Überprüfung von FirePOWER-Modus, Instanz, Hochverfügbarkeits- und Skalierbarkeitskonfiguration

Inhalt

Einleitung

In diesem Dokument wird die Überprüfung der Konfiguration der Hochverfügbarkeit und Skalierbarkeit von Firepower, des Firewall-Modus und des Instanzbereitstellungstyps beschrieben.

Hintergrundinformationen

Die Schritte zur Überprüfung der Hochverfügbarkeits- und Skalierbarkeitskonfiguration, des

Firewall-Modus und des Instanzbereitstellungstyps werden in der Benutzeroberfläche (UI), der Befehlszeilenschnittstelle (CLI), über REST-API-Abfragen, SNMP und in der Fehlerbehebungsdatei angezeigt.

Voraussetzungen

Anforderungen

Grundlegende Produktkenntnisse, REST-API, SNMP.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FirePOWER 11xx
- FirePOWER 21xx
- Firepower 31xx
- FirePOWER 41xx
- FirePOWER Management Center (FMC) Version 7.1.x
- FXOS 2.11.1.x (FirePOWER eXtensible Operating System)
- FirePOWER Device Manager (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

Überprüfen der Konfiguration für hohe Verfügbarkeit und Skalierbarkeit

Hohe Verfügbarkeit bezieht sich auf die Failover-Konfiguration. Die Einrichtung für Hochverfügbarkeit oder Failover fügt sich in zwei Geräte ein, sodass bei Ausfall eines Geräts das andere Gerät übernehmen kann.

Skalierbarkeit bezieht sich auf die Cluster-Konfiguration. Mit einer Clusterkonfiguration können Sie mehrere FTD-Knoten als ein logisches Gerät gruppieren. Ein Cluster bietet den Komfort eines einzelnen Geräts (Verwaltung, Integration in ein Netzwerk) sowie den erhöhten Durchsatz und die Redundanz mehrerer Geräte.

In diesem Dokument werden diese Ausdrücke synonym verwendet:

- Hochverfügbarkeit oder Failover
- Skalierbarkeit oder Cluster

In einigen Fällen ist die Überprüfung der Konfiguration oder des Status für Hochverfügbarkeit und Skalierbarkeit nicht verfügbar. Zum Beispiel gibt es keinen Überprüfungsbefehl für die eigenständige FTD-Konfiguration. Eigenständige Konfigurationen, Failover- und Cluster-Konfigurationen schließen sich gegenseitig aus. Wenn ein Gerät über keine Failover- und Cluster-Konfiguration verfügt, wird davon ausgegangen, dass es im Standalone-Modus betrieben wird.

FMC-Hochverfügbarkeit

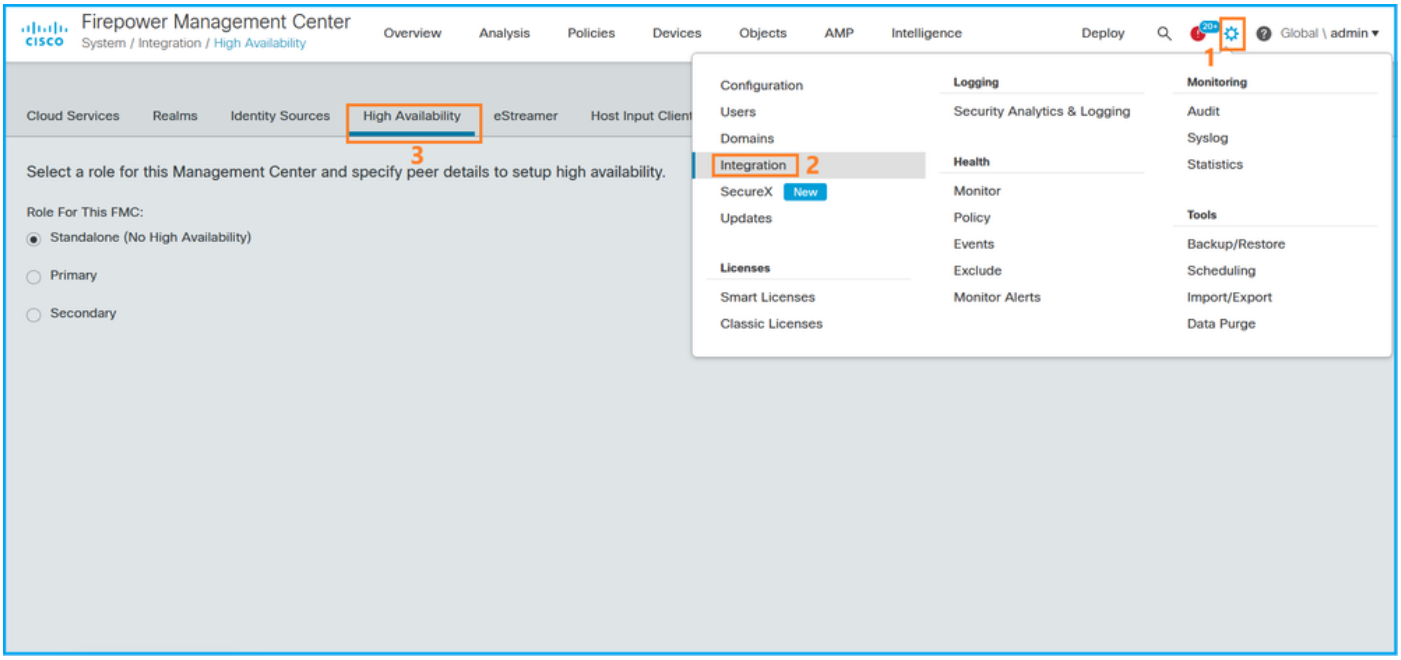
Konfiguration und Status der Hochverfügbarkeit von FMC können mithilfe der folgenden Optionen überprüft werden:

- FMC-Benutzeroberfläche
- FMC-CLI
- REST-API-Anforderung
- FMC-Fehlerbehebungsdatei

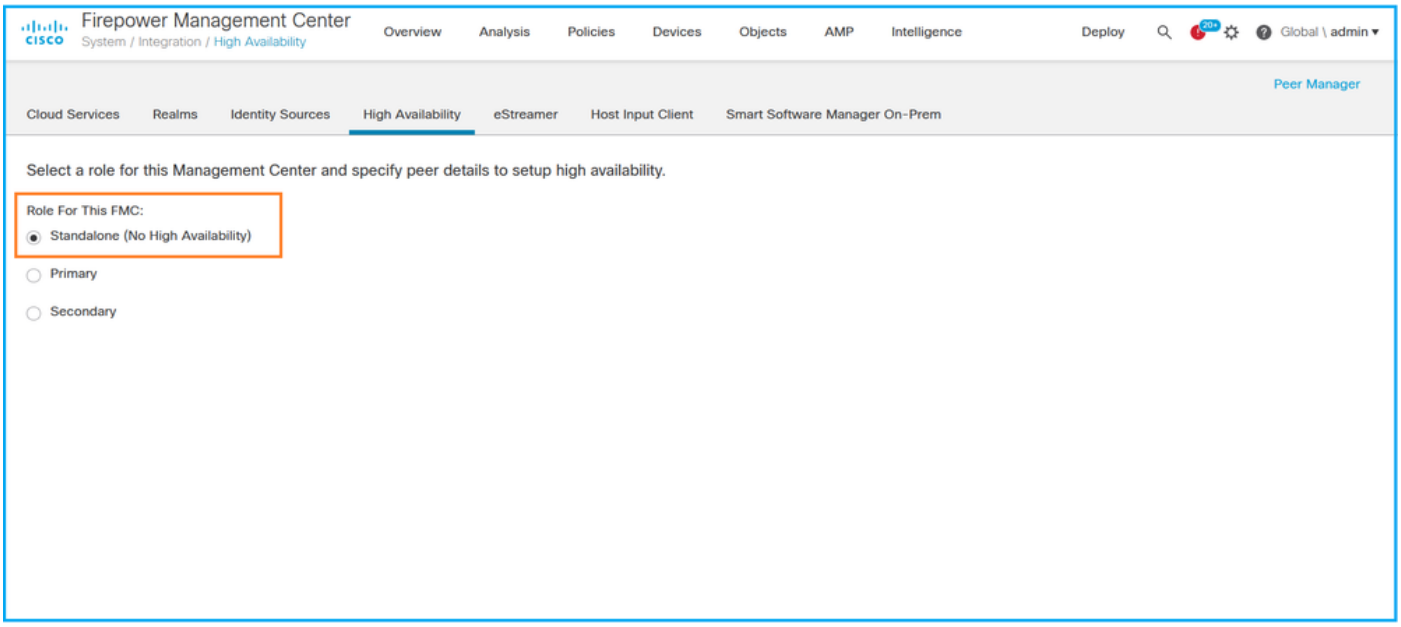
FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die Konfiguration und den Status der FMC-Benutzeroberfläche für hohe Verfügbarkeit zu überprüfen:

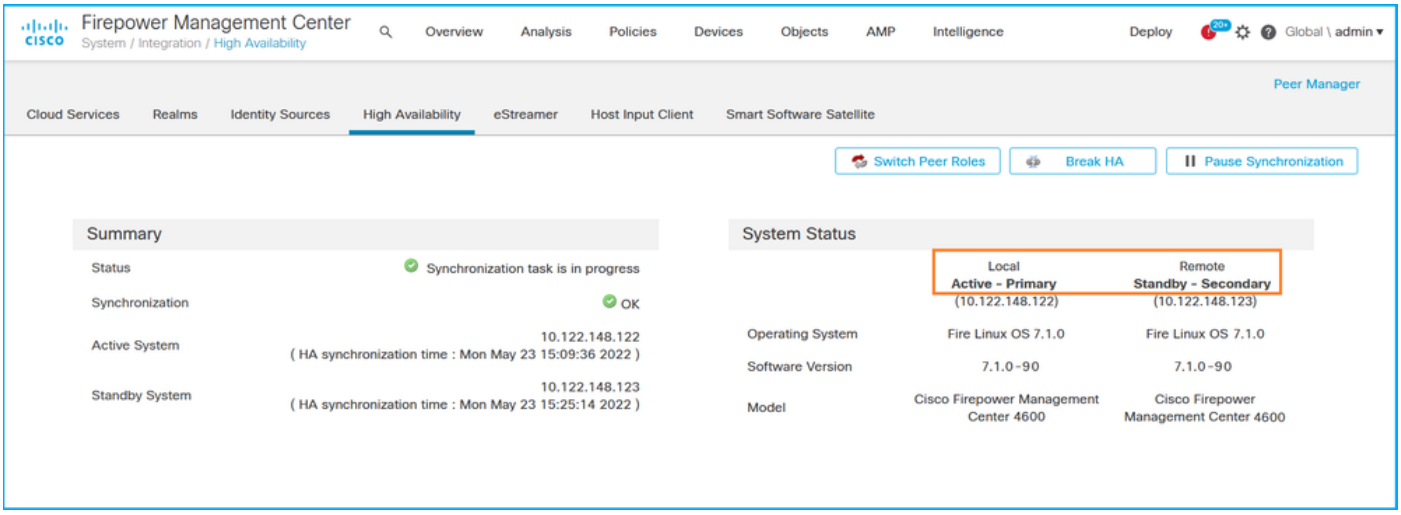
1. Wählen Sie **System > Integration > High Availability:**



2. Überprüfen Sie die Rolle für das FMC. In diesem Fall ist die Hochverfügbarkeit nicht konfiguriert, und das FMC arbeitet in einer eigenständigen Konfiguration:



Wenn eine hohe Verfügbarkeit konfiguriert ist, werden lokale und Remote-Rollen angezeigt:



FMC-CLI

Führen Sie die folgenden Schritte aus, um die Konfiguration und den Status der FMC-CLI für hohe Verfügbarkeit zu überprüfen:

1. Zugriff auf FMC über SSH oder Konsolenverbindung.

2. Führen Sie den Befehl **experte** aus, und führen Sie dann den Befehl **sudo su aus**:

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

3. Führen Sie den Befehl **troubleshoot_HADC.pl aus,** und wählen Sie Option **1 Show HA Info Of FMC aus.** Wenn keine Hochverfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
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
```

Wenn eine hohe Verfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
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
```

> **Anmerkung:** In einer Hochverfügbarkeitskonfiguration kann die FMC-Rolle eine **primäre** oder **sekundäre** Rolle sowie einen **Aktiv**- oder **Standby-**Status haben.

