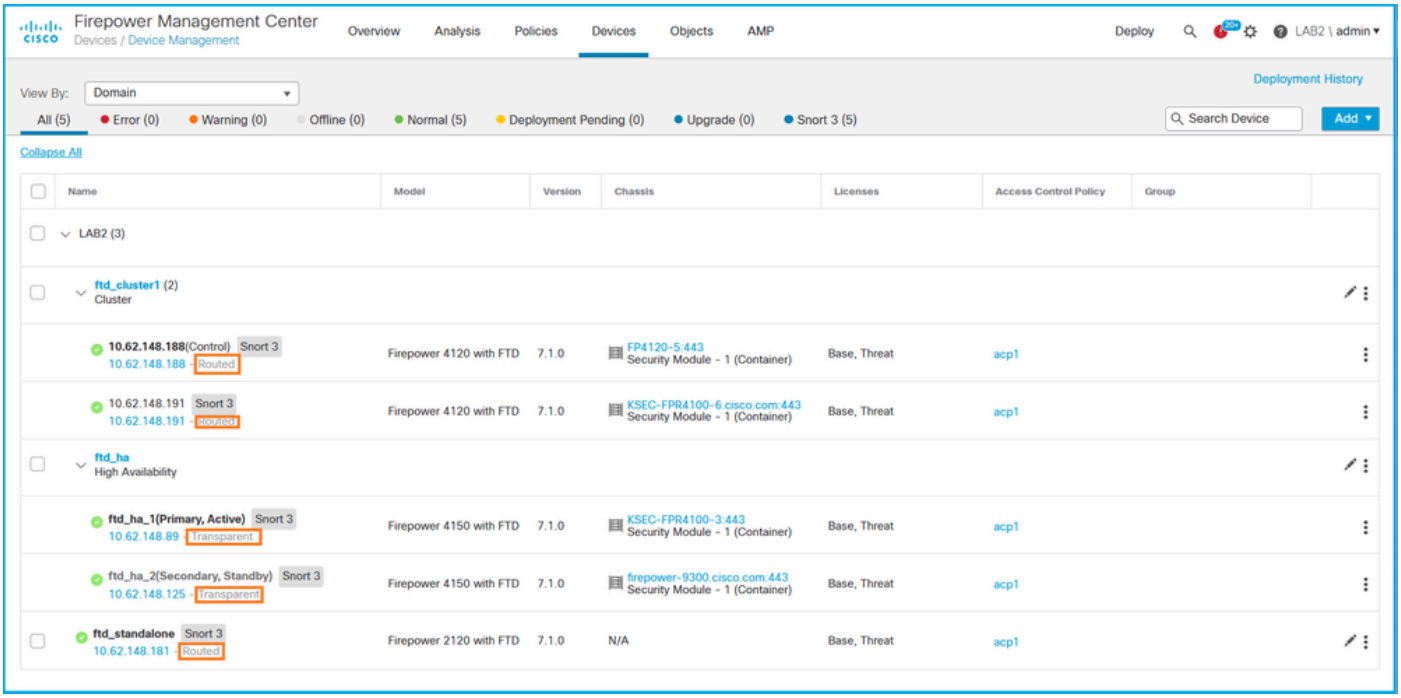
FMC用户界面

按照以下步骤验证FMC UI上的FTD防火墙模式：

1.选择Devices > Device Management:



2.检查标签Routed或Transparent:



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。在本示例中，使用curl:

1. 请求身份验证令牌：

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B
```

```
< X-auth-access-token:
```

```
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

2.标识包含设备的域。在大多数REST API查询中，domain参数是必需的。使用此查询中的令牌检索域列表：

<#root>

```
#
```

```
curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
   "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:

<#root>

#

curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/de

```
{
    "items": [
        {
```

"id": "796eb8f8-d83b-11ec-941d-b9083eb612d8"

