

Verificar a configuração do modo, instância, alta disponibilidade e escalabilidade do Firepower

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Verificar a configuração de alta disponibilidade e escalabilidade](#)

[Alta disponibilidade do FMC](#)

[IU do FMC](#)

[CLI FMC](#)

[FMC REST-API](#)

[Arquivo de solução de problemas do FMC](#)

[Alta Disponibilidade do FDM](#)

[IU do FDM](#)

[API REST do FDM](#)

[CLI de FTD](#)

[Pesquisa SNMP FTD](#)

[Arquivo de Solução de Problemas do FTD](#)

[Alta disponibilidade e escalabilidade de FTD](#)

[CLI de FTD](#)

[SNMP FTD](#)

[Arquivo de Solução de Problemas do FTD](#)

[IU do FMC](#)

[API REST FMC](#)

[IU do FDM](#)

[API REST do FDM](#)

[IU do FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Arquivo show-tech do chassi FXOS](#)

[Alta disponibilidade e escalabilidade do ASA](#)

[CLI do ASA](#)

[SNMP ASA](#)

[Arquivo de show-tech do ASA](#)

[IU do FCM](#)

[CLI FXOS](#)

[FXOS REST-API](#)

[Arquivo show-tech do chassi FXOS](#)

[Verificar o modo Firewall](#)

[Modo de Firewall FTD](#)

[CLI de FTD](#)

[Arquivo de Solução de Problemas do FTD](#)

[IU do FMC](#)

[FMC REST-API](#)

[IU do FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Arquivo show-tech do chassi FXOS](#)

[Modo de firewall ASA](#)

[CLI do ASA](#)

[Arquivo de show-tech do ASA](#)

[IU do FCM](#)

[CLI FXOS](#)

[FXOS REST-API](#)

[Arquivo show-tech do chassi FXOS](#)

[Verificar tipo de Implantação de Instância](#)

[CLI de FTD](#)

[Arquivo de Solução de Problemas do FTD](#)

[IU do FMC](#)

[FMC REST-API](#)

[IU do FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Arquivo show-tech do chassi FXOS](#)

[Verificar o modo de contexto do ASA](#)

[CLI do ASA](#)

[Arquivo de show-tech do ASA](#)

[Verificar o modo do Firepower 2100 com ASA](#)

[CLI do ASA](#)

[CLI FXOS](#)

[arquivo show-tech FXOS](#)

[Problemas conhecidos](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a verificação da configuração de alta disponibilidade e escalabilidade do Firepower, o modo do firewall e o tipo de implantação da instância.

Informações de Apoio

As etapas de verificação para a configuração de alta disponibilidade e escalabilidade, o modo de firewall e o tipo de implantação da instância são mostrados na interface do usuário (UI), na interface de linha de comando (CLI), através de consultas REST-API, SNMP e no arquivo de solução de problemas.

Pré-requisitos

Requisitos

Conhecimento básico do produto, REST-API, SNMP

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) versão 7.1.x
- Sistema operacional extensível Firepower (FXOS) 2.11.1.x
- Firepower Device Manager (FDM) 7.1.x
- Defesa contra ameaças do Firepower 7.1.x
- ASA 9.17.x

Verificar a configuração de alta disponibilidade e escalabilidade

Alta disponibilidade refere-se à configuração de failover. A configuração de alta disponibilidade ou failover une dois dispositivos para que, se um deles falhar, o outro possa assumir o controle.

Escalabilidade refere-se à configuração do cluster. Uma configuração de cluster permite agrupar vários nós FTD como um único dispositivo lógico. Um cluster oferece toda a conveniência de um único dispositivo (gerenciamento, integração em uma rede) e o maior throughput e redundância de vários dispositivos.

Neste documento, essas expressões são usadas de forma intercambiável:

- alta disponibilidade ou failover
- escalabilidade ou cluster

Em alguns casos, a verificação de configuração ou status de alta disponibilidade e escalabilidade não está disponível. Por exemplo, não há nenhum comando de verificação para a configuração autônoma do FTD. Os modos de configuração autônomo, de failover e de cluster são mutuamente exclusivos. Se um dispositivo não tiver failover e configuração de cluster, ele será considerado como operando no modo autônomo.

Alta disponibilidade do FMC

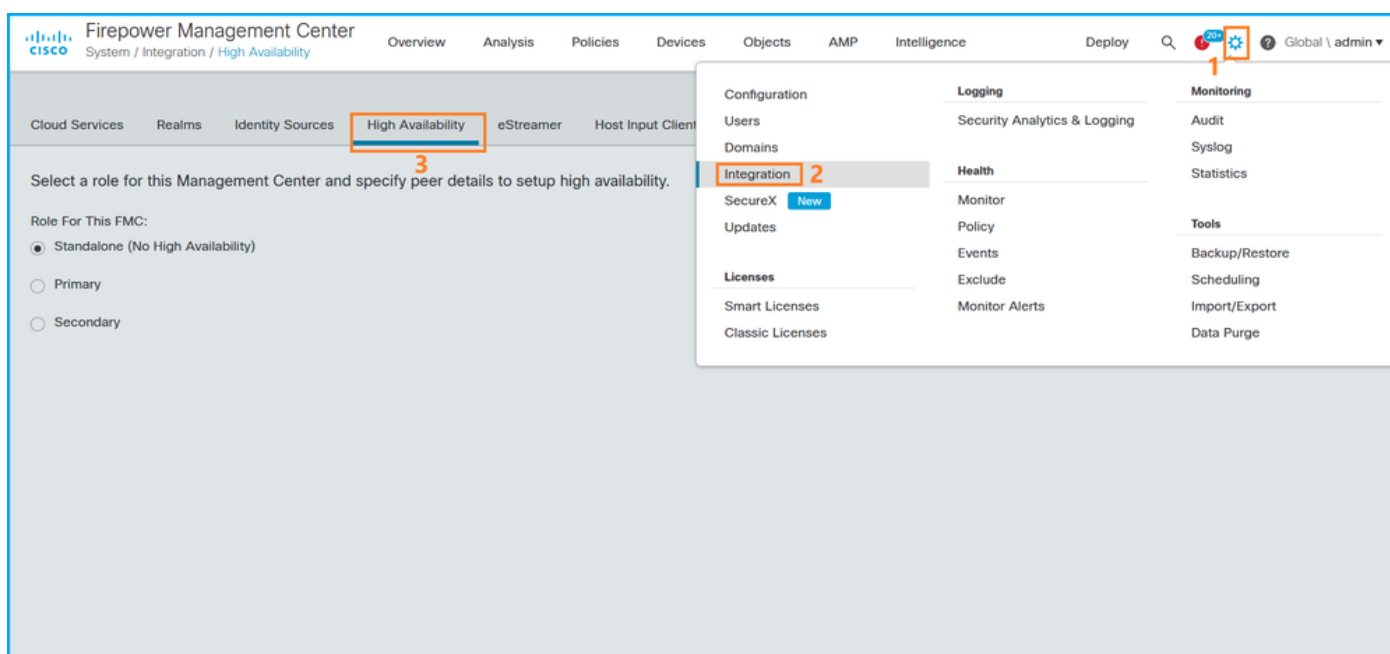
A configuração e o estado de alta disponibilidade dos FMC podem ser verificados com recurso às seguintes opções:

- IU do FMC
- CLI FMC
- Solicitação de API REST
- arquivo de solução de problemas do FMC

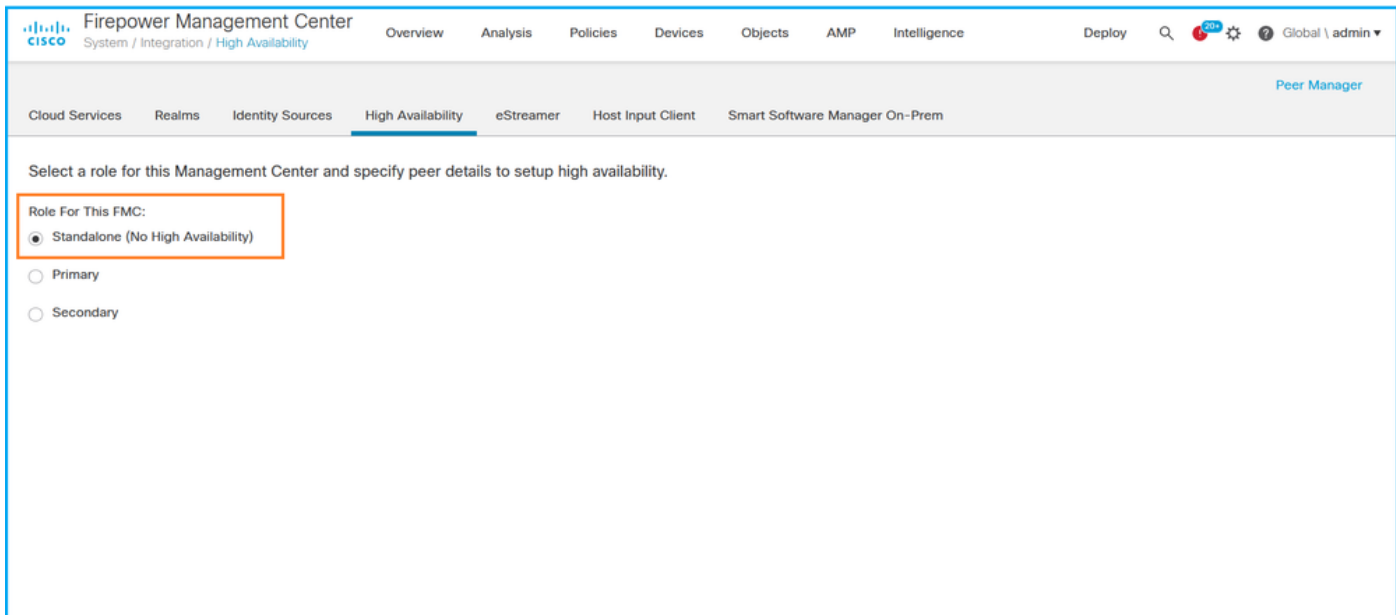
IU do FMC

Siga estas etapas para verificar a configuração e o status de alta disponibilidade do FMC na interface do usuário do FMC:

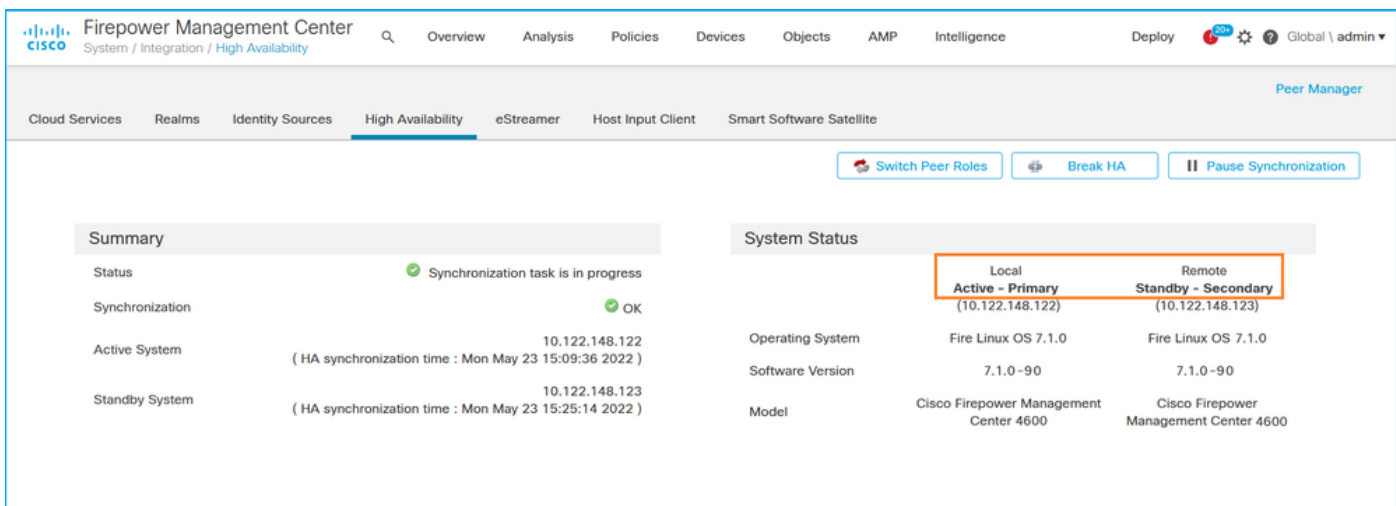
1. Escolha Sistema > Integração > Alta Disponibilidade:



2. Verificar o papel do CVP. Nesse caso, a alta disponibilidade não é configurada e o FMC opera em uma configuração autônoma:



Se a alta disponibilidade estiver configurada, as funções locais e remotas serão mostradas:



CLI FMC

Siga estas etapas para verificar a configuração e o status de alta disponibilidade do FMC na CLI do FMC:

1. Acesse o FMC via SSH ou conexão de console.
2. Execute o comando expert e depois execute o comando sudo su:

```
<#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. Execute o comando `troubleshoot_HADC.pl` e selecione a opção 1 Show HA Info Of FMC. Se a alta disponibilidade não estiver configurada, esta saída será mostrada:

<#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

Se a alta disponibilidade estiver configurada, esta saída será mostrada:

<#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
```



Observação: em uma configuração de alta disponibilidade, a função FMC pode ter um status primário ou secundário e ativo ou standby.

FMC REST-API

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FMC através da REST-API. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicite um token de autenticação:

```
<#root>
```

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

```
...
```

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

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

2. Use o token nesta consulta para localizar o UUID do domínio global:

```
<#root>
```

```
# 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'
```

```
{  "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
}
}

```

 Nota: A parte "| python -m json.tool" do comando é usado para formatar a saída no estilo JSON e é opcional.

3. Use o UUID de domínio global nesta consulta:

<#root>

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

Se a alta disponibilidade não estiver configurada, esta saída será mostrada:

```

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

```


Se a alta disponibilidade estiver configurada, esta saída será mostrada:

```
<#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
  }
}
```

Arquivo de solução de problemas do FMC

Siga estas etapas para verificar a configuração e o status de alta disponibilidade do FMC no arquivo de solução de problemas do FMC:

1. Abra o arquivo de solução de problemas e navegue até a pasta <filename>.tar/results-
<date>—xxxxxx/command-outputs

2. Abra o arquivo usr-local-sf-bin-troubleshoot_HADC.pl -a.output:

Se a alta disponibilidade não estiver configurada, esta saída será mostrada:

```
<#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'  
    }  
];  
(system,gui) - Waiting
```

```
HA Enabled: No
```

```
Sybase Database Name: csmEng  
Arbiter Not Running On This FMC.
```

```
Not In HA
```

Se a alta disponibilidade estiver configurada, esta saída será mostrada:

```
<#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

Alta Disponibilidade do FDM

A configuração e o status de alta disponibilidade do FDM podem ser verificados com o uso destas opções:

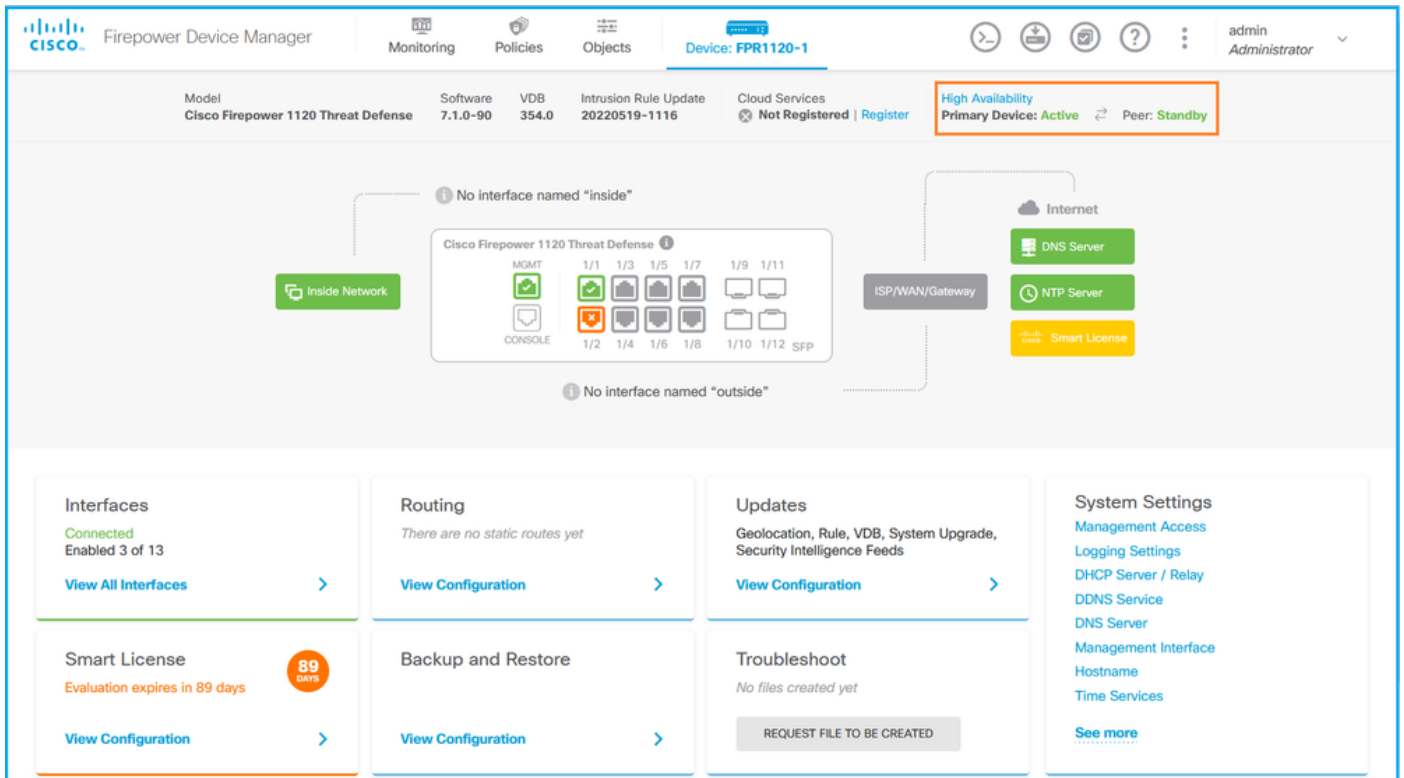
- IU do FDM
- Solicitação de API REST do FDM
- CLI de FTD

- Pesquisa SNMP FTD
- arquivo de solução de problemas do FTD

IU do FDM

Para verificar a configuração e o status de alta disponibilidade do FDM na interface do usuário do FDM, marque Alta Disponibilidade na página principal. Se a alta disponibilidade não estiver configurada, o valor de Alta Disponibilidade será Não Configurado:

Se a alta disponibilidade estiver configurada, a configuração e as funções de failover da unidade peer local e remoto serão mostradas:



API REST do FDM

Siga estas etapas para verificar a configuração e o status de alta disponibilidade do FDM por meio da solicitação REST-API do FDM. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicite um token de autenticação:

```
<#root>
```

```
#
```

```
curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ "grant_type": "password", "username": "admin", "password": "admin", "expires_in": 1800, "refresh_expires_in": 2400, "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlZ2NTMyMDg1MjgsInN1YiI6ImFkbWl1IiwianRpIjoiaWY1YWRhZWMtZDlhYS0xMWVjLWE5MmM1IiwiaWF0IjoiMTY1MjM0MjM0IiwiaXNja3kiOiJ1b250b28uYXNja3kiLCJ0eXBlIjoiYm9hcmRlciJ9", "token_type": "Bearer" }
```

2. Para verificar a configuração de alta disponibilidade, use o valor do token de acesso nesta

Se a alta disponibilidade estiver configurada, esta saída será mostrada:

```
<#root>
{
  "items": [
    {
      "version": "issgb3rw2lix",
      "name": "HA",
      "nodeRole": "HA_PRIMARY",
      "failoverInterface": {
        "version": "ezzafxo5ccti3",
        "name": "",
        "hardwareName": "Ethernet1/1",
        "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
        "type": "physicalinterface"
      },
      ...
    }
  ]
}
```

3. Para verificar o status de alta disponibilidade, use esta consulta:

```
<#root>
#
curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJ1bnkifQ.eyJpYXQiOiJ1bnkifQ'
```

Se a alta disponibilidade não estiver configurada, esta saída será mostrada:

```
<#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"
  }
}
```

Se a alta disponibilidade estiver configurada, esta saída será mostrada:

```
<#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"
  }
}
```

CLI de FTD

Siga as etapas na seção.

Pesquisa SNMP FTD

Siga as etapas na seção.

Arquivo de Solução de Problemas do FTD

Siga as etapas na seção.

Alta disponibilidade e escalabilidade de FTD

A configuração e o status de alta disponibilidade e escalabilidade do FTD podem ser verificados

com o uso destas opções:

- CLI de FTD
- SNMP FTD
- arquivo de solução de problemas do FTD
- IU do FMC
- FMC REST-API
- IU do FDM
- API REST do FDM
- IU do FCM
- CLI FXOS
- FXOS REST-API
- Arquivo show-tech do chassi FXOS

CLI de FTD

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FTD na CLI do FTD:

1. Use estas opções para acessar a CLI do FTD de acordo com a plataforma e o modo de implantação:

- Acesso SSH direto ao FTD - todas as plataformas
- Acesso a partir da CLI do console FXOS (Firepower 1000/2100/3100) por meio do comando `connect ftd`
- Acesso a partir da CLI FXOS por meio de comandos (Firepower 4100/9300):

conecte o módulo <x> [console|telnet], onde x é o slot ID, e conecte ftd [instância], onde a instância é relevante apenas para a implantação de várias instâncias

- Para FTDs virtuais, acesso SSH direto ao FTD ou acesso de console do hipervisor ou da interface de usuário da nuvem

2. Para verificar a configuração e o status de failover do FTD, execute os comandos `show running-config failover` e `show failover state` na CLI.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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====			

Se o failover estiver configurado, esta saída será mostrada:

```

<#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. Para verificar a configuração e o status do cluster FTD, execute os comandos show running-config cluster e show cluster info na CLI.

