Verificación de la Configuración de Firepower Mode, Instance, High Availability y Scalability

Contenido

Introducción

Este documento describe la verificación de la configuración de alta disponibilidad y escalabilidad de Firepower, el modo de firewall y el tipo de implementación de instancia.

Antecedentes

Los pasos de verificación para la configuración de alta disponibilidad y escalabilidad, el modo de firewall y el tipo de implementación de instancias se muestran en la interfaz de usuario (IU), la

interfaz de línea de comandos (CLI), a través de consultas REST-API, SNMP y en el archivo de resolución de problemas.

Prerequisites

Requirements

Conocimiento básico del producto, REST-API, SNMP.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) versión 7.1.x
- Sistema operativo ampliable Firepower (FXOS) 2.11.1.x
- Firepower Device Manager (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

Verificar la configuración de alta disponibilidad y escalabilidad

High Availability hace referencia a la configuración de failover. La configuración de alta disponibilidad o de conmutación por fallo se une a dos dispositivos para que, si uno de ellos falla, el otro dispositivo pueda asumir el control.

Escalabilidad hace referencia a la configuración del clúster. Una configuración de clúster permite agrupar varios nodos FTD juntos como un único dispositivo lógico. Un clúster proporciona toda la comodidad de un único dispositivo (gestión, integración en una red) y el mayor rendimiento y redundancia de varios dispositivos.

En este documento, estas expresiones se utilizan indistintamente:

- alta disponibilidad o conmutación por fallas
- escalabilidad o clúster

En algunos casos, la verificación de la configuración o el estado de alta disponibilidad y escalabilidad no está disponible. Por ejemplo, no hay ningún comando de verificación para la configuración independiente de FTD. Los modos de configuración de clúster, de conmutación por fallas y independientes se excluyen mutuamente. Si un dispositivo no tiene conmutación por fallas

y configuración de clúster, se considera que funciona en modo independiente.

Alta disponibilidad de FMC

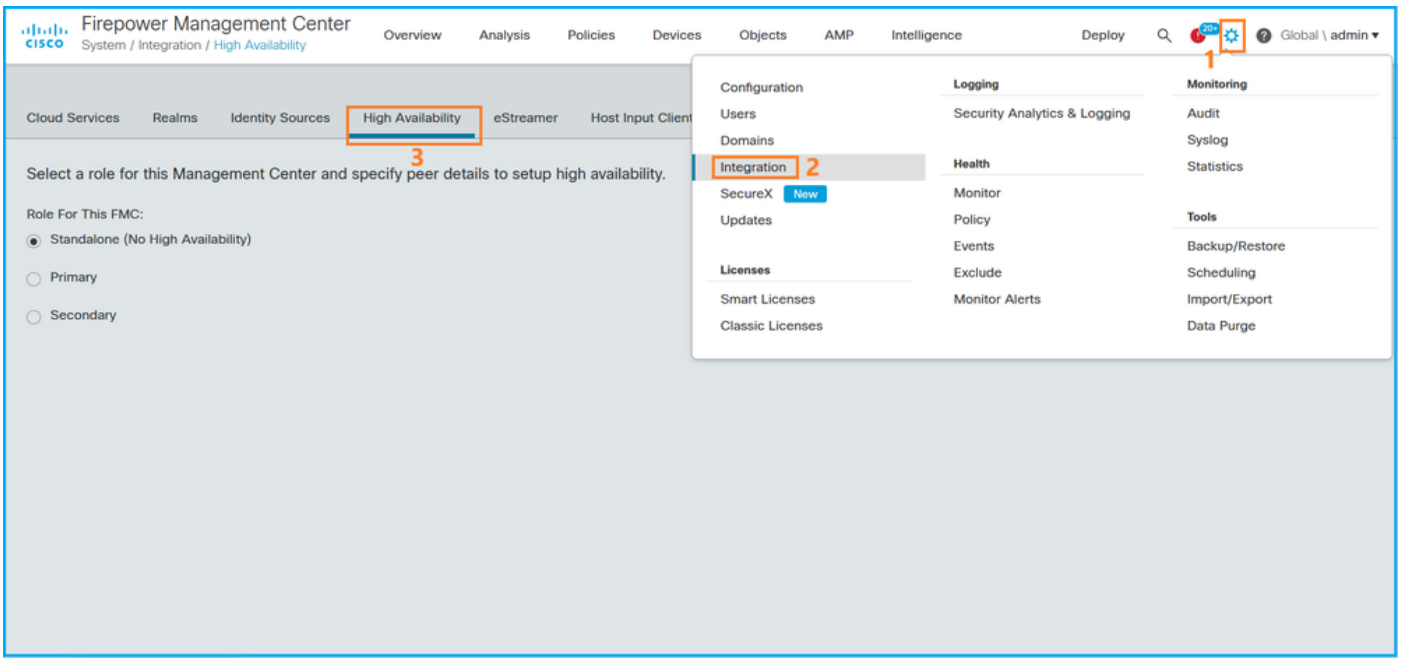
El estado y la configuración de alta disponibilidad de FMC se pueden verificar con el uso de estas opciones:

- Interfaz de usuario de FMC
- CLI de FMC
- solicitud de API REST
- archivo de resolución de problemas de FMC

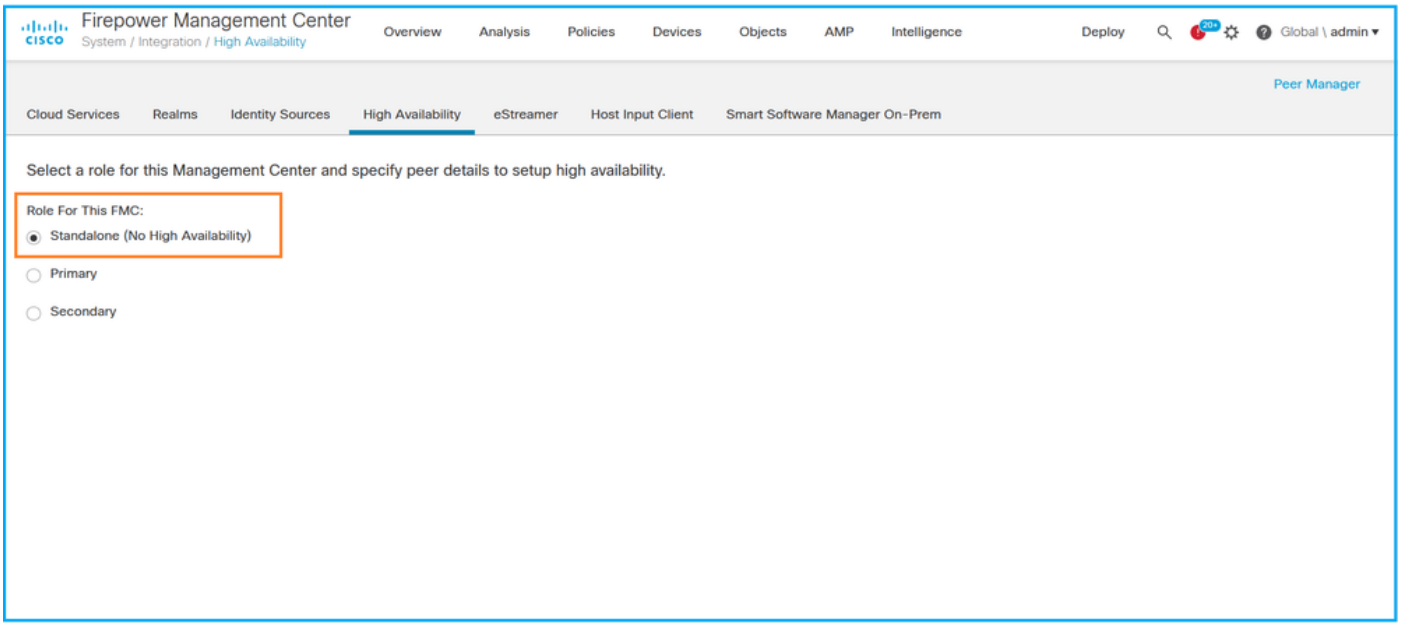
Interfaz de usuario de FMC

Siga estos pasos para verificar la configuración de alta disponibilidad de FMC y el estado en la interfaz de usuario de FMC:

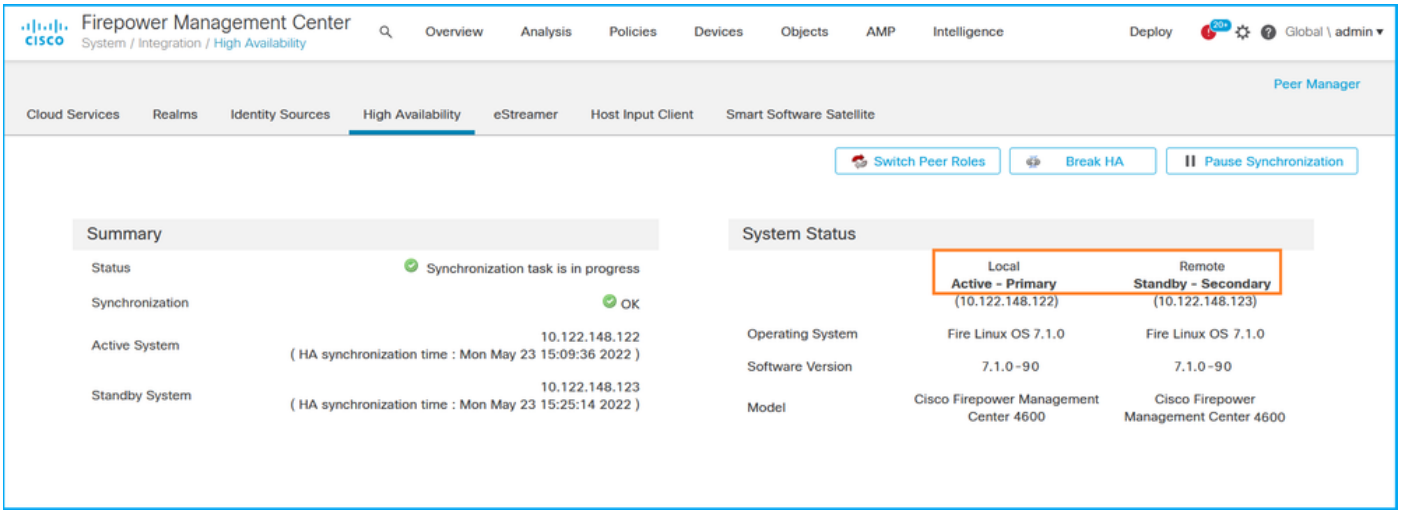
1. Elija **System > Integration > High Availability:**



2. Verifique la función del FMC. En este caso, la alta disponibilidad no está configurada y FMC funciona en una configuración independiente:



Si se configura la alta disponibilidad, se muestran las funciones locales y remotas:



CLI de FMC

Siga estos pasos para verificar la configuración de alta disponibilidad de FMC y el estado en la CLI de FMC:

1. Acceda a FMC a través de SSH o conexión de consola.

2. Ejecute el comando **experto** y luego ejecute el comando **sudo su**:

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

3. Ejecute el comando **trouTroubleshooting_HADC.pl** y seleccione la opción **1 Show HA Info Of FMC.** Si no se configura la alta disponibilidad, se muestra este resultado:

```
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
```

Si se configura la alta disponibilidad, se muestra este resultado:

```
fmc1:/Volume/home/admin# troubleshoot_HADC.pl
*************** Troubleshooting Utility **************
1 Show HA Info Of FMC
2 Execute Sybase DBPing
3 Show Arbiter Status
4 Check Peer Connectivity
5 Print Messages of AQ Task
6 Show FMC HA Operations History (ASC order)
7 Dump To File: FMC HA Operations History (ASC order)
8 Help
0 Exit ************************************************************
Enter choice: 1
HA Enabled: Yes
This FMC Role In HA: Active - Primary
Status out put: vmsDbEngine (system,gui) - Running 29061
In vmsDbEngineStatus(): vmsDbEngine process is running at
/usr/local/sf/lib/perl/5.24.4/SF/Synchronize/HADC.pm line 3471.
Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running)
Sybase Database Connectivity: Accepting DB Connections.
Sybase Database Name: csm_primary
Sybase Role: Active
```

> **Nota:** En una configuración de alta disponibilidad, el rol FMC puede tener un rol **primario** o **secundario**, y un estado **activo** o **en espera**.