```
,
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-00000000000
            },
            "name": "ftd_ha_1",
            "type": "Device"
        },
        ...
```

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

<#root>

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

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

"ftdMode": "ROUTED",

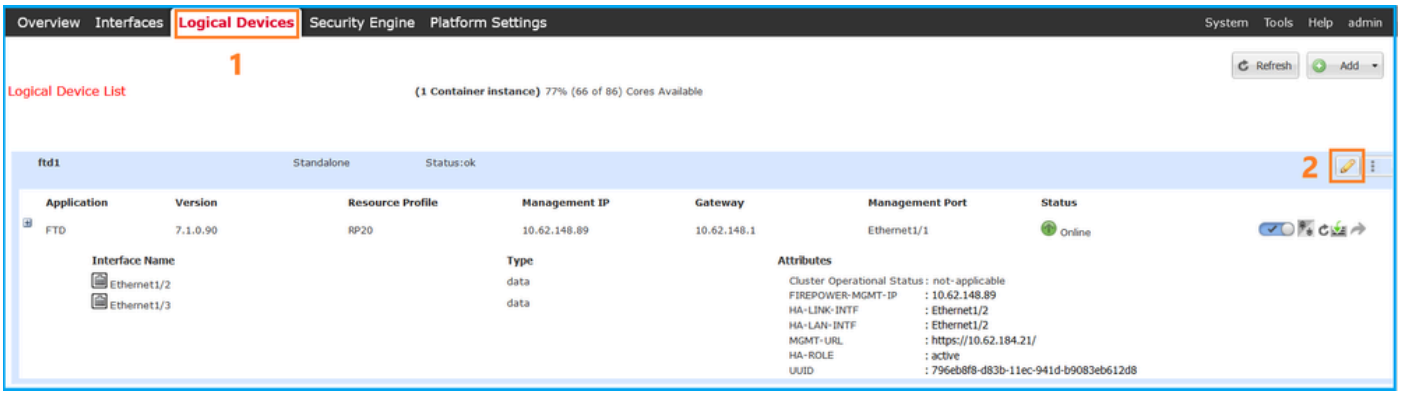
```
...
```

FCM UI

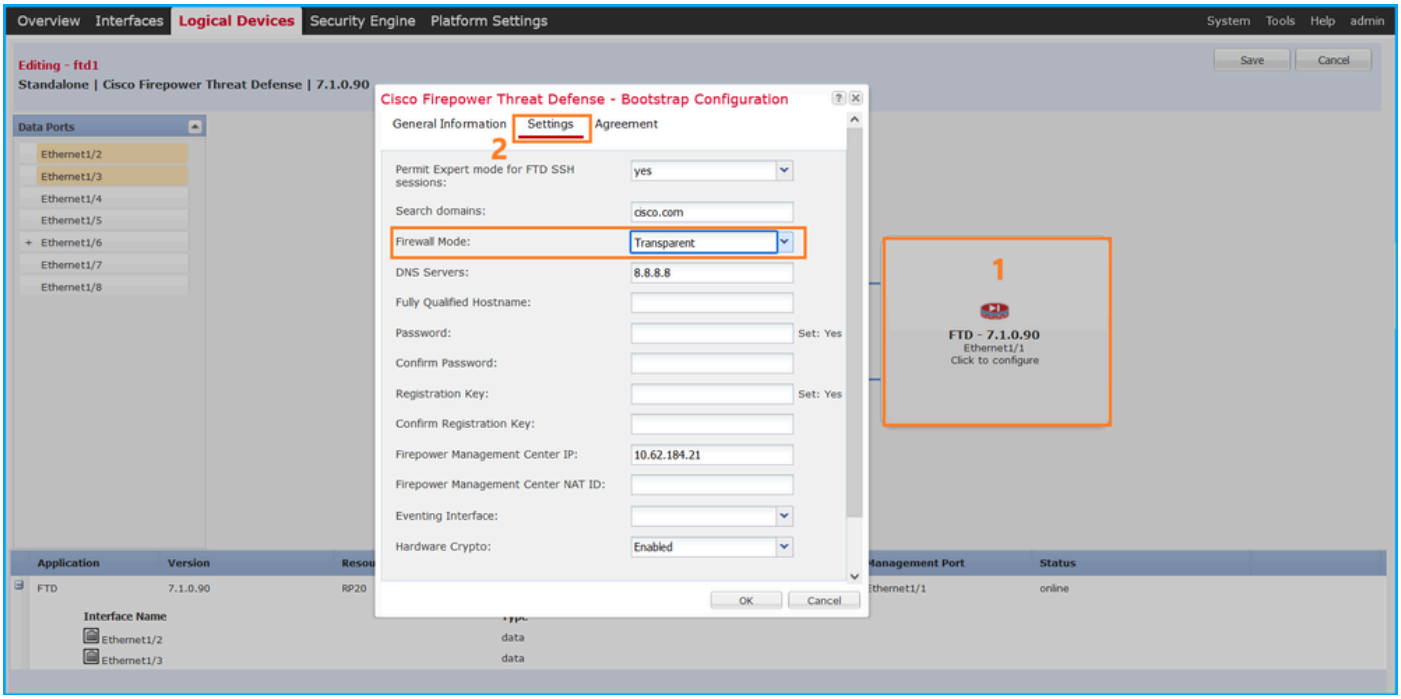
可以在Firepower 4100/9300上验证防火墙模式是否为FTD。

按照以下步骤验证FCM UI上的FTD防火墙模式：

1.编辑Logical Devices页面上的逻辑设备：



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

可以在Firepower 4100/9300上验证防火墙模式是否为FTD。

按照以下步骤验证FXOS CLI上的FTD防火墙模式：

1. 建立到机箱的控制台或SSH连接。
2. 切换到scope ssa，然后切换到specific logical-device，运行show mgmt-bootstrap expand命令，并检查FIREWALL_MODE属性值:

```
<#root>

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 Tim
        ---------- ------------------- --------------- --------------- --------------- ----------------
                 1 Firepower           10.62.148.188   255.255.255.128 10.62.148.129   2022-05-20T13:50

    Bootstrap Key:
        Key                       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支持FXOS REST-API。

按照以下步骤通过FXOS REST-API请求检验FTD防火墙模式。使用REST-API客户端。在本示例中，使用curl:

1. 请求身份验证令牌：

<#root>

 # curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123' https://192.0.2.100/api/ld/ftd_cluster1

```
{
    "refreshPeriod": "0",
    "token": "
```

3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d

```
"
}
```

2.使用此查询中的逻辑设备标识符并检查FIREWALL_MODE键的值：

<#root>

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da445
```

```
...
                        {
```

```
"key": "FIREWALL_MODE",
```

```
                            "rn": "key-FIREWALL_MODE",
                            "updateTimestamp": "2022-05-20T13:28:37.093",
                            "urllink": "https://192.0.2.100/api/ld/ftd_cluster1/mgmt-bootstrap/ftd/key/
```

```
"value": "routed"
```

```
                        },
...
```

机箱show-tech文件

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

按照以下步骤验证机箱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，请打开<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中的sam_techsupportinfo文件

对于早期版本，请在FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar中打开文件sam_techsupportinfo。

2. 检查特定标识符和插槽下的show logical-device detail expand部分：

<#root>

```
# 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

可以使用以下选项验证ASA防火墙模式：

- ASA CLI
- ASA show-tech
- FCM UI
- FXOS CLI
- FXOS REST-API
- 机箱显示技术文件

ASA CLI

按照以下步骤验证ASA CLI上的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:

- 在设备模式下直接通过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
- 从FXOS CLI通过命令(Firepower 4100/9300)访问：

  connect module <x> [console|telnet]，其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接通过SSH访问ASA，或者从虚拟机监控程序或云UI访问控制台

2.在CLI上运行show firewall命令：

<#root>

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：

<#root>

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

FCM UI

按照FCM UI部分中的步骤进行操作。

FXOS CLI

按照FXOS CLI部分中的步骤进行操作。

FXOS REST API

按照FXOS REST API部分中的步骤进行操作。

机箱show-tech文件

按照机箱show-tech文件部分中的步骤进行操作。

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），因此您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。只有FMC管理的FTD支持多实例功能；ASA或FDM管理的FTD不支持此功能。