Se o cluster não estiver configurado, esta saída será mostrada:

```

<#root>

```

```
>  
show running-config cluster
```

```
>  
show cluster info
```

```
Clustering is not configured
```

Se o cluster estiver configurado, esta saída será mostrada:

```
<#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

 Observação: as funções mestre e controle são as mesmas.

SNMP FTD

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade de FTD via SNMP:

1. Verifique se o SNMP está configurado e habilitado. Para FTD gerenciado por FDM, consulte [Configurar e solucionar problemas de SNMP no Firepower FDM](#) para obter as etapas de configuração. Para FTD gerenciado por FMC, consulte [Configurar SNMP em dispositivos NGFW Firepower](#) para obter as etapas de configuração.
2. Para verificar a configuração e o status de failover de FTD, pesquise o OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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"
```

Se o failover estiver configurado, esta saída será mostrada:

```
<#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. Para verificar a configuração e o status do cluster, pesquise o OID 1.3.6.1.4.1.9.9.491.1.8.1.

Se o cluster não estiver configurado, esta saída será mostrada:

```
<#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
```

Se o cluster estiver configurado, mas não habilitado, esta saída será mostrada:

```
<#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
...

```

Se o cluster estiver configurado, habilitado e operacionalmente ativo, esta saída será mostrada:

```

<#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
...

```

Para obter mais informações sobre as descrições do OID, consulte [CISCO-UNIFIED-FIREWALL-MIB](#).

Arquivo de Solução de Problemas do FTD

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FTD no arquivo de solução de problemas do FTD:

1. Abra o arquivo de solução de problemas e navegue até a pasta <filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs.
2. Abra o arquivo 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. Para verificar a configuração e o status de failover, consulte a seção show failover.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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
```

Se o failover estiver configurado, esta saída será mostrada:

```
<#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. Para verificar a configuração e o status do cluster de FTD, consulte a seção show cluster info.

Se o cluster não estiver configurado, esta saída será mostrada:

```
<#root>
----- show cluster info -----

Clustering is not configured
```

Se o cluster estiver configurado e habilitado, esta saída será mostrada:

```
<#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

IU do FMC

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FTD na interface do usuário do FMC:

1. Escolha Devices > Device Management:

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Devices' menu is expanded, showing 'Device Management' as the selected option. Below the navigation bar, there is a table of dashboards. The table has columns for Name, Description, and several status columns (admin, No, No, No, Yes). The 'Device Management' menu is highlighted with a red box, and the 'Device Management' option in the dropdown is also highlighted with a red box.

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

2. Para verificar a configuração de alta disponibilidade e escalabilidade do FTD, verifique os rótulos Alta Disponibilidade ou Cluster. Se nenhum existir, o FTD será executado em uma

configuração independente:

The screenshot shows the Firepower Management Center interface. The 'Devices' tab is active, displaying a list of devices under the 'LAB2' domain. The 'View By' dropdown is set to 'Domain'. The status bar shows 5 Normal devices. The table lists the following devices:

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. Para verificar o status de alta disponibilidade e escalabilidade do FTD, verifique a função da unidade entre parênteses. Se uma função não existir e o FTD não fizer parte de um cluster ou failover, o FTD será executado em uma configuração autônoma:

The screenshot shows the Firepower Management Center interface. The 'Devices' tab is active, displaying a list of devices under the 'LAB2' domain. The 'View By' dropdown is set to 'Domain'. The status bar shows 5 Snort 3 devices. The table lists the following devices:

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	

Observação: no caso de um cluster, apenas a função da unidade de controle é mostrada.

API REST FMC

Nessas saídas, ftd_ha_1, ftd_ha_2, ftd_standalone, ftd_ha, ftd_cluster1 são nomes de dispositivos

configuráveis pelo usuário. Esses nomes não se referem à configuração ou ao status de alta disponibilidade e escalabilidade reais.

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FTD por meio da API REST do FMC. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicitar um token de autenticação:

<#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. Identifique o domínio que contém o dispositivo. Na maioria das consultas da API REST, o parâmetro domain é obrigatório. Use o token nesta consulta para recuperar a lista de domínios:

<#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. Use o UUID do domínio para consultar os registros de dispositivo específicos e o UUID do

dispositivo específico:

```
<#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-4b09-000000000000/de
      },
      "name": "ftd_ha_1",
      "type": "Device"
    },
    ...
  ]
}
```

4. Para verificar a configuração de failover, use o UUID de domínio e o UUID de dispositivo/contêiner da Etapa 3 nesta consulta:

```
<#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. Para verificar o status de failover, use o UUID de domínio e o UUID DeviceHAPair da Etapa 4 nesta consulta:

```
<#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. Para verificar a configuração do cluster, use o UUID do domínio e o UUID do dispositivo/contêiner da Etapa 3 nesta consulta:

<#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-4b09-000000000000
        },

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

```

7. Para verificar o status do cluster, use o UUID do domínio e o UUID do dispositivo/contêiner da Etapa 6 nesta consulta:

```
<#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"
}
```

IU do FDM

Siga as etapas na seção.

API REST do FDM

Siga as etapas na seção.

IU do FCM

A interface do usuário do FCM está disponível no Firepower 4100/9300 e no Firepower 2100 com ASA no modo de plataforma.

Siga estas etapas para verificar o status de alta disponibilidade e escalabilidade do FTD na interface do usuário do FCM:

1. Para verificar o status de failover do FTD, verifique o valor do atributo HA-ROLE na página Dispositivos Lógicos:

The screenshot shows the 'Logical Device List' page in the Firepower GUI. The top navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The page title is 'Logical Device List' and it indicates '(1 Container Instance) 77% (66 of 86) Cores Available'. Below the title, there is a table of logical devices. The first device is 'ftd1', which is 'Standalone' and has a 'Status: ok'. The table has columns for Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. Below the table, there are sections for 'Interface Name' and 'Attributes'. The 'Attributes' section shows 'HA-ROLE' set to 'active', which is highlighted with a red box.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.1.0.90	RP20	10.62.148.89	10.62.148.1	Ethernet1/1	Online

Attributes:

- 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/
- HA-ROLE : active
- UUID : 7962688-d83b-11ec-941d-b9083eb12d8

Observação: o rótulo Standalone ao lado do identificador do dispositivo lógico se refere à configuração do dispositivo lógico do chassi, não à configuração de failover de FTD.

2. Para verificar a configuração e o status do cluster FTD, verifique o rótulo Clustered e o valor do atributo CLUSTER-ROLE na página Dispositivos lógicos:

The screenshot shows the 'Logical Device List' page in the Firepower GUI. The top navigation bar includes 'Overview', 'Interfaces', 'Logical Devices', 'Security Engine', and 'Platform Settings'. The page title is 'Logical Device List' and it indicates '(1 Container Instance) 57% (26 of 46) Cores Available'. Below the title, there is a table of logical devices. The first device is 'ftd_cluster1', which is 'Clustered' and has a 'Status: ok'. The table has columns for Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. Below the table, there are sections for 'Interface Name' and 'Attributes'. The 'Attributes' section shows 'CLUSTER-ROLE' set to 'control', which is highlighted with a red box.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.1.0.90	RP20	10.62.148.188	10.62.148.129	Ethernet1/1	Online

Attributes:

- Cluster Operational Status : in-cluster
- FIREPOWER-MGMT-IP : 10.62.148.188
- CLUSTER-ROLE : control
- CLUSTER-IP : 10.173.1.1
- MGMT-URL : https://10.62.184.21/
- UUID : 3344bc4a-d842-11ec-a995-817e3617ea5

CLI FXOS

A configuração de alta disponibilidade e escalabilidade do FTD e a verificação de status na CLI do FXOS estão disponíveis no Firepower 4100/9300.

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade do FTD na CLI do FXOS:

1. Estabeleça uma conexão de console ou SSH com o chassi.
2. Para verificar o status de alta disponibilidade do FTD, execute o comando `scope ssa` e, em seguida, execute o `scope slot <x>` para alternar para o slot específico onde o FTD é executado e execute o comando `show app-instance expand` :

<#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. Para verificar a configuração e o status do cluster de FTD, execute o comando `scope ssa`, execute o comando `show logical-device <name> detail expand`, onde o nome é o nome do dispositivo lógico e o comando `show app-instance`. Verifique a saída para um slot específico:

```
<#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

API REST FXOS

O FXOS REST-API é compatível com o Firepower 4100/9300.

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade de FTD por meio da solicitação REST-API de FXOS. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicite um token de autenticação:

<#root>

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

{
  "refreshPeriod": "0",
  "token": "
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d
"
}
```

2. Para verificar o status de failover de FTD, use o token e o ID do slot nesta consulta:

```
<#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_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": "",  
  
      "identifiier": "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": "Ethernet1/24"  
        }  
      ]  
    }  
  ]  
}
```

```

        "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-ur
        "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. Para verificar a configuração do cluster de FTD, use o identificador de dispositivo lógico nesta consulta:

```
<#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": [
  {
    "cc1Network": "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",
    "supportCc1Subnet": "supported",
    "updateTimestamp": "2022-05-20T13:38:21.872",
    "urlLink": "https://192.0.2.101/api/1d/ftd_cluster1/cluster-bootstrap",
    "virtualIPv4": "0.0.0.0",
    "virtualIPv6": "::"
  }
],
...

```

4. Para verificar o status do cluster de FTD, use esta consulta:

```
<#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_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": "",

```

```
"fsmRmtInvRs1t": "",
"fsmStageDescr": "",
"fsmStatus": "nop",
"fsmTry": "0",
"hotfix": "",

"identifier": "ftd_cluster1",

"operationalState": "online",
"reasonForDebundle": "",
"resourceProfileName": "RP20",
"runningVersion": "7.1.0.90",
...
```

Arquivo show-tech do chassi FXOS

A configuração e o status de alta disponibilidade e escalabilidade do FTD podem ser verificados no arquivo show-tech do chassi do Firepower 4100/9300.

Siga estas etapas para verificar a configuração e o status de alta disponibilidade e escalabilidade no arquivo show-tech do chassi FXOS:

1. Para as versões 2.7 e posteriores do FXOS, abra o arquivo sam_techsupportinfo em <name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Para versões anteriores, abra o arquivo sam_techsupportinfo em FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar.