FMC REST-API

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FMC a través de FMC REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Utilice el token en esta consulta para encontrar el UUID del dominio global:

```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{    "items": [
       {
           "name": "Global",
           "type": "Domain",
           "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
       },
       {
           "name": "Global/LAB2",
           "type": "Domain",
           "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
       },
       {
           "name": "Global/TEST1",
           "type": "Domain",
           "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
       },
       {
           "name": "Global/TEST2",
           "type": "Domain",
           "uuid": "341a8f03-f831-c364-b751-000000000001"
       }
   ],
   "links": {
       "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
   },
   "paging": {
       "count": 4,
       "limit": 25,
       "offset": 0,
       "pages": 1
   }
}
```

Nota: La parte "**| python -m json.tool**" de la cadena de comandos se utiliza para dar formato al resultado en estilo JSON y es opcional.

3. Utilice el UUID de dominio global en esta consulta:

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/integration/fmchastatuses' -H 'accept: application/json' -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
```

Si no se configura la alta disponibilidad, se muestra este resultado:

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

Si se configura la alta disponibilidad, se muestra este resultado:

```
{
```

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


Archivo de Troubleshooting de FMC

Siga estos pasos para verificar la configuración de alta disponibilidad de FMC y el estado en el archivo de solución de problemas de FMC:

1. Abra el archivo de resolución de problemas y navegue hasta la carpeta **<filename>.tar/results-<date>—xxxxxx/command-output**

2. Abra el archivo **usr-local-sf-bin-trouTroubleshooting_HADC.pl -a.output:**

Si no se configura la alta disponibilidad, se muestra este resultado:

```
# 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
```

Si se configura la alta disponibilidad, se muestra este resultado:

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

# cat "usr-local-sf-bin-troubleshoot_HADC.pl -a.output"
Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:
Status out put: vmsDbEngine (system,gui) - Running 9399
In vmsDbEngineStatus(): vmsDbEngine process is running at
/usr/local/sf/lib/perl/5.24.4/SF/Synchronize/HADC.pm line 3471.
$VAR1 = [
          'Mirror Server => csm_primary',
          {
            'stderr' => undef,
            'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745
Type       Property                  Value
---------  ----------------          ------------------------------
Database   MirrorRole                primary
Database   MirrorState               synchronizing
Database   PartnerState              connected
Database   ArbiterState              connected
Server     ServerName                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 disponibilidad de FDM

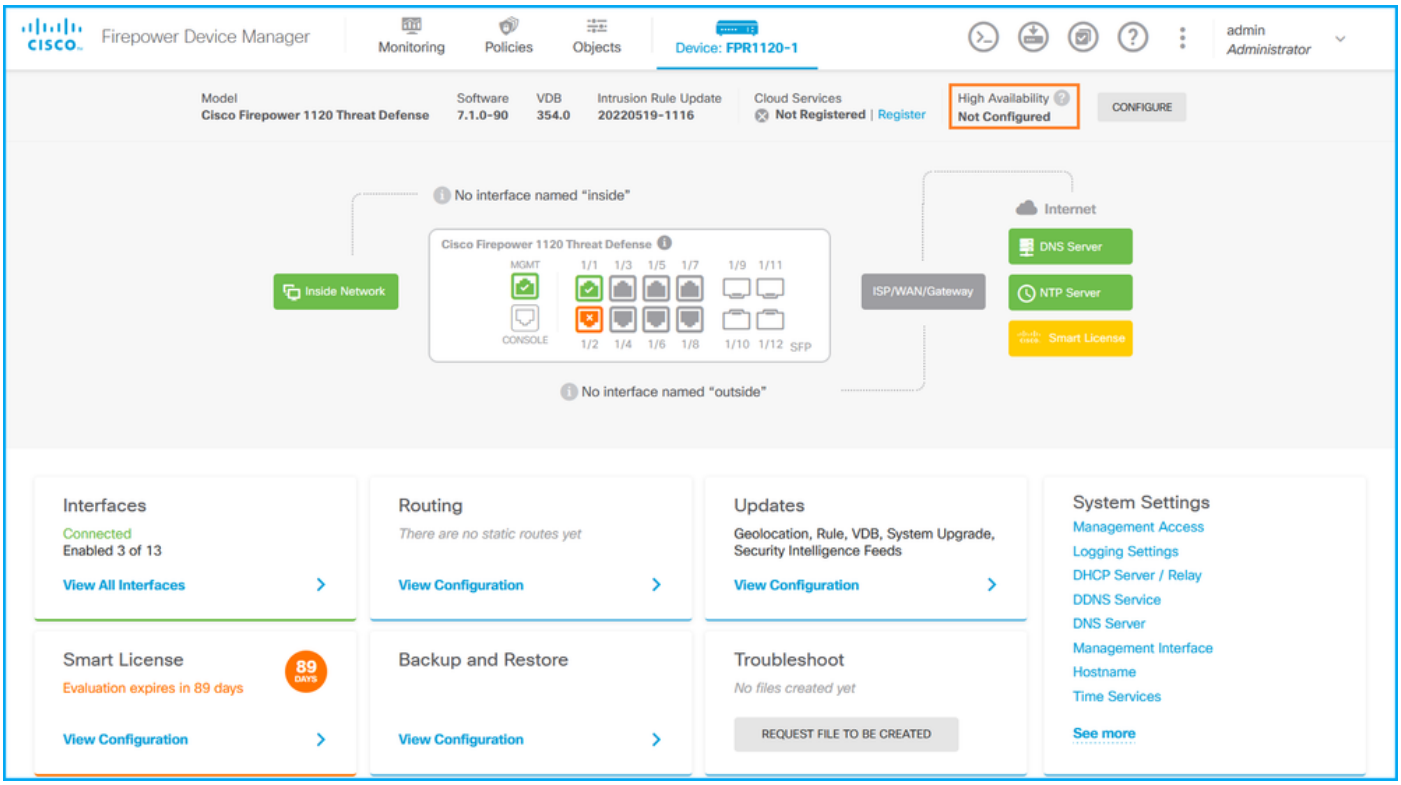
El estado y la configuración de alta disponibilidad de FDM se pueden verificar con el uso de estas opciones:

- Interfaz de usuario de FDM

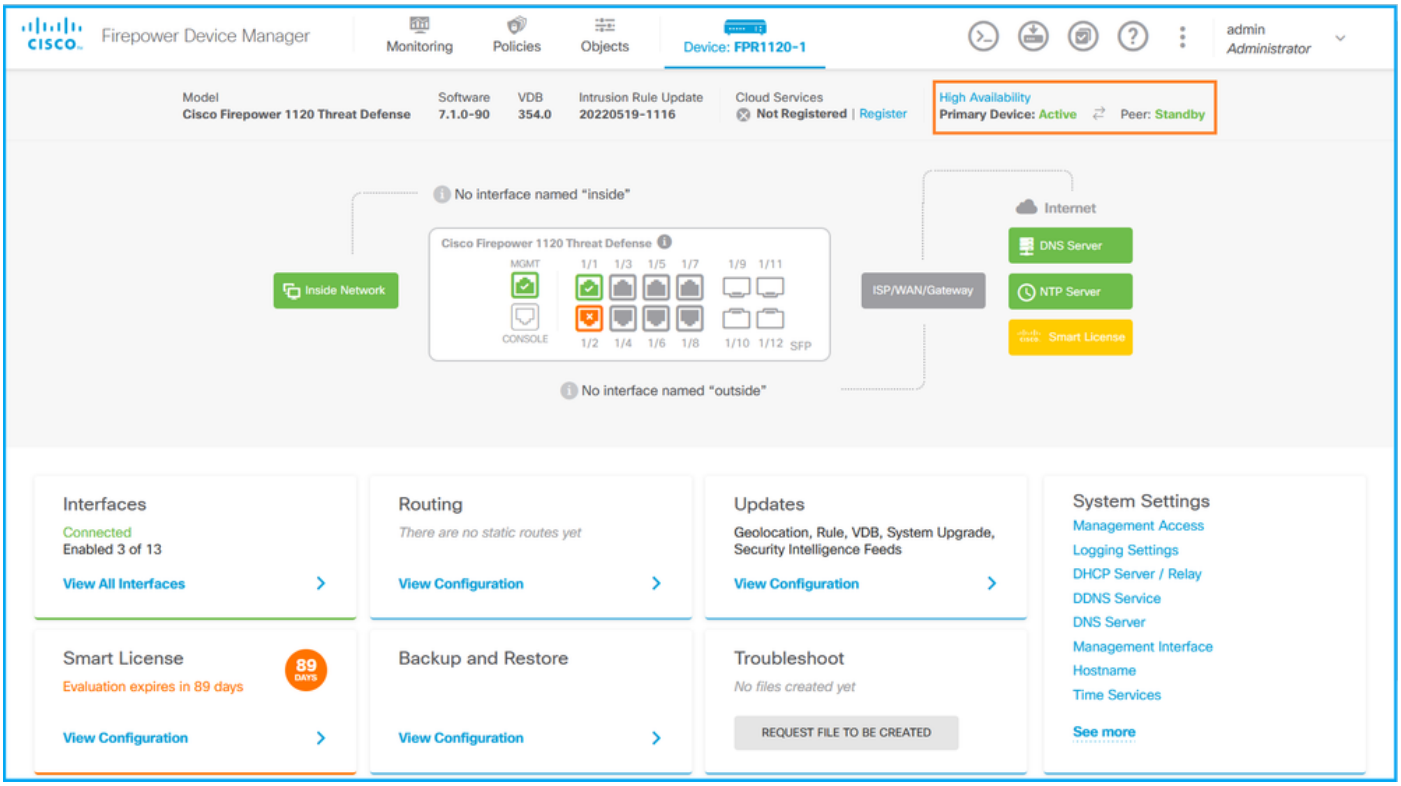
- solicitud de API FDM REST
- CLI FTD
- Sondeo SNMP de FTD
- archivo de resolución de problemas FTD

Interfaz de usuario de FDM

Para verificar la configuración de alta disponibilidad de FDM y el estado en la interfaz de usuario de FDM, verifique **Alta disponibilidad** en la página principal. Si no se configura la alta disponibilidad, el valor **de alta disponibilidad** es **No configurado:**



Si se configura la alta disponibilidad, se muestran la configuración de failover de la unidad peer local y remota y las funciones:



FDM REST-API

Siga estos pasos para verificar la configuración de alta disponibilidad y el estado de FDM a través de la solicitud FDM REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

```
# curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json'
-d '{ "grant_type": "password", "username": "admin", "password": "Cisco123" }'
'https://192.0.2.3/api/fdm/latest/fdm/token'
{
   "access_token":
   "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0
xMWVjLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV
4cGlyZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDg
xZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ
1c2VybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M",
   "expires_in": 1800,
   "refresh_expires_in": 2400,
   "refresh_token":
"eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoiMGU0NGIxYzQtZDI0Mi0xMW
VjLTk4ZWMtYTllOTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LCJleHAiOjE2NTIzOTY1NjksImFjY2Vzc1Rva2VuRXhwaX
Jlc0F0IjoxNjUyMzk1OTY5MDcwLCJyZWZyZXNoQ291bnQiOi0xLCJ0b2tlblR5cGUiOiJKV1RfUmVmcmVzaCIsInVzZXJVdW
lkIjoiYTU3ZGVmMjgtY2M3MC0xMWVjLTk4ZWMtZjk4ODExNjNjZWIwIiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2
luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
   "token_type": "Bearer"
}
```

2. Para verificar la configuración de alta disponibilidad, utilice el valor del token de acceso en esta consulta:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0xMWV
jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV4cGl
```

yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDgxZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/ha/configurations'