只有Firepower 4100/9300或安全防火墙3100/4200上的FTD才支持容器模式实例配置。安全防火墙3100/4200机箱本身可以在本地或容器模式下运行。

可以使用以下选项验证实例部署类型：

- FTD CLI
- FTD Show-tech
- FMC用户界面
- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- 机箱显示技术文件

FTD CLI

按照以下步骤验证FTD CLI上的FTD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:

- 通过SSH直接访问FTD — 所有平台
- 在Firepower 4100/9300上，使用FXOS CLI通过命令访问FTD:

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。

- 在Secure Firewall 3100/4200上，通过connect ftd [instance] 命令从FXOS CLI进行访问，其中实例仅与多实例部署相关。

2. 运行show version system命令。如果出现以下任何情况，则FTD在容器模式下运行：

- 包含字符串SSP Slot Number的行包含"Container"。
- 对于Secure Firewall 3100/4200，如果线路Container Disk:40 GB存在。

```
<#root>

>

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)
```

…

<#root>

>

show version system

```
------------------[ firepower ]---------------------
Model : Cisco Secure Firewall 3140 Threat Defense (80) Version 7.6.1 (Build 291)
UUID : 4ab1bbba-674d-11f0-90a8-fe60a1ff824b
LSP version : lsp-rel-20241211-1948
VDB version : 408
-----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.22(1)21
SSP Operating System Version 2.16(0.3007)

Compiled on Thu 29-May-25 01:38 GMT by fpbesprd
System image file is "disk0:/installables/switch/fxos-k8-fp3k-lfbff.2.16.0.3007.SPA"
Config file at boot was "startup-config"

firepower up 11 days 18 hours
Start-up time 7 secs

Hardware: FPR-3140, 36831 MB RAM, CPU Ryzen Zen 2 2345 MHz, 1 CPU (10 cores)
```

Container Disk: 40 GB

```
...
```

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到文件夹<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:

<#root>

 # 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 Slot Number检查该行。如果符合以下任何条件，则FTD在容器模式下运行：

- 包含字符串SSP Slot Number的行包含"Container"。
- 对于Secure Firewall 3100/4200，如果线路Container Disk:40 GB存在。

<#root>

```
-------------------[ 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)

…
```

<#root>

```
>

show version system


-------------------[ firepower ]--------------------
Model : Cisco Secure Firewall 3140 Threat Defense (80) Version 7.6.1 (Build 291)
UUID : 4ab1bbba-674d-11f0-90a8-fe60a1ff824b
LSP version : lsp-rel-20241211-1948
VDB version : 408
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.22(1)21
SSP Operating System Version 2.16(0.3007)

Compiled on Thu 29-May-25 01:38 GMT by fpbesprd
System image file is "disk0:/installables/switch/fxos-k8-fp3k-lfbff.2.16.0.3007.SPA"
Config file at boot was "startup-config"

firepower up 11 days 18 hours
Start-up time 7 secs

Hardware: FPR-3140, 36831 MB RAM, CPU Ryzen Zen 2 2345 MHz, 1 CPU (10 cores)

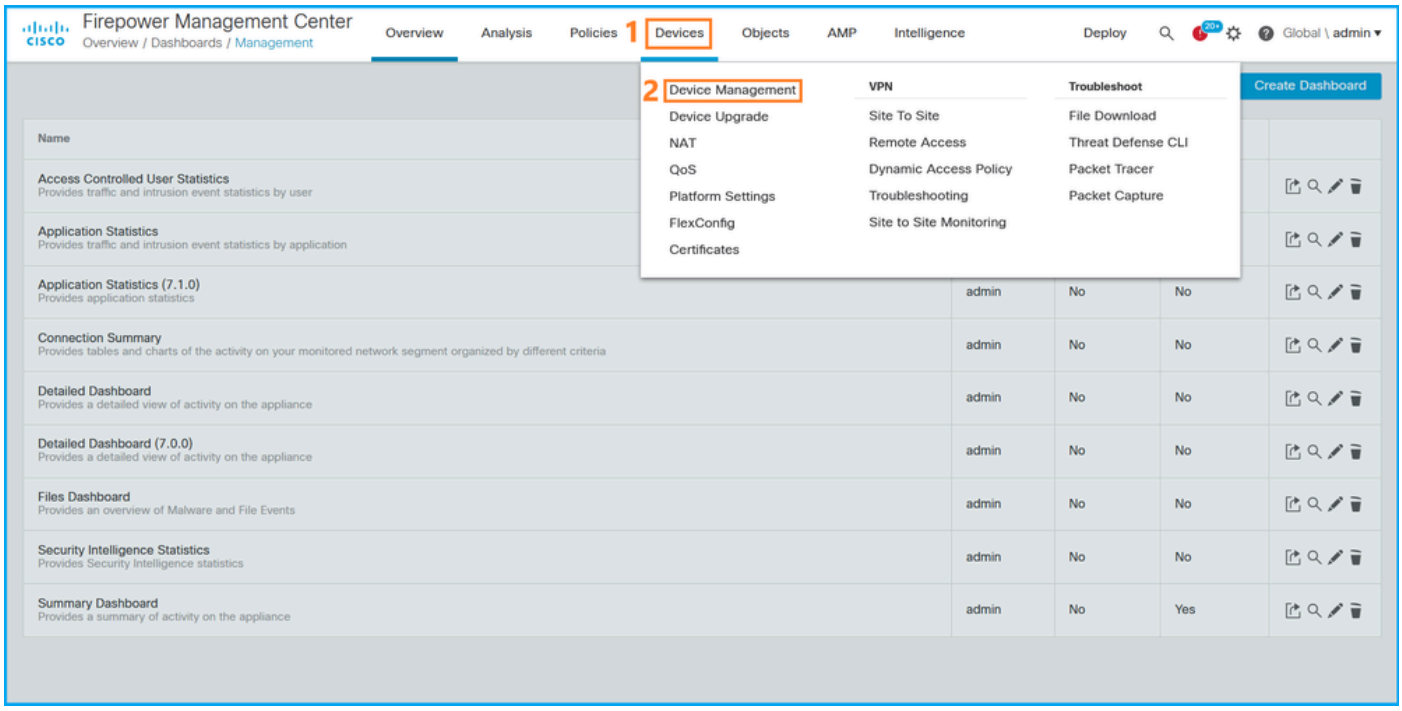
Container Disk: 40 GB


...
```

