

Controleer de Firepower Mode, Instance, hoge beschikbaarheid en schaalbaarheidsconfiguratie

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Controleer de configuratie van hoge beschikbaarheid en schaalbaarheid](#)

[FMC hoge beschikbaarheid](#)

[FMC UI](#)

[FMC CLI](#)

[FMC REST-API](#)

[FMC-bestand voor probleemoplossing](#)

[FDM hoge beschikbaarheid](#)

[FDM UI](#)

[FDM REST-API](#)

[FTD CLI](#)

[FTD SNMP-stemming](#)

[FTD Problemen oplossen](#)

[FTD hoge beschikbaarheid en schaalbaarheid](#)

[FTD CLI](#)

[FTD SNMP](#)

[FTD Problemen oplossen](#)

[FMC UI](#)

[FMC REST API](#)

[FDM UI](#)

[FDM REST-API](#)

[FCM UI](#)

[FXOS CLI](#)

[FXOS REST API](#)

[FXOS-chassis testbestand](#)

[ASA hoge beschikbaarheid en schaalbaarheid](#)

[ASA CLI](#)

[ASA SNMP](#)

[ASA show-tech-bestand](#)

[FCM UI](#)

[FXOS CLI](#)

[FXOS REST-API](#)

[FXOS-chassis testbestand](#)

[Controleer de firewallmodus](#)

[FTD-firewallmodus](#)
[FTD CLI](#)
[FTD Problemen oplossen](#)
[FMC UI](#)
[FMC REST-API](#)
[FCM UI](#)
[FXOS CLI](#)
[FXOS REST API](#)
[FXOS-chassis testbestand](#)
[ASA-firewallmodus](#)
[ASA CLI](#)
[ASA show-tech-bestand](#)
[FCM UI](#)
[FXOS CLI](#)
[FXOS REST-API](#)
[FXOS-chassis testbestand](#)
[Verifiëren van type installatie](#)
[FTD CLI](#)
[FTD Problemen oplossen](#)
[FMC UI](#)
[FMC REST-API](#)
[FCM UI](#)
[FXOS CLI](#)
[FXOS REST API](#)
[FXOS-chassis testbestand](#)
[Controleer de ASA-context-modus](#)
[ASA CLI](#)
[ASA show-tech-bestand](#)
[Controleer de Firepower 2100-modus met ASA](#)
[ASA CLI](#)
[FXOS CLI](#)
[FXOS-toontechnisch bestand](#)
[Bekende problemen](#)
[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de verificatie van de hoge beschikbaarheid en schaalbaarheid van Firepower configuratie, firewallmodus en installatietype.

Achtergrondinformatie

De verificatiestappen voor de hoge beschikbaarheid en schaalbaarheidsconfiguratie, firewallmodus en installatietype worden weergegeven op de gebruikersinterface (UI), de

opdrachtregeel interface (CLI), via REST-API vragen, SNMP en in het probleemoplossingsbestand.

Voorwaarden

Vereisten

Basisproductkennis, REST-API, SNMP.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) versie 7.1.x
- Firepower eXtenable Operating System (FXOS) 2.11.1.x
- Firepower Apparaatbeheer (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

Controleer de configuratie van hoge beschikbaarheid en schaalbaarheid

Hoge beschikbaarheid verwijst naar de configuratie van de overnameconnector. Hoge beschikbaarheid of failover-instelling voegen zich bij twee apparaten zodat als een van de apparaten faalt, het andere apparaat kan overnemen.

Schaalbaarheid verwijst naar de clusterconfiguratie. Met een clusterconfiguratie kunt u meerdere FTD-knooppunten samenvoegen als één logisch apparaat. Een cluster biedt het gemak van één apparaat (beheer, integratie in een netwerk) en de verhoogde doorvoersnelheid en redundantie van meerdere apparaten.

In dit document worden deze uitdrukkingen uitwisselbaar gebruikt:

- hoge beschikbaarheid of failover
- schaalbaarheid of cluster

In sommige gevallen is de verificatie van hoge beschikbaarheid en schaalbaarheidsconfiguratie of -status niet beschikbaar. Er is bijvoorbeeld geen verificatieopdracht voor standalone FTD-configuratie. Standalone, failover, en clusterconfiguratie modi zijn wederzijds exclusief. Als een

apparaat geen failover- en clusterconfiguratie heeft, wordt het geacht te werken in standalone modus.

FMC hoge beschikbaarheid

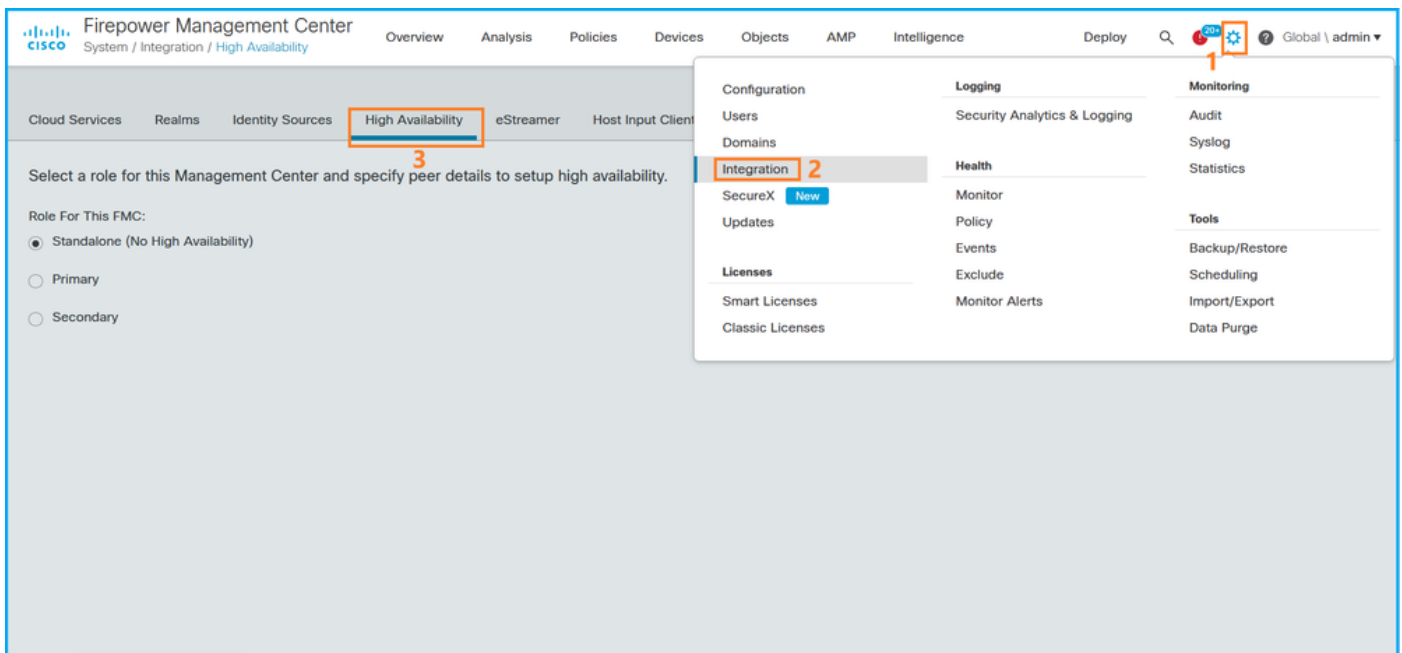
De configuratie en de status van een hoge beschikbaarheid van het VMC kunnen met behulp van deze opties worden geverifieerd:

- FMC UI
- FMC CLI
- REST API-verzoek
- FMC-bestand voor probleemoplossing

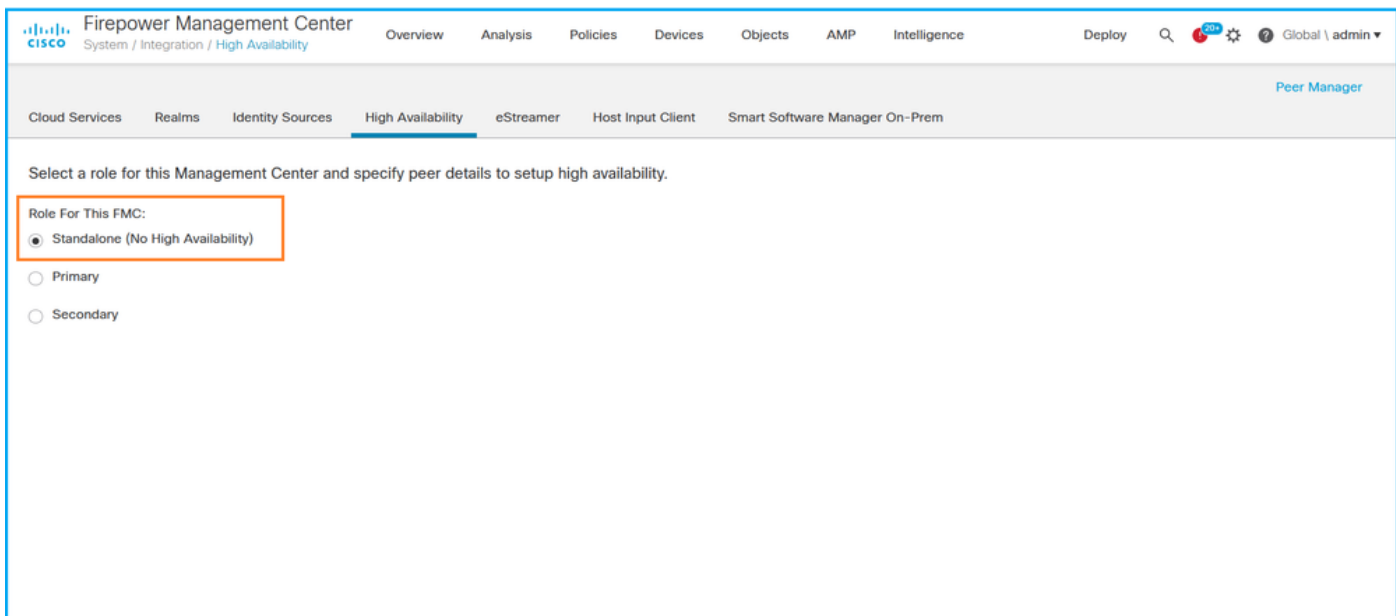
FMC UI

Volg deze stappen om de configuratie en de status van de FMC hoge beschikbaarheid op de FMC UI te controleren:

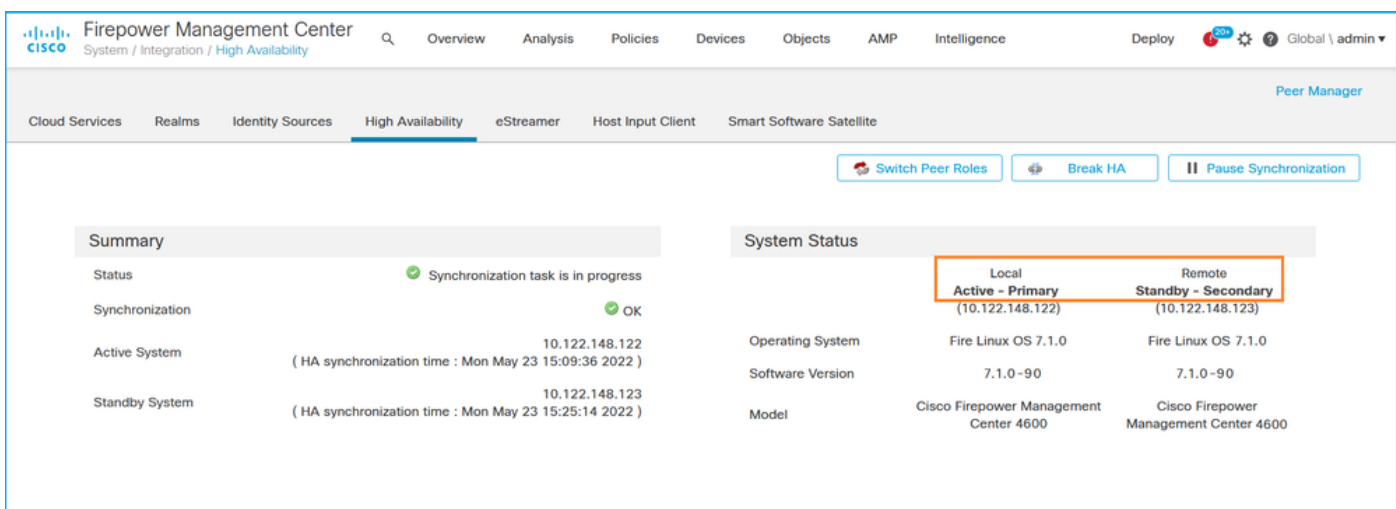
1. Kies **stysteem > Integratie > hoge beschikbaarheid**:



2. Controleer de rol van het VCC. In dit geval wordt een hoge beschikbaarheid niet ingesteld en werkt FMC in een standalone configuratie:



Als een hoge beschikbaarheid is ingesteld, worden de lokale en externe rollen weergegeven:



FMC CLI

Volg deze stappen om de configuratie en de status van de FMC met een hoge beschikbaarheid op de FMC-CLI te controleren:

1. Toegang tot VCC via SSH- of console-verbinding.
2. Start de opdracht van de **expert** en voer vervolgens de **sudo su**-opdracht uit:

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

3. Start de opdracht **probleemoplossing_HADC.pl** en selecteer optie **1 HA-informatie van FMC tonen**. Als een hoge beschikbaarheid niet is ingesteld, wordt deze uitvoer weergegeven:

```
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

Als een hoge beschikbaarheid is ingesteld, wordt deze uitvoer weergegeven:

```

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

```

Opmerking: Bij een hoge beschikbaarheid kan de FMC-rol een primaire of secundaire rol hebben, en **actieve** of **stand-by** status.

FMC REST-API

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van het FMC te controleren via FMC REST-API. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```

# 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. Gebruik het token in deze zoekopdracht om de UUID van het wereldwijde domein te vinden:

```
# 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
  }
}
```

Opmerking: Het gedeelte "| python -m json.tool" van de opdrachtstring wordt gebruikt om de uitvoer in JSON-stijl op te maken en is optioneel.

3. Gebruik het globale domein UID in deze zoekopdracht:

```
# 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
```

Als een hoge beschikbaarheid niet is ingesteld, wordt deze uitvoer weergegeven:

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

Als een hoge beschikbaarheid is ingesteld, wordt deze uitvoer weergegeven:

```

{
  "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": "FMCHASstatus"
    }
  ],
  "links": {
    "self": "https://192.0.2.1/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/integration/fmchastatuses?offset=0&limit=25"
  },
  "paging": {
    "count": 1,
    "limit": 25,
    "offset": 0,
    "pages": 1
  }
}

```

FMC-bestand voor probleemoplossing

Volg deze stappen om de configuratie en de status van de hoge beschikbaarheid van het FMC in het bestand voor probleemoplossing van het FMC te controleren:

1. Open het bestand voor probleemoplossing en navigeer naar de map **<bestandsnaam>.tar/resultaat-<date>—xxxxxx/commando-outputs**

2. Open het bestand **usr-local-sf-bin-problemlshoot_HADC.pl -a.output**:

Als een hoge beschikbaarheid niet is ingesteld, wordt deze uitvoer weergegeven:

```

# 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

Als een hoge beschikbaarheid is ingesteld, wordt deze uitvoer weergegeven:

```
# 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

FDM hoge beschikbaarheid

De FDM-configuratie en -status met een hoge beschikbaarheid kunnen met behulp van deze opties worden geverifieerd:

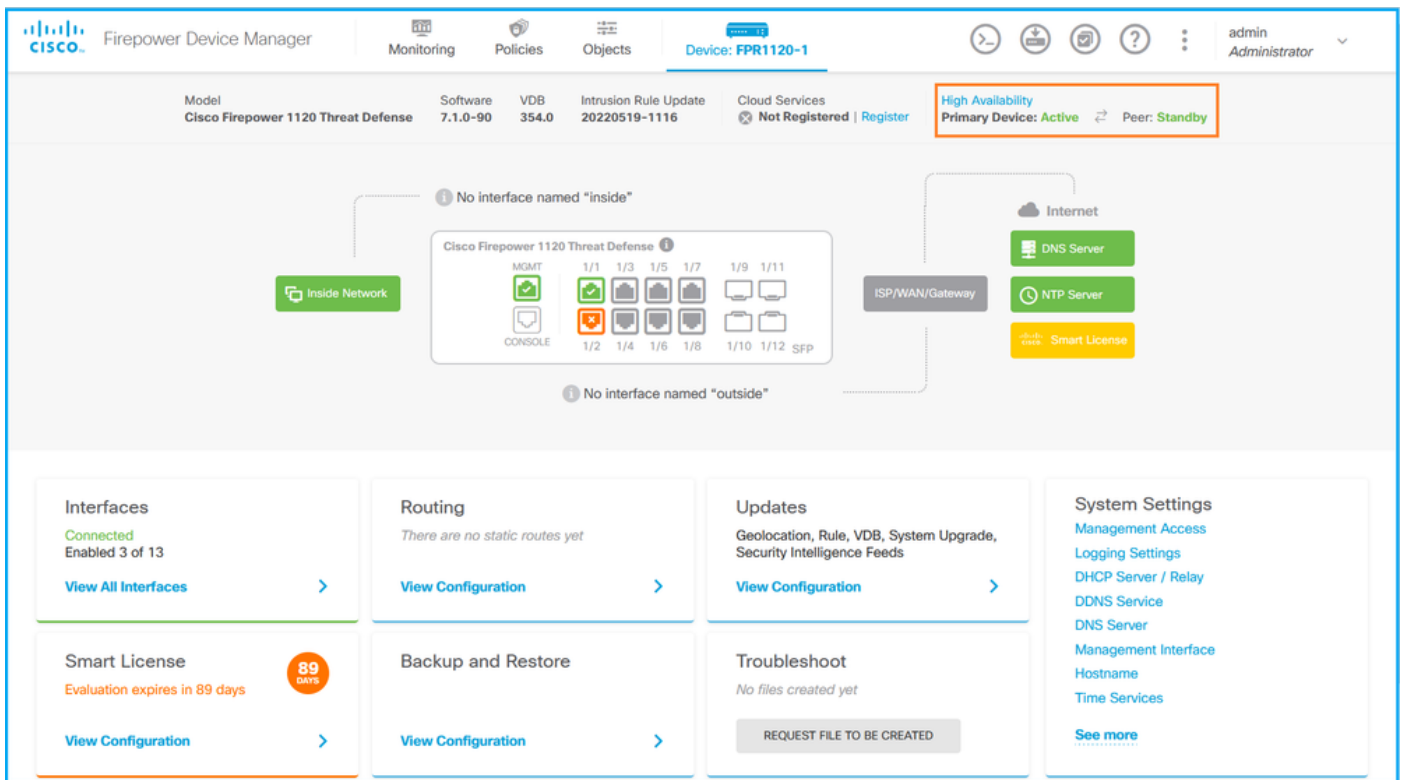
- FDM UI
- FDM REST API-verzoek
- FTD CLI
- FTD SNMP-stemming
- FTD Problemen oplossen

FDM UI

Om de FDM-configuratie en -status voor hoge beschikbaarheid op FDM UI te controleren, controleert u **hoge beschikbaarheid** op de hoofdpagina. Als een hoge beschikbaarheid niet is ingesteld wordt de **hoge beschikbaarheid niet ingesteld**:

The screenshot shows the Cisco Firepower Device Manager (FDM) interface for a Cisco Firepower 1120 Threat Defense device. The top navigation bar includes 'Monitoring', 'Policies', and 'Objects'. The device status is 'Device: FPR1120-1'. The 'High Availability' status is 'Not Configured', highlighted in a red box. The main configuration area shows a network diagram with an 'Inside Network' and an 'ISP/WAN/Gateway' connected to an 'Internet' cloud. The diagram includes various interfaces like MGMT, CONSOLE, and SFP. Below the diagram are several configuration panels: 'Interfaces' (Connected, Enabled 3 of 13), 'Routing' (No static routes yet), 'Updates' (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), 'Smart License' (Evaluation expires in 89 days), 'Backup and Restore' (No files created yet), and 'Troubleshoot' (No files created yet). A 'System Settings' panel is also visible on the right.

Als een hoge beschikbaarheid is ingesteld, worden de configuratie en de rollen van de lokale en externe peer unit-failover weergegeven:



FDM REST-API

Volg deze stappen om de FDM-configuratie en -status met een hoge beschikbaarheid te controleren via het FDM REST-API-verzoek. Gebruik een REST-API client. In dit voorbeeld wordt curl gebruikt:

1. Echtheidstoken aanvragen:

```
# 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.eyJpYXQiOiJlY2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoimjI1YWRhZWMtZDlhYS0xMWVjLWE5MmEtMjk4YjRjZTUxNmJlIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOiJlY2NTMyMTAzMjgsInJ1ZnJlc2h0b2t1bkV4cGlyZXNbdCI6MTY1MzIxMDkyODU2OSwidG9rZW50eXB1Ijois1dUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTNmZDA3ZjMtZDg4ZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXN1c1JvbGU0IjST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcnQ1LCJ1c2VybmFtZSI6ImFkbWluIn0.ai3LUBnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token":
    "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlY2NTIzOTQxNjksInN1YiI6ImFkbWluIiwianRpIjoimGU0NGIxYzQtZDI0Mi0xMWVjLk4ZWMtYT11OTlkZGMwN2Y0IiwibmJmIjoxNjUyMzk0MTY5LWVzZXN0Q291bnQiOi0xLCJ0b2t1b1R5cGU0IjoJKV1RfUmVmcVzaCIsInVzZXJvdWlkIjoiyTU3ZGVmMjgtY2M3M0xMWVjLk4ZWMtZjk4ODExNjNjZWlwiIiwidXN1c1JvbGU0IjST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcnQ1LCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw",
  "token_type": "Bearer"
}
```

2. Gebruik de waarde van het toegangstoken in deze zoekopdracht om de hoge beschikbaarheid te controleren:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlY2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoimjI1YWRhZWMtZDlhYS0xMWVjLWE5MmEtMjk4YjRjZTUxNmJlIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOiJlY2NTMyMTAzMjgsInJ1ZnJlc2h0b2t1bkV4cGlyZXNbdCI6MTY1MzIxMDkyODU2OSwidG9rZW50eXB1Ijois1dUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTNmZDA3ZjMtZDg4ZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXN1c1JvbGU0IjST0xFOX0FETU0Iiwib3JpZ2luIjoicGFzc3dvcnQ1LCJ1c2VybmFtZSI6ImFkbWluIn0.Avga0-isDjQB527d3QWZQb7AS4a9ea5wlbYUn-A9aPw'
```

```
jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2t1bkV4cG1
yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXB1IjoiSlDUX0FjY2VzcyIsInVzZXJvZwWlkIjoiYTNmZDA3ZjMtZDgxZS0
xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXN1c1JvbGUiOiJST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcmQiLCJlc2V
ybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/ha/configurations'
```

Als een hoge beschikbaarheid niet is ingesteld, wordt deze uitvoer weergegeven:

```
{
  "items": [
    {
      "version": "issgb3rw2lix",
      "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
  }
}
```

Als een hoge beschikbaarheid is ingesteld, wordt deze uitvoer weergegeven:

```
{
  "items": [
    {
      "version": "issgb3rw2lix",
      "name": "HA",
      "nodeRole": "HA_PRIMARY",
      "failoverInterface": {
        "version": "ezzafxo5cccti3",
        "name": "",
        "hardwareName": "Ethernet1/1",
        "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
        "type": "physicalinterface"
      }
    }
  ],
  ...
}
```

3. Gebruik deze zoekopdracht om de hoge beschikbaarheid te controleren:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE2NTMyMDg1MjgsInN1YiI6ImFkbWluIiwianRpIjoimjI1YWRhZWMtZDlhYS0xMWVjLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjozNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2t1bkV4cG1yZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXB1IjoislDUX0FjY2VzcyIsInVzZXJvdWlkIjoiyTNmZDA3ZjMtZDgxZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXN1c1JvbGUoIjST0xFOX0FETU1OIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybW90IjoiIiwiaWF0Ijoi1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default'
```

Als een hoge beschikbaarheid niet is ingesteld, wordt deze uitvoer weergegeven:

```
{
  "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"
  }
}
```

Als een hoge beschikbaarheid is ingesteld, wordt deze uitvoer weergegeven:

```
{
  "nodeRole": "HA_PRIMARY",
  "nodeState": "HA_ACTIVE_NODE",
  "peerNodeState": "HA_STANDBY_NODE",
  "configStatus": "IN_SYNC",
  "haHealthStatus": "HEALTHY",
  "disabledReason": "",
  "disabledTimestamp": "",
  "id": "default",
  "type": "hastatus",
  "links": {
    "self": "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
  }
}
```

FTD CLI

Volg de stappen in het gedeelte.

FTD SNMP-stemming

Volg de stappen in het gedeelte.

FTD Problemen oplossen

Volg de stappen in het gedeelte.

FTD hoge beschikbaarheid en schaalbaarheid

De hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van FTD kunnen met het gebruik van deze opties worden geverifieerd:

- FTD CLI
- FTD SNMP
- FTD Problemen oplossen
- FMC UI
- FMC REST-API
- FDM UI
- FDM REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS chassis toverttech-bestand

FTD CLI

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FTD CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de FTD CLI in overeenstemming met het platform en de implementatiemodus:

- Directe SSH-toegang tot FTD - alle platforms
- Toegang van de FXOS-console CLI (Firepower 1000/2100/3100) via commando **verbinden met ftd**
- Toegang van de FXOS CLI via opdrachten (Firepower 4100/9300):
Sluit module <x> [console|telnet] aan, waarbij x de sleuf-ID is, en **sluit** vervolgens **ftd [instantie] aan**, waar de instantie alleen relevant is voor meerkanaals-implementatie
- Voor virtuele FTD's, directe SSH-toegang tot FTD of console-toegang van de hypersupervisor of cloud UI

2. Om de configuratie en de status van de FTD te verifiëren, voer de **show in werking stellen-configuratie-failover** uit en **toon** de opdrachten van de **uitvalstatus** op de CLI.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
> 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==
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
> 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. Om de configuratie en de status van het FTD-cluster te verifiëren, voert u het in werking stellen-configuratiecluster en de opdrachten van het cluster info op de CLI uit.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:

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

Als het cluster is geconfigureerd, wordt deze uitvoer weergegeven:

```
> 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

Opmerking: De master en control rollen zijn hetzelfde.