Si no se configura la alta disponibilidad, se muestra este resultado:


```
{
 "items": [
   {
     "version": "issgb3rw2lixf",
      "name": "HA",
      "nodeRole": null,
     "failoverInterface": null,
     "failoverName": null,
     "primaryFailoverIPv4": null,
     "secondaryFailoverIPv4": null,
     "primaryFailoverIPv6": null,
     "secondaryFailoverIPv6": null,
     "statefulFailoverInterface": null,
     "statefulFailoverName": null,
     "primaryStatefulFailoverIPv4": null,
     "secondaryStatefulFailoverIPv4": null,
     "primaryStatefulFailoverIPv6": null,
     "secondaryStatefulFailoverIPv6": null,
     "sharedKey": null,
     "id": "76ha83ga-c872-11f2-8be8-8e45bb1943c0",
     "type": "haconfiguration",
     "links": {
       "self": "https://192.0.2.2/api/fdm/v6/devices/default/ha/configurations/76ha83ga-c872-
11f2-8be8-8e45bb1943c0"
     }
   }
 ],
 "paging": {
   "prev": [],
   "next": [],
   "limit": 10,
   "offset": 0,
   "count": 1,
   "pages": 0
 }
}
```


Si se configura la alta disponibilidad, se muestra este resultado:


```
{
 "items": [
   {
     "version": "issgb3rw2lixf",
      "name": "HA",
      "nodeRole": "HA_PRIMARY",
     "failoverInterface": {
       "version": "ezzafxo5ccti3",
       "name": "",
       "hardwareName": "Ethernet1/1",
       "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
       "type": "physicalinterface"
     },
...
```


3. Para verificar el estado de alta disponibilidad, utilice esta consulta:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoiMjI1YWRhZWMtZDlhYS0xMWV
jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV4cGl
yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDgxZS0
xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2V
ybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default'
```

Si no se configura la alta disponibilidad, se muestra este resultado:

```
{
 "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"
 }
}
```

Si se configura la alta disponibilidad, se muestra este resultado:

```
{
 "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 FTD

Siga los pasos de la sección.

Sondeo SNMP de FTD

Siga los pasos de la sección.

Archivo de Troubleshooting de FTD

Siga los pasos de la sección.

Alta disponibilidad y escalabilidad de FTD

El estado y la configuración de alta disponibilidad y escalabilidad de FTD se pueden verificar con el uso de estas opciones:

- CLI FTD
- FTD SNMP
- archivo de resolución de problemas FTD
- Interfaz de usuario de FMC
- FMC REST-API
- Interfaz de usuario de FDM
- FDM REST-API
- Interfaz de usuario de FCM
- CLI FXOS
- FXOS REST-API
- Archivo show-tech del chasis FXOS

CLI FTD

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD en la CLI de FTD:

1. Utilice estas opciones para acceder a la CLI de FTD de acuerdo con la plataforma y el modo de implementación:

- Acceso SSH directo a FTD: todas las plataformas
- Acceso desde la CLI de la consola FXOS (Firepower 1000/2100/3100) a través del comando **connect ftd**
- Acceso desde la CLI de FXOS a través de comandos (Firepower 4100/9300): **connect module <x> [console|telnet],** donde x es el ID de ranura, y luego **connect ftd [instance],** donde la instancia sólo es relevante para la implementación de instancias múltiples

- Para los FTD virtuales, acceso SSH directo a FTD o acceso a la consola desde el hipervisor o la interfaz de usuario de la nube

2. Para verificar la configuración y el estado de failover de FTD, ejecute los comandos **show running-config failover** y **show failover state** en la CLI.

Si no se configura la conmutación por fallas, se muestra este resultado:

```
> 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==
```

Si se configura la conmutación por fallas, se muestra este resultado:

```
> 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 la configuración y el estado del clúster FTD, ejecute los comandos **show running-config cluster** y **show cluster info** en la CLI.

Si el clúster no está configurado, se muestra este resultado:

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

Si se configura el clúster, se muestra este resultado:

```
> 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
```

Nota: Las funciones **maestra** y **de control** son las mismas.

FTD SNMP

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD a través de SNMP:

1. Asegúrese de que SNMP esté configurado y habilitado. Para FTD administrado por FDM, consulte Configuración y resolución de problemas de SNMP en FDM de Firepower para ver los pasos de configuración. Para FTD administrado por FMC, consulte Configuración de SNMP en Firepower NGFW Appliances para ver los pasos de configuración.

2. Para verificar la configuración y el estado de failover de FTD, sondee el OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1.**

Si no se configura la conmutación por fallas, se muestra este resultado:

```
# 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"
```

Si se configura la conmutación por fallas, se muestra este resultado:

```
# 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 la configuración y el estado del clúster, sondee el OID **1.3.6.1.4.1.9.9.491.1.8.1.**

Si el clúster no está configurado, se muestra este resultado:

```
# 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
```

Si el clúster está configurado, pero no habilitado, se muestra este resultado:

```
# 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
...
```

Si el clúster está configurado, habilitado y en funcionamiento, se muestra este resultado:

```
# 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 obtener más información sobre las descripciones de OID, refiérase a CISCO-UNIFIED-FIREWALL-MIB.

Archivo de Troubleshooting de FTD

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD en el archivo de solución de problemas de FTD:

1. Abra el archivo de solución de problemas y navegue hasta la carpeta **<filename>-trouTroubleshooting .tar/results-<date>—xxxxxx/command-output.**

2. Abra el archivo **usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output:**

```
# pwd
/ngfw/var/common/results-05-22-2022--102758/command-outputs
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

3. Para verificar la configuración de failover y el estado, verifique la sección **show failover**.

Si no se configura la conmutación por fallas, se muestra este resultado:

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

Si se configura la conmutación por fallas, se muestra este resultado:

```
------------------ 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 la configuración del clúster FTD y el estado, verifique la sección **show cluster info**.

Si el clúster no está configurado, se muestra este resultado:

```
------------------ show cluster info ------------------
Clustering is not configured
```

Si el clúster está configurado y habilitado, se muestra este resultado:

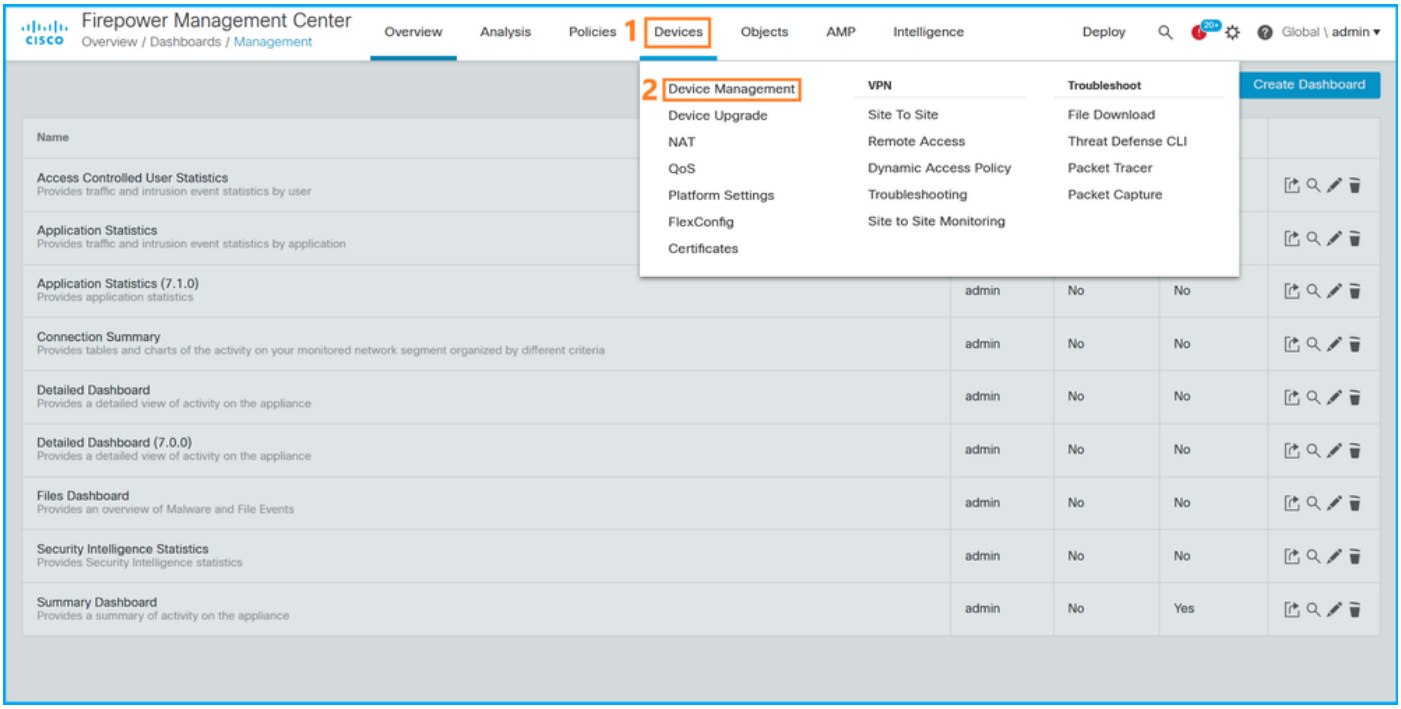
```
------------------ show cluster info ------------------
Cluster ftd_cluster1: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID        : 0
        Site ID   : 1
        Version   : 9.17(1)
        Serial No.: FLM1949C5RR6HE
        CCL IP    : 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
```

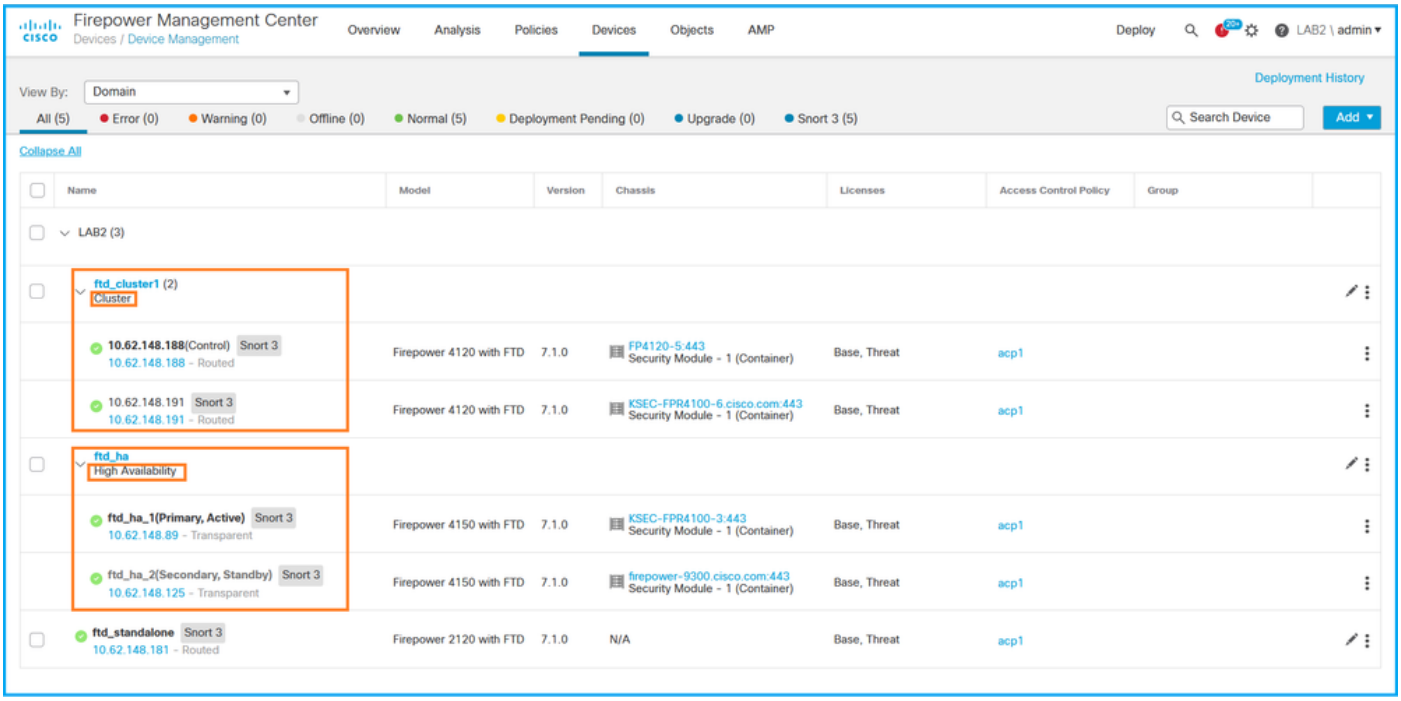
Interfaz de usuario de FMC

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD en la interfaz de usuario de FMC:

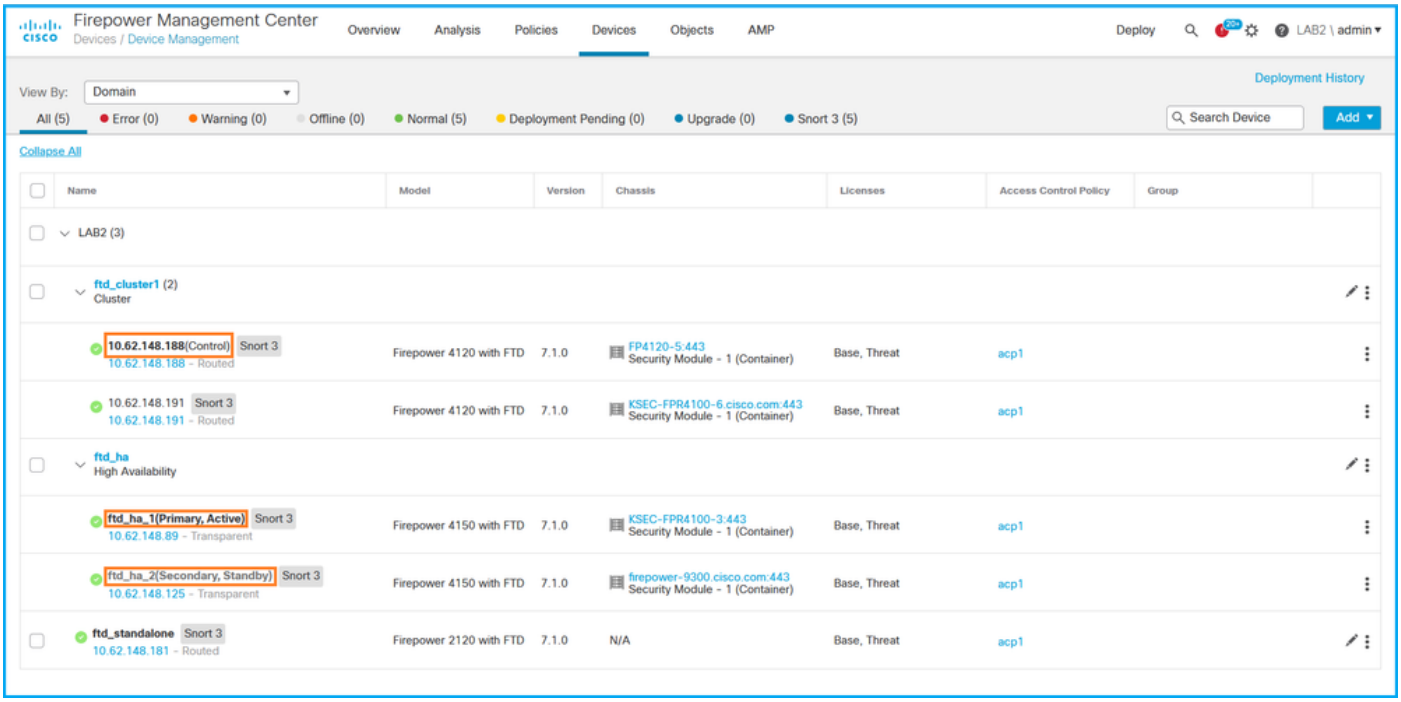
1. Elija **Devices > Device Management**:



2. Para verificar la configuración de alta disponibilidad y escalabilidad de FTD, verifique las etiquetas **High Availability** o **Cluster**. Si no existe ninguno, el FTD se ejecuta en una configuración independiente:



3. Para verificar el estado de alta disponibilidad y escalabilidad de FTD, verifique el rol de unidad entre paréntesis. Si no existe una función y el FTD no forma parte de un clúster o de un failover, el FTD se ejecuta en una configuración independiente:



Nota: En el caso de un clúster, sólo se muestra la función de la unidad **de control**.

API FMC REST

En estos resultados, **ftd_ha_1, ftd_ha_2, ftd_standalone, ftd_ha, ftc_cluster1** son nombres de dispositivos configurables por el usuario. Estos nombres no hacen referencia a la configuración o el estado real de alta disponibilidad y escalabilidad.

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD a través de FMC REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Identifique el dominio que contiene el dispositivo. En la mayoría de las consultas de la API REST, el parámetro **domain** es obligatorio. Utilice el token en esta consulta para recuperar la lista de dominios:

```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
  "items":
[
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
        },
...
```

3. Utilice el UUID de dominio para consultar los **registros** de **dispositivos** específicos y el UUID de dispositivo específico:

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

4. Para verificar la configuración de failover, use el dominio UUID y el dispositivo/contenedor UUID del Paso 3 en esta consulta:

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

```
...
```

5. Para verificar el estado de failover, use el dominio UUID y el DeviceHAPair UUID del Paso 4 en esta consulta:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devicehapairs/ftddevicehapairs/eec3ddfc-d842-11ec-a15e-986001c83f2f' -H 'X-auth-
access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
       "primaryStatus": {
            "currentStatus": "Active",
            "device": {
                "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
                "keepLocalEvents": false,
                "name": "ftd_ha_1"
            }
        },
        "secondaryStatus": {
            "currentStatus": "Standby",
            "device": {
                "id": "e60ca6d0-d83d-11ec-b407-cdc91a553663",
                "keepLocalEvents": false,
                "name": "ftd_ha_2"
            }
        }
...
```

6. Para verificar la configuración del clúster, utilice el UUID del dominio y el UUID del dispositivo/contenedor del Paso 3 en esta consulta:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/3344bc4a-d842-11ec-a995-817e361f7ea5' -H 'X-auth-access-
token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
       "containerDetails": {             "id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/deviceclusters/ftddevicecluster/8e6188c2-d844-11ec-bdd1-6e8d3e226370"
            },
            "name": "ftd_cluster1",
            "type": "DeviceCluster"
        },
...
```

7. Para verificar el estado del clúster, utilice el UUID del dominio y el UUID del dispositivo/contenedor del Paso 6 en esta consulta:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/deviceclusters/ftddevicecluster/8e6188c2-d844-11ec-bdd1-6e8d3e226370' -H 'X-auth-
access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
    "controlDevice": {
        "deviceDetails": {
            "id": "3344bc4a-d842-11ec-a995-817e361f7ea5",
            "name": "10.62.148.188",
            "type": "Device"
        }
    },
    "dataDevices": [
        {
            "deviceDetails": {
```

```
                "id": "a7ba63cc-d842-11ec-be51-f3efcd7cd5e5",
                "name": "10.62.148.191",
                "type": "Device"
            }
        }
    ],
    "id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",
    "name": "ftd_cluster1",
    "type": "DeviceCluster"
}
```

Interfaz de usuario de FDM

Siga los pasos de la sección.

FDM REST-API

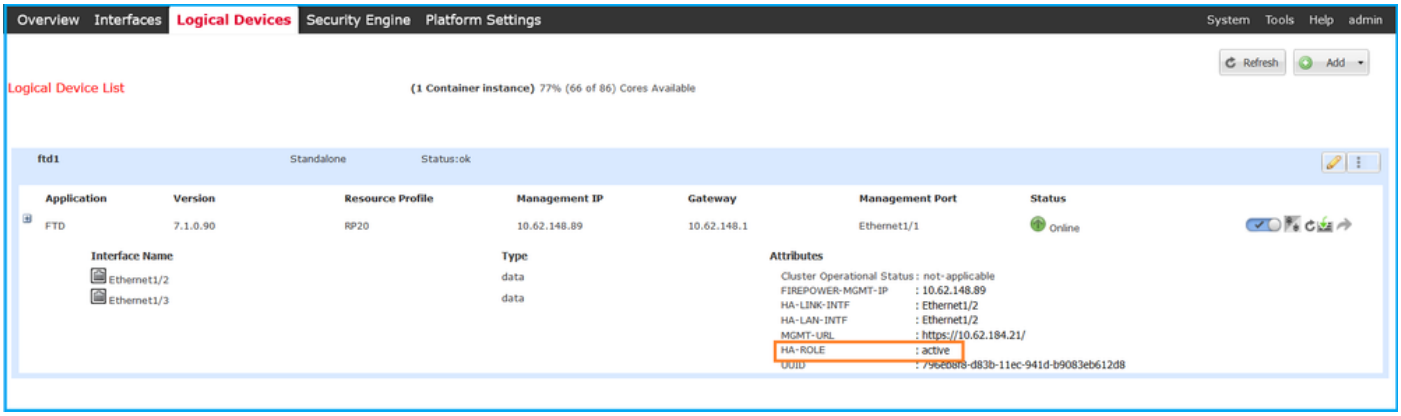
Siga los pasos de la sección.

Interfaz de usuario de FCM

La interfaz de usuario de FCM está disponible en Firepower 4100/9300 y Firepower 2100 con ASA en modo de plataforma.

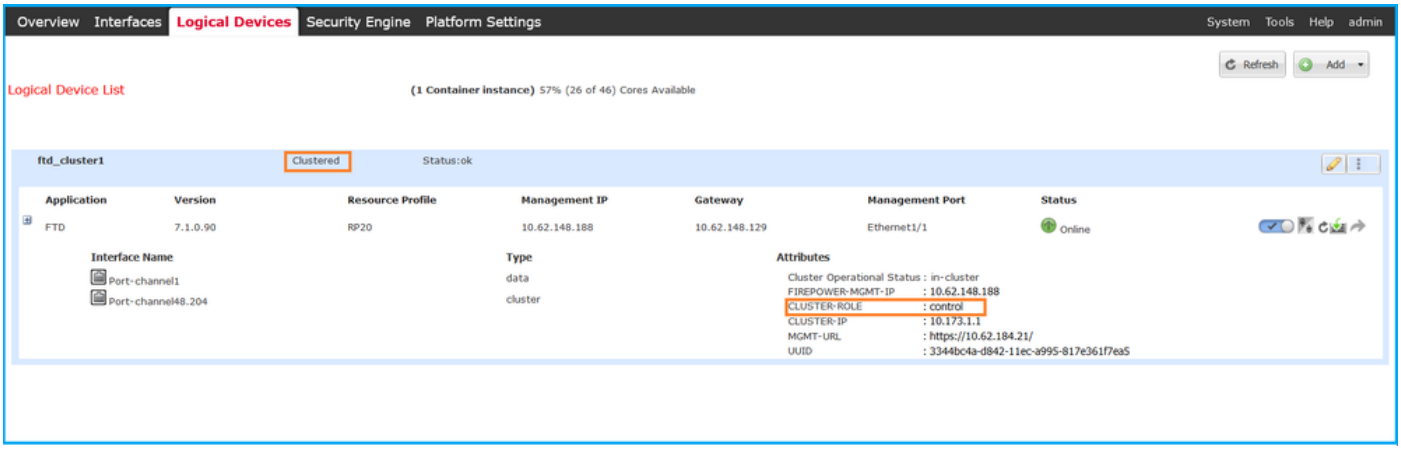
Siga estos pasos para verificar el estado de alta disponibilidad y escalabilidad de FTD en la interfaz de usuario de FCM:

1. Para verificar el estado de failover de FTD, verifique el valor del atributo **HA-ROLE** en la página Dispositivos Lógicos:



> **Nota:** La etiqueta **Independiente** junto al identificador del dispositivo lógico se refiere a la configuración del dispositivo lógico del chasis, no a la configuración de failover de FTD.