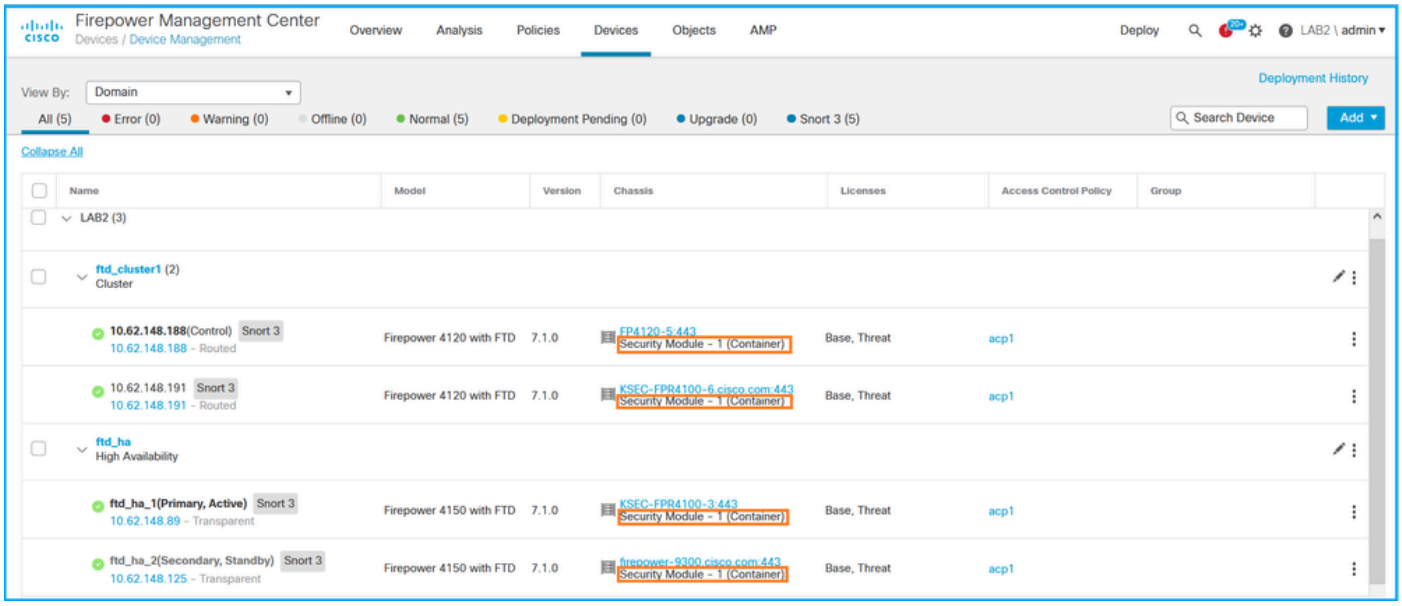
FMC用户界面

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. 选中Chassis列。如果容器存在于行中，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。在本示例中，使用curl:

1. 请求身份验证令牌：

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: B
```

```
< X-auth-access-token:
```

```
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb
```

2.标识包含设备的域。在大多数REST API查询中，domain参数是必需的。使用此查询中的令牌检索域列表：

<#root>

```
#
```

```
curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
   "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:

<#root>

```
#
```

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

```
{
    "items": [
        {

"id": "796eb8f8-d83b-11ec-941d-b9083eb612d8"

,
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-00000000000
            },

"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:

<#root>

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


"name": "ftd_cluster1"

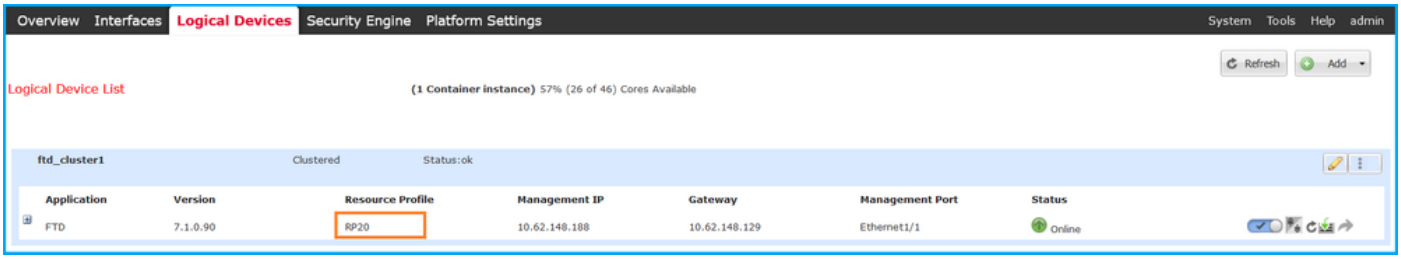
,

     "isMultiInstance": true,

...
```

FCM UI

要验证FTD实例部署类型，请检查Logical Devices中Resource Profile属性的值。如果值不为空，则FTD在容器模式下运行：



FXOS CLI

按照以下步骤验证FXOS CLI上的FTD实例部署类型：

1. 建立到机箱的控制台或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：

```
<#root>

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
```

3.对于安全防火墙3100/4200，整个机箱在本地或容器模式下运行。检查show system命令的输出以验证：

```
<#root>

firepower-3140#

show system


Systems:
    Name       Mode

Deploy Mode

 System IP Address System IPv6 Address
    ---------- ----------- ----------- ----------------- -------------------
    firepower-3140
               Stand Alone

Container

 192.0.2.1      ::
```

