Verifica della configurazione di modalità Firepower, istanza, alta disponibilità e scalabilità

Sommario

Introduzione

Questo documento descrive la verifica della configurazione di elevata disponibilità e scalabilità di Firepower, della modalità firewall e del tipo di distribuzione dell'istanza.

Premesse

I passaggi di verifica per la configurazione della disponibilità e della scalabilità elevate, la modalità firewall e il tipo di distribuzione dell'istanza sono visualizzati nell'interfaccia utente (UI),

nell'interfaccia della riga di comando (CLI), tramite query REST-API, SNMP e nel file di risoluzione dei problemi.

Prerequisiti

Requisiti

Conoscenze base del prodotto, REST-API, SNMP.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) versione 7.1.x
- Firepower eXtensible Operating System (FXOS) 2.1.1.x
- Firepower Device Manager (FDM) 7.1.x
- Firepower Threat Defense 7.1.x
- ASA 9.17.x

Verifica della configurazione di elevata disponibilità e scalabilità

Per elevata disponibilità si intende la configurazione di failover. La configurazione di failover o alta disponibilità unisce due dispositivi in modo che se uno di essi si guasta, l'altro dispositivo può assumere il controllo.

Per scalabilità si intende la configurazione del cluster. Una configurazione cluster consente di raggruppare più nodi FTD come un'unica periferica logica. Un cluster offre tutta la comodità di un singolo dispositivo (gestione, integrazione in una rete) e l'aumento del throughput e della ridondanza di più dispositivi.

Nel presente documento queste espressioni sono utilizzate in modo intercambiabile:

- alta disponibilità o failover
- scalabilità o cluster

In alcuni casi, la verifica della configurazione o dello stato di elevata disponibilità e scalabilità non è disponibile. Ad esempio, non è disponibile alcun comando di verifica per la configurazione FTD standalone. Le modalità di configurazione standalone, failover e cluster si escludono a vicenda.

Se un dispositivo non dispone di failover e configurazione cluster, viene considerato in modalità autonoma.

FMC High Availability

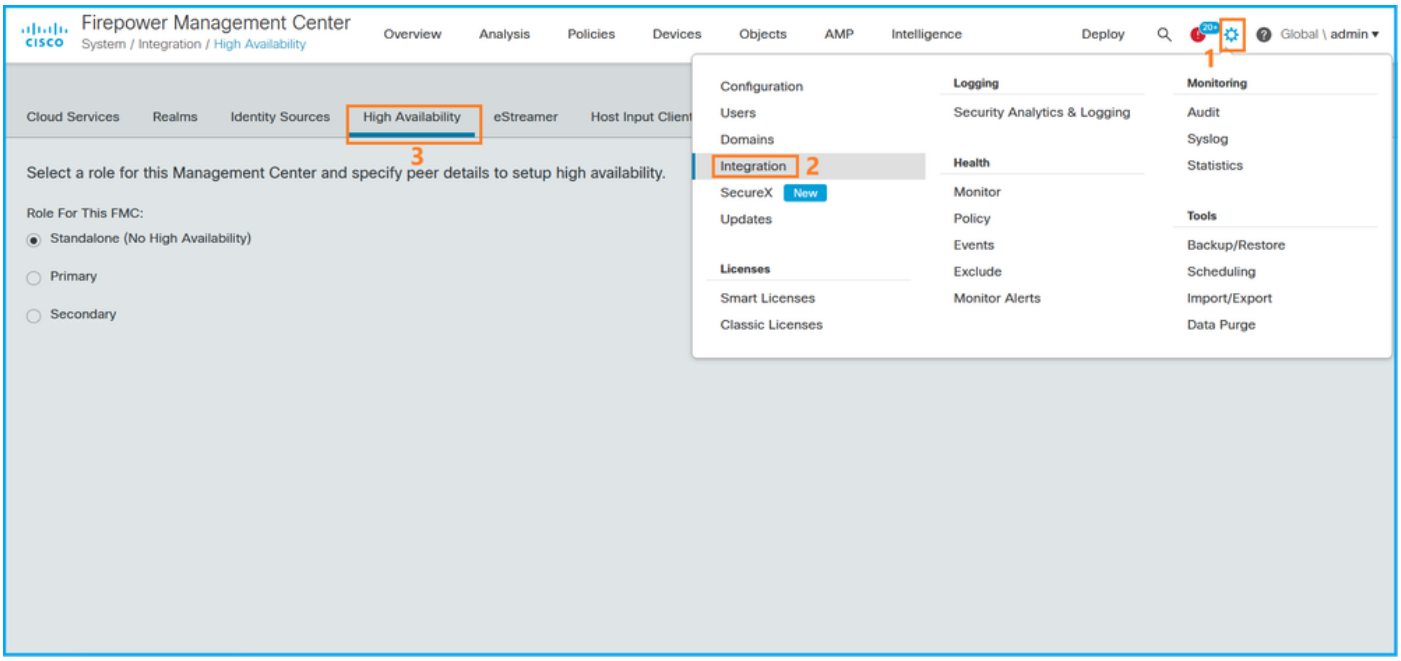
La configurazione e lo stato dell'elevata disponibilità del CCP possono essere verificati utilizzando le seguenti opzioni:

- UI FMC
- CLI FMC
- Richiesta API REST
- File di risoluzione dei problemi di FMC

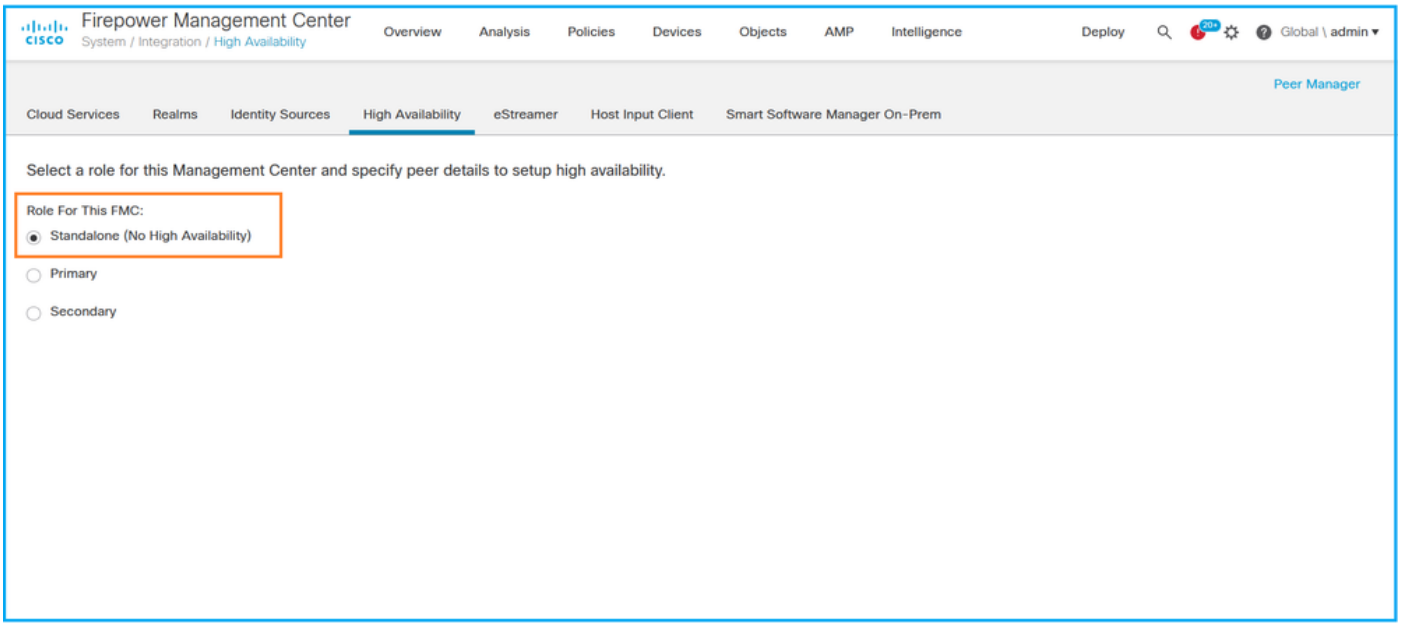
UI FMC

Per verificare lo stato e la configurazione dell'alta disponibilità del CCP nell'interfaccia utente del CCP, eseguire la procedura seguente:

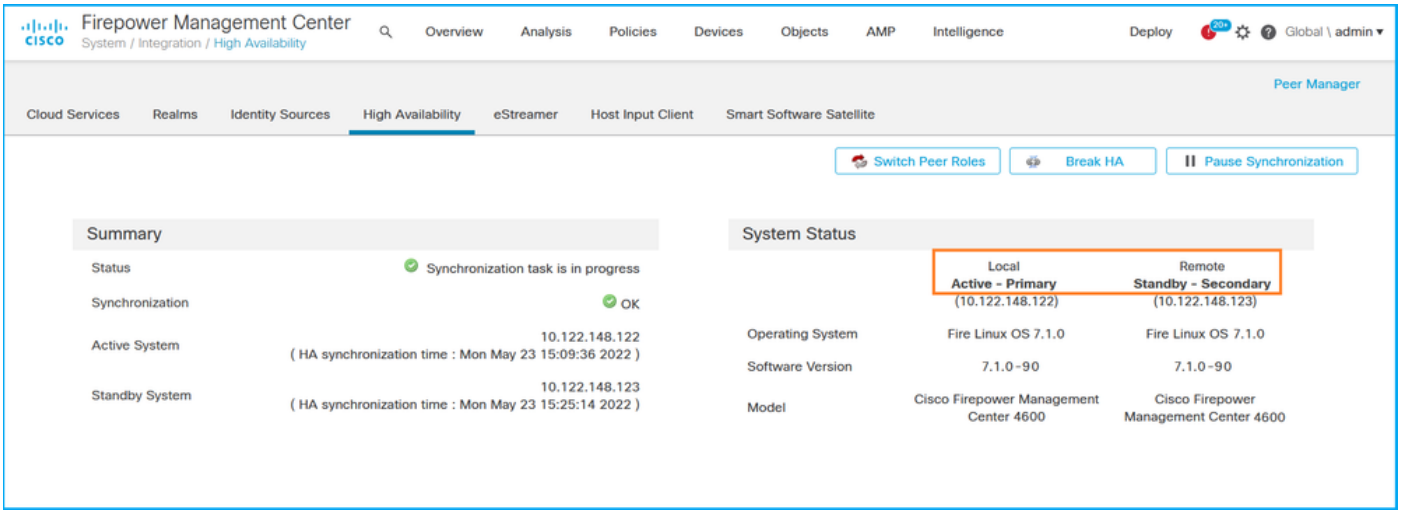
1. Scegliere **Sistema > Integrazione > Alta disponibilità:**



2. Controllare il ruolo del CCP. In questo caso, l'alta disponibilità non è configurata e FMC funziona in una configurazione autonoma:



Se è configurata la disponibilità elevata, vengono visualizzati i ruoli locale e remoto:



CLI FMC

Per verificare lo stato e la configurazione dell'alta disponibilità del CLI del CLI del CLI del CLI del CLI, eseguire le operazioni seguenti:

1. Accedere a FMC tramite connessione SSH o console.

2. Eseguire il comando **expert** ed eseguire il comando **sudo su**:

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

3. Eseguire il comando **troubleshoot_HADC.pl** e selezionare l'opzione **1** Mostra informazioni HA di FMC. Se l'alta disponibilità non è configurata, viene visualizzato questo output:

```
fmc1:/Volume/home/admin# troubleshoot_HADC.pl
**************  Troubleshooting Utility  *************    1   Show HA Info Of FMC
```

```
 2   Execute Sybase DBPing
 3   Show Arbiter Status
 4   Check Peer Connectivity
 5   Print Messages of AQ Task
 6   Show FMC HA Operations History (ASC order)
 7   Dump To File: FMC HA Operations History (ASC order)
 8   Last Successful Periodic Sync Time (When it completed)
 9   Print HA Status Messages
 10  Compare active and standby device list
 11  Check manager status of standby missing devices
 12  Check critical PM processes details
 13   Help
 0   Exit

************************************************************
Enter choice: 1
HA Enabled: No
```

Se è configurata la disponibilità elevata, viene visualizzato questo output:

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

> **Nota:** In una configurazione ad alta disponibilità, il ruolo FMC può avere un ruolo **primario** o **secondario** e uno stato **attivo** o **standby**.

API REST FMC

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità tramite l'API REST di FMC. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedere un token di autenticazione:

```
# 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. Utilizzare il token in questa query per trovare l'UUID del dominio globale:

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

Nota: La parte "**| python -m json.tool**" della stringa di comando viene utilizzata per formattare l'output in stile JSON ed è facoltativa.

3. Utilizzare l'UUID del dominio globale nella query:

```
# 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
```

Se l'alta disponibilità non è configurata, viene visualizzato questo output:

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

Se è configurata la disponibilità elevata, viene visualizzato questo output:

```
{
   "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
   }
}
```


File di risoluzione dei problemi di FMC

Per verificare la configurazione e lo stato dell'alta disponibilità del CCP nel file di risoluzione dei problemi del CCP, eseguire la procedura seguente:

1. Aprire il file per la risoluzione dei problemi e selezionare la cartella **<nomefile>.tar/results-<data>—xxxxxx/command-outputs**

2. Aprire il file **usr-local-sf-bin-troubleshoot_HADC.pl -a.output:**

Se l'alta disponibilità non è configurata, viene visualizzato questo output:

```
# 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
```

Se è configurata la disponibilità elevata, viene visualizzato questo output:

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

# cat "usr-local-sf-bin-troubleshoot_HADC.pl -a.output"
Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:
Status out put: vmsDbEngine (system,gui) - Running 9399
In vmsDbEngineStatus(): vmsDbEngine process is running at
/usr/local/sf/lib/perl/5.24.4/SF/Synchronize/HADC.pm line 3471.
$VAR1 = [
          'Mirror Server => csm_primary',
          {
            'stderr' => undef,
            'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745
Type       Property                 Value
---------  ---------------          ----------------------------
Database   MirrorRole               primary
Database   MirrorState              synchronizing
Database   PartnerState             connected
Database   ArbiterState             connected
Server     ServerName               csm_primary
Ping database successful.
',
            'rcode' => 0
          }
        ];

(system,gui) - Running 8185

...
HA Enabled: Yes
This FMC Role In HA: Active - Primary
Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running)
Sybase Database Connectivity: Accepting DB Connections.
Sybase Database Name: csm_primary
Sybase Role: Active

Sybase Database Name: csm_primary
Arbiter Running On This FMC.

Peer Is Connected
```

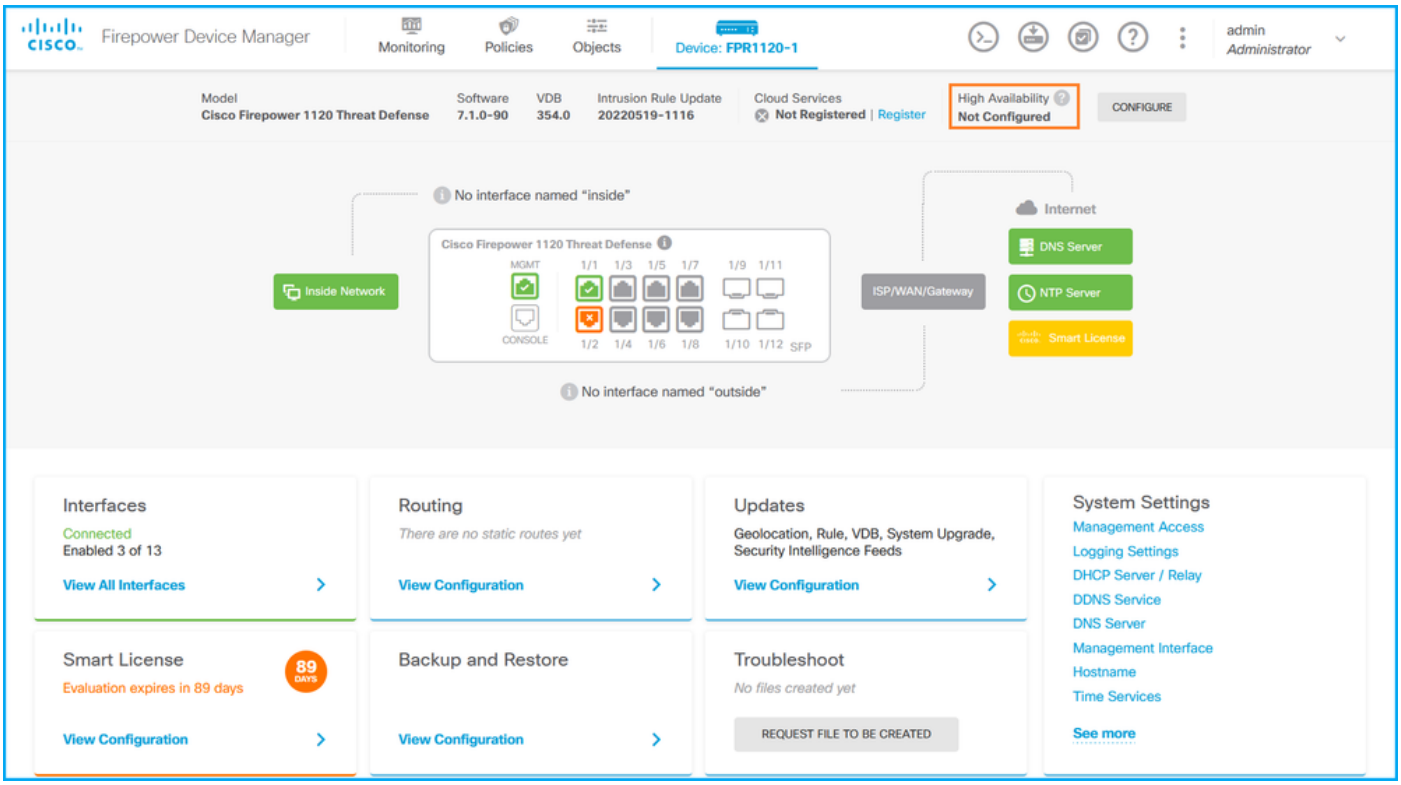
FDM alta disponibilità

La configurazione e lo stato dell'elevata disponibilità di FDM possono essere verificati utilizzando le seguenti opzioni:

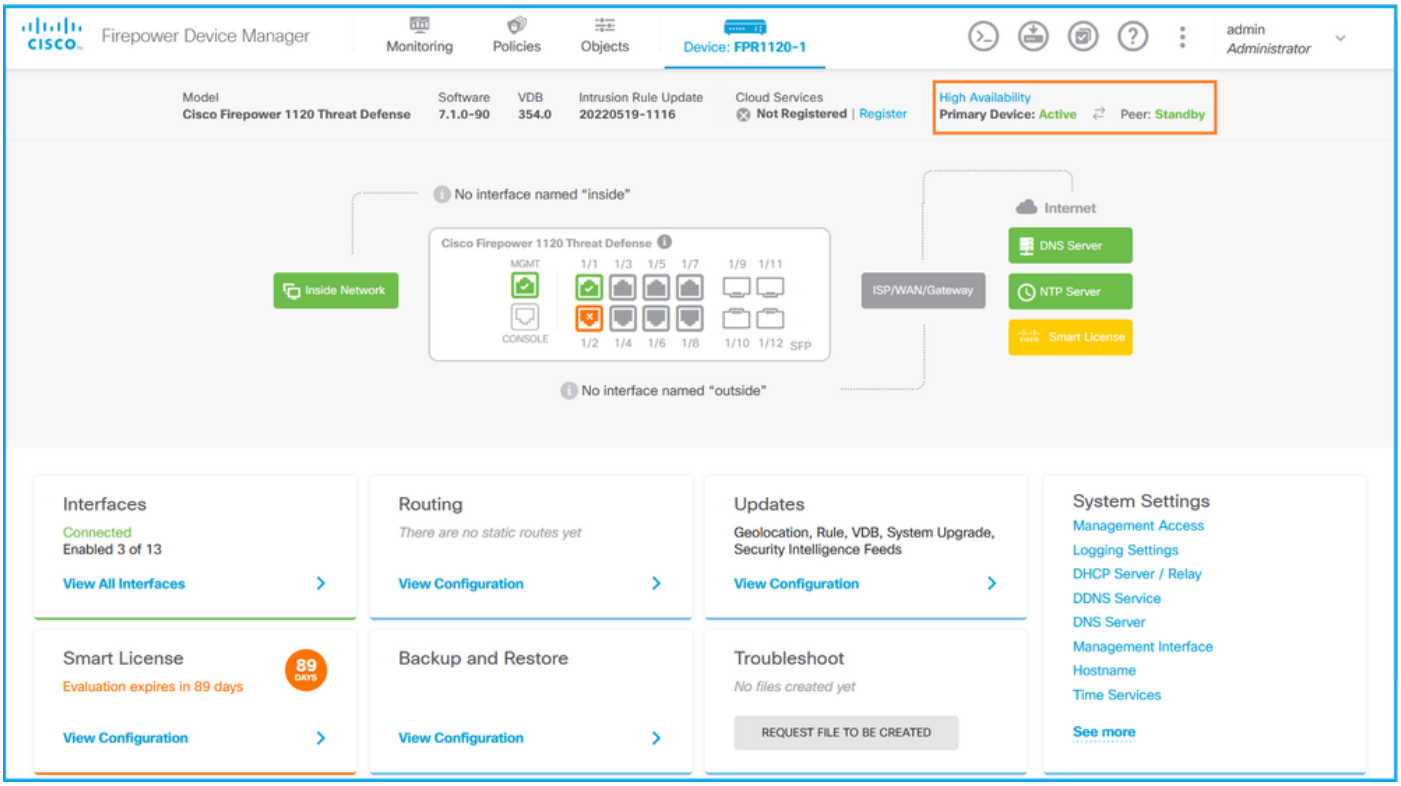
- UI FDM
- Richiesta API REST FDM
- CLI FTD
- Polling SNMP FTD
- File di risoluzione dei problemi FTD

UI FDM

Per verificare la configurazione e lo stato dell'elevata disponibilità di FDM sull'interfaccia utente di FDM, selezionare **Alta disponibilità** nella pagina principale**. Se l'alta disponibilità non è configurata, il valore Alta disponibilità** è **Non configurato:**



Se è configurata la disponibilità elevata, vengono visualizzati la configurazione e i ruoli di failover dell'unità peer locale e remota:



FDM REST-API

Seguire questi passaggi per verificare la configurazione e lo stato dell'elevata disponibilità di FDM tramite la richiesta FDM REST-API. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedere un token di autenticazione:

```
# 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. Per verificare la configurazione della disponibilità elevata, utilizzare il valore del token di accesso in questa query:

```
# 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'

Se l'alta disponibilità non è configurata, viene visualizzato questo output:


```
{
 "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
 }
}
```


Se è configurata la disponibilità elevata, viene visualizzato questo output:


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


3. Per verificare lo stato di elevata disponibilità, utilizzare questa query:

```
# 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'
```

Se l'alta disponibilità non è configurata, viene visualizzato questo output:

```
{
 "nodeRole" : null,
  "nodeState" : "SINGLE_NODE",
  "peerNodeState" : "HA_UNKNOWN_NODE",
 "configStatus" : "UNKNOWN",
 "haHealthStatus" : "HEALTHY",
 "disabledReason" : "",
 "disabledTimestamp" : null,
 "id" : "default",
 "type" : "hastatus",
 "links" : {
   "self" : "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
 }
}
```

Se è configurata la disponibilità elevata, viene visualizzato questo output:

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

CLI FTD

Seguire i passaggi descritti nella sezione.

Polling SNMP FTD

Seguire i passaggi descritti nella sezione.

File di risoluzione dei problemi FTD

Seguire i passaggi descritti nella sezione.

FTD alta disponibilità e scalabilità

La configurazione e lo stato di elevata disponibilità e scalabilità FTD possono essere verificati utilizzando le seguenti opzioni:

- CLI FTD
- SNMP FTD
- File di risoluzione dei problemi FTD
- UI FMC
- API REST FMC
- UI FDM
- FDM REST-API
- UI FCM
- CLI FXOS
- API REST FXOS
- File show-tech dello chassis FXOS

CLI FTD

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità FTD sulla CLI FTD:

1. Utilizzare queste opzioni per accedere alla CLI FTD in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto SSH a FTD - tutte le piattaforme
- Accesso dalla CLI della console FXOS (Firepower 1000/2100/3100) tramite il comando **connect ftd**
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300):
  connettere il modulo <x> [console|telnet], dove x è l'ID dello slot, quindi **connettere ftd [istanza],** dove l'istanza è rilevante solo per la distribuzione a più istanze

- Per i FTD virtuali, accesso diretto SSH al FTD o accesso alla console dall'interfaccia utente dell'hypervisor o del cloud

2. Per verificare la configurazione e lo stato del failover FTD, eseguire i comandi **show running-config failover** e **show failover state** sulla CLI.

Se il failover non è configurato, viene visualizzato questo output:

```
> show running-config failover
no failover
>show failover state
                State          Last Failure Reason      Date/Time
This host  -    Secondary
               Disabled       None
Other host -   Primary
               Not Detected   None
====Configuration State===
====Communication State==
```

Se il failover è configurato, viene visualizzato questo output:

```
> 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. Per verificare la configurazione e lo stato del cluster FTD, eseguire i comandi **show running-config cluster** e **show cluster info** sulla CLI.

Se il cluster non è configurato, viene visualizzato questo output:

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

Se il cluster è configurato, viene visualizzato questo output:

```
> show running-config cluster
cluster group ftd_cluster1
 key *****
 local-unit unit-1-1
 cluster-interface Port-channel48.204 ip 10.173.1.1 255.255.0.0
 priority 9
 health-check holdtime 3
 health-check data-interface auto-rejoin 3 5 2
 health-check cluster-interface auto-rejoin unlimited 5 1
 health-check system auto-rejoin 3 5 2
 health-check monitor-interface debounce-time 500
 site-id 1
 no unit join-acceleration
 enable

> show cluster info
Cluster ftd_cluster1: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID        : 0
        Site ID   : 1
        Version   : 9.17(1)
        Serial No.: FLM1949C5RR6HE
        CCL IP    : 10.173.1.1
        CCL MAC   : 0015.c500.018f
        Module    : FPR4K-SM-24
        Resource  : 20 cores / 44018 MB RAM
        Last join : 13:53:52 UTC May 20 2022
        Last leave: N/A
Other members in the cluster:
    Unit "unit-2-1" in state SLAVE
        ID        : 1
        Site ID   : 1
```

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

Nota: I ruoli **master** e **control** coincidono.

SNMP FTD

Per verificare lo stato e la configurazione della scalabilità e della disponibilità elevata dell'FTD tramite SNMP, attenersi alla procedura seguente:

1. Verificare che il protocollo SNMP sia configurato e abilitato. Per un FTD gestito da FDM, fare riferimento a Configurazione e risoluzione dei problemi di SNMP su Firepower FDM per i passaggi di configurazione. Per i passaggi di configurazione relativi all'FTD gestito da FMC, fare riferimento a Configurazione di SNMP su appliance Firepower NGFW.

2. Per verificare la configurazione e lo stato del failover FTD, eseguire il polling di OID **.1.3.6.1.4.1.9.9.147.1.2.1.1.1.**

Se il failover non è configurato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.5 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit (this device)"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

Se il failover è configurato, viene visualizzato questo output:

```
# 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. Per verificare la configurazione e lo stato del cluster, eseguire il polling a OID **1.3.6.1.4.1.9.9.491.1.8.1.**

Se il cluster non è configurato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 192.0.2.5 .1.3.6.1.4.1.9.9.491.1.8.1
SNMPv2-SMI::enterprises.9.9.491.1.8.1.1.0 = INTEGER: 0
```

Se il cluster è configurato ma non abilitato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.7 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0                    <-- Cluster status, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0                    <-- Cluster unit state, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "ftd_cluster1"        <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"            <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0  <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1                    <-- Cluster side ID
...
```

Se il cluster è configurato, abilitato e operativo, viene visualizzato questo output:

```
# 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
...
```

Per ulteriori informazioni sulle descrizioni degli OID, consultare il documento CISCO-UNIFIED-FIREWALL-MIB.

File di risoluzione dei problemi FTD

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità FTD nel file di risoluzione dei problemi FTD:

1. Aprire il file per la risoluzione dei problemi e selezionare la cartella **<nomefile>-troubleshoot .tar/results-<data>—xxxxxx/command-outputs.**

2. Aprire il file **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. Per verificare la configurazione e lo stato del failover, controllare la sezione **show failover**.

Se il failover non è configurato, viene visualizzato questo output:

```
----------------- show failover -----------------

Failover Off
Failover unit Secondary
```

```
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1292 maximum
MAC Address Move Notification Interval not set
```

Se il failover è configurato, viene visualizzato questo output:

```
------------------ 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. Per verificare la configurazione e lo stato del cluster FTD, controllare la sezione **show cluster info**.

Se il cluster non è configurato, viene visualizzato questo output:

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

Se il cluster è configurato e abilitato, viene visualizzato questo output:

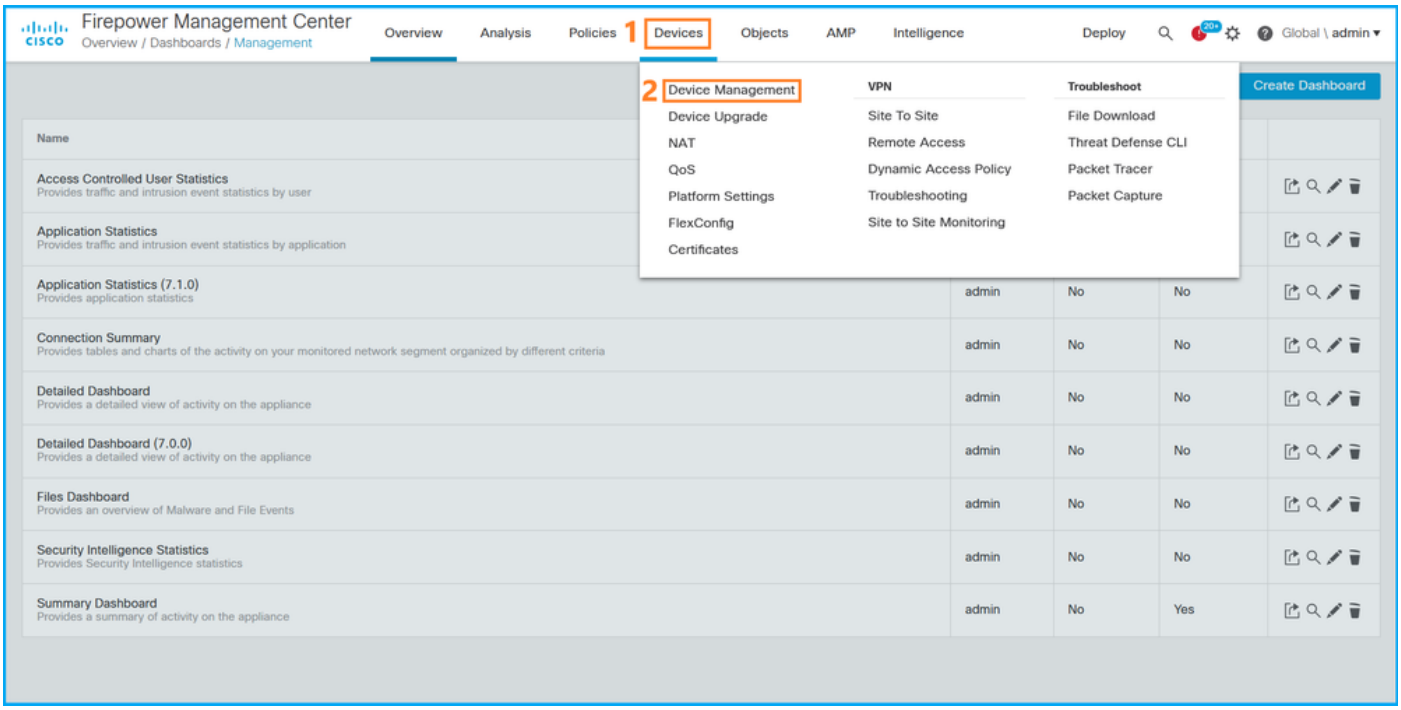
```
------------------ show cluster info ------------------
Cluster ftd_cluster1: On
    Interface mode: spanned
Cluster Member Limit : 16
    This is "unit-1-1" in state MASTER
        ID        : 0
        Site ID   : 1
        Version   : 9.17(1)
        Serial No.: FLM1949C5RR6HE
        CCL IP 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