2. Para verificar la configuración y el estado del clúster de FTD, verifique la etiqueta **Clúster** y el valor del atributo **CLUSTER-ROLE** en la página Dispositivos Lógicos:



CLI FXOS

La configuración de alta disponibilidad y escalabilidad de FTD y la verificación de estado en la CLI de FXOS están disponibles en Firepower 4100/9300.

Siga estos pasos para verificar la configuración y el estado de alta disponibilidad y escalabilidad de FTD en la CLI de FXOS:

1. Establezca una conexión de consola o SSH al chasis.

2. Para verificar el estado de alta disponibilidad de FTD, ejecute el comando **scope ssa** y luego ejecute **scope slot <x>** para cambiar a la ranura específica donde se ejecuta FTD y ejecute el comando **show app-instance expanda**:

```
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 la configuración y el estado del clúster de FTD, ejecute el comando **scope ssa** , ejecute el comando **show lógico-device <name> detail extend**, donde el nombre es el nombre del

dispositivo lógico, y el comando **show app-instance**. Verifique la salida para un slot específico:

```
firepower # scope ssa
firepower /ssa # show logical-device ftd_cluster1 detail expand

Logical Device:
    Name: ftd_cluster1
    Description:
    Slot ID: 1
    Mode: Clustered
    Oper State: Ok
    Template Name: ftd
    Error Msg:
    Switch Configuration Status: Ok
    Sync Data External Port Link State with FTD: Disabled
    Current Task:
…
firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- -------------- -------------- --
--------- ---------- ------------ -------------- ------------
ftd        ftd_cluster1 1          Enabled     Online           7.1.0.90       7.1.0.90
Container   No         RP20         In Cluster      Master
```

FXOS REST API

FXOS REST-API es compatible con Firepower 4100/9300.

Siga estos pasos para verificar la configuración de alta disponibilidad y escalabilidad de FTD y el estado a través de la solicitud FXOS REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Para verificar el estado de failover de FTD, utilice el token y el ID de slot en esta consulta:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.100/api/slot/1/app-inst'
...
{     "smAppInstance": [         {             "adminState": "enabled",             "appDn":
"sec-svc/app-ftd-7.1.0.90",             "appInstId": "ftd_001_JAD201200R43VLP1G3",
"appName": "ftd",             "clearLogData": "available",
"clusterOperationalState": "not-applicable",             "clusterRole": "none",
"currentJobProgress": "100",             "currentJobState": "succeeded",
"currentJobType": "start",             "deployType": "container",             "dn": "slot/1/app-
inst/ftd-ftd1",             "errorMsg": "",             "eventMsg": "",
"executeCmd": "ok",             "externallyUpgraded": "no",             "fsmDescr": "",
            "fsmProgr": "100",             "fsmRmtInvErrCode": "none",
"fsmRmtInvErrDescr": "",             "fsmRmtInvRslt": "",             "fsmStageDescr": "",
```

```
            "fsmStatus": "nop",             "fsmTry": "0",             "hotfix": "",
 "identifier": "ftd1",
            "operationalState": "online",
            "reasonForDebundle": "",
            "resourceProfileName": "RP20",
            "runningVersion": "7.1.0.90",
            "smAppAttribute": [
                {
                    "key": "firepower-mgmt-ip",
                    "rn": "app-attribute-firepower-mgmt-ip",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
firepower-mgmt-ip",
                    "value": "192.0.2.5"
                },
                {
                    "key": "ha-link-intf",
                    "rn": "app-attribute-ha-link-intf",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-link-intf",
                    "value": "Ethernet1/2"
                },
                {
                    "key": "ha-lan-intf",
                    "rn": "app-attribute-ha-lan-intf",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-lan-intf",
                    "value": "Ethernet1/2"
                },
                {
                    "key": "mgmt-url",
                    "rn": "app-attribute-mgmt-url",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-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. Para verificar la configuración del clúster FTD, utilice el identificador del dispositivo lógico en esta consulta:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.102/api/ld/ftd_cluster1'
{
    "smLogicalDevice": [
        {
            "description": "",
```

```
            "dn": "ld/ftd_cluster1",
            "errorMsg": "",
            "fsmDescr": "",
            "fsmProgr": "100",
            "fsmRmtInvErrCode": "none",
            "fsmRmtInvErrDescr": "",
            "fsmRmtInvRslt": "",
            "fsmStageDescr": "",
            "fsmStatus": "nop",
            "fsmTaskBits": "",
            "fsmTry": "0",
            "ldMode": "clustered",
            "linkStateSync": "disabled",
            "name": "ftd_cluster1",
            "operationalState": "ok",
   "slotId": "1",             "smClusterBootstrap": [                 {
"cclNetwork": "10.173.0.0",                    "chassisId": "1",
"gatewayv4": "0.0.0.0",                    "gatewayv6": "::",                    "key": "",
                    "mode": "spanned-etherchannel",                    "name": "ftd_cluster1",
                    "netmaskv4": "0.0.0.0",                    "poolEndv4": "0.0.0.0",
           "poolEndv6": "::",                    "poolStartv4": "0.0.0.0",
"poolStartv6": "::",                    "prefixLength": "",                    "rn": "cluster-
bootstrap",                    "siteId": "1",                    "supportCclSubnet":
"supported",                    "updateTimestamp": "2022-05-20T13:38:21.872",
                    "urllink": "https://192.0.2.101/api/ld/ftd_cluster1/cluster-bootstrap",
                    "virtualIPv4": "0.0.0.0",                    "virtualIPv6": "::"
                }             ], ...
```


4. Para verificar el estado del clúster de FTD, utilice esta consulta:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.102/api/slot/1/app-inst'
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_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",
...
```

Archivo show-tech del chasis FXOS

El estado y la configuración de alta disponibilidad y escalabilidad de FTD se pueden verificar en el archivo show-tech del chasis Firepower 4100/9300.

Siga estos pasos para verificar la configuración de alta disponibilidad y escalabilidad y el estado en el archivo show-tech del chasis FXOS:

1. Para las versiones 2.7 y posteriores de FXOS, abra el archivo **sam_techsupportinfo** en **<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Para versiones anteriores, abra el archivo **sam_techsupportinfo** en **FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar.**

2. Para verificar el estado de failover, verifique el valor del valor del atributo **ha-role** bajo el slot específico en la sección **`show slot extend detail` :**

```
# 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. Para verificar la configuración del clúster de FTD, verifique el valor del valor del atributo **Mode** en la ranura específica de la sección **`show Logical-device detail extend`** :

```
`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 el estado del clúster de FTD, verifique el valor de los valores de los atributos **Estado del clúster** y **Función del clúster** bajo el slot específico en la sección **`show slot expandetail`** :

```
`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 disponibilidad y escalabilidad de ASA

El estado y la configuración de alta disponibilidad y escalabilidad de ASA se pueden verificar con el uso de estas opciones:

- CLI de ASA
- sondeo de ASA SNMP
- archivo show-tech ASA
- Interfaz de usuario de FCM
- CLI FXOS
- FXOS REST-API
- Archivo show-tech del chasis FXOS

CLI de ASA

Siga estos pasos para verificar la configuración de alta disponibilidad y escalabilidad de ASA en ASA CLI:

1. Utilice estas opciones para acceder a ASA CLI de acuerdo con la plataforma y el modo de implementación:

- Acceso directo de Telnet/SSH a ASA en Firepower 1000/3100 y Firepower 2100 en modo de dispositivo
- Acceso desde la CLI de la consola FXOS en Firepower 2100 en el modo de plataforma y conexión a ASA a través del comando **connect asa**
- Acceso desde FXOS CLI a través de comandos (Firepower 4100/9300): **connect module <x> [console|telnet],** donde x es el ID de ranura, y luego **connect asa**

- Para ASA virtual, acceso SSH directo al ASA o acceso a la consola desde el hipervisor o la interfaz de usuario de la nube

2. Para verificar la configuración y el estado de failover de ASA, ejecute los comandos **show running-config failover** y **show failover state** en la CLI de ASA.

Si no se configura la conmutación por fallas, se muestra este resultado:

```
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==
```

Si se configura la conmutación por fallas, se muestra este resultado:

```
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. Para verificar la configuración y el estado del clúster ASA, ejecute los comandos **show running-config cluster** y **show cluster info** en la CLI.

Si el clúster no está configurado, se muestra este resultado:

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

Si se configura el clúster, se muestra este resultado:

```
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
...
```

SNMP ASA

Siga estos pasos para verificar la configuración de alta disponibilidad y escalabilidad de ASA a través de SNMP:

1. Asegúrese de que SNMP esté configurado y habilitado.

2. Para verificar la configuración de failover y el sondeo de estado, el OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1.

Si no se configura la conmutación por fallas, se muestra este resultado:

```
# 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"
```

Si se configura la conmutación por fallas, se muestra este resultado:

```
# 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 la configuración y el estado del clúster, sondee el OID 1.3.6.1.4.1.9.9.491.1.8.1.

Si el clúster no está configurado, se muestra este resultado:

```
# 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
```

Si el clúster está configurado, pero no habilitado, se muestra este resultado:

```
# 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
...
```

Si el clúster está configurado, habilitado y en funcionamiento, se muestra este resultado:

```
# 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 obtener más información sobre las descripciones de OID, refiérase a CISCO-UNIFIED-FIREWALL-MIB.

archivo show-tech ASA

1. Para verificar la configuración y el estado de failover de ASA, verifique la sección **show failover**.

Si no se configura la conmutación por fallas, se muestra este resultado:

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

Si se configura la conmutación por fallas, se muestra este resultado:

```
----------------- 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 la configuración del clúster y el estado, verifique la sección **show cluster info**.

Si el clúster no está configurado, se muestra este resultado:

```
------------------ show cluster info ------------------
Clustering is not configured
```

Si el clúster está configurado y habilitado, se muestra este resultado:

```
------------------ 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
...
```

Interfaz de usuario de FCM

Siga los pasos de la sección.

CLI FXOS

Siga los pasos de la sección.

FXOS REST-API

Siga los pasos de la sección.

Archivo show-tech del chasis FXOS

Siga los pasos de la sección.

Verificar el modo Firewall

modo Firewall FTD

El modo de firewall hace referencia a una configuración de firewall ruteada o transparente.

El modo de firewall FTD se puede verificar con estas opciones:

- CLI FTD
- show-tech de FTD
- Interfaz de usuario de FMC
- FMC REST-API
- Interfaz de usuario de FCM
- CLI FXOS
- FXOS REST-API
- Archivo show-tech del chasis FXOS

Nota: FDM no admite el modo transparente.

CLI FTD

Siga estos pasos para verificar el modo de firewall FTD en la CLI de FTD:

1. Utilice estas opciones para acceder a la CLI de FTD de acuerdo con la plataforma y el modo de implementación:

- Acceso SSH directo a FTD: todas las plataformas
- Acceso desde la CLI de la consola FXOS (Firepower 1000/2100/3100) a través del comando **connect ftd**
- Acceso desde la CLI de FXOS a través de comandos (Firepower 4100/9300): **connect module <x> [console|telnet],** donde x es el ID de ranura, y luego

  connect ftd [instance], donde la instancia sólo es relevante para la implementación de varias instancias.