FTD SNMP

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FTD via SNMP te controleren:

1. Zorg ervoor dat SNMP is ingesteld en ingeschakeld. Raadpleeg voor FDM-Managed FTD [SNMP configureren en probleemoplossing in Firepower FDM](#) voor configuratiestappen. Raadpleeg voor FMC-beheerde FTD [SNMP configureren op FirePOWER NGFW-applicaties](#) voor configuratiestappen.
2. Om de configuratie en de status van de FTD-uitvalbeveiliging te verifiëren, dient u de OID **.1.3.6.1.4.1.9.9.147.1.2.1.1** te raadplegen.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
# 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"
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
# 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. Om de configuratie en de status van het cluster te verifiëren, dient u de OID **1.3.6.1.4.1.9.9.491.1.8.1** te raadplegen.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:


```
# 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
```

Als het cluster is ingesteld maar niet ingeschakeld, wordt deze uitvoer weergegeven:

```
# 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
...
```

Als het cluster is ingesteld, ingeschakeld en operationeel omhoog, wordt deze uitvoer weergegeven:

```
# 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
...
```

Raadpleeg voor meer informatie over de OID-beschrijvingen de [CISCO-UNIFIED-FIREWALL-MIB](#).

FTD Problemen oplossen

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en status van de FTD probleemoplossing te controleren:

1. Open het bestand voor probleemoplossing en navigeer naar de map <bestandsnaam>-probleemoplossing .tar/resultaat-<date>—xxxxxx/opdrachtoutput.
2. Open het bestand `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. Om de configuratie en de status van de failover te controleren, dient u de sectie **over de failover te controleren**.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
----- 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
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
----- 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. Om de configuratie en de status van het FTD-cluster te verifiëren, controleert u de sectie van de **showclusterinfo**.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:

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

Clustering is not configured

Als het cluster is ingesteld en ingeschakeld, wordt deze uitvoer weergegeven:

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

Cluster ftd_cluster1: On

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

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

```
ID : 0
Site ID : 1
Version : 9.17(1)
Serial No.: FLM1949C5RR6HE
CCL IP : 10.173.1.1
CCL MAC : 0015.c500.018f
Module : FPR4K-SM-24
```

Resource : 20 cores / 44018 MB RAM
Last join : 13:53:52 UTC May 20 2022
Last leave: N/A

Other members in the cluster:

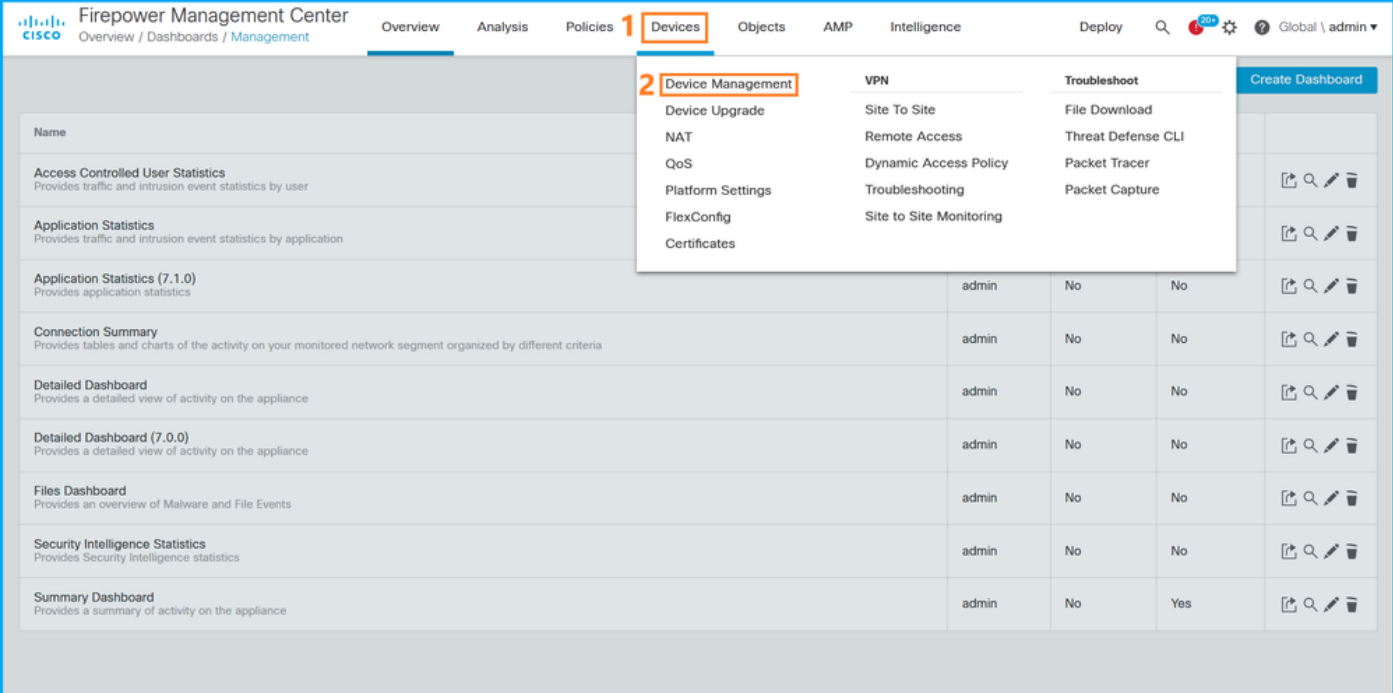
Unit "unit-2-1" in state SLAVE

ID : 1
Site ID : 1
Version : 9.17(1)
Serial No.: FLM2108V9YG7S1
CCL IP : 10.173.2.1
CCL MAC : 0015.c500.028f
Module : FPR4K-SM-24
Resource : 20 cores / 44018 MB RAM
Last join : 14:02:46 UTC May 20 2022
Last leave: 14:02:31 UTC May 20 2022

FMC UI

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FMC UI te controleren:

1. Kies apparaten > Apparaatbeheer:



The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', and 'Deploy'. The 'Devices' menu is open, showing 'Device Management' selected. The main dashboard area displays various statistics and dashboards for the appliances.

Name	admin	No	No	
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. Om de hoge beschikbaarheid en schaalbaarheidsconfiguratie van de FTD te controleren, dient u de **hoge beschikbaarheid** of **Cluster** van de labels te controleren. Als geen van beide bestaat, werkt de FTD in een standalone configuratie:

The screenshot shows the Firepower Management Center interface. The 'Devices' tab is active, displaying a list of devices. The 'View By' dropdown is set to 'Domain'. The status bar shows 5 Normal devices, 0 Errors, 0 Warnings, 0 Offline, 0 Deployment Pending, 0 Upgrade, and 5 Snort 3. The table lists devices under the 'LAB2' group. Two clusters are highlighted with orange boxes: 'ftd_cluster1' and 'ftd_ha'.

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. Om de hoge beschikbaarheid en de hoge schaalbaarheidsstatus van de FTD te verifiëren, dient de rol van de eenheid als parentese te worden gecontroleerd. Als een rol niet bestaat en de FTD geen deel uitmaakt van een cluster of een failover, dan draait FTD in een standalone configuratie:

This screenshot is similar to the first one, but with orange boxes highlighting the role of each device in the cluster and HA configuration. The roles are: Control for the first device in the cluster, Primary/Active for the first HA device, and Secondary/Standby for the second HA device.

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	

Opmerking: In het geval van een cluster wordt alleen de rol van de **regeleenheid** weergegeven.

FMC REST API

In deze output zijn `ftd_ha_1`, `ftd_ha_2`, `ftd_standalone`, `ftd_ha`, `ftc_cluster1` gebruikersaanpasbare apparaatnamen. Deze namen verwijzen niet naar de eigenlijke hoge beschikbaarheid en schaalbaarheidsconfiguratie of -status.

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de

FTD te controleren via FMC REST-API. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het token in deze query om de lijst met domeinen op te halen:

```
# 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. Gebruik het domein UID om zoekopdrachten naar de specifieke **apparaten** en de specifieke apparatuur UID uit te voeren:

```
# 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. Om de configuratie van de failover te verifiëren, gebruik het domein UID en het apparaat/de container UID van Stap 3 in deze query:

```
# 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. Om de overvalstatus te controleren, gebruikt u het domein UID en het apparaatHAPair UID uit stap 4 in deze zoekopdracht:

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

...

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

...

6. Om de clusterconfiguratie te controleren, gebruikt u het domein UID en het apparaat/de container UID uit stap 3 in deze zoekopdracht:

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

...

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

...

7. Om de clusterstatus te controleren gebruikt u het domein UID en het apparaat/de container UID uit stap 6 in deze query:

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/deviceclusters/ftdddevicecluster/8e6188c2-d844-11ec-bdd1-6e8d3e226370' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
```

{

```
  "controlDevice": {
    "deviceDetails": {
      "id": "3344bc4a-d842-11ec-a995-817e361f7ea5",
      "name": "10.62.148.188",
      "type": "Device"
    }
  },
}
```

```

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

```

FDM UI

Volg de stappen in het gedeelte.