2. Para verificar o status de failover, verifique o valor do atributo ha-role sob o slot específico na seção `show slot expand detail` :

```
<#root>
```

```
# pwd
```

```
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_a11/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. Para verificar a configuração do cluster de FTD, verifique o valor do atributo Mode sob o slot específico na seção `show logical-device detail expand` :

<#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. Para verificar o status do cluster FTD, verifique o valor dos valores dos atributos Cluster State e Cluster Role no slot específico da seção `show slot expand detail` :

<#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:

Alta disponibilidade e escalabilidade do ASA

A configuração e o status de alta disponibilidade e escalabilidade do ASA podem ser verificados com o uso destas opções:

- CLI do ASA
- ASA SNMP poll
- Arquivo de show-tech do ASA
- IU do FCM
- CLI FXOS
- FXOS REST-API
- Arquivo show-tech do chassi FXOS

CLI do ASA

Siga estas etapas para verificar a configuração de alta disponibilidade e escalabilidade do ASA na CLI do ASA:

1. Use estas opções para acessar a CLI do ASA de acordo com a plataforma e o modo de implantação:
 - Acesso Telnet/SSH direto ao ASA no Firepower 1000/3100 e no Firepower 2100 no modo de dispositivo
 - Acesso a partir da CLI do console FXOS no Firepower 2100 no modo de plataforma e conexão ao ASA através do comando `connect asa`.
 - Acesso a partir da CLI do FXOS através de comandos (Firepower 4100/9300):

conecte o módulo `<x>` `[console|telnet]`, onde `x` é o ID do slot, e conecte-se como
 - Para ASA virtual, acesso SSH direto ao ASA ou acesso de console a partir da interface de usuário do hipervisor ou da nuvem
2. Para verificar a configuração e o status do failover do ASA, execute os comandos `show running-config failover` e `show failover state` na CLI do ASA.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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====

Se o failover estiver configurado, esta saída será mostrada:

```
<#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
====Configuration State====
              Sync Done
====Communication State====
              Mac set
```

19:42:22 UTC May 21 2022

3. Para verificar a configuração e o status do cluster ASA, execute os comandos `show running-config cluster` e `show cluster info` na CLI.

Se o cluster não estiver configurado, esta saída será mostrada:

```
<#root>
```

```
asa#
```

```
show running-config cluster
```

```
asa#
```

```
show cluster info
```

```
Clustering is not configured
```

Se o cluster estiver configurado, esta saída será mostrada:

```
<#root>
```

```
asa#
```

```
show running-config cluster
```

```
cluster group asa_cluster1
```

```
key *****
```

```
local-unit unit-1-1
```

```
cluster-interface Port-channel148.205 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
```

...

SNMP ASA

Siga estas etapas para verificar a configuração de alta disponibilidade e escalabilidade do ASA via SNMP:

1. Verifique se o SNMP está configurado e habilitado.
2. Para verificar a configuração de failover e o poll de status do OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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"
```

Se o failover estiver configurado, esta saída será mostrada:

```
<#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. Para verificar a configuração e o status do cluster, pesquise o OID 1.3.6.1.4.1.9.9.491.1.8.1.

Se o cluster não estiver configurado, esta saída será mostrada:

```

<#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

```

Se o cluster estiver configurado, mas não habilitado, esta saída será mostrada:

```

<#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
...

```

Se o cluster estiver configurado, habilitado e operacionalmente ativo, esta saída será mostrada:

```

<#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
...

```

Para obter mais informações sobre as descrições do OID, consulte [CISCO-UNIFIED-FIREWALL-MIB](#).

Arquivo de show-tech do ASA

1. Para verificar a configuração e o status do failover do ASA, consulte a seção show failover.

Se o failover não estiver configurado, esta saída será mostrada:

```
<#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
```

Se o failover estiver configurado, esta saída será mostrada:

```
<#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. Para verificar a configuração e o status do cluster, consulte a seção show cluster info.

Se o cluster não estiver configurado, esta saída será mostrada:

```
<#root>
----- show cluster info -----

Clustering is not configured
```

Se o cluster estiver configurado e habilitado, esta saída será mostrada:

```
<#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
...

```

IU do FCM

Siga as etapas na seção.

CLI FXOS

Siga as etapas na seção.

FXOS REST-API

Siga as etapas na seção.

Arquivo show-tech do chassi FXOS

Siga as etapas na seção.

Verificar o modo Firewall

Modo de Firewall FTD

O modo de firewall refere-se a uma configuração de firewall roteada ou transparente.

O modo de firewall FTD pode ser verificado com o uso destas opções:

- CLI de FTD
- FTD show-tech
- IU do FMC
- FMC REST-API
- IU do FCM
- CLI FXOS
- FXOS REST-API
- Arquivo show-tech do chassi FXOS



Observação: o FDM não oferece suporte ao modo transparente.

CLI de FTD

Siga estas etapas para verificar o modo de firewall FTD na CLI FTD:

1. Use estas opções para acessar a CLI do FTD de acordo com a plataforma e o modo de implantação:

- Acesso SSH direto ao FTD - todas as plataformas
- Acesso a partir da CLI do console FXOS (Firepower 1000/2100/3100) por meio do comando `connect ftd`
- Acesso a partir da CLI FXOS por meio de comandos (Firepower 4100/9300):

conecte o módulo <x> [console|telnet], onde x é o ID do slot, e

`connect ftd [instância]`, onde a instância é relevante apenas para a implantação de várias instâncias.

- Para FTDs virtuais, acesso SSH direto ao FTD ou acesso de console do hipervisor ou da interface de usuário da nuvem

2. Para verificar o modo de firewall, execute o comando `show firewall` na CLI:

```
<#root>
```

```
>
```

```
show firewall
```

```
Firewall mode: Transparent
```


Arquivo de Solução de Problemas do FTD

Siga estas etapas para verificar o modo de firewall FTD no arquivo de solução de problemas de FTD:

1. Abra o arquivo de solução de problemas e navegue até a pasta <filename>-troubleshoot.tar/results-<date>—xxxxxx/command-outputs.
2. Abra o arquivo 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. Para verificar o modo de firewall FTD, verifique a seção show firewall:

```
<#root>
```

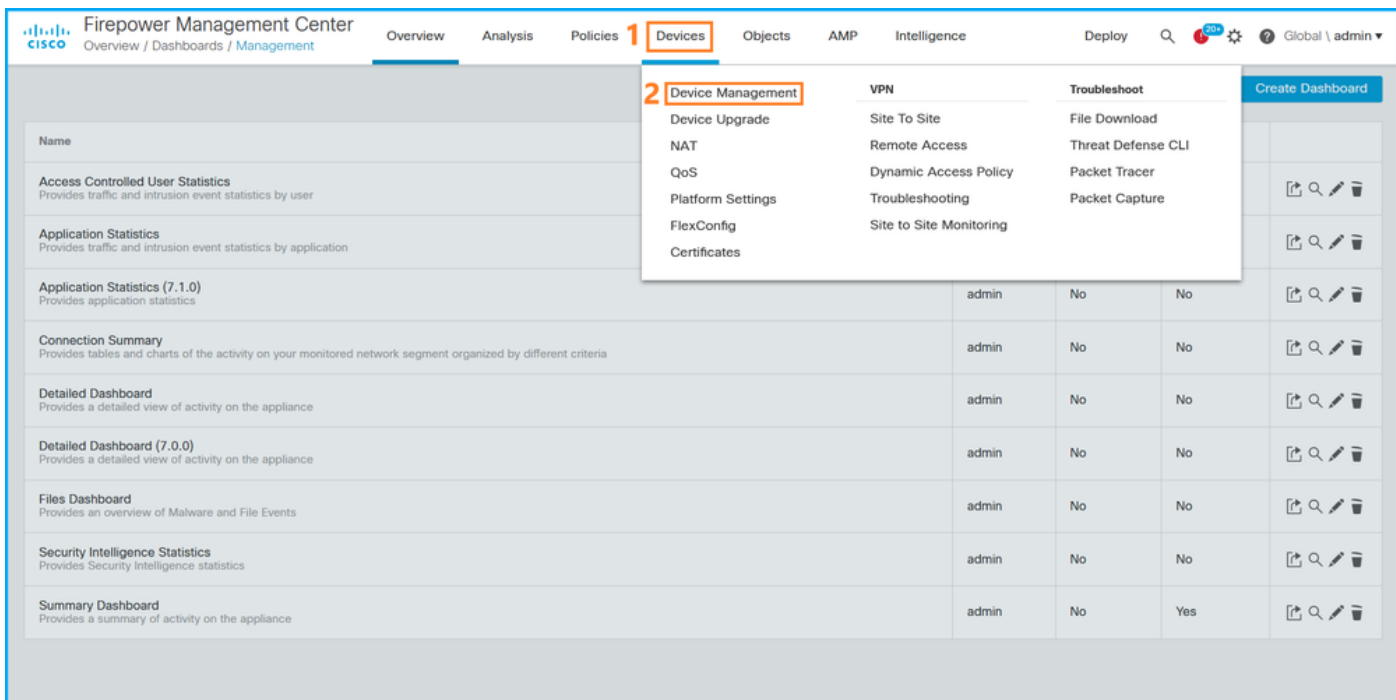
```
----- show firewall -----
```

```
Firewall mode: Transparent
```

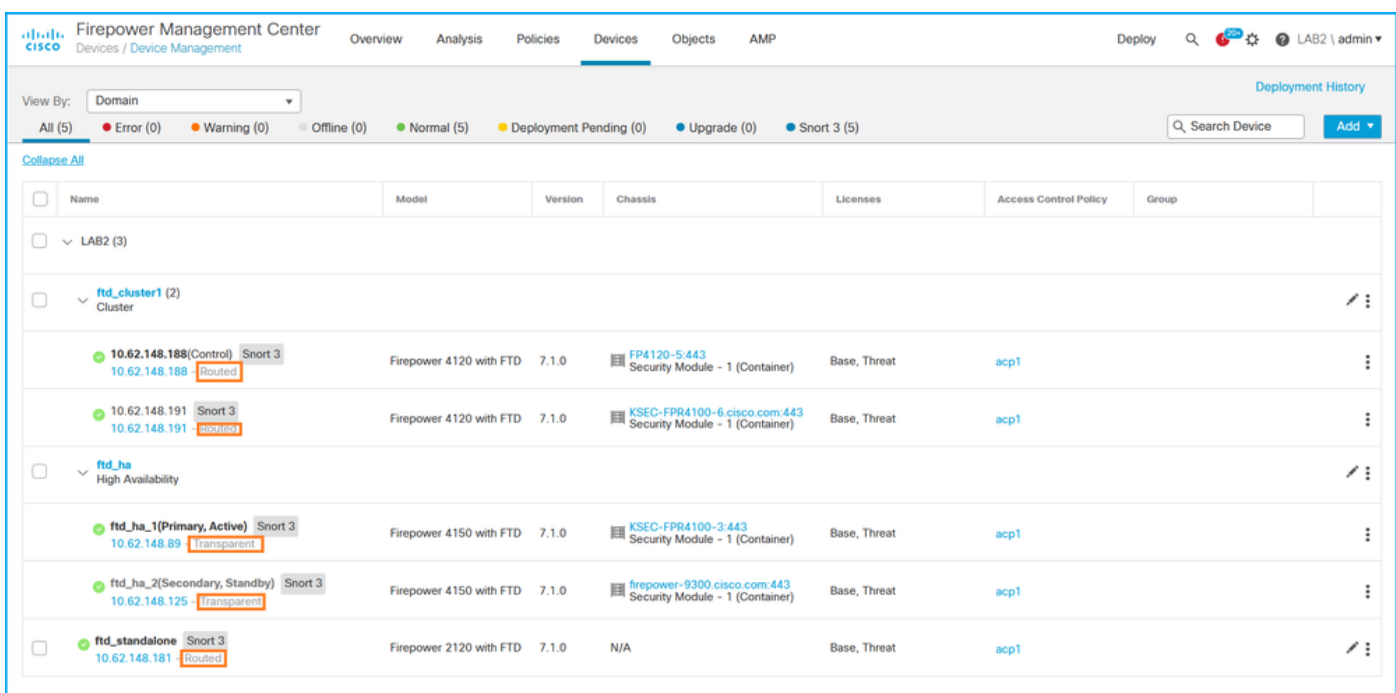
IU do FMC

Siga estas etapas para verificar o modo de firewall FTD na interface do usuário do FMC:

1. Escolha Devices > Device Management:



2. Verifique os labels Roteados ou Transparentes:



FMC REST-API

Siga estas etapas para verificar o modo de firewall FTD através do FMC REST-API. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicitar um token de autenticação:

```
<#root>
```

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

< X-auth-access-token:

5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb

2. Identifique o domínio que contém o dispositivo. Na maioria das consultas da API REST, o parâmetro domain é obrigatório. Use o token nesta consulta para recuperar a lista de domínios:

<#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. Use o UUID do domínio para consultar os registros de dispositivo específicos e o UUID do dispositivo específico:

<#root>

#

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

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

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

```

    "links": {
      "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000",
    },
    "name": "ftd_ha_1",
    "type": "Device"
  },
  ...