FMC REST-API

Befolgen Sie diese Schritte, um die Konfiguration und den Status der FMC-Hochverfügbarkeit und -Skalierbarkeit über die FMC REST-API zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

```
# 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. Verwenden Sie das Token in dieser Abfrage, um die UUID der globalen Domäne zu ermitteln:

```
# 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
   }
}
```

Anmerkung: Der Teil "**| python -m json.tool**" der Befehlszeichenfolge dient zur Formatierung der Ausgabe im JSON-Stil und ist optional.

3. Verwenden Sie die globale Domänen-UUID in dieser Abfrage:

```
# 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
```

Wenn keine Hochverfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

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

Wenn eine hohe Verfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

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


FMC-Fehlerbehebungsdatei

Führen Sie die folgenden Schritte aus, um die Konfiguration und den Status der FMC-Fehlerbehebungsdatei für hohe Verfügbarkeit zu überprüfen:

1. Öffnen Sie die Fehlerbehebungsdatei, und navigieren Sie zum Ordner **<Dateiname>.tar/results-<date>—xxxxxx/command-output.**

2. Öffnen Sie die Datei **usr-local-sf-bin-troubleshoot_HADC.pl -a.output:**

Wenn keine Hochverfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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
```

Wenn eine hohe Verfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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
```

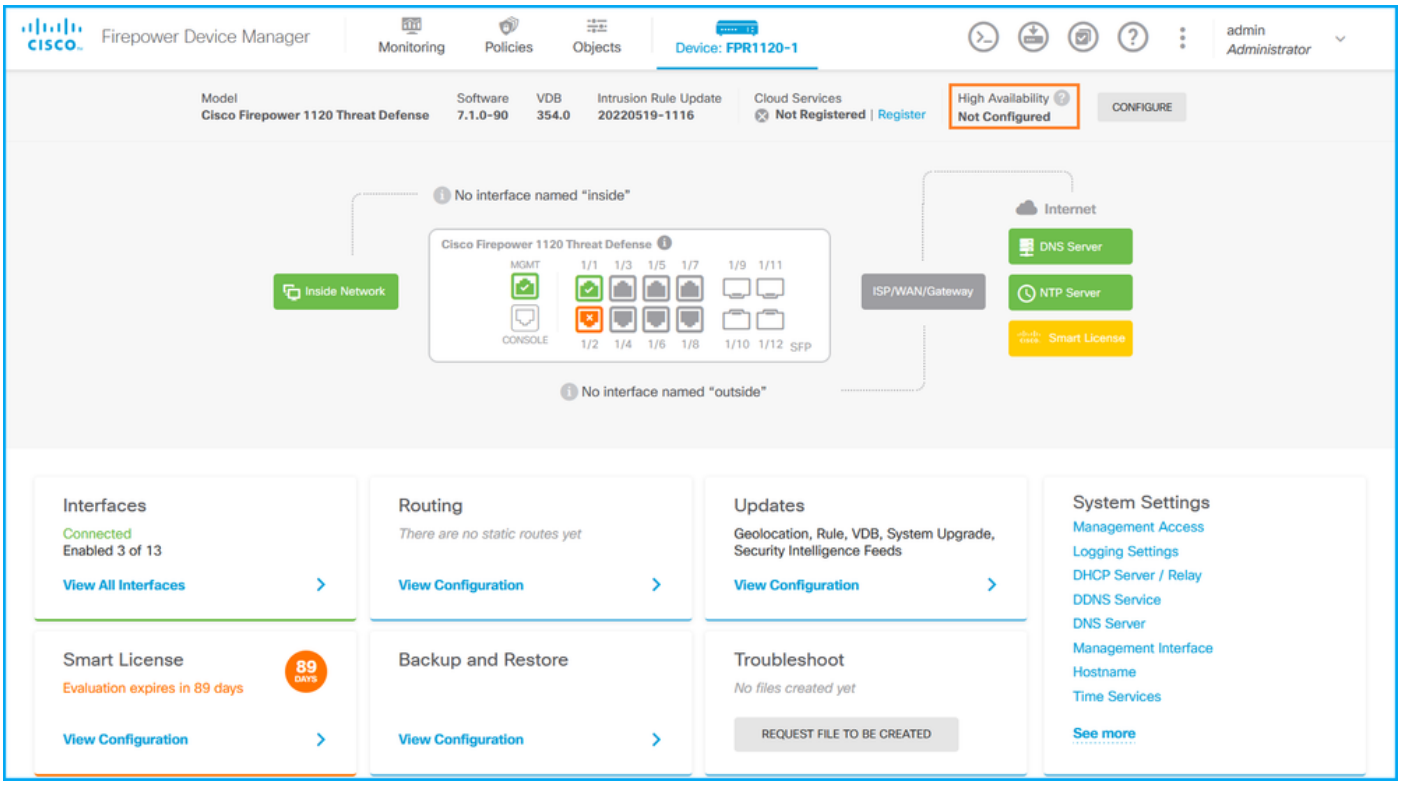
Hochverfügbarkeit von FDM

Konfiguration und Status der Hochverfügbarkeit von FDM können mithilfe der folgenden Optionen überprüft werden:

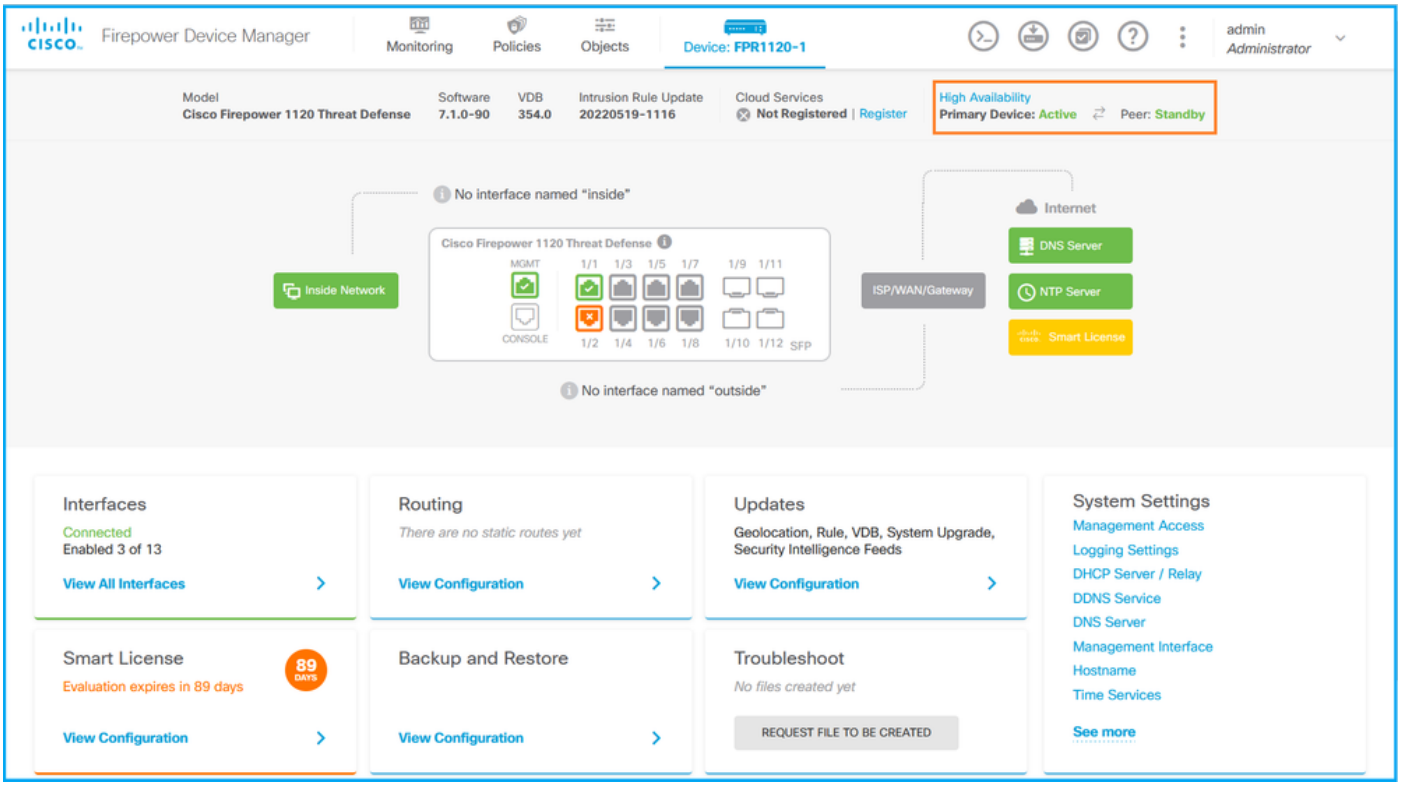
- FDM-Benutzeroberfläche
- FDM REST API-Anforderung
- FTD-CLI
- FTD-SNMP-Umfrage
- FTD-Fehlerbehebungsdatei

FDM-Benutzeroberfläche

Um die Konfiguration und den Status der FDM-Hochverfügbarkeit auf der FDM-Benutzeroberfläche zu überprüfen, überprüfen Sie die **Hochverfügbarkeit** auf der Hauptseite. Wenn keine Hochverfügbarkeit konfiguriert ist, ist der Wert **für hohe Verfügbarkeit nicht konfiguriert:**



Wenn eine hohe Verfügbarkeit konfiguriert ist, werden die Failover-Konfiguration und -Rollen der lokalen und Remote-Peer-Einheit angezeigt:



FDM REST-API

Führen Sie diese Schritte aus, um die Konfiguration und den Status der FDM-Hochverfügbarkeit über eine FDM-REST-API-Anforderung zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

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

2. Verwenden Sie zum Verifizieren der Konfiguration für eine hohe Verfügbarkeit den Tokenwert in dieser Abfrage:

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

jLWE5MmEtMjk4YjRjZTUxNmJjIiwibmJmIjoxNjUzMjA4NTI4LCJleHAiOjE2NTMyMTAzMjgsInJlZnJlc2hUb2tlbkV4cGlyZXNBdCI6MTY1MzIxMDkyODU2OSwidG9rZW5UeXBlIjoiSldUX0FjY2VzcyIsInVzZXJVdWlkIjoiYTNmZDA3ZjMtZDgxZS0xMWVjLWE5MmEtYzk5N2UxNDcyNTM0IiwidXNlclJvbGUiOiJST0xFX0FETUlOIiwib3JpZ2luIjoicGFzc3dvcmQiLCJ1c2VybmFtZSI6ImFkbWluIn0.ai3LUbnsLOJTN6exKOANsEG5qTD6L-ANd_1V6TbFe6M'
'https://192.0.2.3/api/fdm/v6/devices/default/ha/configurations'

Wenn keine Hochverfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:


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


Wenn eine hohe Verfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:


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


3. Verwenden Sie folgende Abfrage, um den Hochverfügbarkeitsstatus zu überprüfen:

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

Wenn keine Hochverfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
{
 "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"
 }
}
```