- Para los FTD virtuales, acceso SSH directo a FTD o acceso a la consola desde el hipervisor o la interfaz de usuario de la nube

2. Para verificar el modo de firewall, ejecute el comando **show firewall** en la CLI:

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

Archivo de Troubleshooting de FTD

Siga estos pasos para verificar el modo de firewall FTD en el archivo de solución de problemas FTD:

1. Abra el archivo de solución de problemas y navegue hasta la carpeta **<filename>-trouTroubleshooting .tar/results-<date>—xxxxxx/command-output.**

2. Abra el archivo **usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output:**

```
# pwd
/ngfw/var/common/results-05-22-2022--102758/command-outputs
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

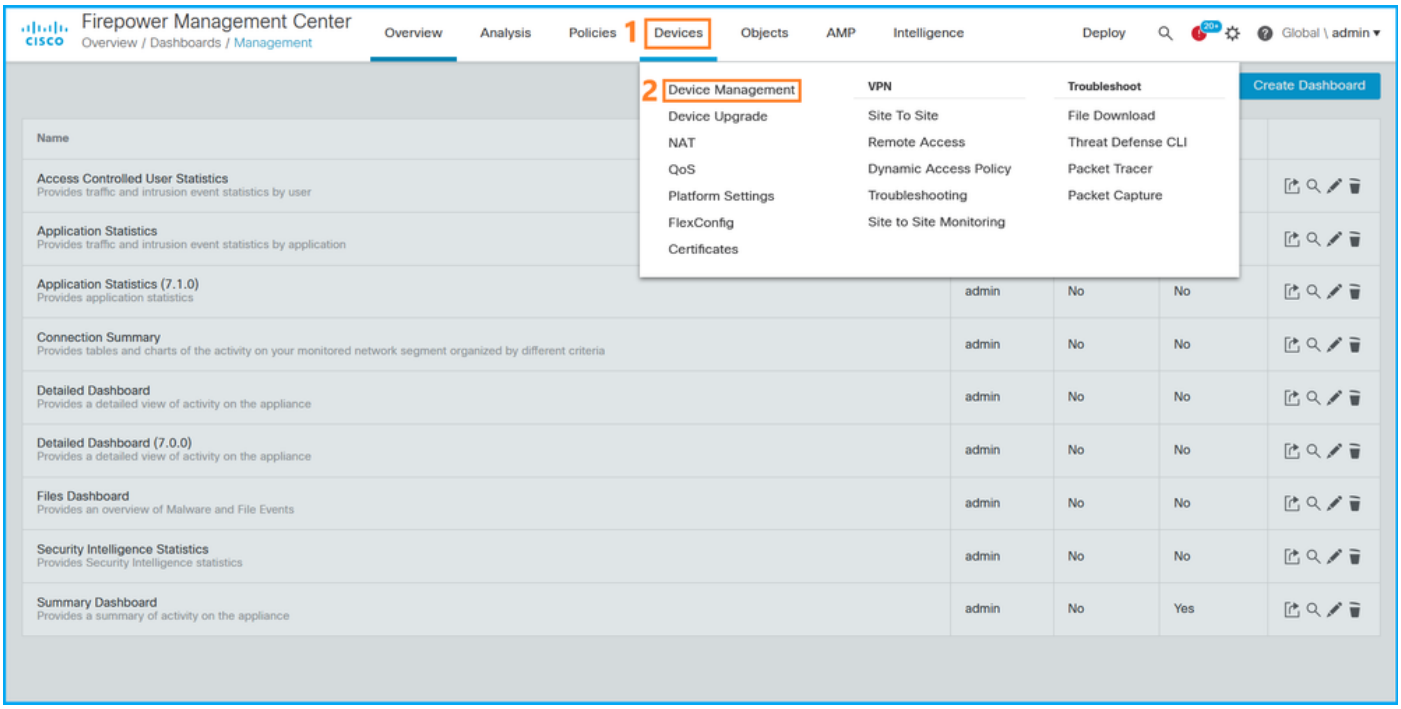
3. Para verificar el modo de firewall FTD, verifique la sección **show firewall**:

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

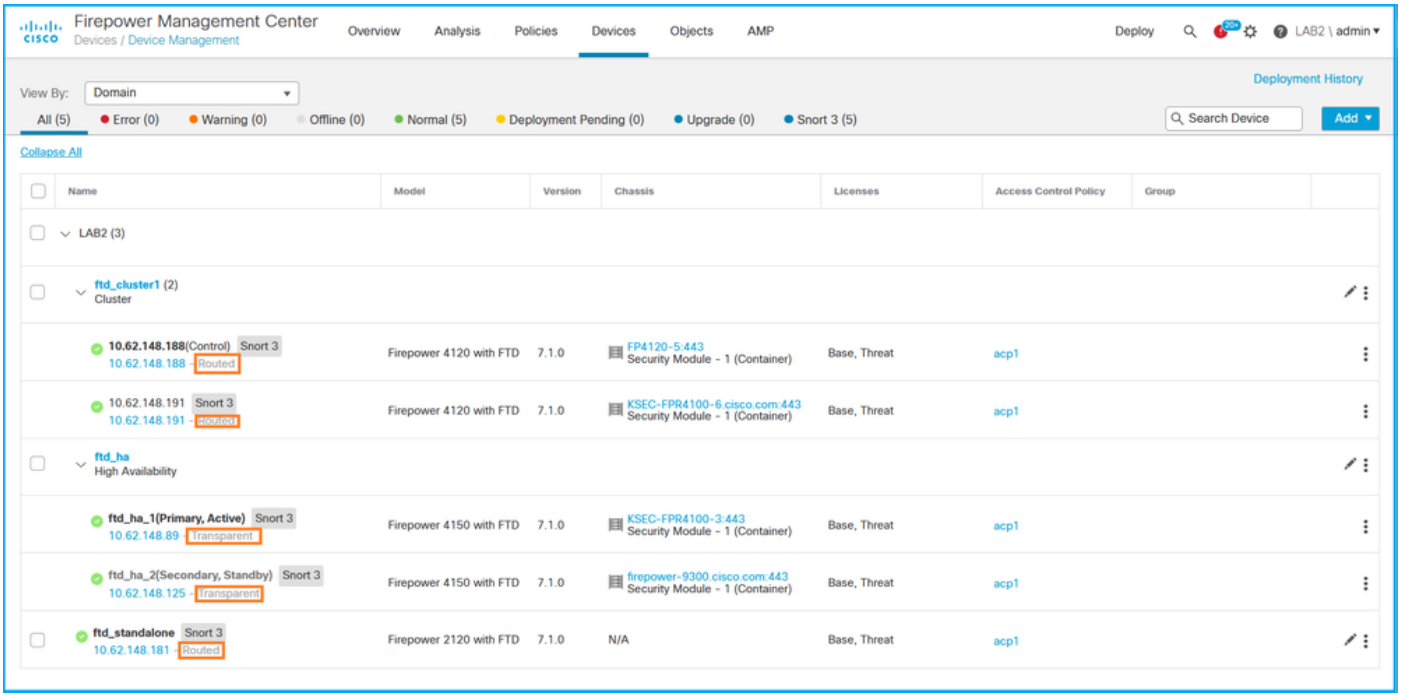
Interfaz de usuario de FMC

Siga estos pasos para verificar el modo de firewall FTD en la interfaz de usuario de FMC:

1. Elija **Devices > Device Management**:



2. Verifique las etiquetas **Ruteadas** o **Transparentes**:



FMC REST-API

Siga estos pasos para verificar el modo de firewall FTD a través de FMC REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Identifique el dominio que contiene el dispositivo. En la mayoría de las consultas de la API REST, el parámetro **domain** es obligatorio. Utilice el token en esta consulta para recuperar la lista de dominios:

```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
  "items":
[
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
        },
...
```

3. Utilice el UUID de dominio para consultar los **registros** de **dispositivos** específicos y el UUID de dispositivo específico:

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

4. Utilice el UUID de dominio y el UUID de dispositivo/contenedor del Paso 3 en esta consulta, y verifique el valor de **ftdMode**:

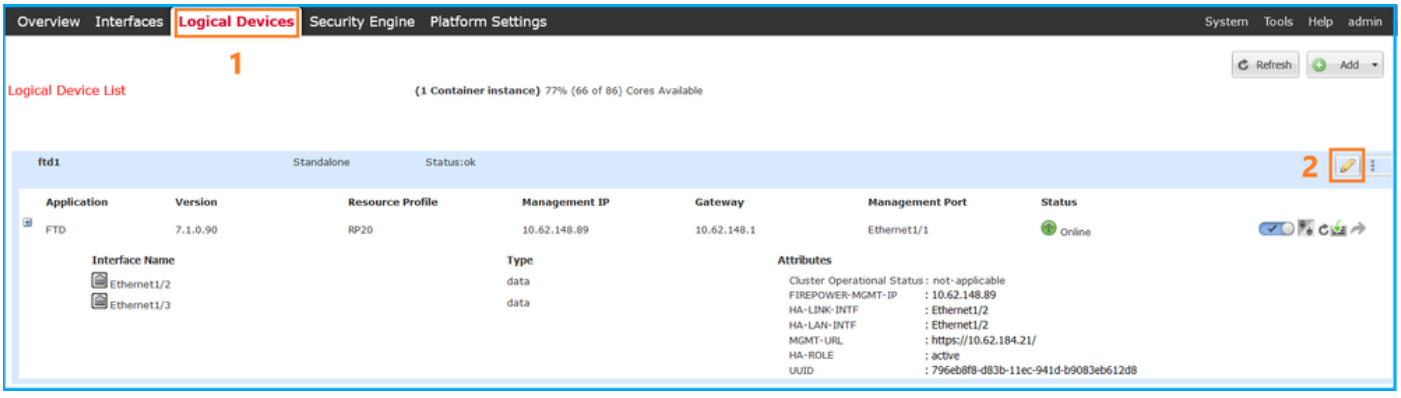
```
# curl -s -k -X 'GET'  'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept: application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
{
    "accessPolicy": {
        "id": "00505691-3a23-0ed3-0006-536940224514",
        "name": "acp1",
        "type": "AccessPolicy"
    },
    "advanced": {
        "enableOGS": false
    },
    "description": "NOT SUPPORTED",
    "ftdMode": "ROUTED",
...
```

Interfaz de usuario de FCM

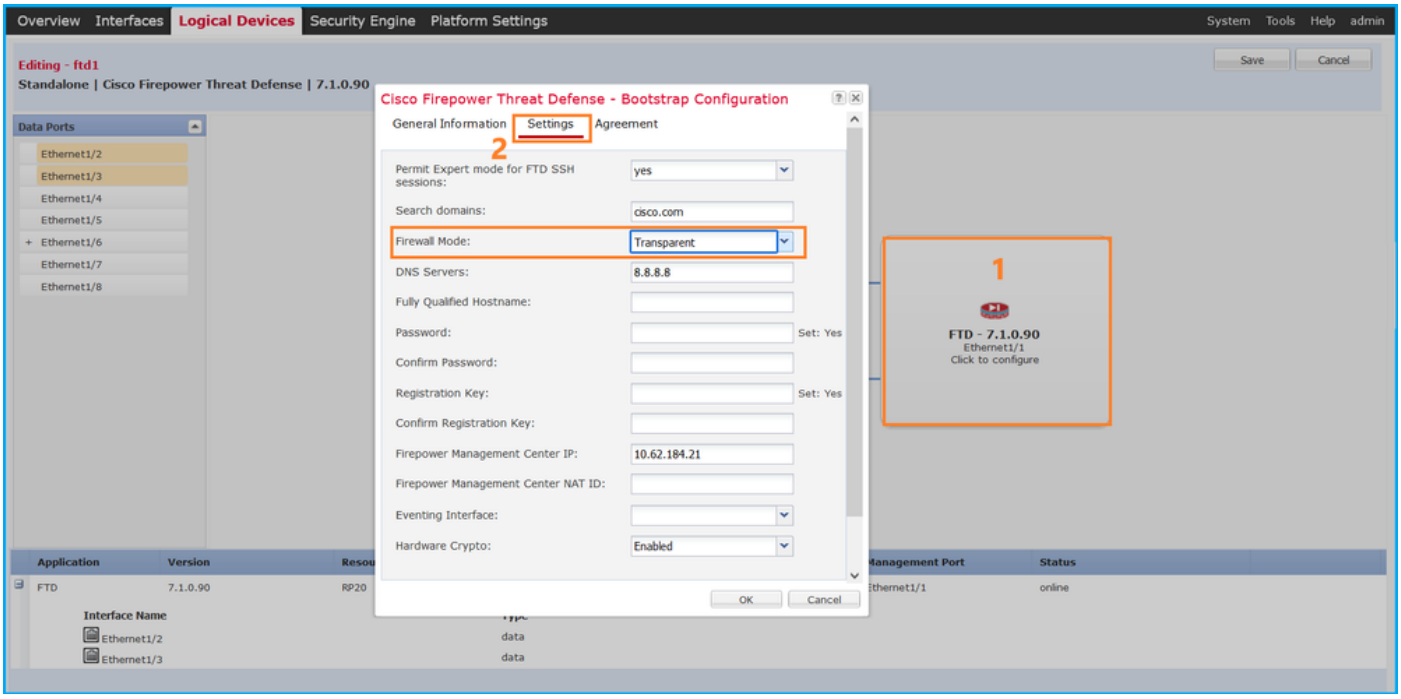
El modo de firewall se puede verificar para FTD en Firepower 4100/9300.

Siga estos pasos para verificar el modo de firewall FTD en la interfaz de usuario de FCM:

1. Edite el dispositivo lógico en la página **Dispositivos lógicos**:



2. Haga clic en el icono de la aplicación y verifique el **Modo Firewall** en la **ficha Configuración**:



CLI FXOS

El modo de firewall se puede verificar para FTD en Firepower 4100/9300.

Siga estos pasos para verificar el modo de firewall FTD en la CLI de FXOS:

1. Establezca una conexión de consola o SSH al chasis.
2. Cambie al alcance ssa, luego cambie al **dispositivo lógico** específico**, ejecute el comando show mgmt-bootstrap expanda** y verifique el valor del atributo FIREWALL_MODE:

```
firepower# scope ssa
firepower /ssa # scope logical-device ftd_cluster1
firepower /ssa/logical-device # show mgmt-bootstrap expand

Management Configuration:
    App Name: ftd

    Secret Bootstrap Key:
        Key                       Value
        ------------------------- -----
        PASSWORD
        REGISTRATION_KEY

    IP v4:
        Slot ID    Management Sub Type IP Address      Netmask         Gateway         Last
Updated Timestamp
        ---------- ------------------ -------------- --------------- --------------- ---------
-------------
                1 Firepower           10.62.148.188   255.255.255.128 10.62.148.129   2022-05-
20T13:50:06.238

    Bootstrap Key:
        Key                       Value
        ------------------------- -----
        DNS_SERVERS               192.0.2.250
        FIREPOWER_MANAGER_IP      10.62.184.21
        FIREWALL_MODE             routed
```

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

FXOS REST API

FXOS REST-API es compatible con Firepower 4100/9300.

Siga estos pasos para verificar el modo de firewall FTD a través de la solicitud FXOS REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Utilice el identificador de dispositivo lógico en esta consulta y verifique el valor de la clave **FIREWALL_MODE**:

```
# 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/ld/ftd_cluster1/mgmt-
bootstrap/ftd/key/FIREWALL_MODE",
                            "value": "routed"
                        },
...
```

Archivo show-tech del chasis FXOS

El modo de firewall para FTD se puede verificar en el archivo show-tech de Firepower 4100/9300.

Siga estos pasos para verificar el modo de firewall FTD en el archivo show-tech del chasis FXOS:

1. Para las versiones 2.7 y posteriores de FXOS, abra el archivo **sam_techsupportinfo** en **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

   Para versiones anteriores, abra el archivo **sam_techsupportinfo** en **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Verifique la sección **"show Logical-device detail extend"** bajo el identificador específico y la ranura:

```
# 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
...
```

modo Firewall ASA

El modo de firewall ASA se puede verificar con estas opciones:

- CLI de ASA
- show-tech ASA
- Interfaz de usuario de FCM
- CLI FXOS
- FXOS REST-API
- Archivo show-tech del chasis FXOS

CLI de ASA

Siga estos pasos para verificar el modo de firewall ASA en ASA CLI:

1. Utilice estas opciones para acceder a ASA CLI de acuerdo con la plataforma y el modo de implementación:

- Acceso directo de Telnet/SSH a ASA en Firepower 1000/3100 y Firepower 2100 en modo de dispositivo
- Acceso desde la CLI de la consola FXOS en Firepower 2100 en el modo de plataforma y conexión a ASA a través del comando **connect asa**
- Acceso desde FXOS CLI a través de comandos (Firepower 4100/9300): **connect module <x> [console|telnet],** donde x es el ID de ranura, y luego **connect asa**

- Para ASA virtual, acceso SSH directo al ASA o acceso a la consola desde el hipervisor o la interfaz de usuario de la nube

2. Ejecute el comando **show firewall** en la CLI:

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

archivo show-tech ASA

Para verificar el modo de firewall ASA, verifique la sección **show firewall**:

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

Interfaz de usuario de FCM

Siga los pasos de la sección.

CLI FXOS

Siga los pasos de la sección.

FXOS REST-API

Siga los pasos de la sección.

Archivo show-tech del chasis FXOS

Siga los pasos de la sección.

Verificar tipo de implementación de instancia

Hay dos tipos de implementación de instancias de aplicación:

- Instancia nativa: una instancia nativa utiliza todos los recursos (CPU, RAM y espacio en disco) del módulo/motor de seguridad, por lo que sólo puede instalar una instancia nativa.
- Instancia de contenedor: una instancia de contenedor utiliza un subconjunto de recursos del módulo/motor de seguridad. La capacidad de varias instancias sólo se admite para el FTD administrado por FMC; no es compatible con el ASA o el FTD administrado por FDM.

La configuración de la instancia del modo contenedor se soporta solamente para FTD en Firepower 4100/9300.

El tipo de implementación de instancia se puede verificar con el uso de estas opciones:

- CLI FTD
- FTD Show-tech
- Interfaz de usuario de FMC
- FMC REST-API
- Interfaz de usuario de FCM
- CLI FXOS
- FXOS REST-API

- Archivo show-tech del chasis FXOS

CLI FTD

Siga estos pasos para verificar el tipo de implementación de instancia de FTD en la CLI de FTD:

1. Utilice estas opciones para acceder a la CLI de FTD de acuerdo con la plataforma y el modo de implementación:

- Acceso SSH directo a FTD: todas las plataformas
- Acceso desde la CLI de FXOS a través de comandos (Firepower 4100/9300):

connect module <x> [console|telnet], donde x es el ID de ranura, y luego **connect ftd [instance],** donde la instancia sólo es relevante para la implementación de instancias múltiples.

2. Ejecute el comando **show version system** y verifique la línea con la cadena **SSP Slot Number**. Si el **contenedor** existe en esta línea, el FTD se ejecuta en modo contenedor:

```
> 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)
…
```

Archivo de Troubleshooting de FTD

Siga estos pasos para verificar el tipo de implementación de instancia de FTD en el archivo de solución de problemas de FTD:

1. Abra el archivo de solución de problemas y navegue hasta la carpeta **<filename>-trouTroubleshooting .tar/results-<date>—xxxxxx/command-output.**
2. Abra el archivo **usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output:**

```
# pwd
/ngfw/var/common/results-05-22-2022--102758/command-outputs
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

3. Verifique la línea con la cadena **SSP Slot Number**. Si el **contenedor** existe en esta línea, el FTD se ejecuta en modo contenedor:

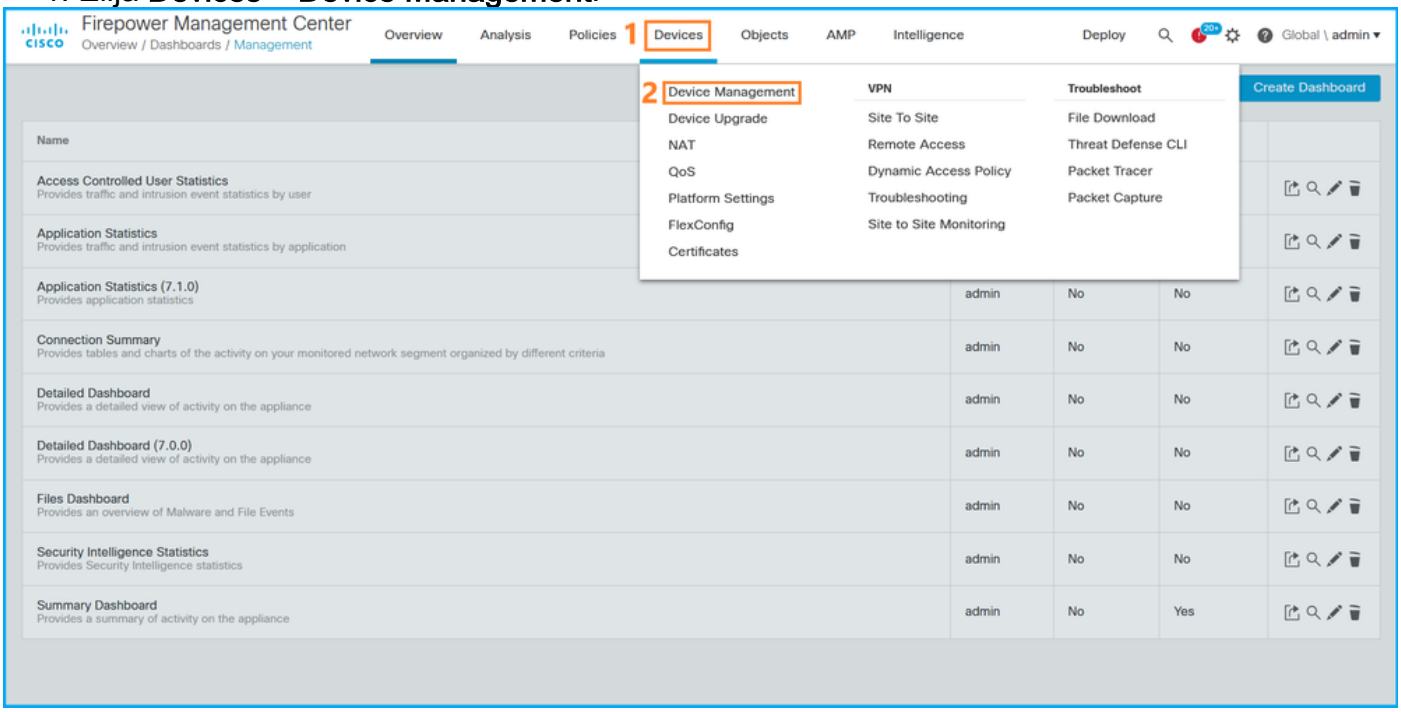
```
------------------[ firepower ]--------------------
```

```
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)
…
```