```

4. Use o UUID de domínio e o UUID de dispositivo/contêiner da Etapa 3 nesta consulta e verifique o valor de ftdMode:

<#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",
  ...

```

IU do FCM

O modo de firewall pode ser verificado para FTD no Firepower 4100/9300.

Siga estas etapas para verificar o modo de firewall FTD na interface do usuário do FCM:

1. Edite o dispositivo lógico na página Dispositivos Lógicos:

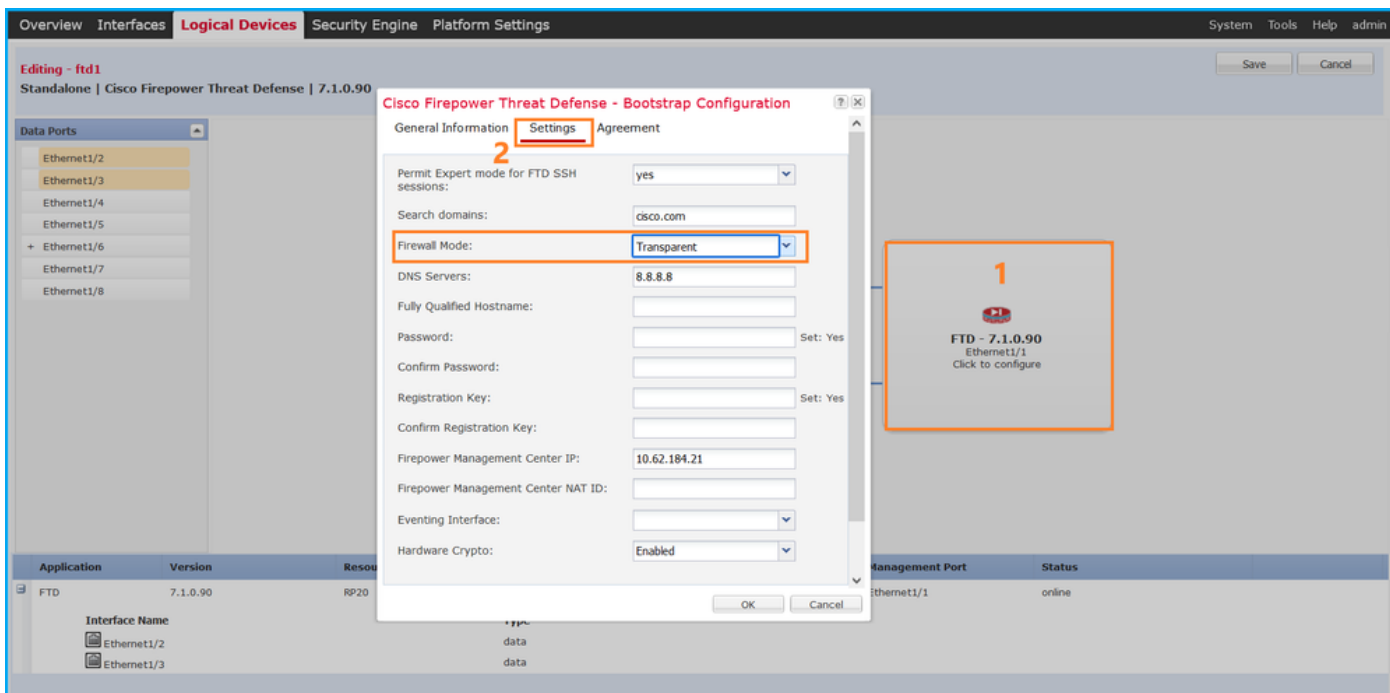
The screenshot shows the Cisco Firepower Management Center (FCM) interface. The 'Logical Devices' tab is selected, and a table of logical devices is displayed. The device 'ftd1' is highlighted, and its details are shown below the table. The details include the application 'FTD', version '7.1.0.90', resource profile 'RP20', management IP '10.62.148.89', gateway '10.62.148.1', management port 'Ethernet1/1', and status 'Online'. The interface names are listed as 'Ethernet1/2' and 'Ethernet1/3'. The attributes section shows the cluster operational status as 'not-applicable', the firepower-mgmt-ip as '10.62.148.89', the ha-link-intf as 'Ethernet1/2', the ha-lan-intf as 'Ethernet1/2', the mgmt-url as 'https://10.62.184.21/', the ha-role as 'active', and the uuid as '796eb8f8-d83b-11ec-941d-b9083eb612d8'.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.1.0.90	RP20	10.62.148.89	10.62.148.1	Ethernet1/1	Online

Attributes

- 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/
- HA-ROLE: active
- UUID: 796eb8f8-d83b-11ec-941d-b9083eb612d8

2. Clique no ícone do aplicativo e verifique o Modo de firewall na guia Configurações:



CLI FXOS

O modo de firewall pode ser verificado para FTD no Firepower 4100/9300.

Siga estas etapas para verificar o modo de firewall FTD na CLI FXOS:

1. Estabeleça uma conexão de console ou SSH com o chassi.
2. Mude para o ssa do escopo, mude para o dispositivo lógico específico, execute o comando `show mgmt-bootstrap expand` e verifique o valor do atributo `FIREWALL_MODE`:

```
<#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 Time
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
```

...

API REST FXOS

O FXOS REST-API é compatível com o Firepower 4100/9300.

Siga estas etapas para verificar o modo de firewall FTD através da solicitação REST-API FXOS. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicitar um token de autenticação:

```
<#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. Use o identificador de dispositivo lógico nesta consulta e verifique o valor da chave FIREWALL_MODE:

```
<#root>
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d' https://192.0.2.100/api/ld/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/"

"value": "routed"

...
},
...

```

Arquivo show-tech do chassi FXOS

O modo de firewall para FTD pode ser verificado no arquivo show-tech do Firepower 4100/9300.

Siga estas etapas para verificar o modo de firewall FTD no arquivo show-tech do chassi FXOS:

1. Para as versões 2.7 e posteriores do FXOS, abra o arquivo sam_techsupportinfo em <name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Para versões anteriores, abra o arquivo sam_techsupportinfo em FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Verifique a seção `show logical-device detail expand` sob o identificador específico e o slot:

```
<#root>
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_a11/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

...

Modo de firewall ASA

O modo de firewall ASA pode ser verificado com o uso destas opções:

- CLI do ASA
- ASA show-tech
- IU do FCM
- CLI FXOS
- FXOS REST-API
- Arquivo show-tech do chassi FXOS

CLI do ASA

Siga estas etapas para verificar o modo de firewall do ASA na CLI do ASA:

1. Use estas opções para acessar a CLI do ASA de acordo com a plataforma e o modo de implantação:

- Acesso Telnet/SSH direto ao ASA no Firepower 1000/3100 e no Firepower 2100 no modo de dispositivo
- Acesso a partir da CLI do console FXOS no Firepower 2100 no modo de plataforma e conexão ao ASA através do comando `connect asa`.
- Acesso a partir da CLI do FXOS através de comandos (Firepower 4100/9300):

conecte o módulo <x> [console|telnet], onde x é o ID do slot, e conecte-se como

- Para ASA virtual, acesso SSH direto ao ASA ou acesso de console a partir da interface de usuário do hipervisor ou da nuvem

2. Execute o comando `show firewall` na CLI:

```
<#root>
```

```
asa#
```

```
show firewall
```

```
Firewall mode: Routed
```


Arquivo de show-tech do ASA

Para verificar o modo de firewall ASA, verifique a seção show firewall:

```
<#root>
```

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

IU do FCM

Siga as etapas na seção.

CLI FXOS

Siga as etapas na seção.

FXOS REST-API

Siga as etapas na seção.

Arquivo show-tech do chassi FXOS

Siga as etapas na seção.

Verificar tipo de Implantação de Instância

Há dois tipos de implantação de instância de aplicativo:

- Instância nativa - Uma instância nativa usa todos os recursos (CPU, RAM e espaço em disco) do módulo/mecanismo de segurança, de modo que você pode instalar apenas uma instância nativa.
- Instância do contêiner - Uma instância do contêiner usa um subconjunto de recursos do módulo/mecanismo de segurança. O recurso de várias instâncias só é suportado para o FTD gerenciado pelo FMC; não é suportado para o ASA ou o FTD gerenciado pelo FDM.

A configuração da instância do modo de contêiner é suportada apenas para FTD no Firepower 4100/9300.

O tipo de implantação da instância pode ser verificado com o uso destas opções:

- CLI de FTD
- FTD Show-tech
- IU do FMC

- FMC REST-API
- IU do FCM
- CLI FXOS
- FXOS REST-API
- Arquivo show-tech do chassi FXOS

CLI de FTD

Siga estas etapas para verificar o tipo de implantação da instância de FTD na CLI de FTD:

1. Use estas opções para acessar a CLI do FTD de acordo com a plataforma e o modo de implantação:

- Acesso SSH direto ao FTD - todas as plataformas
- Acesso a partir da CLI FXOS por meio de comandos (Firepower 4100/9300):

conecte o módulo <x> [console|telnet], onde x é o slot ID, e conecte ftd [instância], onde a instância é relevante apenas para a implantação de várias instâncias.

2. Execute o comando `show version system` e verifique a linha com a string SSP Slot Number. Se o Contêiner existir nesta linha, o FTD será executado em um modo de contêiner:

```
<#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)
```

```
...
```

Arquivo de Solução de Problemas do FTD

Siga estas etapas para verificar o tipo de implantação da instância de FTD no arquivo de solução

de problemas de FTD:

1. Abra o arquivo de solução de problemas e navegue até a pasta <filename>-troubleshooting.tar/results-<date>—xxxxx/command-outputs.
2. Abra o arquivo 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. Verifique a linha com a string SSP Slot Number. Se o Contêiner existir nesta linha, o FTD será executado em um modo de contêiner:

```
<#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
```

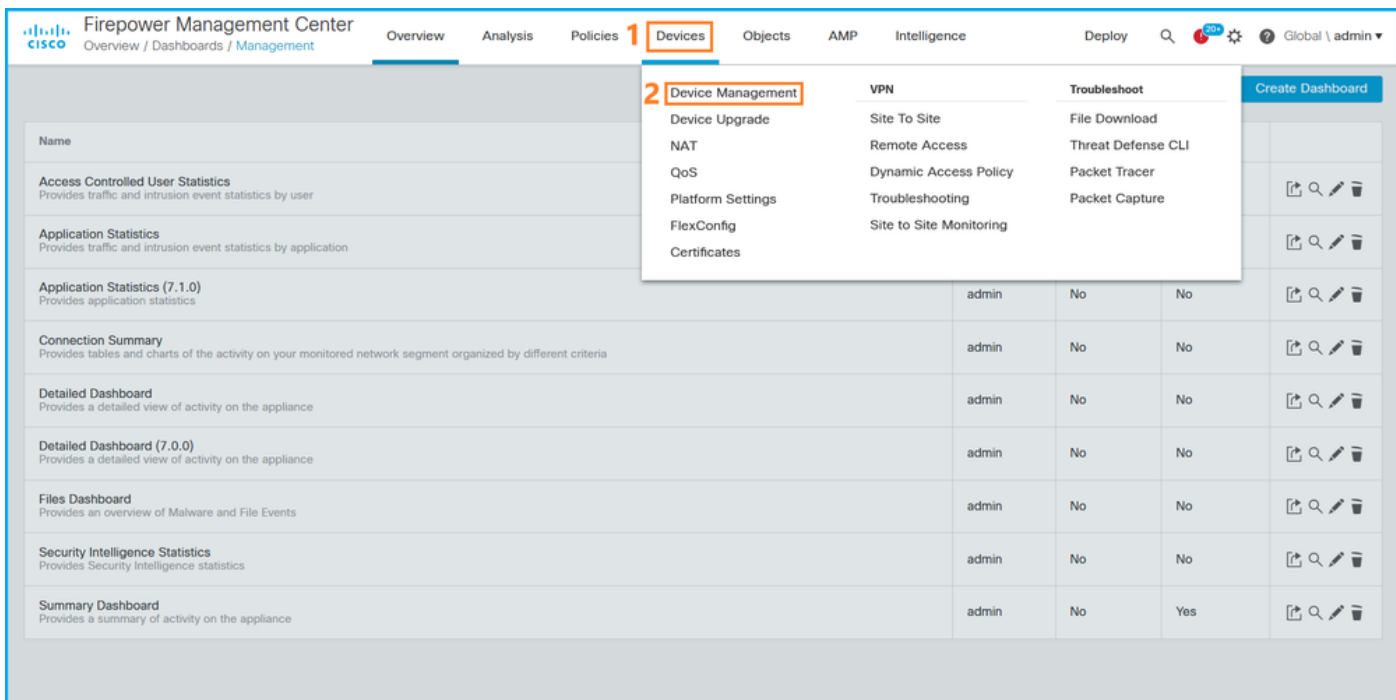
```
SSP Slot Number: 1 (Container)
```

```
...
```

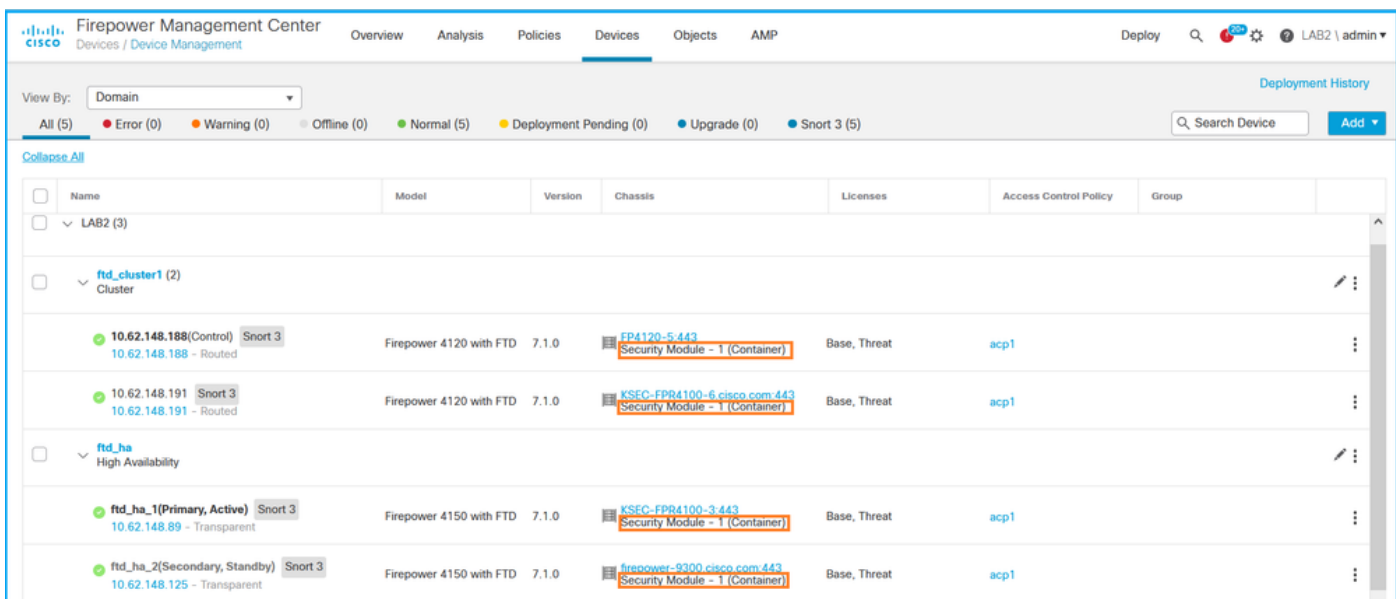
IU do FMC

Siga estas etapas para verificar o tipo de implantação da instância do FTD na interface do usuário do FMC:

1. Escolha Devices > Device Management:



2. Verifique a coluna Chassis. Se o Contêiner existir na linha, o FTD será executado no modo de contêiner.



FMC REST-API

Siga estas etapas para verificar o tipo de implantação da instância de FTD por meio da API REST do FMC. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicitar um token de autenticação:

```
<#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. Identifique o domínio que contém o dispositivo. Na maioria das consultas da API REST, o parâmetro domain é obrigatório. Use o token nesta consulta para recuperar a lista de domínios:

<#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. Use o UUID do domínio para consultar os registros de dispositivo específicos e o UUID do dispositivo específico:

<#root>

#

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

```
{
  "items": [
    {
      "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
    },
    ,
  ]
}
```

```

    "links": {
      "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000",
    },

"name": "ftd_ha_1",

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

```

4. Use o UUID de domínio e o UUID de dispositivo/contêiner da Etapa 3 nesta consulta e verifique o valor de isMultiInstance:

<#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,
...

```

IU do FCM

Para verificar o tipo de implantação da instância de FTD, verifique o valor do atributo de Perfil de Recurso em Dispositivos Lógicos. Se o valor não estiver vazio, o FTD será executado no modo de contêiner:

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.1.0.90	RP20	10.62.148.188	10.62.148.129	Ethernet1/1	Online

CLI FXOS

Siga estas etapas para verificar o tipo de implantação da instância de FTD na CLI FXOS:

1. Estabeleça uma conexão de console ou SSH com o chassi.
2. Alterne para o ssa do escopo e execute o comando show app-instance e verifique a coluna Tipo de Implantação do FTD específico com base no slot e no identificador:

```
<#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
```

API REST FXOS

Siga estas etapas para verificar o tipo de implantação da instância de FTD por meio de uma solicitação REST-API de FXOS. Use um cliente REST-API. Neste exemplo, curl é usado:

1. Solicitar um token de autenticação:

```
<#root>
```

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

```
{  
  "refreshPeriod": "0",  
  "token": "  
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d
```

```
"  
}
```

```
"
```

```
}
```

2. Especifique o token, a ID do slot nesta consulta e verifique o valor de deployType:

```
<#root>
```

```
#
```

```
curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da44530
```

```
...
{
  "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",
      ...
    }
  ]
}
```

Arquivo show-tech do chassi FXOS

Siga estas etapas para verificar o modo de firewall FTD no arquivo show-tech do chassi FXOS:

1. Para as versões 2.7 e posteriores do FXOS, abra o arquivo sam_techsupportinfo em <name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Para versões anteriores, abra o arquivo sam_techsupportinfo em FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Verifique a seção `show slot expand detail` para obter o slot específico e o identificador:

```
<#root>
```

```
# pwd
```

```
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_a11/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

Verificar o modo de contexto do ASA

O ASA suporta modos de contexto único e múltiplo. O FTD não oferece suporte ao modo de contexto múltiplo.

O tipo de contexto pode ser verificado com o uso destas opções:

- CLI do ASA
- ASA show-tech

CLI do ASA

Siga estas etapas para verificar o modo de contexto do ASA na CLI do ASA:

1. Use estas opções para acessar a CLI do ASA de acordo com a plataforma e o modo de implantação:
 - Acesso Telnet/SSH direto ao ASA no Firepower 1000/3100 e no Firepower 2100 no modo de dispositivo
 - Acesso a partir da CLI do console FXOS no Firepower 2100 no modo de plataforma e conexão ao ASA através do comando `connect asa`.
 - Acesso a partir da CLI do FXOS através de comandos (Firepower 4100/9300):

conecte o módulo `<x>` `[console|telnet]`, onde `x` é o ID do slot, e conecte-se como
 - Para ASA virtual, acesso SSH direto ao ASA ou acesso de console a partir da interface de usuário do hipervisor ou da nuvem

2. Execute o comando `show mode` no CLI:

```
<#root>
```

```
ASA#
```

```
show mode
```

Security context mode:

multiple

ASA#

show mode

Security context mode:

single

Arquivo de show-tech do ASA

Siga estas etapas para verificar o modo de contexto do ASA no arquivo show-tech do ASA:

1. Verifique a seção show context detail no arquivo show-tech. Nesse caso, o modo de contexto é múltiplo, pois há vários contextos:

<#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

Verificar o modo do Firepower 2100 com ASA

O Firepower 2100 com ASA pode ser executado em um destes modos:

- Modo de plataforma - parâmetros operacionais básicos e configurações de interface de hardware são configurados no FXOS. Essas configurações incluem as interfaces admin state change, EtherChannel configuration, NTP, image management e mais. A interface da Web do FCM ou a CLI do FXOS podem ser usadas para a configuração do FXOS.
- Modo de dispositivo (o padrão) - O modo de dispositivo permite que os usuários configurem todas as políticas no ASA. Somente comandos avançados estão disponíveis na CLI FXOS.

O modo Firepower 2100 com ASA pode ser verificado com o uso destas opções:

- CLI do ASA
- CLI FXOS
- FXOS show-tech

CLI do ASA

Siga estas etapas para verificar o modo Firepower 2100 com ASA na CLI do ASA:

1. Use telnet/SSH para acessar o ASA no Firepower 2100.
2. Execute o comando show fxos mode no CLI:

```
<#root>
```

```
ciscoasa(config)#
```

```
show fxos mode
```

```
Mode is currently set to platform
```


Modo do dispositivo:

```
<#root>
```

```
ciscoasa(config)#
```

```
show fxos mode
```

```
Mode is currently set to appliance
```

 Observação: no modo multicontexto, o comando show fxos mode está disponível no system ou no admin context.