Wenn eine hohe Verfügbarkeit konfiguriert ist, wird diese Ausgabe angezeigt:

```
{
 "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

Befolgen Sie die Schritte im Abschnitt.

FTD-SNMP-Umfrage

Befolgen Sie die Schritte im Abschnitt.

FTD-Fehlerbehebungsdatei

Befolgen Sie die Schritte im Abschnitt.

FTD Hohe Verfügbarkeit und Skalierbarkeit

Die Konfiguration und der Status der hochverfügbaren FTD-Hardware sowie die Skalierbarkeit können mithilfe der folgenden Optionen überprüft werden:

- FTD-CLI
- FTD-SNMP
- FTD-Fehlerbehebungsdatei
- FMC-Benutzeroberfläche
- FMC REST-API
- FDM-Benutzeroberfläche
- FDM REST-API
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

FTD-CLI

Gehen Sie folgendermaßen vor, um die Konfiguration und den Status der FTD-CLI für hohe Verfügbarkeit und Skalierbarkeit zu überprüfen:

1. Verwenden Sie die folgenden Optionen, um in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus auf die FTD-CLI zuzugreifen:

- Direkter SSH-Zugriff auf FTD - alle Plattformen
- Zugriff von der FXOS-Konsolen-CLI (Firepower 1000/2100/3100) über Befehl **connect ftd**
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):
  connect module <x> [console|telnet], wobei x die Steckplatz-ID ist, und dann **connect ftd [instance],** wobei die Instanz nur für die Bereitstellung mehrerer Instanzen relevant ist

- Für virtuelle FTDs direkter SSH-Zugriff auf FTD oder Konsolenzugriff über Hypervisor oder Cloud-Benutzeroberfläche

2. Um die FTD-Failover-Konfiguration und den Status zu überprüfen, führen Sie den **Failover show running-config aus** und **zeigen** Befehle für den Failover-Status in der CLI an.

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

```
> 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==
```

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
> 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. Um die Konfiguration und den Status des FTD-Clusters zu überprüfen, führen Sie das **show running-config-Cluster aus,** und **zeigen Sie Cluster-Info-**Befehle in der CLI an.

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

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

Wenn der Cluster konfiguriert ist, wird diese Ausgabe angezeigt:

```
> 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
```

Anmerkung: Die **Master-** und Kontrollrollen sind identisch.

FTD-SNMP

Befolgen Sie diese Schritte, um die Konfiguration und den Status der hochverfügbaren FTD-Hardware sowie die Skalierbarkeit über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP konfiguriert und aktiviert ist. Informationen zu FDM-verwalteten FTD finden Sie unter Konfigurieren und Beheben von SNMP auf FirePOWER FDM für Konfigurationsschritte. Informationen zu FMC-verwalteten FTD finden Sie unter Konfigurieren von SNMP auf Firepower NGFW-Appliances für Konfigurationsschritte.

2. Um die FTD-Failover-Konfiguration und den Status zu überprüfen, suchen Sie die OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1.**

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

```
# 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"
```

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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. Um die Clusterkonfiguration und den Cluster-Status zu überprüfen, suchen Sie die OID **1.3.6.1.4.1.9.9.491.1.8.1.**

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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
```

Wenn der Cluster konfiguriert, aber nicht aktiviert ist, wird diese Ausgabe angezeigt:

```
# 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
...
```

Wenn der Cluster konfiguriert, aktiviert und betriebsbereit ist, wird diese Ausgabe angezeigt:

```
# 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
...
```

Weitere Informationen zu den OID-Beschreibungen finden Sie in der CISCO-UNIFIED-FIREWALL-MIB.

FTD-Fehlerbehebungsdatei

Führen Sie die folgenden Schritte aus, um die Konfiguration und den Status der FTD-Fehlerbehebungsdatei für hohe Verfügbarkeit und Skalierbarkeit zu überprüfen:

1. Öffnen Sie die Datei zur Fehlerbehebung, und navigieren Sie zum Ordner **<Dateiname>-troubleshoot .tar/results-<date>—xxxxxx/command-output.**

2. Öffnen Sie die Datei **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. Um die Failover-Konfiguration und den Status zu überprüfen, überprüfen Sie den Abschnitt **show failover**.

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

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

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
------------------ 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. Um die Konfiguration und den Status des FTD-Clusters zu überprüfen, aktivieren Sie den Abschnitt show cluster info.

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

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

Wenn der Cluster konfiguriert und aktiviert ist, wird diese Ausgabe angezeigt:

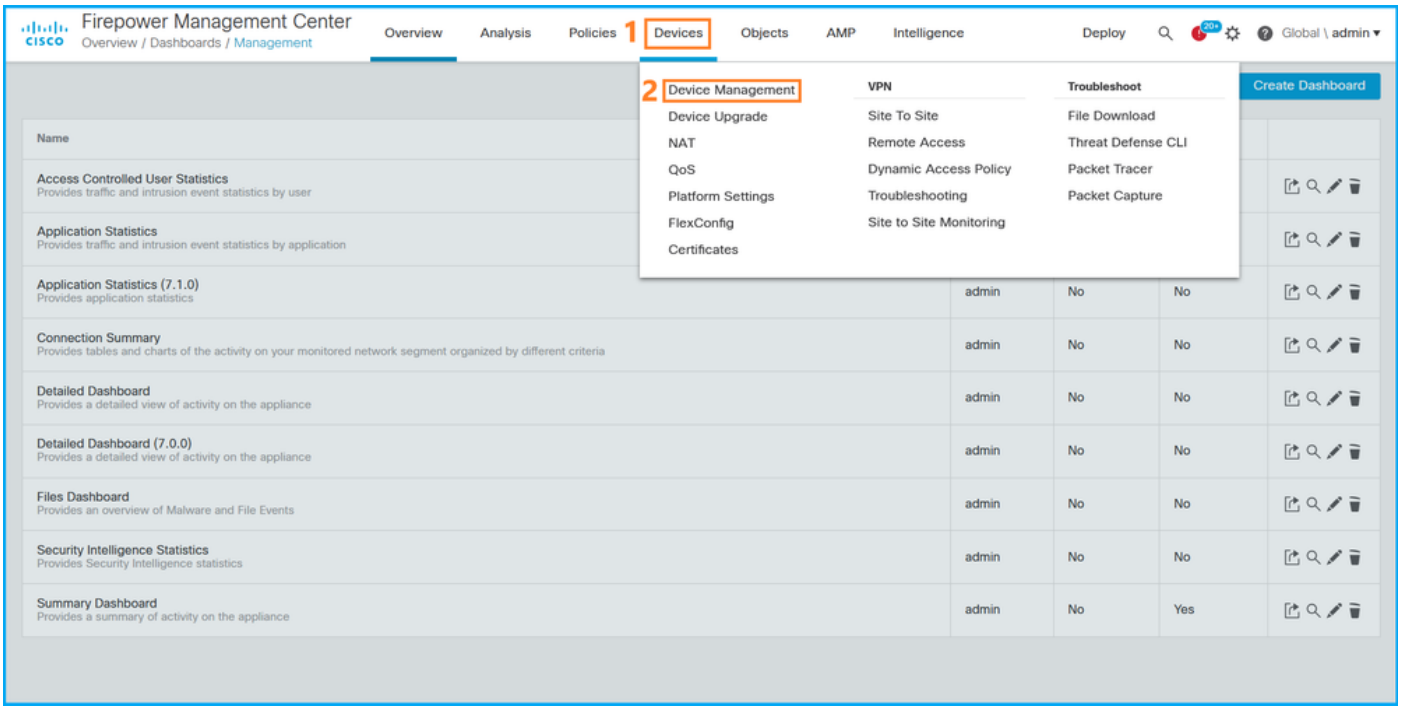
```
------------------ show cluster info ------------------
Cluster ftd_cluster1: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID        : 0
        Site ID   : 1
        Version   : 9.17(1)
        Serial No.: FLM1949C5RR6HE
        CCL IP 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

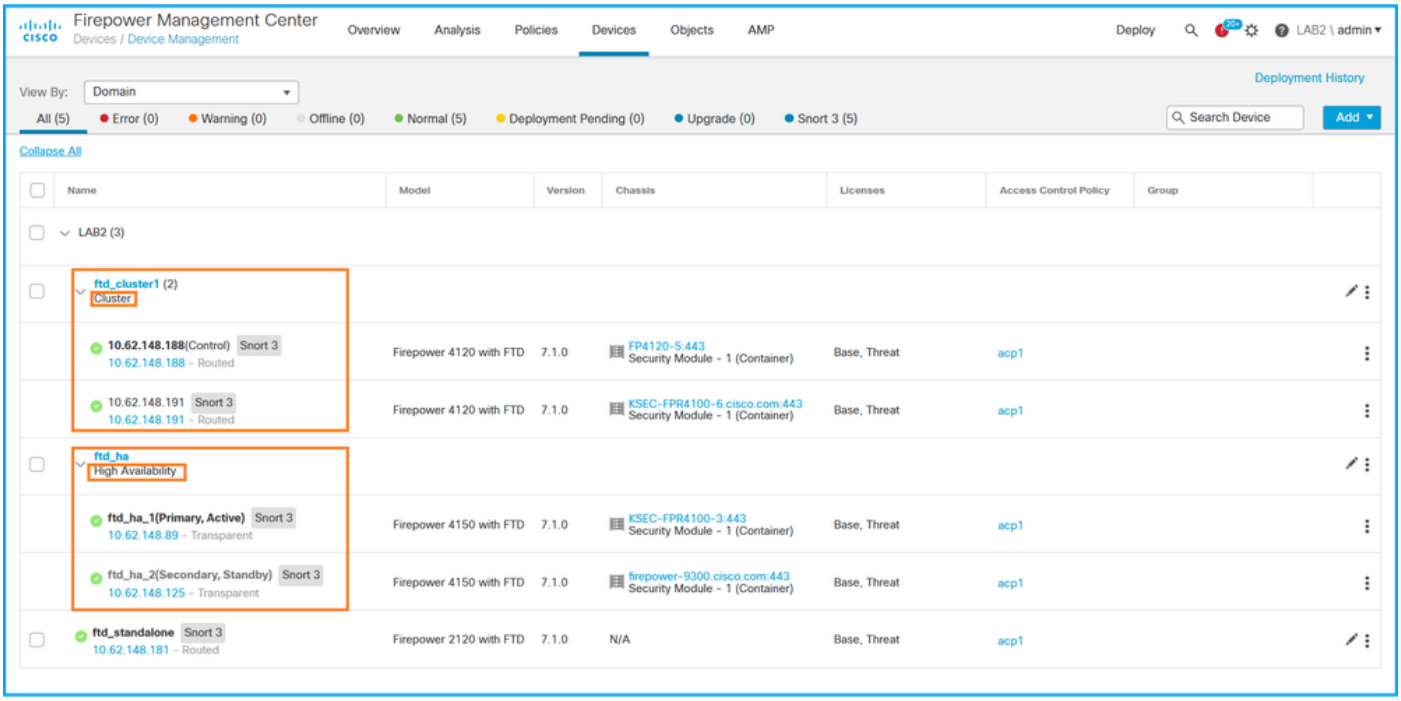
FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um die Konfiguration und den Status der FMC-Benutzeroberfläche für hohe Verfügbarkeit und Skalierbarkeit in FTD zu überprüfen:

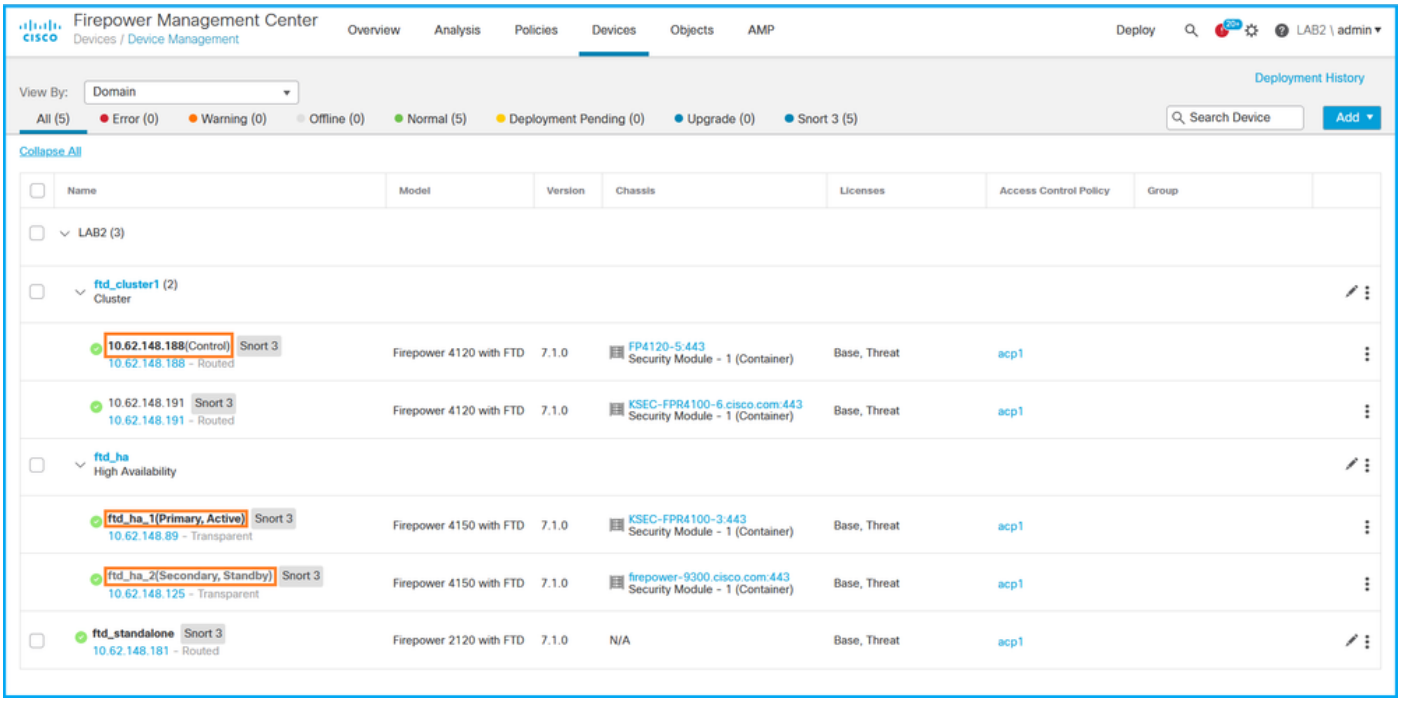
1. Wählen Sie **Geräte > Gerätemanagement**:



2. Überprüfen Sie zur Überprüfung der FTD-Konfiguration für hohe Verfügbarkeit und Skalierbarkeit die Beschriftungen **High Availability** oder **Cluster**. Wenn keine dieser Optionen vorhanden ist, wird die FTD in einer eigenständigen Konfiguration ausgeführt:



3. Überprüfen Sie zur Überprüfung des FTD-Hochverfügbarkeits- und Skalierbarkeitsstatus die Einheitenrolle in Klammern. Wenn eine Rolle nicht vorhanden ist und die FTD nicht Teil eines Clusters oder Failovers ist, wird FTD in einer eigenständigen Konfiguration ausgeführt:



Anmerkung: Im Fall eines Clusters wird nur die Rolle der **Steuerungseinheit** angezeigt.

FMC REST-API

In diesen Ausgaben sind **ftd_ha_1, ftd_ha_2, ftd_standalone, ftd_ha, ftc_cluster1** vom Benutzer konfigurierbare Gerätenamen. Diese Namen beziehen sich nicht auf die tatsächliche Konfiguration oder den Status der Hochverfügbarkeit und Skalierbarkeit.

Befolgen Sie diese Schritte, um die Konfiguration und den Status der FTD-Hochverfügbarkeit und Skalierbarkeit über die FMC REST-API zu überprüfen. Verwenden eines REST-API-Clients In

diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