FDM REST-API

Volg de stappen in het gedeelte.

FCM UI

FCM UI is beschikbaar op Firepower 4100/9300 en Firepower 2100 met ASA in platform modus.

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsstatus van FTD op de FCM UI te controleren:

1. Om de FTD-status te controleren, controleert u de waarde **HA-ROLE** op de pagina Logical Devices:

The screenshot shows the 'Logical Devices' page in the FCM UI. The page title is 'Logical Device List' and it indicates '(1 Container instance) 77% (66 of 86) Cores Available'. The main content area shows a table with the following columns: Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. The first row shows an FTD instance with version 7.1.0.90, resource profile RP20, management IP 10.62.148.89, gateway 10.62.148.1, and management port Ethernet1/1. The status is 'Online'. Below the table, there are sections for 'Interface Name' (Ethernet1/2 and Ethernet1/3) and 'Attributes'. The 'Attributes' section includes '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', and 'UUID: 7962088-d83b-11ec-941d-b9083eb612d8'. The 'HA-ROLE' attribute is highlighted with a red box.

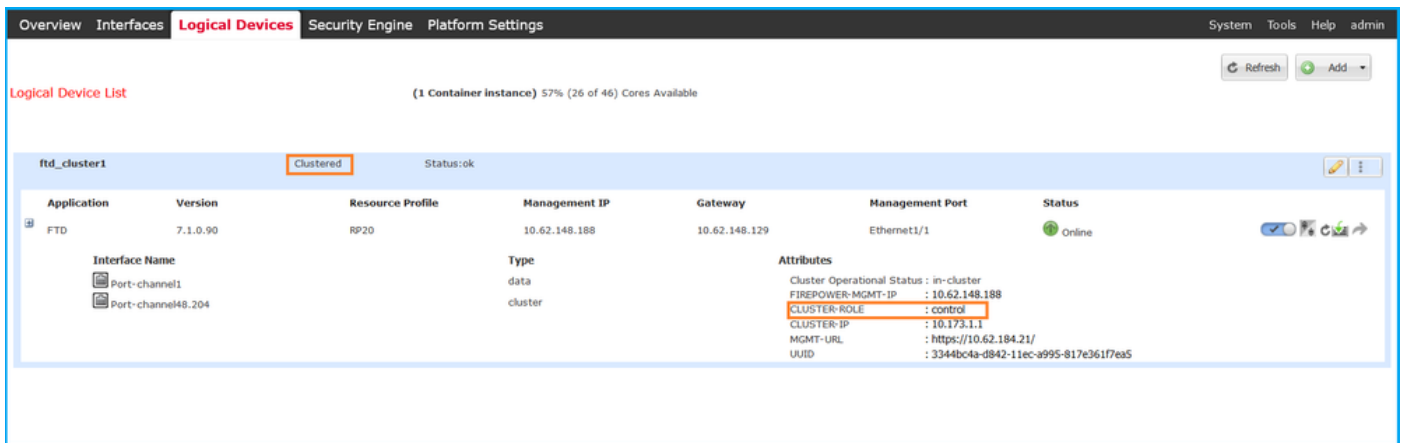
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	7.1.0.90	RP20	10.62.148.89	10.62.148.1	Ethernet1/1	Online

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: 7962088-d83b-11ec-941d-b9083eb612d8

Opmerking: Het **Standalone** label naast de logische apparaatidentificatie verwijst naar de configuratie van het chassis logische apparaat, niet naar de FTD failover-configuratie.

2. Om de configuratie en de status van het FTD-cluster te controleren, controleert u het label en de waarde van de **CLUSTER-ROLE**-eigenschap op de pagina Logical Devices:



FXOS CLI

De hoge beschikbaarheid en schaalbaarheidsconfiguratie en de statusverificatie van de FXOS CLI zijn beschikbaar op Firepower 4100/9300.

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FXOS CLI te controleren:

1. Maak een console of SSH-verbinding met het chassis.

2. Om de FTD hoge beschikbaarheidsstatus te controleren, voer de **scope SA**-opdracht uit, en **gebruik** vervolgens de **scope sleuf <x>** om naar de specifieke sleuf te switches waar de FTD loopt en voer de **show-app-instantie** opdracht uit:

```
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. Om de configuratie en de status van het FTD-cluster te controleren, voert u de opdracht **scope SA** uit, voert u de opdracht **Show logical-device <name> detail** uit, waarbij de naam de naam van

het logische apparaat is en de opdracht **Show app-instantie**. Controleer de uitvoer voor een bepaalde sleuf:

```
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 wordt ondersteund op Firepower 4100/9300.

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FTD te verifiëren via FXOS REST-API-verzoek. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

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

2. Gebruik het token en de sleuf-ID in deze zoekopdracht om de FTD-status te controleren:

```
# 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": "",
    "fsmStatus": "nop",
    "fsmRmtInvRslt": "",
    "fsmTry": "0",
    "fsmStageDescr": "",
    "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. Om de configuratie van het FTD-cluster te controleren, gebruikt u de logische apparaatidentificatie in deze zoekopdracht:

```

# 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. Om de FTD-clusterstatus te controleren, gebruikt u deze vraag:

```

# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.102/api/slot/1/app-inst'
{
  "smAppInstance": [
    {
      "adminState": "enabled",
      "appDn": "sec-svc/app-ftd-7.1.0.90",
      "appInstId": "ftd_001_JAD19500BABIYA30058",
      "appName": "ftd",
      "clearLogData": "available",
"clusterOperationalState": "in-cluster",
"clusterRole": "master",
      "currentJobProgress": "100",
      "currentJobState": "succeeded",
      "currentJobType": "start",
      "deployType": "container",
      "dn": "slot/1/app-inst/ftd-ftd_cluster1",
      "errorMsg": "",
      "eventMsg": "",
      "executeCmd": "ok",
      "externallyUpgraded": "no",
      "fsmDescr": "",
      "fsmProgr": "100",
      "fsmRmtInvErrCode": "none",
      "fsmRmtInvErrDescr": "",
      "fsmRmtInvRslt": "",
      "fsmStageDescr": "",
      "fsmStatus": "nop",
      "fsmTry": "0",
      "hotfix": "",
"identifier": "ftd_cluster1",

```

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

...

FXOS-chassis testbestand

De hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status van de FTD kunnen worden geverifieerd in het Firepower 4100/9300 Chassis show-tech-bestand.

Volg deze stappen om de hoge beschikbaarheid en schaalbaarheidsconfiguratie en status in het FXOS chassis show-tech-bestand te controleren:

1. Open het bestand **sam_techsupportinfo** in **<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar** voor FXOS versies 2.7 en hoger

Open voor eerdere versies het bestand **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**.

2. Om de overnamestatus te controleren, controleert u de waarde van de waarde van de **ha-rol**-eigenschap onder de specifieke sleuf in de sectie **"Show sleuf uitbreiden"**:

```
# 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. Om de configuratie van het FTD-cluster te controleren, controleert u de waarde van de waarde van de **Mode**-eigenschap onder de specifieke sleuf in de sectie "**show logical device detail**":

```
`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. Om de FTD-clusterstatus te controleren, controleert u de waarde van de waarden van de **Cluster State** en de **Cluster Roll** onder de specifieke sleuf in de sectie "**Show sleuf expo detail**":

```
`show slot expand detail`
```

```
Slot:  
  Slot ID: 1  
  Log Level: Info
```

Admin State: Ok
Oper State: Online
Disk Format State: Ok
Disk Format Status:
Clear Log Data: Available
Error Msg:

Application Instance:

App Name: ftd
Identifier: ftd_cluster1
Admin State: Enabled
Oper State: Online
Running Version: 7.1.0.90
Startup Version: 7.1.0.90
Deploy Type: Native
Turbo Mode: No
Profile Name:
Hotfixes:
Externally Upgraded: No
Cluster State: In Cluster
Cluster Role: Master
Current Job Type: Start
Current Job Progress: 100
Current Job State: Succeeded
Clear Log Data: Available
Error Msg:
Current Task:

ASA hoge beschikbaarheid en schaalbaarheid

ASA kan een hoge beschikbaarheid en schaalbaarheidsconfiguratie en -status met behulp van deze opties controleren:

- ASA CLI
- ASA SNMP-stemming
- ASA show-tech-bestand
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS chassis toverttech-bestand

ASA CLI

Volg deze stappen om de ASA hoge beschikbaarheid en schaalbaarheidsconfiguratie op de ASA CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de ASA CLI in overeenstemming met het platform en de implementatiemodus:
 - Toegang tot ASA-telefoon/SSH op FirePOWER 1000/3100 en Firepower 2100 in de toevoermodus
 - Toegang van FXOS-console CLI op Firepower 2100 in platform modus en verbinding met ASA via **connect als** opdracht
 - Toegang van FXOS CLI via opdrachten (Firepower 4100/9300):
Sluit module <x> [console|telnet] aan, waar x de sleuf-ID is, en **sluit** vervolgens **aan als**