CLI FXOS

Siga estas etapas para verificar o modo Firepower 2100 com ASA na CLI FXOS:

1. Use telnet/SSH para acessar o ASA no Firepower 2100.
2. Execute o comando connect fxos:

```
<#root>
ciscoasa/admin(config)#
connect fxos

Configuring session.
.
Connecting to FXOS.
...
Connected to FXOS. Escape character sequence is 'CTRL-^X'.
```

 Observação: no modo de contexto múltiplo, o comando connect fxos está disponível no contexto admin .

3. Execute o comando show fxos-mode:

```
<#root>
firepower-2140#
show fxos mode

Mode is currently set to plaftorm
```

Modo do dispositivo:

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

arquivo show-tech FXOS

Siga estas etapas para verificar o modo Firepower 2100 com ASA no arquivo show-tech do chassi FXOS:

1. Abra o arquivo tech_support_brief em <name>_FPRM.tar.gz/<name>_FPRM.tar
2. Verifique a seção `show fxos-mode`:

```
<#root>
```

```
# pwd
```

```
/var/tmp/fp2k-1_FPRM/
```

```
# cat tech_support_brief
```

```
...
```

```
`show fxos-mode`
```

```
Mode is currently set to platform
```

Modo do dispositivo:

```
<#root>
```

```
# pwd
```

```
/var/tmp/fp2k-1_FPRM/
```

```
# cat tech_support_brief
```

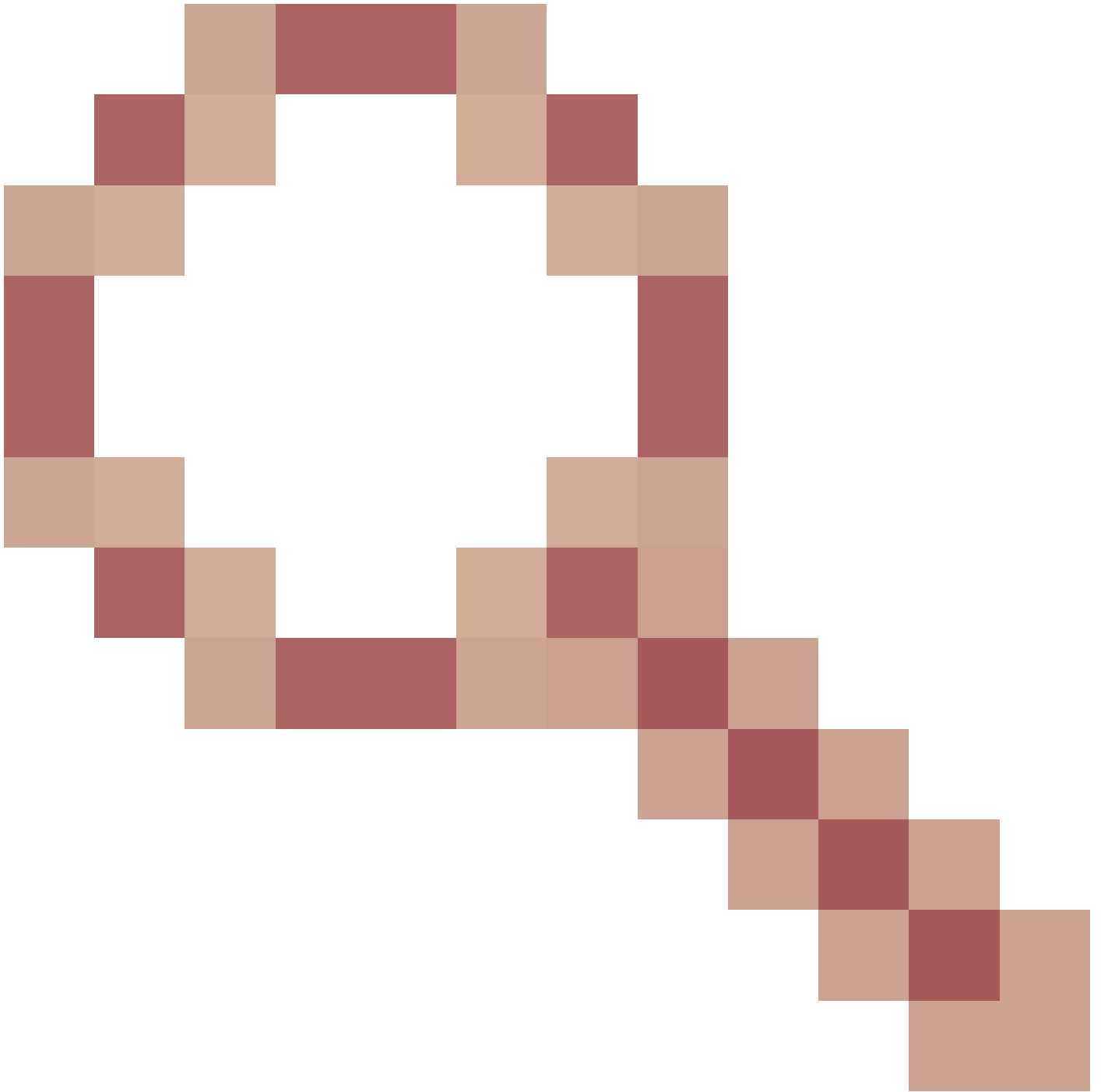
```
...
```

```
`show fxos-mode`
```

```
Mode is currently set to appliance
```

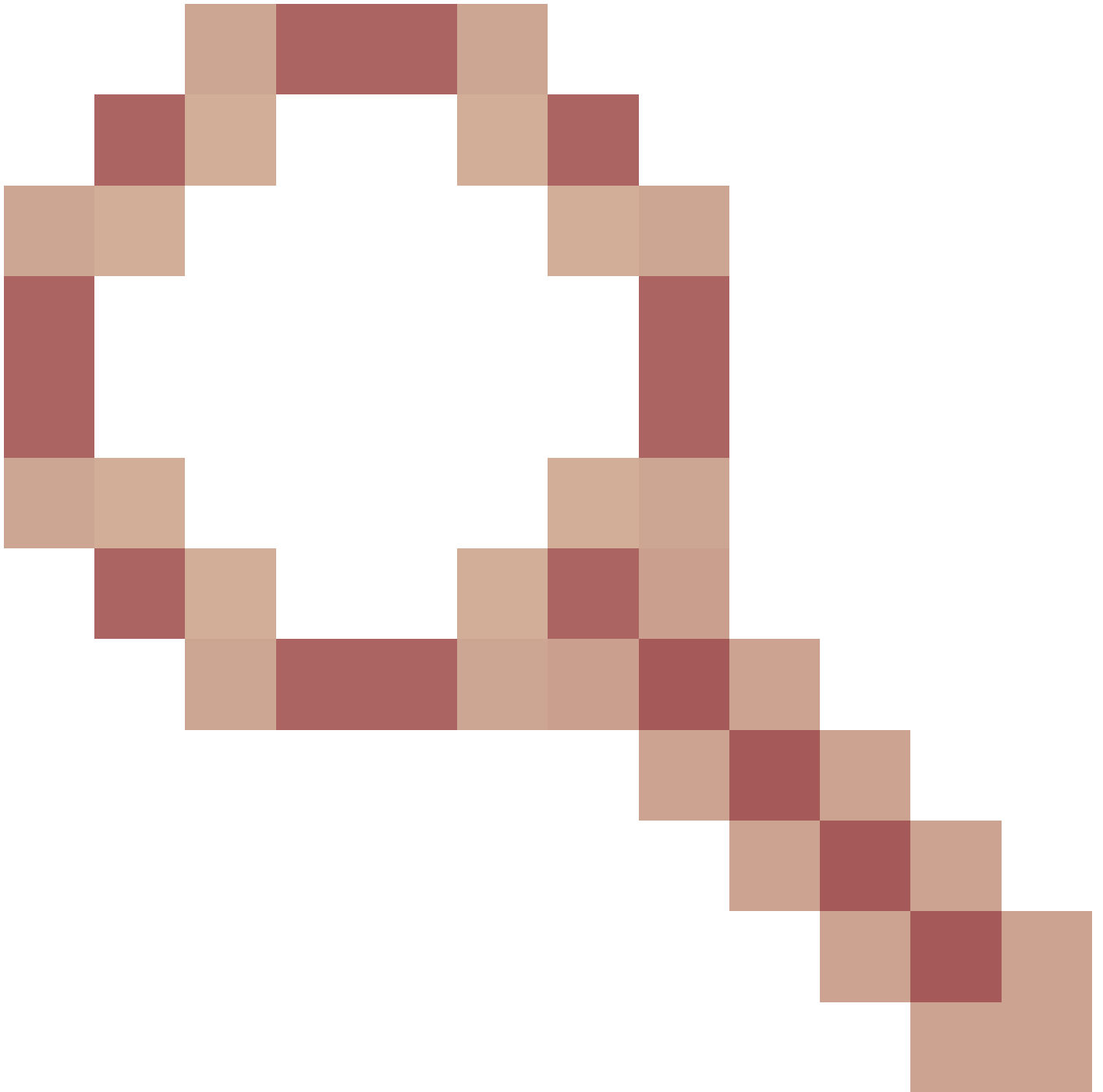
Problemas conhecidos

ID de bug da Cisco [CSCwb94424](#)



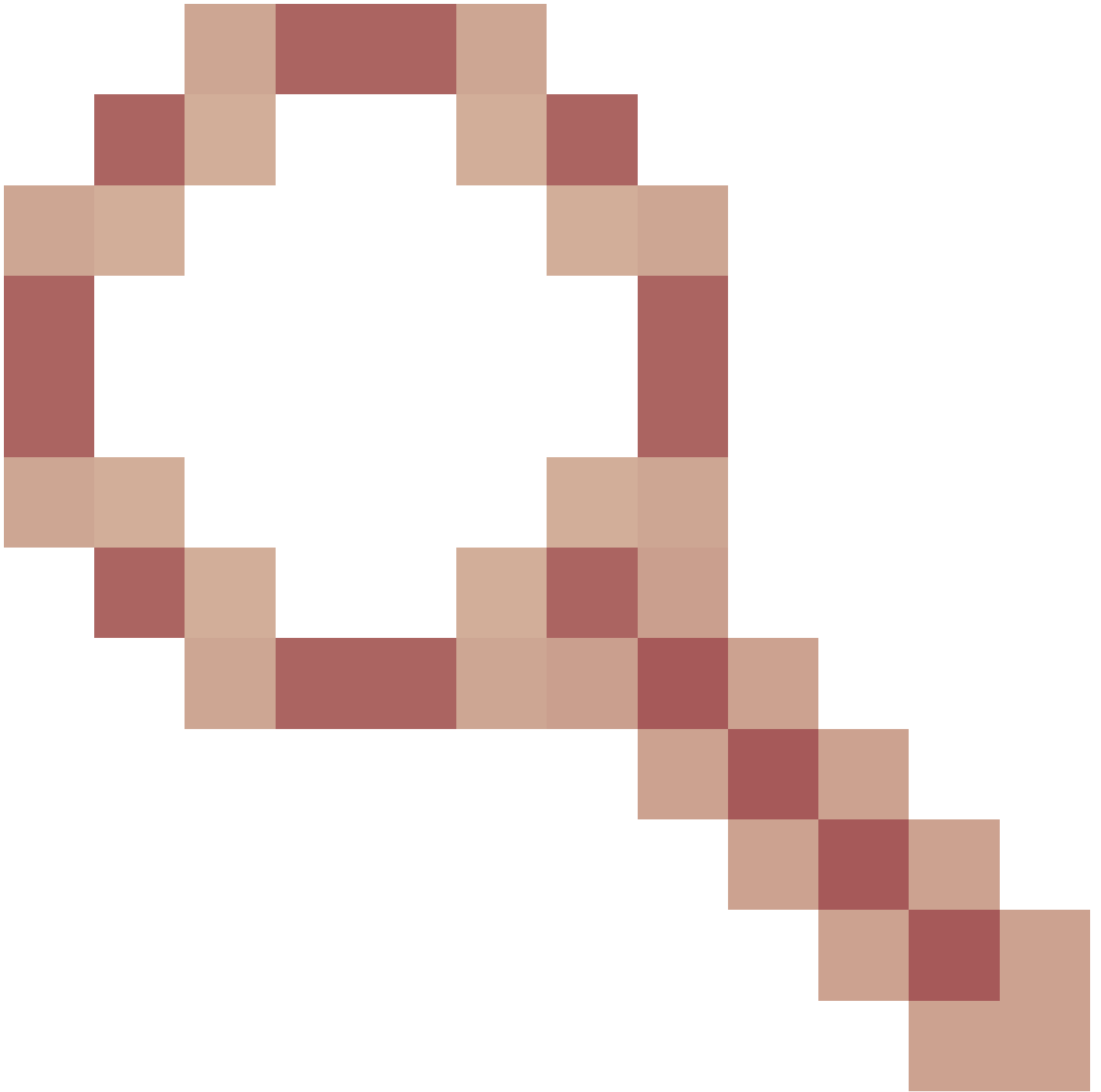
ENH: Add a CLISH command for FMC HA configuration verify