```
# 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. Identifizieren Sie die Domäne, die das Gerät enthält. In den meisten REST-API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das Token in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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. Verwenden Sie die Domänen-UUID, um die spezifischen **Gerätedatensätze** und die UUID des jeweiligen Geräts abzufragen:

```
# 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. Um die Failover-Konfiguration zu überprüfen, verwenden Sie in dieser Abfrage die Domänen-UUID und die Geräte-/Container-UUID aus Schritt 3:

```
# 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. Um den Failover-Status zu überprüfen, verwenden Sie in dieser Abfrage die Domänen-UUID und die DeviceHAPair-UUID aus Schritt 4:

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

6. Verwenden Sie zum Verifizieren der Clusterkonfiguration in dieser Abfrage die Domänen-UUID und die Geräte-/Container-UUID aus Schritt 3:

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

7. Um den Cluster-Status zu überprüfen, verwenden Sie die Domänen-UUID und die Geräte-/Container-UUID aus Schritt 6 in dieser Abfrage:

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

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


FDM-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

FDM REST-API

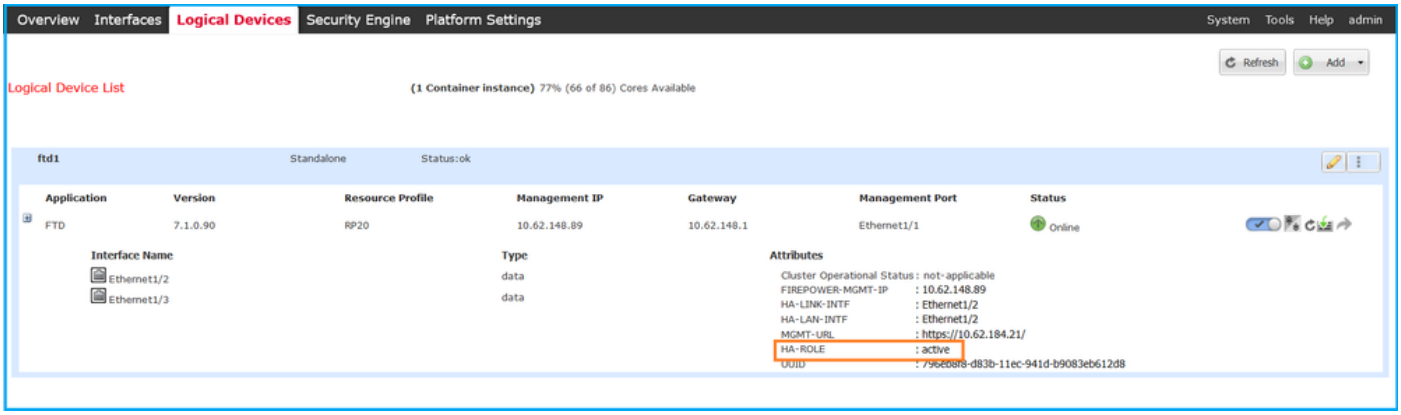
Befolgen Sie die Schritte im Abschnitt.

FCM-Benutzeroberfläche

Die FCM-Benutzeroberfläche ist für Firepower 4100/9300 und Firepower 2100 mit ASA im Plattformmodus verfügbar.

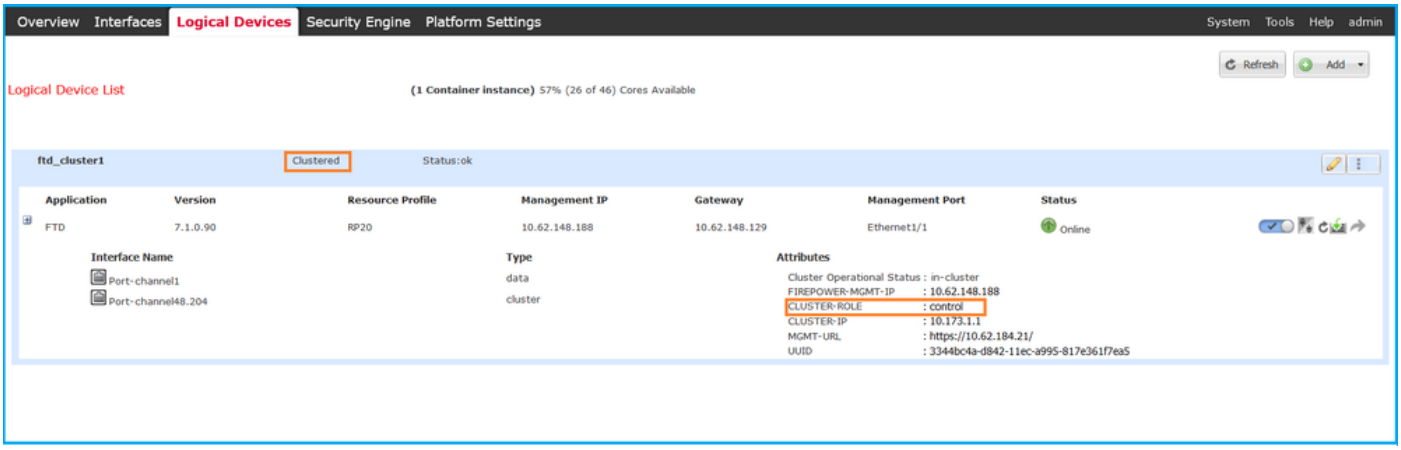
Gehen Sie folgendermaßen vor, um den FTD-Hochverfügbarkeits- und Skalierbarkeitsstatus auf der FCM-Benutzeroberfläche zu überprüfen:

1. Um den FTD-Failover-Status zu überprüfen, überprüfen Sie den Attributwert **HA-ROLE** auf der Seite Logical Devices (Logische Geräte):



> **Anmerkung:** Das **Standalone**-Label neben der logischen Gerätekennung bezieht sich auf die Konfiguration des logischen Chassis-Geräts und nicht auf die FTD-Failover-Konfiguration.

2. Um die FTD-Cluster-Konfiguration und den Status zu überprüfen, überprüfen Sie das **Clustered** Label und den Attributwert **CLUSTER-ROLE** auf der Seite Logical Devices (Logische Geräte):



FXOS-CLI

Die FTD-Konfiguration für hohe Verfügbarkeit und Skalierbarkeit sowie die Statusüberprüfung der FXOS-CLI sind für Firepower 4100/9300 verfügbar.