- Voor virtuele ASA directe SSH-toegang tot ASA of console-toegang van de hypersupervisor of cloud UI

2. Om de ASA failover configuratie en de status te verifiëren, voer de **show in werking stellen-fig** en **toon** de opdrachten **van de** overnamestatus op de ASA CLI.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
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==
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
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. Om de ASA clusterconfiguratie en -status te controleren, voert u de **show-run-configuratiecluster** uit en **toont u** opdrachten **clusterinfo** op de CLI.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:

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

Als het cluster is geconfigureerd, wordt deze uitvoer weergegeven:

```
asa# show running-config cluster
cluster group asa_cluster1
key *****
local-unit unit-1-1
cluster-interface Port-channel48.205 ip 10.174.1.1 255.255.0.0
priority 9
health-check holdtime 3
health-check data-interface auto-rejoin 3 5 2
health-check cluster-interface auto-rejoin unlimited 5 1
```

```
health-check system auto-rejoin 3 5 2
health-check monitor-interface debounce-time 500
site-id 1
no unit join-acceleration
enable
```

```
asa# show cluster info
```

```
Cluster asa_cluster1: On
```

```
Interface mode: spanned
```

```
Cluster Member Limit : 16
```

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

```
ID          : 0
Site ID     : 1
Version     : 9.17(1)
Serial No.  : FLM2949C5232IT
CCL IP      : 10.174.1.1
CCL MAC     : 0015.c500.018f
Module      : FPR4K-SM-24
```

```
...
```

ASA SNMP

Volg deze stappen om de ASA hoge beschikbaarheid en schaalbaarheidsconfiguratie via SNMP te controleren:

1. Zorg ervoor dat SNMP is ingesteld en ingeschakeld.
2. Om de configuratie en de status van de failover te verifiëren, dient de OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1** te worden geraadpleegd.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
# 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"
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
# 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. Om de configuratie en de status van het cluster te verifiëren, dient u de OID **1.3.6.1.4.1.9.9.491.1.8.1** te raadplegen.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:

```
# 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
```

Als het cluster is ingesteld maar niet ingeschakeld, wordt deze uitvoer weergegeven:

```
# 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
...
```

Als het cluster is ingesteld, ingeschakeld en operationeel omhoog, wordt deze uitvoer weergegeven:

```
# 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
...
```

Raadpleeg voor meer informatie over de OID-beschrijvingen de [CISCO-UNIFIED-FIREWALL-MIB](#).

ASA show-tech-bestand

1. Om de ASA failover configuratie en de status te verifiëren, controleer de **show-overvalsectie**.

Als de failover niet is geconfigureerd wordt deze uitvoer weergegeven:

```
----- 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
```

Als de failover is ingesteld, wordt deze uitvoer weergegeven:

```
----- 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. Controleer de sectie van **showclusterinfo** om de clusterconfiguratie en -status te verifiëren.

Als het cluster niet is ingesteld, wordt deze uitvoer weergegeven:

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

Als het cluster is ingesteld en ingeschakeld, wordt deze uitvoer weergegeven:

```
----- show cluster info -----
Cluster asa_cluster1: On
  Interface mode: spanned
Cluster Member Limit : 16
  This is "unit-1-1" in state MASTER
  ID          : 0
  Site ID     : 1
  Version     : 9.17(1)
  Serial No.  : FLM2949C5232IT
  CCL IP      : 10.174.1.1
  CCL MAC     : 0015.c500.018f
  Module      : FPR4K-SM-24
```

...

FCM UI

Volg de stappen in het gedeelte.

FXOS CLI

Volg de stappen in het gedeelte.

FXOS REST-API

Volg de stappen in het gedeelte.

FXOS-chassis testbestand

Volg de stappen in het gedeelte.

Controleer de firewallmodus

FTD-firewallmodus

De firewallmodus verwijst naar een Routed of Transparent firewallconfiguratie.

De FTD firewallmodus kan met het gebruik van deze opties worden geverifieerd:

- FTD CLI
- FTD-show-tech
- FMC UI
- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS chassis toverttech-bestand

Opmerking: FDM ondersteunt geen transparante modus.

FTD CLI

Volg deze stappen om de FTD firewallmodus op de FTD CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de FTD CLI in overeenstemming met het platform en de implementatiemodus:

- Directe SSH-toegang tot FTD - alle platforms
- Toegang van de FXOS-console CLI (Firepower 1000/2100/3100) via commando **verbinden met ftd**
- Toegang van de FXOS CLI via opdrachten (Firepower 4100/9300):
Sluit module <x> [console|telnet] aan, waar x de sleuf-ID is, en dan

verbinding met ftd [instantie], waarbij de instantie alleen relevant is voor meerkanaals-implementatie.

- Voor virtuele FTD's, directe SSH-toegang tot FTD of console-toegang van de hypersupervisor of cloud UI

2. Om de firewallmodus te controleren, voert u de opdracht **Firewall** op de CLI uit:

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

FTD Problemen oplossen

Volg deze stappen om de modus van de FTD-firewall in het FTD-bestand te controleren:

1. Open het bestand voor probleemoplossing en navigeer naar de map **<bestandsnaam>-**

probleemoplossing .tar/resultaat-<date>—xxxxxx/opdrachtoutput.

2. Open het bestand `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. Controleer de FTD firewallmodus en controleer de sectie van de **show Firewall**:

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

FMC UI

Volg deze stappen om de FTD firewallmodus op de FMC UI te controleren:

1. Kies apparaten > Apparaatbeheer:

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', and 'Deploy'. The 'Devices' menu is open, displaying a list of options: 'Device Management', 'VPN', and 'Troubleshoot'. The 'Device Management' option is highlighted with a red box and a '2'. The 'Devices' menu item in the top navigation bar is highlighted with a red box and a '1'. Below the menu, there is a table with columns for Name, admin, No, and Yes, and a 'Create Dashboard' button.

Name	admin	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. Controleer de Routed of Transparent-etiketten:

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
LAB2 (3)						
ftd_cluster1 (2) Cluster						
10.62.148.188 (Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - 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	

FMC REST-API

Volg deze stappen om de FTD firewallmodus via FMC REST-API te controleren. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het token in deze query om de lijst met domeinen op te halen:

```
# 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. Gebruik het domein UID om zoekopdrachten naar de specifieke **apparaten** en de specifieke apparatuur UID uit te voeren:

```
# 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. Gebruik het domein UID en het apparaat/de container UID van Stap 3 in deze query en controleer de waarde van **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": "acpl",
    "type": "AccessPolicy"
  },
  "advanced": {
    "enableOGS": false
  },
  "description": "NOT SUPPORTED",
  "ftdMode": "ROUTED",
  ...
}
```

FCM UI

De firewallmodus kan voor FTD worden geverifieerd op Firepower 4100/9300.

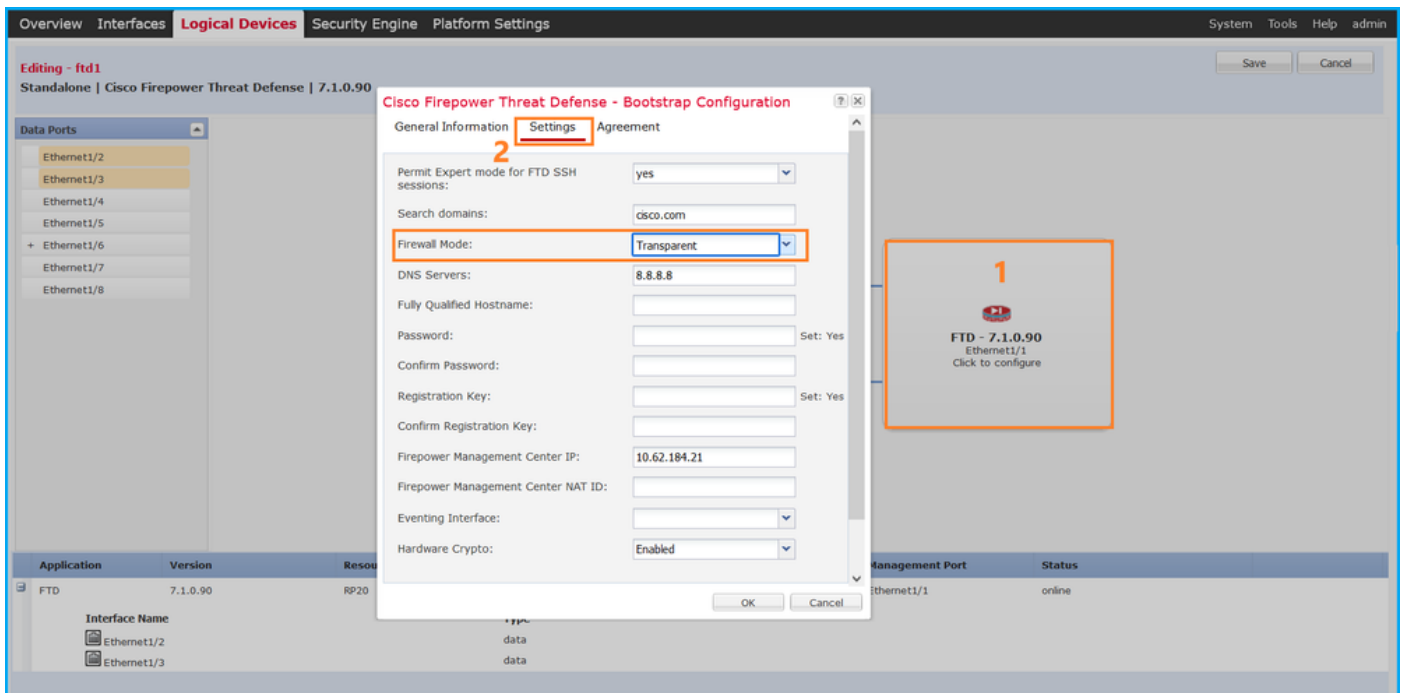
Volg deze stappen om de FTD firewallmodus op de FCM UI te controleren:

1. Bewerk het logische apparaat op de pagina **Logische apparaten**:

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

Interface Name	Type	Attributes
Ethernet1/2	data	Cluster Operational Status: not-applicable
Ethernet1/3	data	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. Klik op het pictogram van de toepassing en controleer de **firewallmodus** in het tabblad **Instellingen**:



FXOS CLI

De firewallmodus kan voor FTD worden geverifieerd op Firepower 4100/9300.

Volg deze stappen om de firewallmodus in de FXOS CLI te controleren:

1. Maak een console of SSH-verbinding met het chassis.
2. Switch naar de scope ssa, dan switch naar het specifieke logische apparaat, voer de **show mgmt-bootstrap** opdracht uit en controleer de **FIREWALL_MODE**waarde:

```
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 wordt ondersteund op Firepower 4100/9300.

Volg deze stappen om de FTD firewallmodus te controleren via FXOS REST-API-verzoek. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

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

2. Gebruik het logische device identifier in deze query en controleer de waarde van de **FIREWALL_MODE** toets:

```
# 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"
      },
...

```

FXOS-chassis testbestand

De firewallmodus voor FTD kan worden geverifieerd in het toverttech-bestand van Firepower 4100/9300.

Volg deze stappen om de firewallmodus in de FXOS chassis-show-tech-bestand te controleren:

1. Open het bestand **sam_techsupportinfo** in

<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar voor FXOS versies 2.7 en hoger

Open voor eerdere versies het bestand **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**.

2. Controleer de sectie van het **logische-apparaatdetail** onder de specifieke identificator en de sleuf:

```
# pwd
/var/tmp/20220313201802_F241-01-11-FPR-2_BC1_all/FPRM_A_TechSupport/
```



```

# cat sam_techsupportinfo
...
`show logical-device detail expand`
Logical Device:      Name: ftd_cluster1
  Description:
    Slot ID: 1
  Mode: Clustered
  Oper State: Ok
  Template Name: ftd
  Error Msg:
  Switch Configuration Status: Ok
  Sync Data External Port Link State with FTD: Disabled
  Current Task:
...
  Bootstrap Key:
    Key: DNS_SERVERS
    Value: 192.0.2.250
    Last Updated Timestamp: 2022-05-20T13:28:37.093

    Key: FIREPOWER_MANAGER_IP
    Value: 10.62.184.21
    Last Updated Timestamp: 2022-05-20T13:28:37.093

    Key: FIREWALL_MODE
    Value: routed
    Last Updated Timestamp: 2022-05-20T13:28:37.093
...

```

ASA-firewallmodus

De ASA firewallmodus kan met het gebruik van deze opties worden geverifieerd:

- ASA CLI
- ASA show-tech
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS chassis toverttech-bestand

ASA CLI

Volg deze stappen om de ASA firewallmodus op de ASA CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de ASA CLI in overeenstemming met het platform en de implementatiemodus:
 - Toegang tot ASA-telefoon/SSH op FirePOWER 1000/3100 en Firepower 2100 in de toevoermodus
 - Toegang van FXOS-console CLI op Firepower 2100 in platform modus en verbinding met ASA via **connect als** opdracht
 - Toegang van FXOS CLI via opdrachten (Firepower 4100/9300):
 - Sluit module <x> [console|telnet] aan**, waar x de sleuf-ID is, en **sluit vervolgens aan als**
 - Voor virtuele ASA directe SSH-toegang tot ASA of console-toegang van de hypersupervisor of cloud UI

2. Start de opdracht **Firewall** op de CLI:

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

ASA show-tech-bestand

Om ASA firewallmodus te controleren, controleert u het gedeelte **Show firewall**:

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

FCM UI

Volg de stappen in het gedeelte.

FXOS CLI

Volg de stappen in het gedeelte.

FXOS REST-API

Volg de stappen in het gedeelte.

FXOS-chassis testbestand

Volg de stappen in het gedeelte.

Verifiëren van type installatie

Er zijn 2 inzetbaarheidstypes van toepassingsinstanties:

- Bijvoorbeeld inheemse instantie - Een inheemse instantie gebruikt alle middelen (CPU, RAM, en schijfruimte) van de veiligheidsmodule/motor, zodat u slechts één geboorteland kunt installeren.
- containerinstantie - Een containerinstantie gebruikt een deelgroep van middelen van de veiligheidsmodule/motor. Mogelijkheid van meerdere exemplaren wordt alleen ondersteund voor het door het VCC beheerde FTD; het wordt niet ondersteund voor de ASA of de FTD die door FDM wordt beheerd.

De configuratie van de containermodus wordt alleen ondersteund voor FTD op Firepower 4100/9300.

Het inzettype van de instantie kan met behulp van deze opties worden geverifieerd:

- FTD CLI
- FTD Show-tech
- FMC UI

- FMC REST-API
- FCM UI
- FXOS CLI
- FXOS REST-API
- FXOS chassis tovertech-bestand

FTD CLI

Volg deze stappen om het type FTD-instel op de FTD CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de FTD CLI in overeenstemming met het platform en de implementatiemodus:

- Directe SSH-toegang tot FTD - alle platforms
- Toegang van de FXOS CLI via opdrachten (Firepower 4100/9300):

Sluit module <x> [console|telnet] aan, waarbij x de sleuf-ID is, en **sluit** vervolgens **ftd [instantie] aan**, waar de instantie alleen relevant is voor meerkanaals-implementatie.

2. Start het opdracht **versiesysteem** tonen en controleer de lijn met het **SSP sleuf-nummer**. Als de **container** op deze lijn bestaat, draait de FTD in een containermodus:

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

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

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

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

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

FTD Problemen oplossen

Volg deze stappen om het type implementatie van de FTD-instantie in het FTD-probleemoplossingsbestand te controleren:

1. Open het bestand voor probleemoplossing en navigeer naar de map **<bestandsnaam>-probleemoplossing .tar/resultaat-<date>-xxxxxx/opdrachtoutput**.
2. Open het bestand **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. Controleer de lijn met het string **SSP sleuf nummer**. Als de **container** op deze lijn bestaat, draait de FTD in een containermodus:

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

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

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

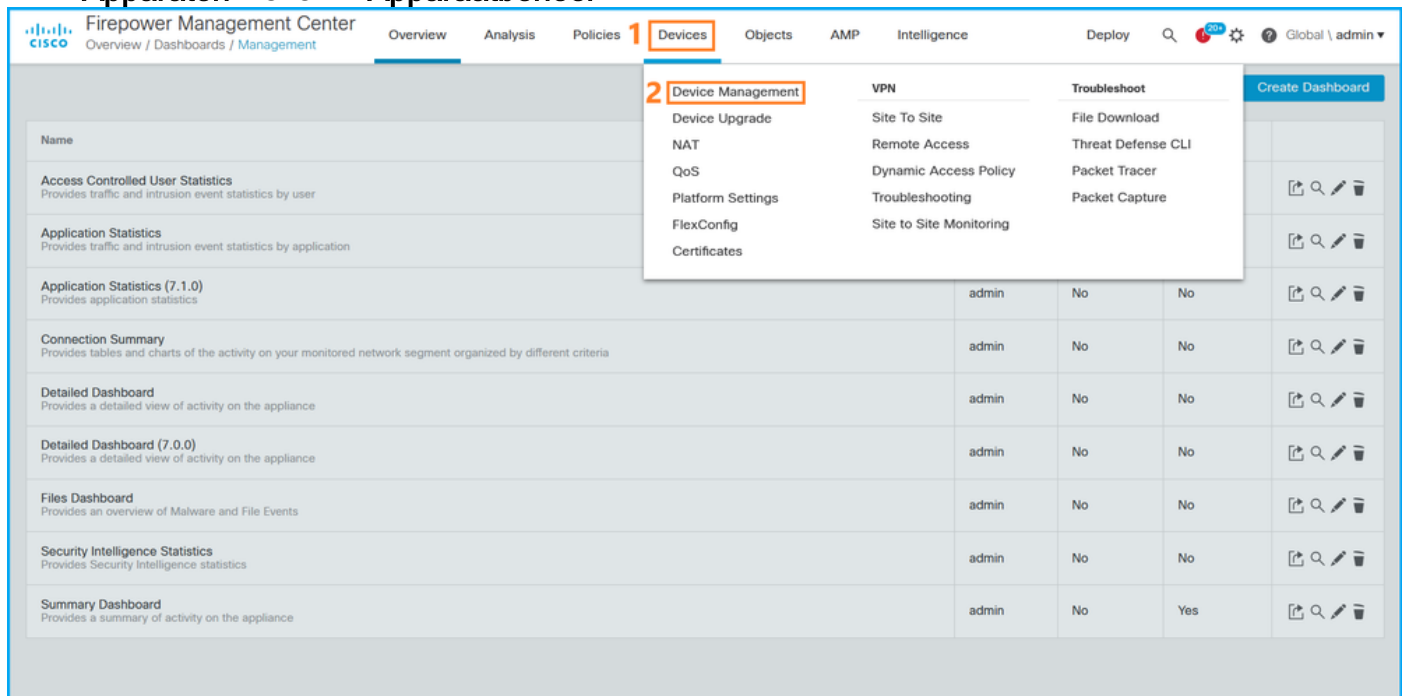
firepower up 2 days 19 hours
Start-up time 3 secs

SSP Slot Number: 1 (Container)
...

FMC UI

Volg deze stappen om het inzettype van de FTD-instantie op de FMC UI te controleren:

1. Apparaten kiezen > Apparaatbeheer:



2. Controleer de kolom **Chassis**. Als de **container** in de regel bestaat, draait FTD in de containermodus.

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	

FMC REST-API

Volg deze stappen om het type FTD-exemplaar te controleren via FMC REST-API. Gebruik een REST-API client. In dit voorbeeld wordt **curl** gebruikt:

1. Echtheidstoken aanvragen:

```
# 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. Identificeer het domein dat het apparaat bevat. Bij de meeste REST API-vragen is de **domeinparameter** verplicht. Gebruik het token in deze query om de lijst met domeinen op te halen:

```
# 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. Gebruik het domein UID om zoekopdrachten naar de specifieke **apparaten** en de specifieke apparaatuur UID uit te voeren:

```
# 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. Gebruik het domein UID en het apparaat/de container UID van Stap 3 in deze query en controleer de waarde van **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,
...

```

FCM UI

Om het type inzet van een FTD-instantie te controleren, controleert u de waarde van de toeschrijving van **een** resourceprofiel in Logische Apparaten. Als de waarde niet leeg is, draait de FTD in containermodus:

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

FXOS CLI

Volg deze stappen om het type FTD-invoeging op de FXOS CLI te controleren:

1. Maak een console of SSH-verbinding met het chassis.
2. Switch naar het bereik **ssa** en voer de opdracht **show app-instantie** uit, controleer dan de kolom **Deploy Type** van de specifieke FTD op basis van de sleuf en de identificator:

```

firepower # scope ssa
firepower /ssa # show app-instantie
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

Volg deze stappen om het type FTD-invoeging te controleren via een FXOS REST-API-verzoek. Gebruik een REST-API client. In dit voorbeeld wordt `curl` gebruikt:

1. Echtheidstoken aanvragen:

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

2. Specificeer het token, sleuf-ID in deze query en controleer de waarde van `implementationType`:

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

FXOS-chassis testbestand

Volg deze stappen om de firewallmodus in de FXOS chassis-show-tech-bestand te controleren:

1. Open het bestand `sam_techsupportinfo` in

`<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar` voor FXOS versies 2.7 en hoger

Open voor eerdere versies het bestand `sam_techsupportinfo` in `FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar`.

2. Controleer het gedeelte "Show groeve expo detail" voor de specifieke sleuf en de identificator:

```
# 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

Controleer de ASA-context-modus

ASA ondersteunt single-context-modi. FTD ondersteunt multi-context mode niet.

Het type context kan met behulp van deze opties worden geverifieerd:

- ASA CLI
- ASA show-tech

ASA CLI

Volg deze stappen om de ASA context-modus op de ASA CLI te controleren:

1. Gebruik deze opties om toegang te krijgen tot de ASA CLI in overeenstemming met het platform en de implementatiemodus:

- Toegang tot ASA-telefoon/SSH op FirePOWER 1000/3100 en Firepower 2100 in de toevoermodus
- Toegang van FXOS-console CLI op Firepower 2100 in platform modus en verbinding met ASA via **connect als** opdracht
- Toegang van FXOS CLI via opdrachten (Firepower 4100/9300):
Sluit module <x> [console|telnet] aan, waar x de sleuf-ID is, en **sluit** vervolgens **aan als**

- Voor virtuele ASA directe SSH-toegang tot ASA of console-toegang van de hypersupervisor of cloud UI

2. Start de opdracht **showmode** op CLI:

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

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

ASA show-tech-bestand

Volg deze stappen om de ASA context-modus in het ASA show-tech-bestand te controleren:

1. Controleer de sectie **van** de **show**-contextdetails in het show-tech-bestand. In dit geval is de contextmodus veelvoudig omdat er meerdere contexten zijn:

----- 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

Controleer de Firepower 2100-modus met ASA

Firepower 2100 met ASA kan op een van deze modi draaien:

- Platform mode - fundamentele bedrijfsparameters en hardware-interface-instellingen worden ingesteld in FXOS. Deze instellingen zijn onder meer interfaces, state change, EtherChannel-configuratie, NTP, beeldbeheer en meer. FCM web interface voor FXOS CLI kan worden gebruikt voor de configuratie van FXOS.
- Toepassingsmodus (de standaardinstelling) - De applicatiemodus stelt gebruikers in staat om alle beleid in de ASA te configureren. Er zijn alleen geavanceerde opdrachten van de FXOS CLI beschikbaar.

Firepower 2100-modus met ASA wordt geverifieerd met het gebruik van deze opties:

- ASA CLI
- FXOS CLI
- FXOS-toontechnologie

ASA CLI

Volg deze stappen om de FirePOWER 2100-modus met ASA te controleren op de ASA CLI:

1. Gebruik telnet/SSH voor toegang tot de ASA op Firepower 2100.
2. Start de opdracht **Show fxos mode** op CLI:

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

Toepassingsmodus:

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

Opmerking: In multi-context modus, is de opdracht **Show fxos Mode** beschikbaar in het systeem of de **admin** context.

FXOS CLI

Volg deze stappen om de FirePOWER 2100-modus met ASA te controleren op de FXOS CLI:

1. Gebruik telnet/SSH voor toegang tot de ASA op Firepower 2100.

2. Start de opdracht **Connect fxos**:

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

Opmerking: In multi-context modus, is de opdracht **Connect fxos** beschikbaar in de **admin** context.

3. Start de opdracht **Show fxos-mode**:

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

Toepassingsmodus:

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

FXOS-toontechnisch bestand

Volg deze stappen om de Firepower 2100-modus met ASA in het FXOS chassis show-tech-bestand te controleren:

1. Open bestand **tech_support_brief** in **<name>_FPRM.tar.gz/<name>_FPRM.tar**

2. Controleer het gedeelte "**show fxos-mode**":

```
# pwd
```

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

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

Bekende problemen

Cisco bug-id [CSCwb9424](#) ENH: Voeg een CLISH-opdracht toe voor de verificatie van de FMC-configuratie

Cisco bug-id [CSCvn3162](#) ENH: Voeg FXOS SNMP OIDs toe aan de configuratie van logisch apparaat en app-instantie

Cisco bug-id [CSCwb9767](#) ENH: OID toevoegen voor verificatie van het type inzet van een FTD-exemplaar

Cisco bug-id [CSCwb9772](#) ENH: Omvat de uitvoer van de "show fxos Mode" in show-tech van ASA op Firepower 2100

Cisco bug-id [CSCwb9751](#) OID 1.3.6.1.4.1.9.9.491.1.6.1.1 voor een transparante verificatie van de firewallmodus is niet beschikbaar

Gerelateerde informatie

- [Secure Firewall Management Center REST API Quick Start Guide, versie 7.1](#)
- [SNMP configureren op Firepower NGFW applicaties](#)
- [Cisco Firepower Threat Defense REST API-gids](#)
- [Cisco FXOS REST API-referentie](#)
- [Cisco ASA-compatibiliteit](#)
- [Firepower 1000/2100 en Secure Firewall 3100 ASA en FXOS-bundelversies](#)
- [Gebundelde componenten](#)
- [Procedures voor het genereren van bestanden voor firewalls](#)
- [Cisco Firepower 2100 Introductiegids](#)
- [Cisco Firepower Threat Defense-compatibiliteitsgids](#)