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。在本示例中，使用curl:

1. 请求身份验证令牌：

<#root>

```
# curl -k -X POST -H 'USERNAME: admin' -H 'PASSWORD: Cisco123'  'https://10.62.148.88/api/login'

{
    "refreshPeriod": "0",
    "token": "

3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d

"
}
```

2.在此查询中指定令牌、插槽ID，并检查deployType的值：

<#root>

```
#

curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453c


…
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_JAD20120OR43VLP1G3",
            "appName": "ftd",
            "clearLogData": "available",
            "clusterOperationalState": "not-applicable",
            "clusterRole": "none",
            "currentJobProgress": "100",
            "currentJobState": "succeeded",
            "currentJobType": "start",

            "deployType": "container",
...
```

机箱show-tech文件

在Firepower 4100/9300上，按照以下步骤验证机箱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，请打开<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar中的sam_techsupportinfo文件

对于早期版本，请在FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar中打开文件sam_techsupportinfo。

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

<#root>

```
# 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
```

在安全防火墙3100/4200上，检查文件tech_support_brief中的scope system部分以验证机箱部署模式：

<#root>

```
`scope system`
```

`show detail`

```
Systems:
    Name: firepower-3140
    Mode: Stand Alone
    System IP Address: 192.0.2.1
    System IPv6 Address: ::
    System Owner:
    System Site:

Deploy Mode: Container

    Description for System
```

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上下文类型：

- ASA CLI
- ASA show-tech

ASA CLI

按照以下步骤验证ASA CLI上的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:

- 在设备模式下直接通过telnet/SSH访问Firepower 1000/3100/4200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
- 从FXOS CLI通过命令(Firepower 4100/9300)访问：

  connect module <x> [console|telnet]，其中x是插槽ID，然后连接asa

- 对于虚拟ASA，直接通过SSH访问ASA，或者从虚拟机监控程序或云UI访问控制台

2.在CLI上运行show mode命令：

```
<#root>

ASA#

show mode

Security context mode:

multiple
```

```
ASA#
show mode

Security context mode:
single
```

ASA show-tech文件

按照以下步骤验证ASA show-tech文件中的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，情景模式是多情景模式，因为存在多个情景：

```
<#root>
------------------ 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中运行：

- 平台模式 — 在FXOS中配置基本操作参数和硬件接口设置。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） — 设备模式允许用户配置ASA中的所有策略。FXOS CLI仅提供高级命令。

使用以下选项可以验证具有ASA的Firepower 2100模式：

- ASA CLI
- FXOS CLI
- 机箱显示技术文件

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：

```
<#root>

ciscoasa(config)#

show fxos mode


Mode is currently set to plaftorm
```

设备模式：

```
<#root>

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admin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：

```
<#root>

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：

```
<#root>

firepower-2140#

show fxos mode


Mode is currently set to plaftorm
```

设备模式：

```
<#root>

firepower-2140#

show fxos mode
Mode is currently set to appliance
```

机箱show-tech文件

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

1.打开<name>_FPRM.tar.gz/<name>_FPRM.tar中的tech_support_brief文件

2.检查“show fxos-mode”部分：

<#root>

```
# pwd

/var/tmp/fp2k-1_FPRM/

# cat tech_support_brief
...

`show fxos-mode`

Mode is currently set to platform
```

设备模式：

<#root>

```
# pwd

/var/tmp/fp2k-1_FPRM/

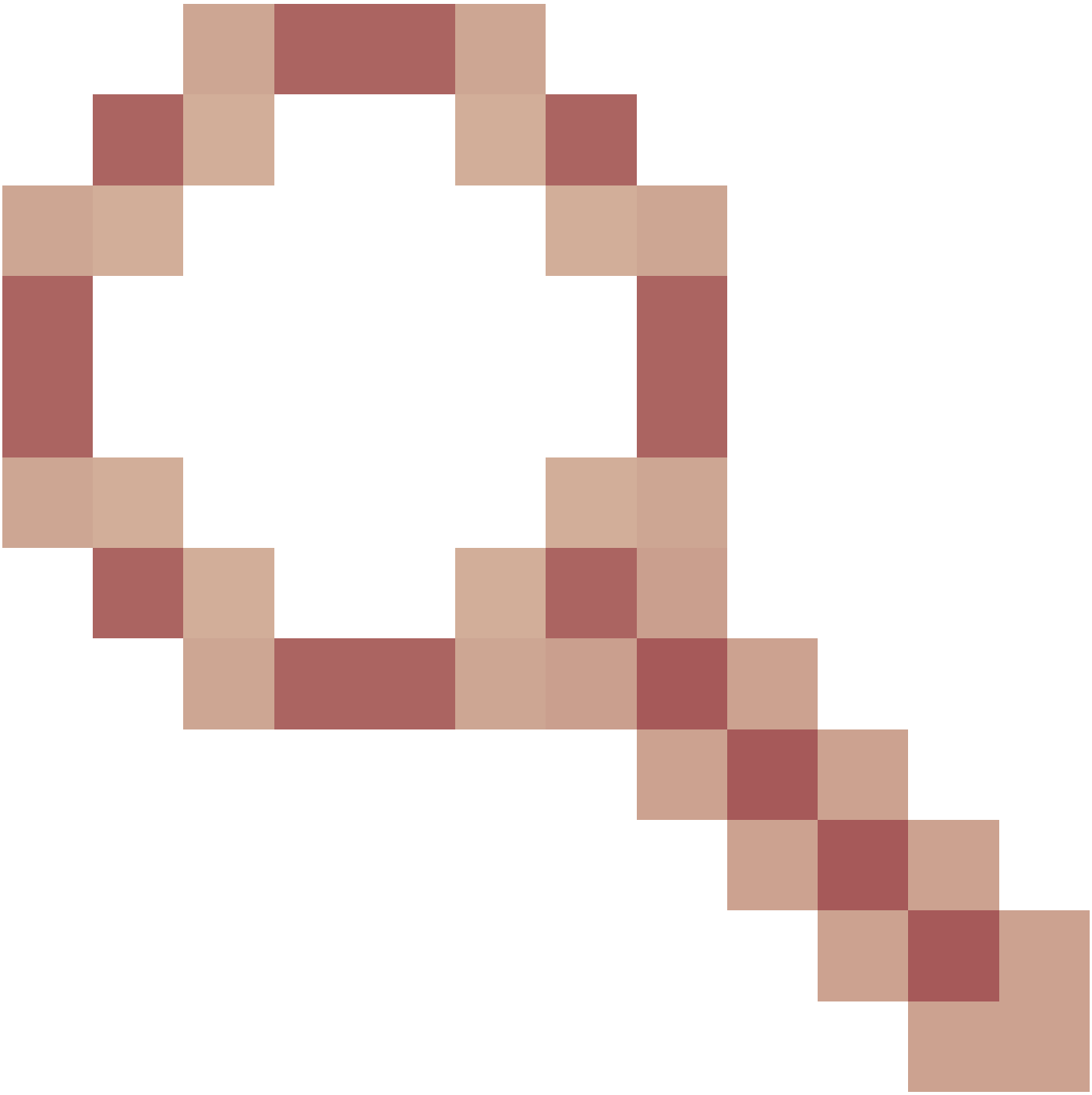
# cat tech_support_brief
...