Gehen Sie folgendermaßen vor, um die Konfiguration und den Status der FXOS-CLI für FTD-Hochverfügbarkeit und Skalierbarkeit zu überprüfen:

1. Stellen Sie eine Konsolen- oder SSH-Verbindung zum Chassis her.

2. Um den FTD-Hochverfügbarkeitsstatus zu überprüfen, führen Sie den Befehl **scope ssa** aus, und starten Sie dann den **Scope-Steckplatz <x>**, um zu dem spezifischen Steckplatz zu wechseln, in dem die FTD ausgeführt wird, und führen Sie den Befehl **show app-instance extends aus**:

```
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. Um die Konfiguration und den Status des FTD-Clusters zu überprüfen, führen Sie den Befehl **scope ssa** aus, führen Sie den Befehl **show logy-device <name> detail extends** aus, wobei der

Name der logische Gerätename und der Befehl **show app-instance lautet.** Prüfen Sie die Ausgabe für einen bestimmten Steckplatz:

```
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 wird von Firepower 4100/9300 unterstützt.

Befolgen Sie diese Schritte, um die Konfiguration und den Status der FTD-Hochverfügbarkeit und Skalierbarkeit über eine FXOS-REST-API-Anfrage zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

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

2. Verwenden Sie zur Überprüfung des FTD-Failover-Status das Token und die Steckplatz-ID in dieser Abfrage:

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

```
            "fsmProgr": "100",             "fsmRmtInvErrCode": "none",
"fsmRmtInvErrDescr": "",             "fsmRmtInvRslt": "",             "fsmStageDescr": "",
            "fsmStatus": "nop",             "fsmTry": "0",             "hotfix": "",
 "identifier": "ftd1",
            "operationalState": "online",
            "reasonForDebundle": "",
            "resourceProfileName": "RP20",
            "runningVersion": "7.1.0.90",
            "smAppAttribute": [
                {
                    "key": "firepower-mgmt-ip",
                    "rn": "app-attribute-firepower-mgmt-ip",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
firepower-mgmt-ip",
                    "value": "192.0.2.5"
                },
                {
                    "key": "ha-link-intf",
                    "rn": "app-attribute-ha-link-intf",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-link-intf",
                    "value": "Ethernet1/2"
                },
                {
                    "key": "ha-lan-intf",
                    "rn": "app-attribute-ha-lan-intf",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-lan-intf",
                    "value": "Ethernet1/2"
                },
                {
                    "key": "mgmt-url",
                    "rn": "app-attribute-mgmt-url",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
mgmt-url",
                    "value": "https://192.0.2.1/"
                },
                {
                    "key": "ha-role",
                    "rn": "app-attribute-ha-role",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
ha-role",
                    "value": "active"
                },
                {
                    "key": "uuid",
                    "rn": "app-attribute-uuid",
                    "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-
uuid",
                    "value": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
                }
            ],
...
```

3. Um die FTD-Cluster-Konfiguration zu überprüfen, verwenden Sie die logische Geräte-ID in dieser Abfrage:

```
# 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. Verwenden Sie die folgende Abfrage, um den FTD-Cluster-Status zu überprüfen:


```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
'https://192.0.2.102/api/slot/1/app-inst'
{
    "smAppInstance": [
        {
            "adminState": "enabled",
            "appDn": "sec-svc/app-ftd-7.1.0.90",
            "appInstId": "ftd_001_JAD19500BABIYA3OO58",
            "appName": "ftd",
            "clearLogData": "available",
            "clusterOperationalState": "in-cluster",
            "clusterRole": "master",
            "currentJobProgress": "100",
            "currentJobState": "succeeded",
            "currentJobType": "start",
            "deployType": "container",
            "dn": "slot/1/app-inst/ftd-ftd_cluster1",
            "errorMsg": "",
            "eventMsg": "",
            "executeCmd": "ok",
            "externallyUpgraded": "no",
            "fsmDescr": "",
            "fsmProgr": "100",
            "fsmRmtInvErrCode": "none",
            "fsmRmtInvErrDescr": "",
            "fsmRmtInvRslt": "",
            "fsmStageDescr": "",
            "fsmStatus": "nop",
            "fsmTry": "0",
            "hotfix": "",
```

```
            "identifier": "ftd_cluster1",
            "operationalState": "online",
            "reasonForDebundle": "",
            "resourceProfileName": "RP20",
            "runningVersion": "7.1.0.90",
...
```

FXOS-Chassis-Show-Tech-Datei

Die Konfiguration und der Status der FTD-Hochverfügbarkeit und Skalierbarkeit können in der Show-Tech-Datei des FirePOWER 4100/9300-Chassis überprüft werden.

Gehen Sie folgendermaßen vor, um die Konfiguration und den Status der Hochverfügbarkeit und Skalierbarkeit in der show-tech-Datei des FXOS-Chassis zu überprüfen:

1. Öffnen Sie für FXOS-Versionen 2.7 und höher die Datei **sam_techsupportinfo** in **<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

   Für ältere Versionen öffnen Sie die Datei **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar.**

2. Um den Failover-Status zu überprüfen, überprüfen Sie den Wert des **ha-role-**Attributwerts unter dem jeweiligen Steckplatz im Abschnitt **"show slot extends Detail" (Auszubildende Steckplatz anzeigen):**

```
# 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. Um die FTD-Cluster-Konfiguration zu überprüfen, überprüfen Sie den Wert des **Mode**-Attributwerts unter dem jeweiligen Steckplatz im Abschnitt **"show logy-device detail extends"** :

```
`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. Um den FTD-Cluster-Status zu überprüfen, überprüfen Sie den Wert der Attributwerte **Cluster State** und **Cluster Role** unter dem jeweiligen Steckplatz im Abschnitt **"show slot extends detail" (Erweiterungssteckplatz anzeigen):**

```
`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 Hohe Verfügbarkeit und Skalierbarkeit

Konfiguration und Status der ASA-Hochverfügbarkeit und Skalierbarkeit können mithilfe der folgenden Optionen überprüft werden:

- ASA-CLI
- ASA-SNMP-Umfrage
- ASA-Showtech-Datei
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

ASA-CLI

Führen Sie die folgenden Schritte aus, um die Konfiguration der ASA-Hochverfügbarkeit und Skalierbarkeit in der ASA-CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen für den Zugriff auf die ASA-CLI in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus:

- Direkter Telnet-/SSH-Zugriff auf ASA mit Firepower 1000/3100 und Firepower 2100 im Appliance-Modus
- Zugriff von der FXOS-Konsolen-CLI auf der FirePOWER 2100 im Plattform-Modus und Verbindung mit ASA über den Befehl **connect as a**

- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):
  Verbinden Sie das Modul <x> [console|telnet], wobei x die Steckplatz-ID ist, und **verbinden Sie** sich dann **als**

- Für virtuelle ASA direkter SSH-Zugriff auf ASA oder Konsolenzugriff über die Hypervisor- oder Cloud-Benutzeroberfläche

2. Um die ASA-Failover-Konfiguration und den ASA-Status zu überprüfen, führen Sie den **Failover show running-config aus** und **zeigen** Befehle für den Failover-Status in der ASA CLI an.

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

```
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==
```

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
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. Um die Konfiguration und den Status des ASA-Clusters zu überprüfen, führen Sie das **show running-config-Cluster aus,** und **zeigen Sie Cluster-Info-**Befehle in der CLI an.

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

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

Wenn der Cluster konfiguriert ist, wird diese Ausgabe angezeigt:

```
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

Führen Sie die folgenden Schritte aus, um die Konfiguration der Hochverfügbarkeit und Skalierbarkeit der ASA über SNMP zu überprüfen:

1. Stellen Sie sicher, dass SNMP konfiguriert und aktiviert ist.
2. Um die Failover-Konfiguration und den Status zu überprüfen, wählen Sie die OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1 aus.

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

```
# 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"
```

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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. Um die Clusterkonfiguration und den Status zu überprüfen, wählen Sie die OID **1.3.6.1.4.1.9.9.491.1.8.1 aus.**

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

```
# 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
```

Wenn der Cluster konfiguriert, aber nicht aktiviert ist, wird diese Ausgabe angezeigt:

```
# 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
...
```

Wenn der Cluster konfiguriert, aktiviert und betriebsbereit ist, wird diese Ausgabe angezeigt:

```
# 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
...
```

Weitere Informationen zu den OID-Beschreibungen finden Sie in der CISCO-UNIFIED-FIREWALL-MIB.

ASA-Showtech-Datei

1. Um die ASA-Failover-Konfiguration und den Status zu überprüfen, aktivieren Sie den Abschnitt **show failover**.

Wenn das Failover nicht konfiguriert ist, wird folgende Ausgabe angezeigt:

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

Wenn das Failover konfiguriert ist, wird diese Ausgabe angezeigt:

```
------------------ 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. Um die Clusterkonfiguration und den Status zu überprüfen, aktivieren Sie den Abschnitt **show cluster info**.

Wenn der Cluster nicht konfiguriert ist, wird diese Ausgabe angezeigt:

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

Wenn der Cluster konfiguriert und aktiviert ist, wird diese Ausgabe angezeigt:

```
------------------ 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-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

FXOS-CLI

Befolgen Sie die Schritte im Abschnitt.

FXOS REST-API

Befolgen Sie die Schritte im Abschnitt.

FXOS-Chassis-Show-Tech-Datei

Befolgen Sie die Schritte im Abschnitt.

Überprüfen des Firewall-Modus

FTD-Firewall-Modus

Der Firewall-Modus bezieht sich auf eine Routing- oder transparente Firewall-Konfiguration.

Der FTD-Firewall-Modus kann mithilfe der folgenden Optionen überprüft werden:

- FTD-CLI
- FTD-Showtech
- FMC-Benutzeroberfläche
- FMC REST-API
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

Anmerkung: FDM unterstützt keinen transparenten Modus.

FTD-CLI

Führen Sie die folgenden Schritte aus, um den FTD-Firewall-Modus in der FTD-CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen, um in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus auf die FTD-CLI zuzugreifen:

- Direkter SSH-Zugriff auf FTD - alle Plattformen
- Zugriff von der FXOS-Konsolen-CLI (Firepower 1000/2100/3100) über Befehl **connect ftd**
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):
  connect module <x> [console|telnet], wobei x die Steckplatz-ID ist, und

  connect ftd [instance], wobei die Instanz nur für die Bereitstellung mehrerer Instanzen relevant ist.

- Für virtuelle FTDs direkter SSH-Zugriff auf FTD oder Konsolenzugriff über Hypervisor oder Cloud-Benutzeroberfläche

2. Um den Firewall-Modus zu überprüfen, führen Sie den Befehl **show firewall** in der CLI aus:

```
> show firewall
```

```
Firewall mode: Transparent
```

FTD-Fehlerbehebungsdatei

Befolgen Sie diese Schritte, um den FTD-Firewall-Modus in der FTD-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Datei zur Fehlerbehebung, und navigieren Sie zum Ordner **<Dateiname>-troubleshoot .tar/results-<date>—xxxxxx/command-output.**

2. Öffnen Sie die Datei **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'
```