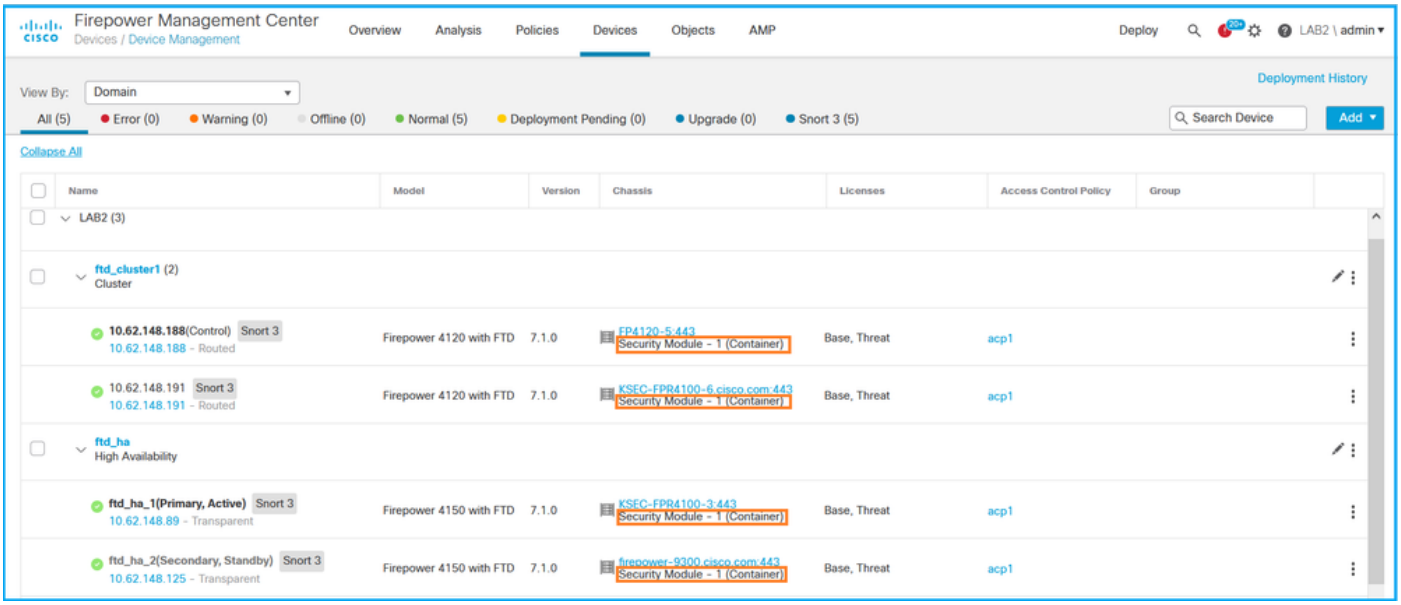
Interfaz de usuario de FMC

Siga estos pasos para verificar el tipo de implementación de instancia de FTD en la interfaz de usuario de FMC:

1. Elija **Devices > Device Management**:



2. Compruebe la columna **Chasis**. Si el **contenedor** existe en la línea, el FTD se ejecuta en modo contenedor.



FMC REST-API

Siga estos pasos para verificar el tipo de implementación de instancia de FTD a través de FMC REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Identifique el dominio que contiene el dispositivo. En la mayoría de las consultas de la API REST, el parámetro **domain** es obligatorio. Utilice el token en esta consulta para recuperar la lista de dominios:

```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
{
  "items":
[
        {
            "name": "Global",
            "type": "Domain",
            "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
        },
        {
            "name": "Global/LAB2",
            "type": "Domain",
            "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
        },
...
```

3. Utilice el UUID de dominio para consultar los **registros** de **dispositivos** específicos y el UUID de dispositivo específico:

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

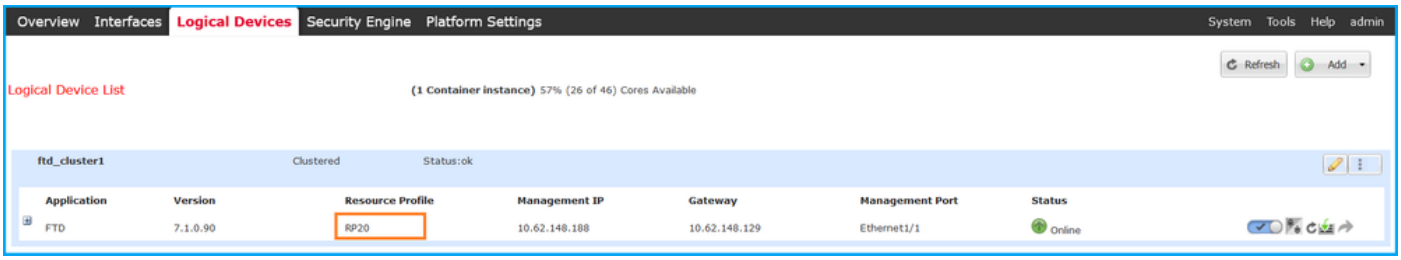
```
{
    "items": [
        {
            "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
            },
            "name": "ftd_ha_1",
            "type": "Device"
        },
...
```

4. Utilice el dominio UUID y el dispositivo/contenedor UUID del Paso 3 en esta consulta y verifique el valor de **isMultiInstance**:

```
# curl -s -k -X 'GET'  'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
...
            "name": "ftd_cluster1",
     "isMultiInstance": true,
...
```

Interfaz de usuario de FCM

Para verificar el tipo de implementación de instancia de FTD, verifique el valor del atributo **Resource Profile** en Logical Devices. Si el valor no está vacío, el FTD se ejecuta en modo contenedor:



CLI FXOS

Siga estos pasos para verificar el tipo de implementación de instancia de FTD en la CLI de FXOS:

1. Establezca una conexión de consola o SSH al chasis.
2. Cambie al **scope ssa** y ejecute el comando **show app-instance** y luego verifique la columna **Deploy Type** del FTD específico basado en la ranura y el identificador:

```
firepower # scope ssa
firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup Version
Deploy Type Turbo Mode Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- -------------- -------------- --
--------- ---------- ------------ --------------- ------------
ftd        ftd_cluster1 1          Enabled     Online          7.1.0.90       7.1.0.90
Container   No         RP20         In Cluster      Master
```

FXOS REST API

Siga estos pasos para verificar el tipo de implementación de instancia de FTD a través de una solicitud FXOS REST-API. Utilice un cliente REST-API. En este ejemplo, se utiliza **curl**:

1. Solicitar un token de autenticación:

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

2. Especifique el token, el ID de ranura en esta consulta y verifique el valor de **DeployType**:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
https://192.0.2.100/api/slot/1/app-inst
… {     "smAppInstance": [         {             "adminState": "enabled",             "appDn":
"sec-svc/app-ftd-7.1.0.90",             "appInstId": "ftd_001_JAD201200R43VLP1G3",
"appName": "ftd",             "clearLogData": "available",
"clusterOperationalState": "not-applicable",             "clusterRole": "none",
"currentJobProgress": "100",             "currentJobState": "succeeded",
"currentJobType": "start",             "deployType": "container",
...
```

Archivo show-tech del chasis FXOS

Siga estos pasos para verificar el modo de firewall FTD en el archivo show-tech del chasis FXOS:

1. Para las versiones 2.7 y posteriores de FXOS, abra el archivo **sam_techsupportinfo** en **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Para versiones anteriores, abra el archivo **sam_techsupportinfo** en **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Verifique la sección **"mostrar detalles de expansión de ranura"** para el slot específico y el identificador:

```
# 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
```

Verificar el modo de contexto ASA

ASA admite modos de contexto único y múltiple. FTD no admite el modo multicontexto.

El tipo de contexto se puede verificar con el uso de estas opciones:

- CLI de ASA
- show-tech ASA

CLI de ASA

Siga estos pasos para verificar el modo de contexto ASA en ASA CLI:

1. Utilice estas opciones para acceder a ASA CLI de acuerdo con la plataforma y el modo de implementación:

- Acceso directo de Telnet/SSH a ASA en Firepower 1000/3100 y Firepower 2100 en modo de dispositivo
- Acceso desde la CLI de la consola FXOS en Firepower 2100 en el modo de plataforma y conexión a ASA a través del comando **connect asa**
- Acceso desde FXOS CLI a través de comandos (Firepower 4100/9300): **connect module <x> [console|telnet],** donde x es el ID de ranura, y luego **connect asa**

- Para ASA virtual, acceso SSH directo al ASA o acceso a la consola desde el hipervisor o la interfaz de usuario de la nube

2. Ejecute el comando **show mode** en la CLI:

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

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

archivo show-tech ASA

Siga estos pasos para verificar el modo de contexto ASA en el archivo show-tech ASA:

1. Verifique la sección **show context detail** en el archivo show-tech. En este caso, el modo de contexto es múltiple ya que hay varios contextos:

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

Verifique el modo Firepower 2100 con ASA

Firepower 2100 con ASA puede ejecutarse en uno de estos modos:

- Modo de plataforma: los parámetros operativos básicos y la configuración de la interfaz de hardware se configuran en FXOS. Estos parámetros incluyen el cambio de estado de administración de las interfaces, la configuración de EtherChannel, NTP, la administración de imágenes y mucho más. La interfaz web de FCM o FXOS CLI se pueden utilizar para la configuración de FXOS.
- Modo de dispositivo (el valor predeterminado): el modo de dispositivo permite a los usuarios configurar todas las políticas en el ASA. Solamente los comandos avanzados están disponibles en la CLI de FXOS.

El modo Firepower 2100 con ASA debe verificarse con el uso de estas opciones:

- CLI de ASA
- CLI FXOS
- FXOS show-tech

CLI de ASA

Siga estos pasos para verificar el modo Firepower 2100 con ASA en ASA CLI:

1. Utilice telnet/SSH para acceder al ASA en Firepower 2100.

2. Ejecute el comando **show fxos mode** en la CLI:

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

Modo de dispositivo:

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

> **Nota:** En el modo multicontexto, el comando **show fxos mode** está disponible en el **sistema** o en el contexto **admin** .

CLI FXOS

Siga estos pasos para verificar el modo Firepower 2100 con ASA en la CLI de FXOS:

1. Utilice telnet/SSH para acceder al ASA en Firepower 2100.

2. Ejecute el comando **connect fxos**:

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

> **Nota:** En el modo multicontexto, el comando **connect fxos** está disponible en el contexto **admin**.

3. Ejecute el comando **show fxos-mode**:

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

Modo de dispositivo:

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

archivo show-tech FXOS

Siga estos pasos para verificar el modo Firepower 2100 con ASA en el archivo show-tech del chasis FXOS:

1. Abrir archivo **tech_support_brief** en **<name>_FPRM.tar.gz/<name>_FPRM.tar**

2. Verifique la sección **`show fxos-mode`**:

```
# pwd
```

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

Modo de dispositivo:

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

Problemas conocidos

Id. de bug Cisco CSCwb94424 ENH: Agregar un comando CLISH para la verificación de la configuración FMC HA

Id. de bug Cisco CSCvn31622 ENH: Agregar OID SNMP de FXOS para sondear la configuración de instancias de aplicaciones y dispositivos lógicos

Id. de bug Cisco CSCwb97767 ENH: Agregar OID para la verificación del tipo de implementación de instancia de FTD

Id. de bug Cisco CSCwb97772 ENH: Incluya la salida de 'show fxos mode' en show-tech de ASA en Firepower 2100

Id. de bug Cisco CSCwb97751 OID 1.3.6.1.4.1.9.9.491.1.6.1.1 para la verificación del modo de firewall transparente no está disponible

Información Relacionada

- Guía de inicio rápido de la API REST de Secure Firewall Management Center, versión 7.1
- Configuración de SNMP en dispositivos Firepower NGFW
- Guía de API REST de Cisco Firepower Threat Defense
- Referencia de API REST de Cisco FXOS
- Compatibilidad con Cisco ASA
- Firepower 1000/2100 y Secure Firewall 3100 ASA y versiones de paquetes FXOS
- Componentes empaquetados
- Solución de problemas de Firepower, procedimientos de generación de archivos
- Guía de inicio de Cisco Firepower 2100
- Guía de compatibilidad de Cisco Firepower Threat Defense