ID de bug Cisco [CSCvn31622](#)



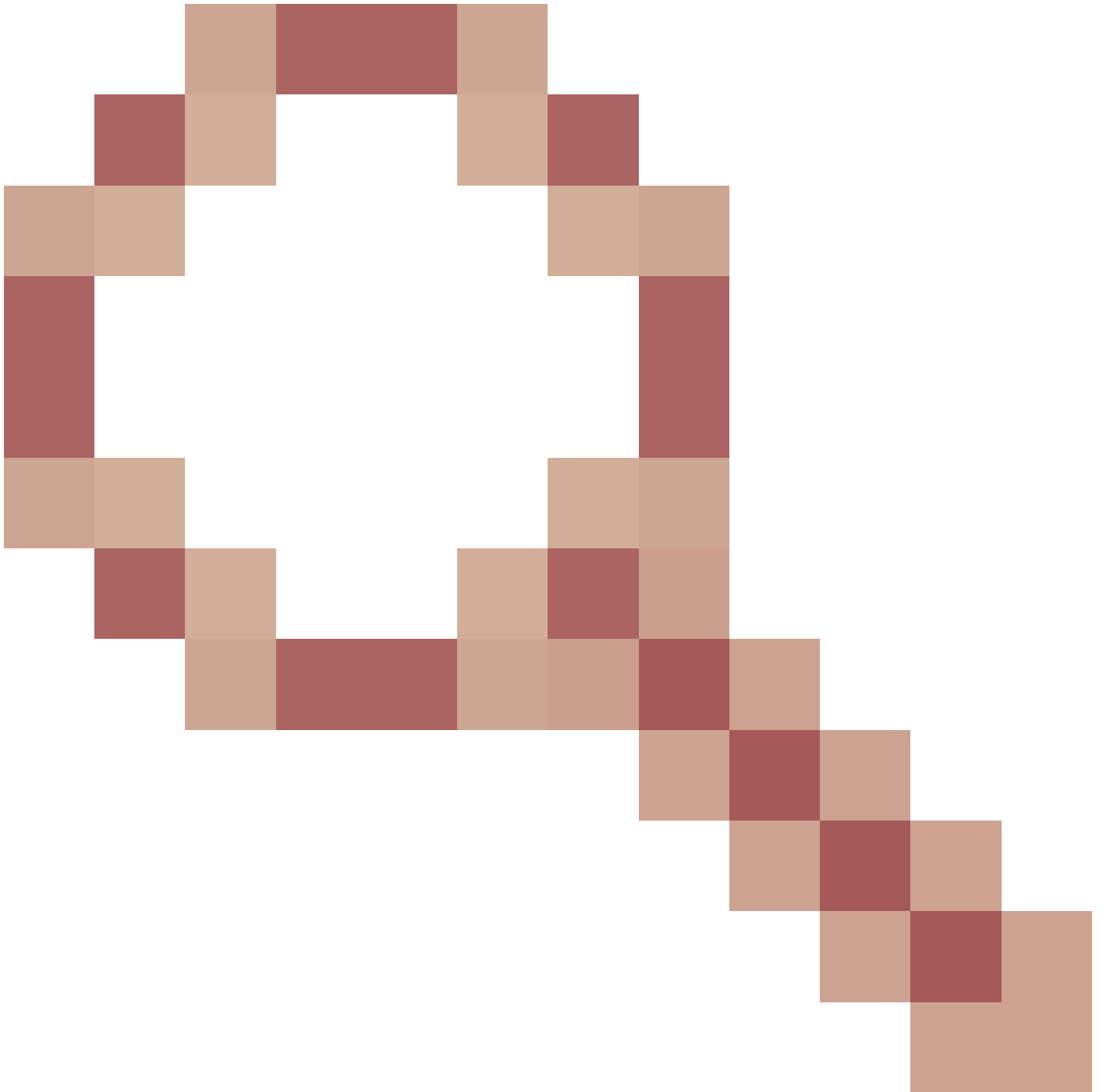
ENH: Add FXOS SNMP OIDs to poll logical device and app-instance configuration

ID de bug da Cisco [CSCwb9767](https://tools.cisco.com/bugtools/bugs/show_bug.do?bugID=CSCwb9767)



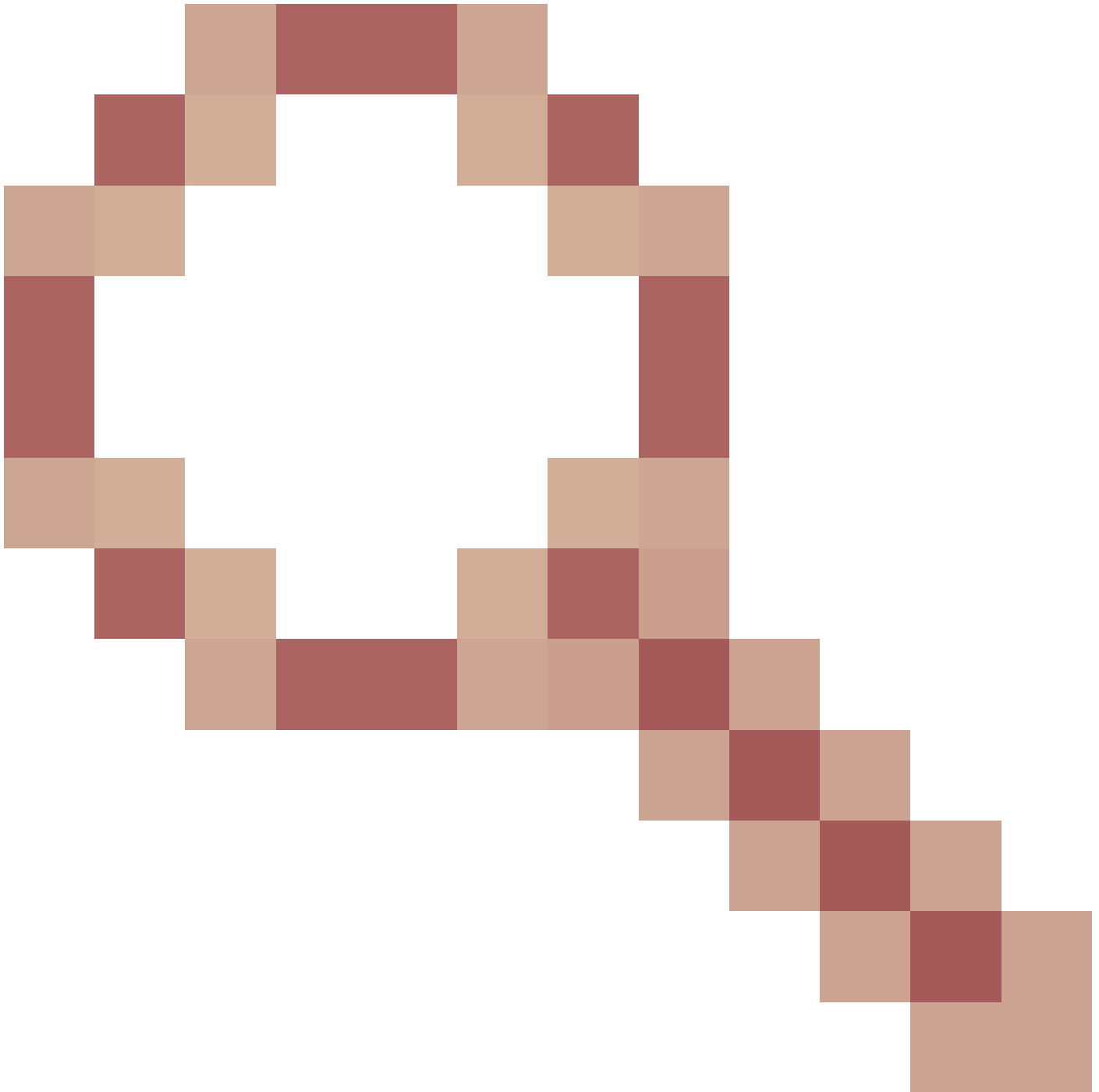
ENH: Add OID for verify of FTD instance deployment type (Adicionar OID para verificação do tipo de implantação da instância de FTD)

ID de bug da Cisco [CSCwb9772](https://www.cisco.com/cisco/web/bugtools/bugsearch.html?bugid=CSCwb9772)



ENH: Incluir saída de 'show fxos mode' em show-tech de ASA no Firepower 2100

O bug da Cisco ID [CSCwb97751](https://www.cisco.com/cisco/web/bugtools/bugdetail.do?moduleId=3&bugtype=bug&bugid=CSCwb97751)



OID 1.3.6.1.4.1.9.9.491.1.6.1.1 para verificação do modo de firewall transparente não está disponível

Informações Relacionadas

- [Guia de início rápido da API REST do Secure Firewall Management Center, versão 7.1](#)
- [Configurar o SNMP em dispositivos Firepower NGFW](#)
- [Guia da API REST do Cisco Firepower Threat Defense](#)
- [Referência da API REST do Cisco FXOS](#)
- [Compatibilidade com o Cisco ASA](#)
- [Versões do pacote Firepower 1000/2100 e Secure Firewall 3100 ASA e FXOS](#)
- [Componentes em pacote](#)
- [Procedimentos de geração de arquivos para solução de problemas do Firepower](#)

- [Guia de introdução do Cisco Firepower 2100](#)
- [Guia de compatibilidade do Cisco Firepower Threat Defense](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.