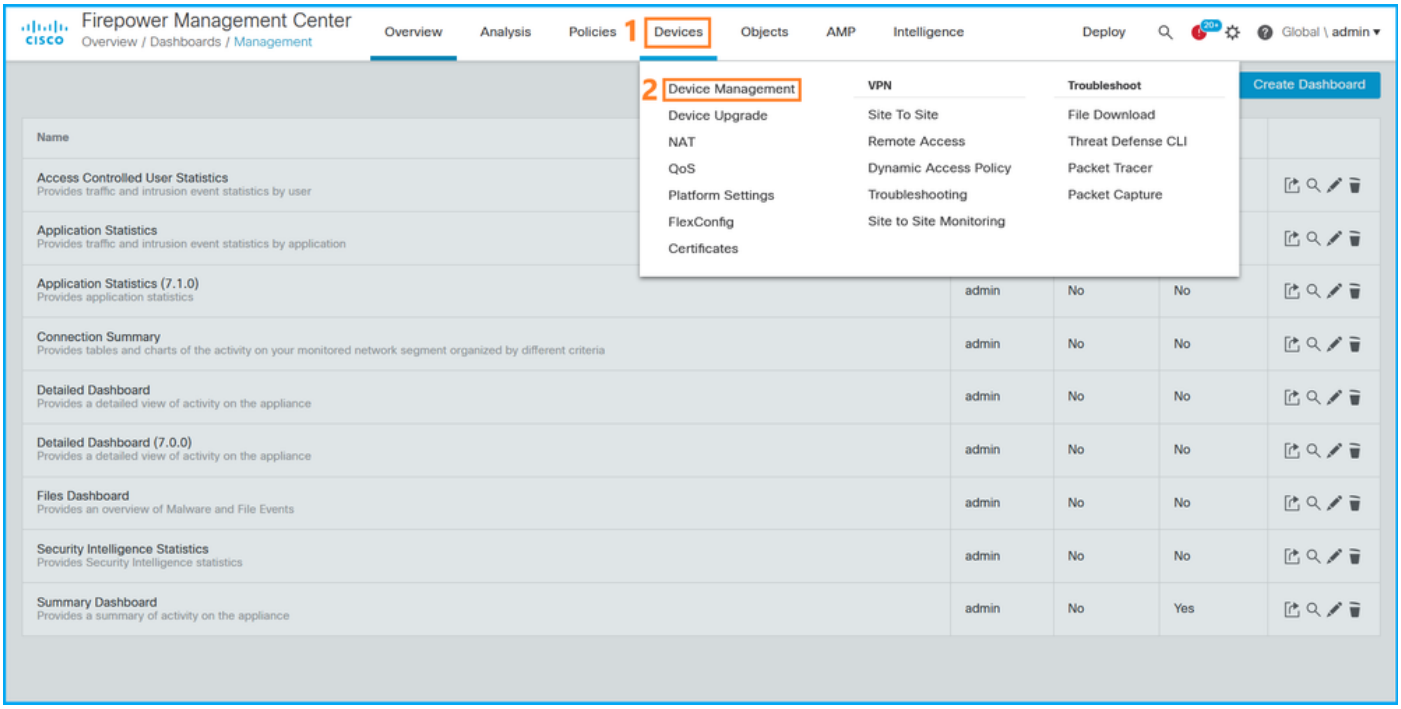
3. Um den FTD-Firewall-Modus zu überprüfen, aktivieren Sie den Abschnitt **"Firewall anzeigen"**:

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

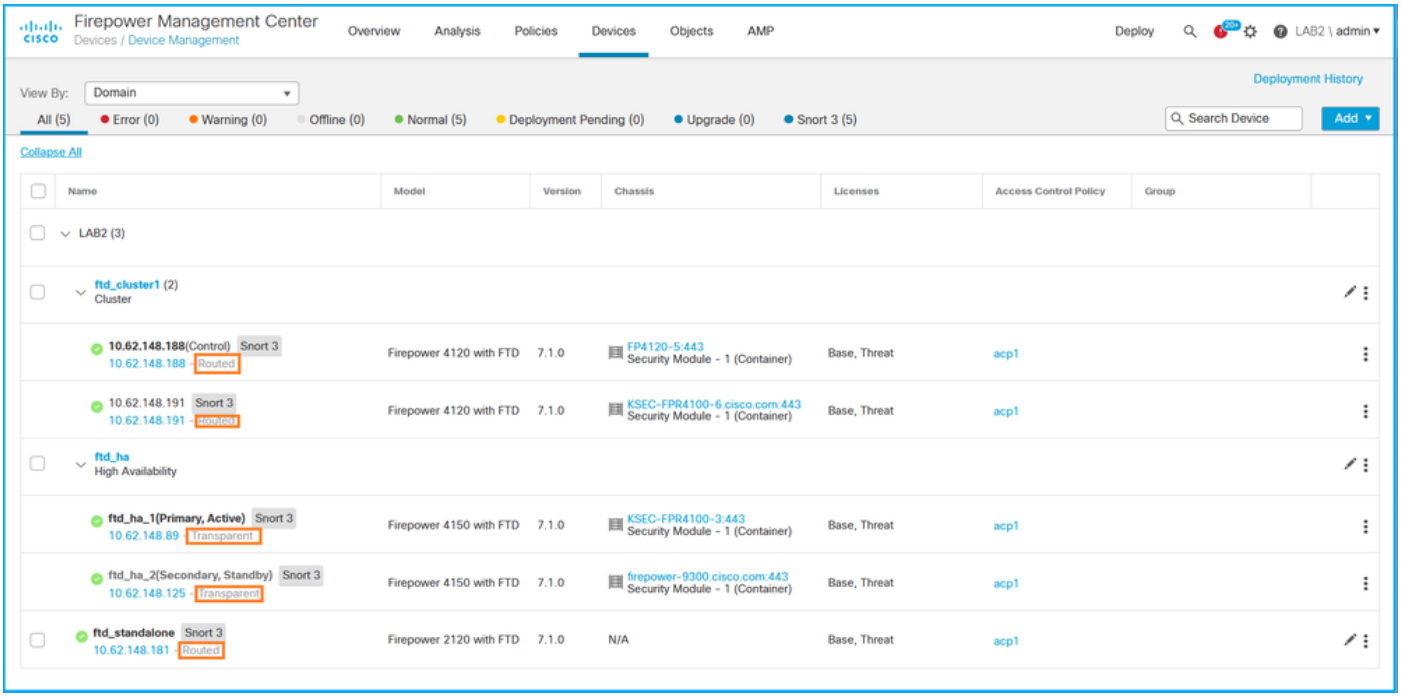
FMC-Benutzeroberfläche

Führen Sie die folgenden Schritte aus, um den FTD-Firewall-Modus auf der FMC-Benutzeroberfläche zu überprüfen:

1. Wählen Sie **Geräte > Gerätemanagement**:



2. Überprüfen Sie die Bezeichnungen **Routed** oder **Transparent**:



FMC REST-API

Befolgen Sie diese Schritte, um den FTD-Firewall-Modus über FMC REST-API zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

```
# 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. Identifizieren Sie die Domäne, die das Gerät enthält. In den meisten REST-API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das Token in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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. Verwenden Sie die Domänen-UUID, um die spezifischen **Gerätedatensätze** und die UUID des jeweiligen Geräts abzufragen:

```
# 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. Verwenden Sie in dieser Abfrage die Domänen-UUID und die Geräte-/Container-UUID aus Schritt 3, und überprüfen Sie den Wert von **ftdMode**:

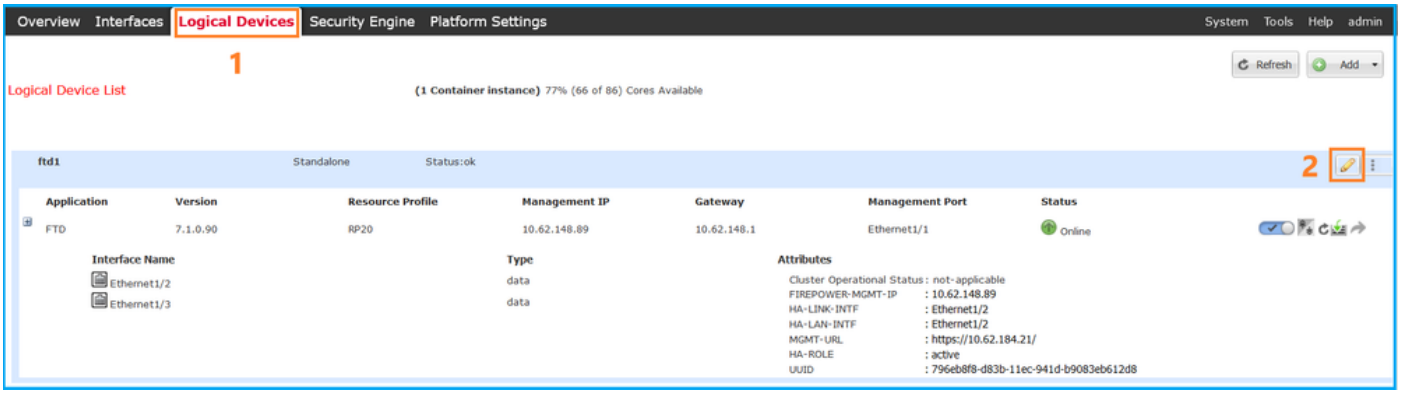
```
# curl -s -k -X 'GET'  'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept:
application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m
json.tool
...
{
    "accessPolicy":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

FCM-Benutzeroberfläche

Der Firewall-Modus kann für FTD auf Firepower 4100/9300 überprüft werden.

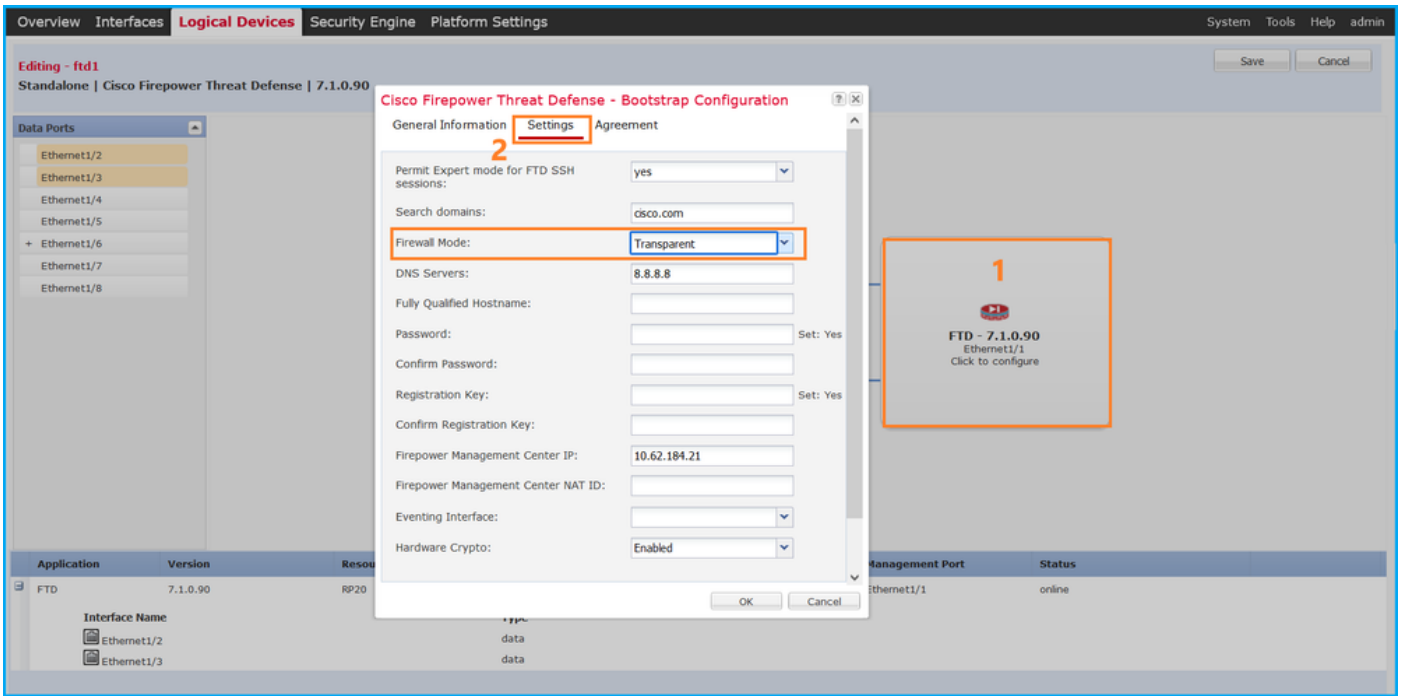
Gehen Sie folgendermaßen vor, um den FTD-Firewall-Modus auf der FCM-Benutzeroberfläche zu überprüfen:

1. Bearbeiten Sie das logische Gerät auf der Seite **Logical Devices (Logische Geräte)**:



2. Klicken Sie auf das Anwendungssymbol, und überprüfen Sie den **Firewall-Modus** auf der

Registerkarte **Einstellungen**:



FXOS-CLI

Der Firewall-Modus kann für FTD auf Firepower 4100/9300 überprüft werden.

Gehen Sie folgendermaßen vor, um den FTD-Firewall-Modus in der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolen- oder SSH-Verbindung zum Chassis her.
2. Wechseln Sie zum Gültigkeitsbereich ssa, wechseln Sie zum spezifischen **logischen Gerät,** führen Sie den Befehl **show mgmt-bootstrap extends** aus, und überprüfen Sie den Attributwert **FIREWALL_MODE:**

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

Management Configuration:
    App Name: ftd

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

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

    Bootstrap Key:
        Key                       Value
```

```
        ------------------------ -----
        DNS_SERVERS              192.0.2.250
        FIREPOWER_MANAGER_IP     10.62.184.21
        FIREWALL_MODE            routed
        PERMIT_EXPERT_MODE       yes
        SEARCH_DOMAINS           cisco.com
...
```