`show fxos-mode`

Mode is currently set to appliance
```

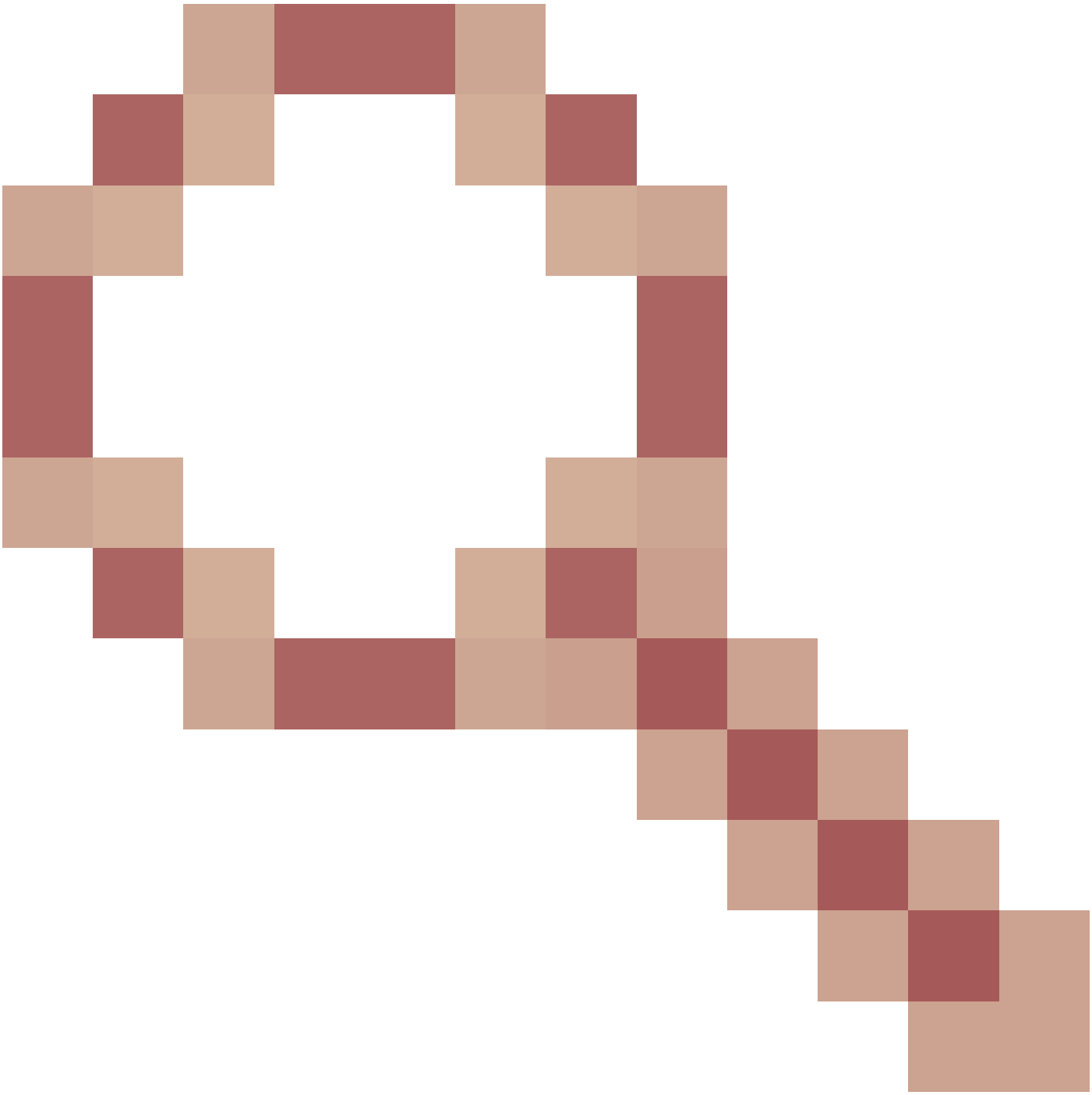
已知问题

Cisco Bug ID CSCwb94424



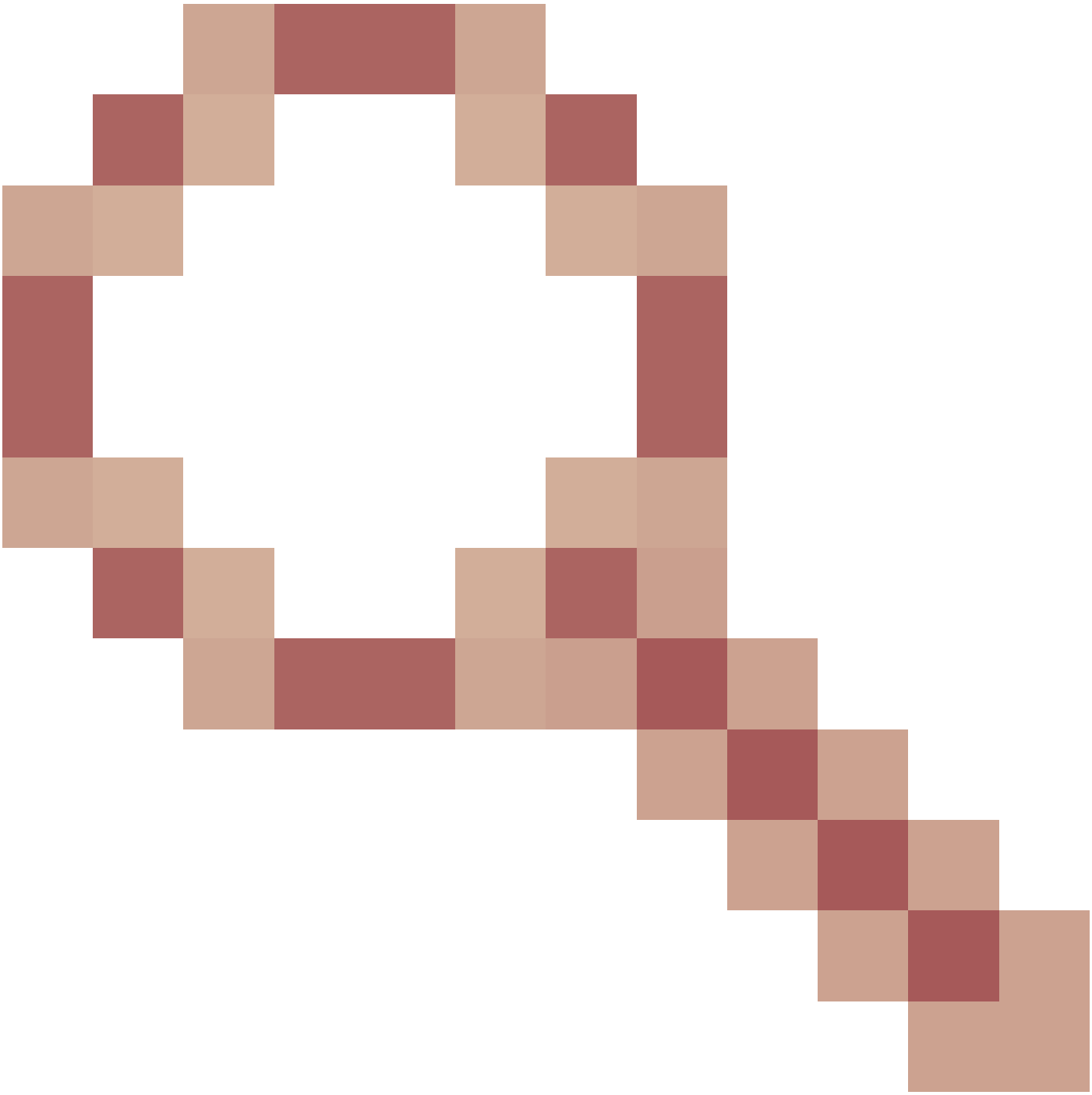
增强版：添加用于FMC HA配置验证的CLISH命令

Cisco Bug ID CSCvn31622



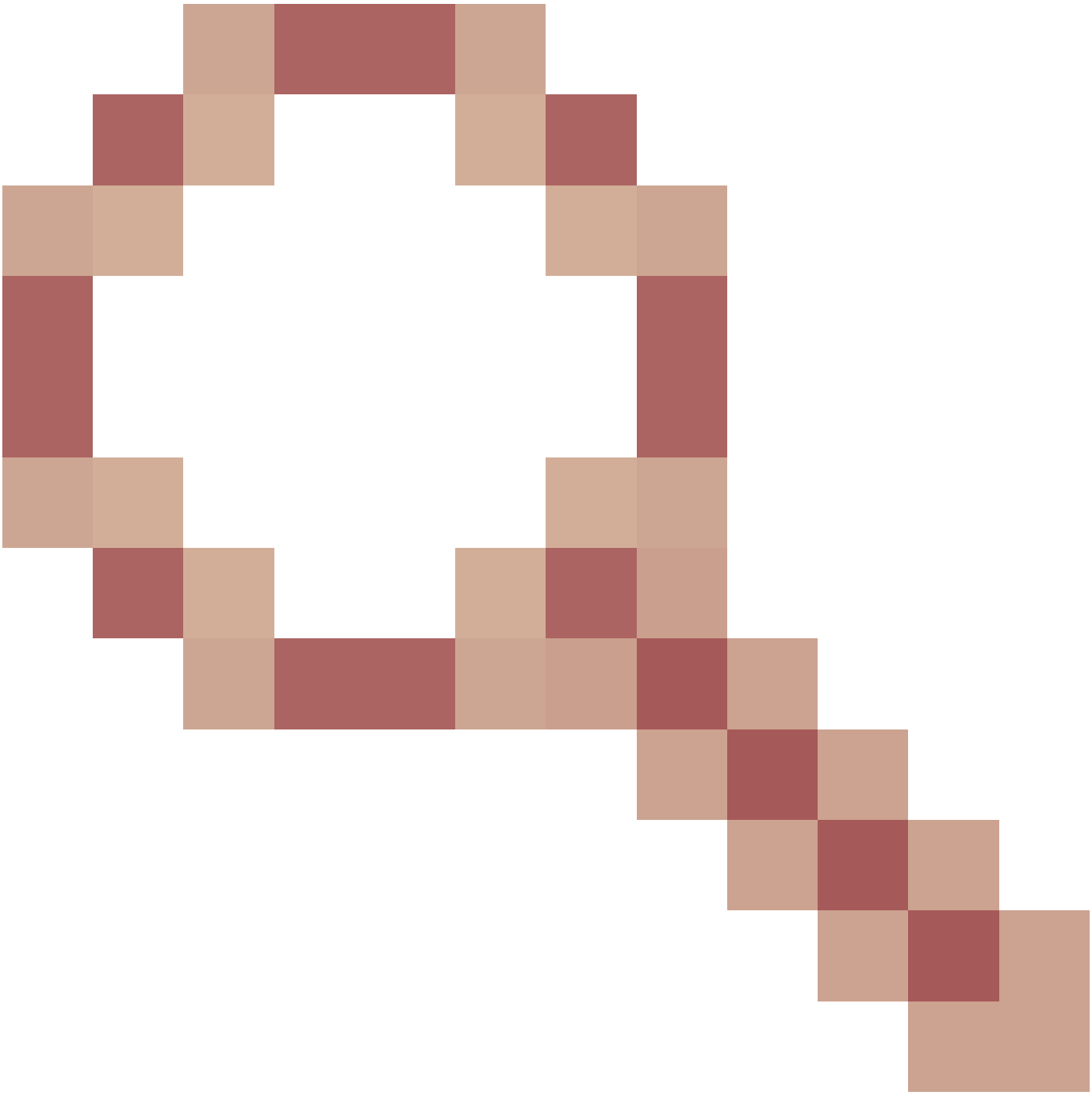