FXOS REST-API

FXOS REST-API wird von Firepower 4100/9300 unterstützt.

Befolgen Sie diese Schritte, um den FTD-Firewall-Modus über eine FXOS-REST-API-Anforderung zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

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

2. Verwenden Sie die ID für logische Geräte in dieser Abfrage, und überprüfen Sie den Wert des **FIREWALL_MODE-**Schlüssels:

```
# 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-Show-Tech-Datei

Der Firewall-Modus für FTD kann in der show-tech Datei der Firepower 4100/9300 überprüft werden.

Gehen Sie folgendermaßen vor, um den FTD-Firewall-Modus in der Show-Tech-Datei des FXOS-Chassis zu überprüfen:

1. Öffnen Sie für FXOS-Versionen 2.7 und höher die Datei **sam_techsupportinfo** in **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Für ältere Versionen öffnen Sie die Datei **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Überprüfen Sie den Abschnitt **"show logy-device detail extends"** unter der spezifischen Kennzeichnung und im Steckplatz:

```
# 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 Firewall-Modus

Der ASA-Firewall-Modus kann mithilfe der folgenden Optionen überprüft werden:

- ASA-CLI
- ASA Showtech
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

ASA-CLI

Führen Sie die folgenden Schritte aus, um den ASA-Firewall-Modus in der ASA CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen für den Zugriff auf die ASA-CLI in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus:

- Direkter Telnet-/SSH-Zugriff auf ASA mit Firepower 1000/3100 und Firepower 2100 im Appliance-Modus
- Zugriff von der FXOS-Konsolen-CLI auf der FirePOWER 2100 im Plattform-Modus und Verbindung mit ASA über den Befehl connect as a

- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):
  Verbinden Sie das Modul <x> [console|telnet], wobei x die Steckplatz-ID ist, und **verbinden Sie** sich dann **als**

- Für virtuelle ASA direkter SSH-Zugriff auf ASA oder Konsolenzugriff über die Hypervisor- oder Cloud-Benutzeroberfläche

2. Führen Sie den Befehl **show firewall** in der CLI aus:

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

ASA-Showtech-Datei

Um den ASA-Firewall-Modus zu überprüfen, aktivieren Sie den Abschnitt **show firewall**:

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

FCM-Benutzeroberfläche

Befolgen Sie die Schritte im Abschnitt.

FXOS-CLI

Befolgen Sie die Schritte im Abschnitt.

FXOS REST-API

Befolgen Sie die Schritte im Abschnitt.

FXOS-Chassis-Show-Tech-Datei

Befolgen Sie die Schritte im Abschnitt.

Typ der Instanzbereitstellung überprüfen

Es gibt zwei Bereitstellungstypen für Anwendungsinstanzen:

- Native Instanz - Eine systemeigene Instanz verwendet alle Ressourcen (CPU, RAM und Festplattenspeicher) des Sicherheitsmoduls bzw. -moduls, sodass Sie nur eine systemeigene Instanz installieren können.
- Containerinstanz - Eine Containerinstanz verwendet eine Teilmenge von Ressourcen des Sicherheitsmoduls/der -Engine. Multi-Instance-Funktionen werden nur für die von FMC verwaltete FTD unterstützt. Es wird für die ASA oder die vom FDM verwaltete FTD nicht unterstützt.

Die Instanzkonfiguration des Containermodus wird nur für FTD auf Firepower 4100/9300 unterstützt.

Der Instanzbereitstellungstyp kann mithilfe der folgenden Optionen überprüft werden:

- FTD-CLI
- FTD Show-Tech
- FMC-Benutzeroberfläche
- FMC REST-API
- FCM-Benutzeroberfläche
- FXOS-CLI
- FXOS REST-API
- FXOS-Chassis-Show-Tech-Datei

FTD-CLI

Gehen Sie folgendermaßen vor, um den FTD-Instanzbereitstellungstyp auf der FTD-CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen, um in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus auf die FTD-CLI zuzugreifen:

- Direkter SSH-Zugriff auf FTD - alle Plattformen
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300):

connect module <x> [console|telnet], wobei x die Steckplatz-ID ist, und dann **connect ftd [instance],** wobei die Instanz nur für die Bereitstellung mehrerer Instanzen relevant ist.

2. Führen Sie den Befehl **show version system** aus, und überprüfen Sie die Zeile mit der Zeichenfolge **SSP Slot Number**. Wenn der **Container** in dieser Zeile vorhanden ist, wird der FTD in einem Containermodus ausgeführt:

```
> 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-Fehlerbehebungsdatei

Gehen Sie folgendermaßen vor, um den Typ der FTD-Instanzbereitstellung in der FTD-Fehlerbehebungsdatei zu überprüfen:

1. Öffnen Sie die Datei zur Fehlerbehebung, und navigieren Sie zum Ordner **<Dateiname>-troubleshoot .tar/results-<date>—xxxxxx/command-output.**
2. Öffnen Sie die Datei **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'
```

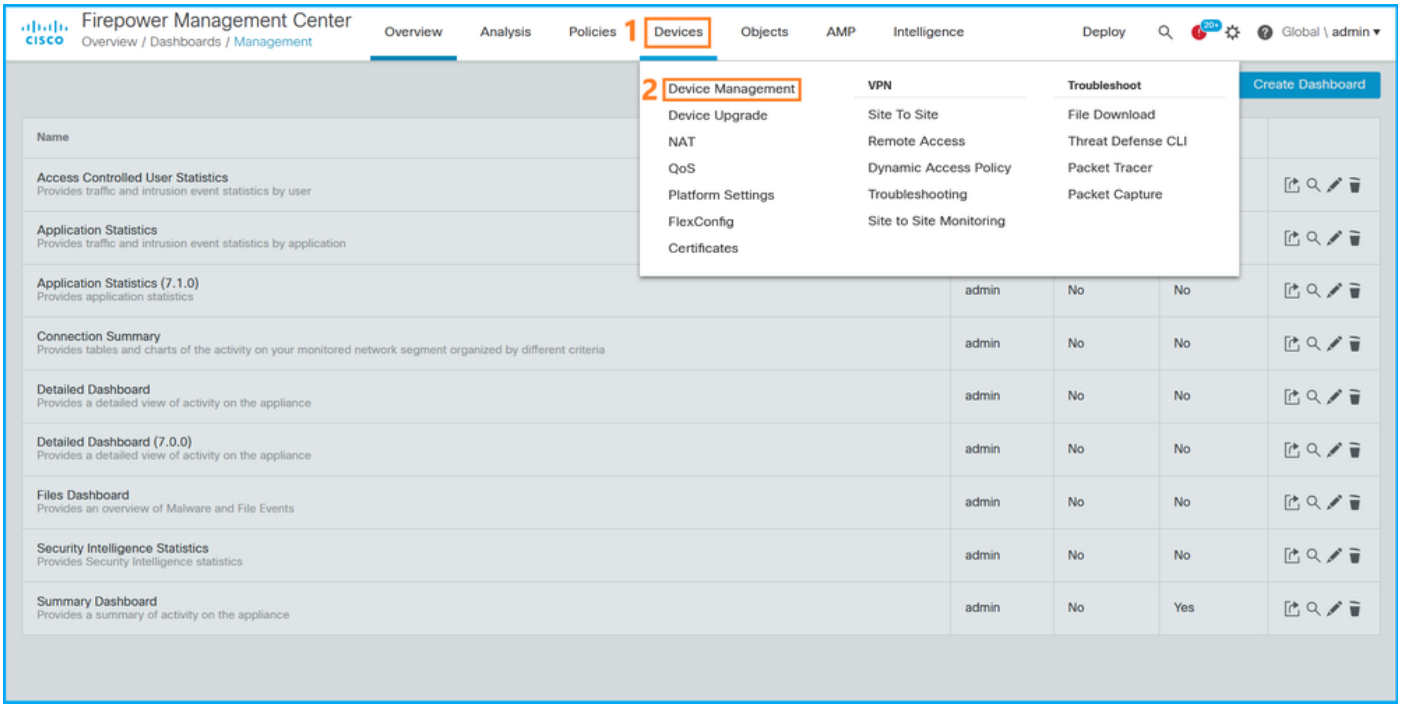
3. Überprüfen Sie die Zeile mit der Zeichenfolge **SSP-Steckplatznummer**. Wenn der **Container** in dieser Zeile vorhanden ist, wird der FTD in einem Containermodus ausgeführt:

```
------------------[ 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)
…
```