增强版：添加FXOS SNMP OID以轮询逻辑设备和应用实例配置

Cisco Bug ID CSCwb97767



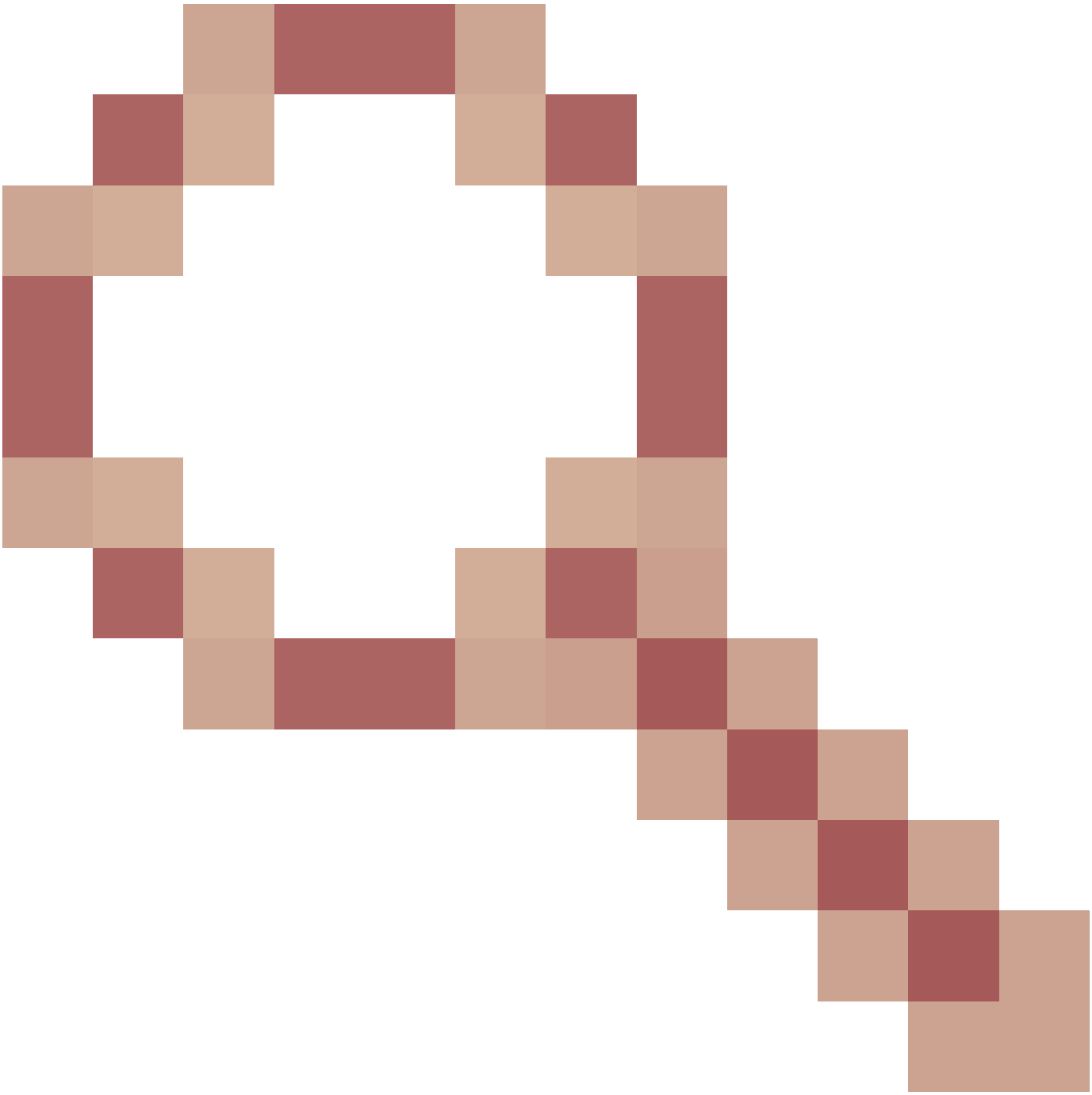
增强版：添加OID以验证FTD实例部署类型

Cisco Bug ID CSCwb97772



增强版：在Firepower 2100上ASA的show-tech中包括“show fxos mode”的输出

Cisco Bug ID CSCwb97751



OID 1.3.6.1.4.1.9.9.491.1.6.1.1不可用于透明防火墙模式验证

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
- Cisco FXOS REST API参考
- Cisco 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故障排除文件生成过程
- Cisco Firepower 2100入门指南

- 思科Firepower威胁防御兼容性指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。