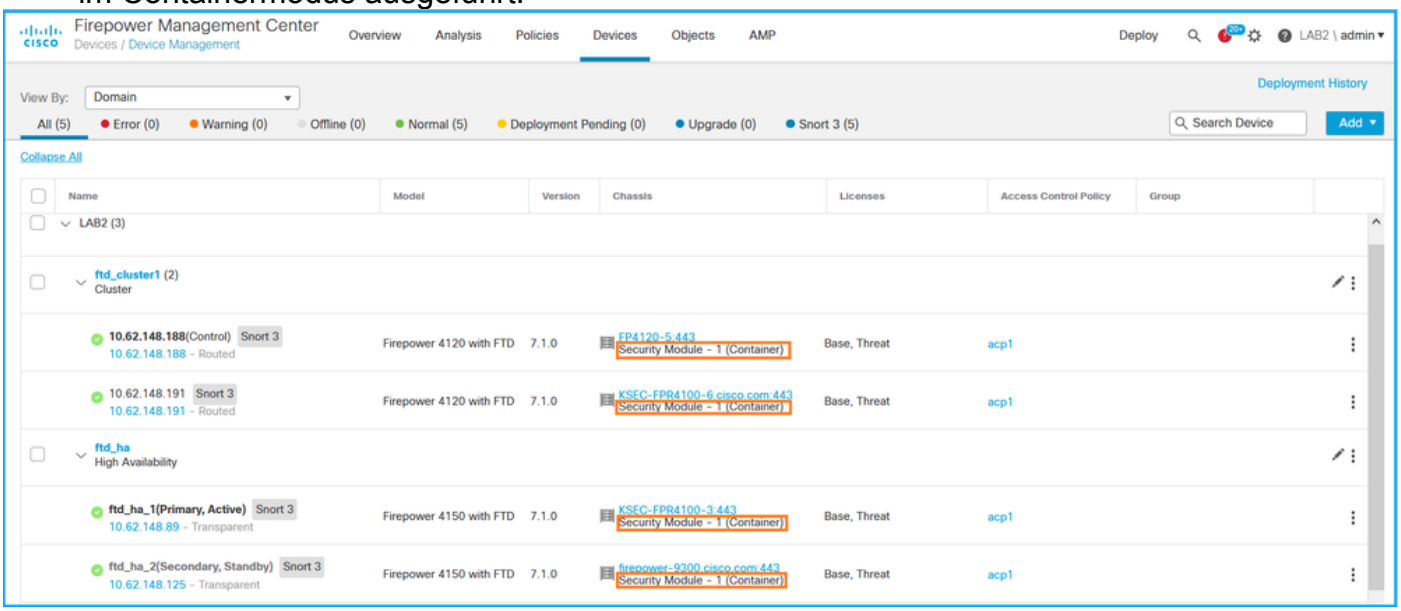
FMC-Benutzeroberfläche

Gehen Sie folgendermaßen vor, um den Typ der FTD-Instanzbereitstellung auf der FMC-Benutzeroberfläche zu überprüfen:

1. Wählen Sie **Geräte > Gerätemanagement**:



2. Überprüfen Sie die Spalte **Chassis**. Wenn der **Container** in der Zeile vorhanden ist, wird FTD im Containermodus ausgeführt.



FMC REST-API

Befolgen Sie diese Schritte, um den Typ der FTD-Instanzbereitstellung über FMC REST-API zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

```
# 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. Identifizieren Sie die Domäne, die das Gerät enthält. In den meisten REST-API-Abfragen ist der **Domänenparameter** obligatorisch. Verwenden Sie das Token in dieser Abfrage, um die Liste der Domänen abzurufen:

```
# 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. Verwenden Sie die Domänen-UUID, um die spezifischen **Gerätedatensätze** und die UUID des jeweiligen Geräts abzufragen:

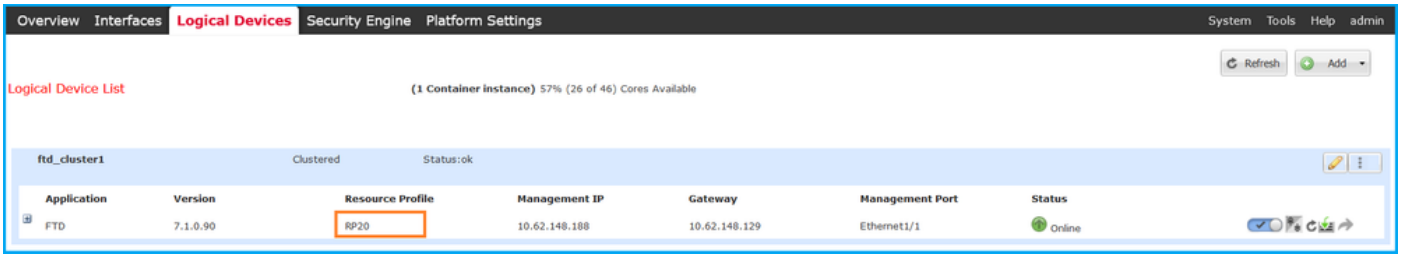
```
# curl -s -k -X 'GET'  'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords' -H 'accept: application/json'  -H 'X-auth-access-token:
5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
{
    "items": [
        {
            "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
            "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. Verwenden Sie in dieser Abfrage die Domänen-UUID und die Geräte-/Container-UUID aus Schritt 3, und überprüfen Sie den Wert von **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-Benutzeroberfläche

Um den Bereitstellungstyp der FTD-Instanz zu überprüfen, überprüfen Sie den Wert des **Resource Profile**-Attributs in Logical Devices. Wenn der Wert nicht leer ist, wird der FTD im Containermodus ausgeführt:



FXOS-CLI

Gehen Sie folgendermaßen vor, um den FTD-Instanzbereitstellungstyp in der FXOS-CLI zu überprüfen:

1. Stellen Sie eine Konsolen- oder SSH-Verbindung zum Chassis her.
2. Wechseln Sie zum **Gültigkeitsbereich ssa,** und führen Sie den Befehl **show app-instance** aus. Aktivieren Sie dann die Spalte **Deploy Type (Bereitstellungstyp)** der spezifischen FTD basierend auf dem Steckplatz und der Kennung:

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

FXOS REST-API

Befolgen Sie diese Schritte, um den Typ der FTD-Instanzbereitstellung über eine FXOS-REST-API-Anforderung zu überprüfen. Verwenden eines REST-API-Clients In diesem Beispiel wird **curl** verwendet:

1. Authentifizierungstoken anfordern:

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

2. Geben Sie das Token, die Steckplatz-ID in dieser Abfrage an, und überprüfen Sie den Wert von **deployType**:

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

FXOS-Chassis-Show-Tech-Datei

Gehen Sie folgendermaßen vor, um den FTD-Firewall-Modus in der Show-Tech-Datei des FXOS-Chassis zu überprüfen:

1. Öffnen Sie für FXOS-Versionen 2.7 und höher die Datei **sam_techsupportinfo** in **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Für ältere Versionen öffnen Sie die Datei **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Überprüfen Sie den Abschnitt **"show slot extends Detail" (Details anzeigen)** für den jeweiligen Steckplatz und die Kennzeichnung:

```
# 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
```

ASA-Kontextmodus überprüfen

ASA unterstützt Single- und Multi-Context-Modi. FTD unterstützt keinen Multi-Context-Modus.

Der Kontexttyp kann mithilfe der folgenden Optionen überprüft werden:

- ASA-CLI
- ASA Showtech

ASA-CLI

Gehen Sie folgendermaßen vor, um den ASA-Kontextmodus auf der ASA CLI zu überprüfen:

1. Verwenden Sie die folgenden Optionen für den Zugriff auf die ASA-CLI in Übereinstimmung mit dem Plattform- und Bereitstellungsmodus:

- Direkter Telnet-/SSH-Zugriff auf ASA mit Firepower 1000/3100 und Firepower 2100 im Appliance-Modus
- Zugriff von der FXOS-Konsolen-CLI auf der FirePOWER 2100 im Plattform-Modus und Verbindung mit ASA über den Befehl **connect as a**
- Zugriff von der FXOS-CLI über Befehle (Firepower 4100/9300): **Verbinden Sie das Modul <x> [console|telnet],** wobei x die Steckplatz-ID ist, und **verbinden Sie** sich dann **als**

- Für virtuelle ASA direkter SSH-Zugriff auf ASA oder Konsolenzugriff über die Hypervisor- oder Cloud-Benutzeroberfläche

2. Führen Sie den Befehl **show mode** in der CLI aus:

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

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

ASA-Showtech-Datei

Gehen Sie folgendermaßen vor, um den ASA-Kontext-Modus in der ASA-Showtech-Datei zu überprüfen:

1. Überprüfen Sie den Abschnitt **show context detail** in der show-tech Datei. In diesem Fall ist der Kontextmodus mehrere Kontexte:

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

Überprüfen Sie den FirePOWER 2100-Modus mit ASA.

Firepower 2100 mit ASA kann in einem der folgenden Modi ausgeführt werden:

- Plattformmodus: In FXOS werden grundlegende Betriebsparameter und Hardware-Schnittstelleneinstellungen konfiguriert. Zu diesen Einstellungen gehören die Änderung des Administrationszustands, die EtherChannel-Konfiguration, NTP, die Image-Verwaltung und vieles mehr. Für die FXOS-Konfiguration kann die FCM-Webschnittstelle oder die FXOS-CLI verwendet werden.
- Appliance-Modus (Standard) - Im Appliance-Modus können Benutzer alle Richtlinien in der ASA konfigurieren. Über die FXOS-CLI sind nur erweiterte Befehle verfügbar.

Der FirePOWER 2100-Modus mit ASA kann mithilfe der folgenden Optionen überprüft werden:

- ASA-CLI
- FXOS-CLI
- FXOS-Showtech

ASA-CLI

Führen Sie die folgenden Schritte aus, um den FirePOWER 2100-Modus mit ASA in der ASA CLI zu überprüfen:

1. Verwenden Sie Telnet/SSH für den Zugriff auf die ASA auf Firepower 2100.

2. Führen Sie den Befehl **show fxos mode** in der CLI aus:

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

Appliance-Modus:

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

> **Anmerkung:** Im Multi-Context-Modus ist der Befehl **show fxos mode** im **System** oder im **Admin-**Kontext verfügbar.

FXOS-CLI

Führen Sie die folgenden Schritte aus, um den FirePOWER 2100-Modus mit ASA in der FXOS-CLI zu überprüfen:

1. Verwenden Sie Telnet/SSH für den Zugriff auf die ASA auf Firepower 2100.

2. Führen Sie den Befehl **connect fxos** aus:

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

> **Anmerkung:** Im Multi-Context-Modus ist der Befehl **connect fxos** im **Admin-**Kontext verfügbar.

3. Führen Sie den Befehl **show fxos-mode aus**:

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

Appliance-Modus:

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

FXOS-Showtech-Datei

Führen Sie die folgenden Schritte aus, um den FirePOWER 2100-Modus mit ASA im FXOS-Chassis-Anzeigedatei zu überprüfen:

1. Öffnen Sie die Datei **tech_support_brief** in **<name>_FPRM.tar.gz/<name>_FPRM.tar**

2. Überprüfen Sie den Abschnitt **"show fxos-mode"**:

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

Appliance-Modus:

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

Bekannte Probleme

Cisco Bug-ID CSCwb94424 ENH: Hinzufügen eines CLISH-Befehls zur Überprüfung der FMC HA-Konfiguration

Cisco Bug-ID CSCvn31622 ENH: Hinzufügen von FXOS-SNMP-OIDs zum Abfragen der Konfiguration von logischen Geräten und Anwendungsinstanzen

Cisco Bug-ID CSCwb97767 ENH: Hinzufügen einer OID zur Überprüfung des Bereitstellungstyps einer FTD-Instanz

Cisco Bug-ID CSCwb97772 ENH: Ausgabe von "show fxos mode" in show-tech der ASA auf FirePOWER 2100 einschließen

Cisco Bug-ID CSCwb97751 Die OID 1.3.6.1.4.1.9.9.491.1.6.1.1 für die Überprüfung des transparenten Firewall-Modus ist nicht verfügbar.

Zugehörige Informationen

- Secure Firewall Management Center REST API Schnellstartanleitung, Version 7.1
- SNMP auf FirePOWER NGFW-Appliances konfigurieren
- REST API-Leitfaden für Cisco FirePOWER Threat Defense
- Referenz zur Cisco FXOS REST API
- Kompatibilität mit Cisco ASA
- Firepower 1000/2100 und Secure Firewall 3100 ASA- und FXOS-Paketversionen
- Paketkomponenten
- FirePOWER-Fehlerbehebung zur Dateigenerierung
- Cisco FirePOWER 2100: Erste Schritte
- Cisco FirePOWER Threat Defense-Kompatibilitätsleitfaden