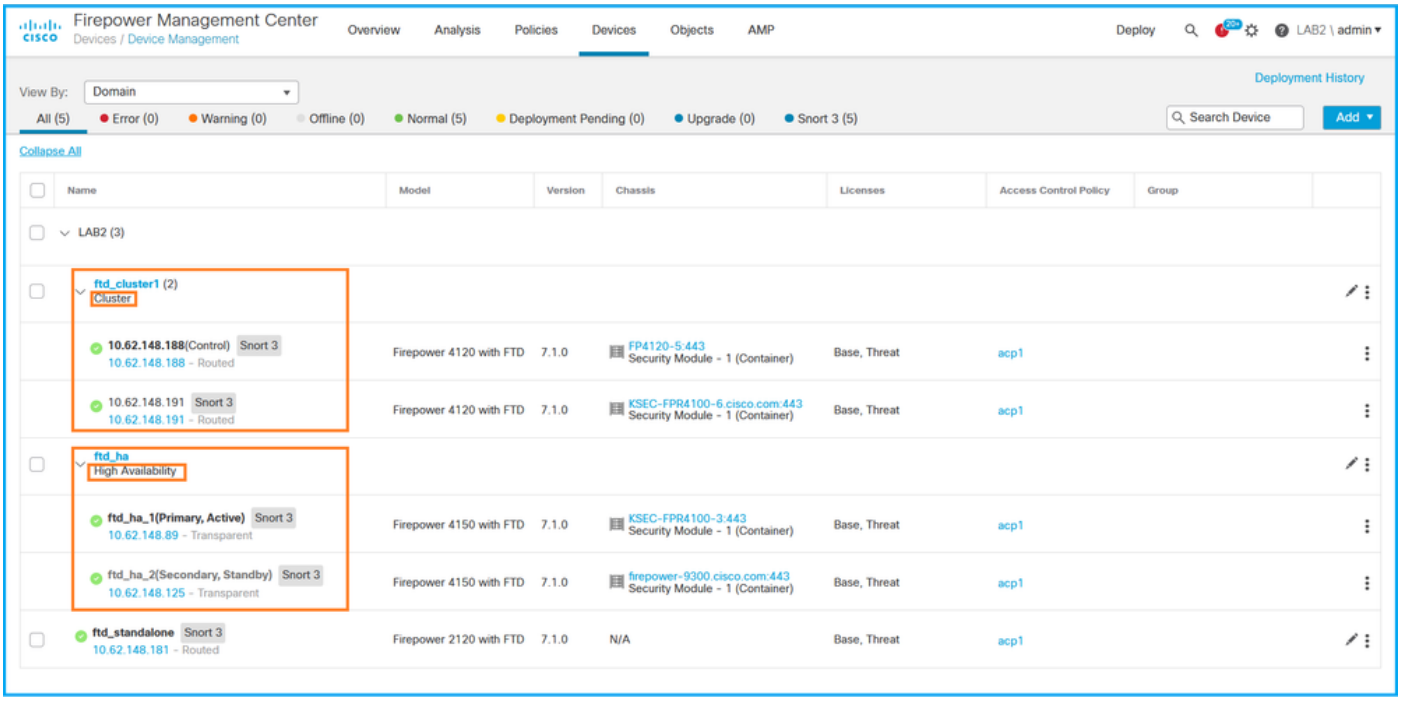
UI FMC

Per verificare lo stato e la configurazione della scalabilità e dell'elevata disponibilità FTD sull'interfaccia utente del FMC, eseguire le operazioni riportate di seguito.

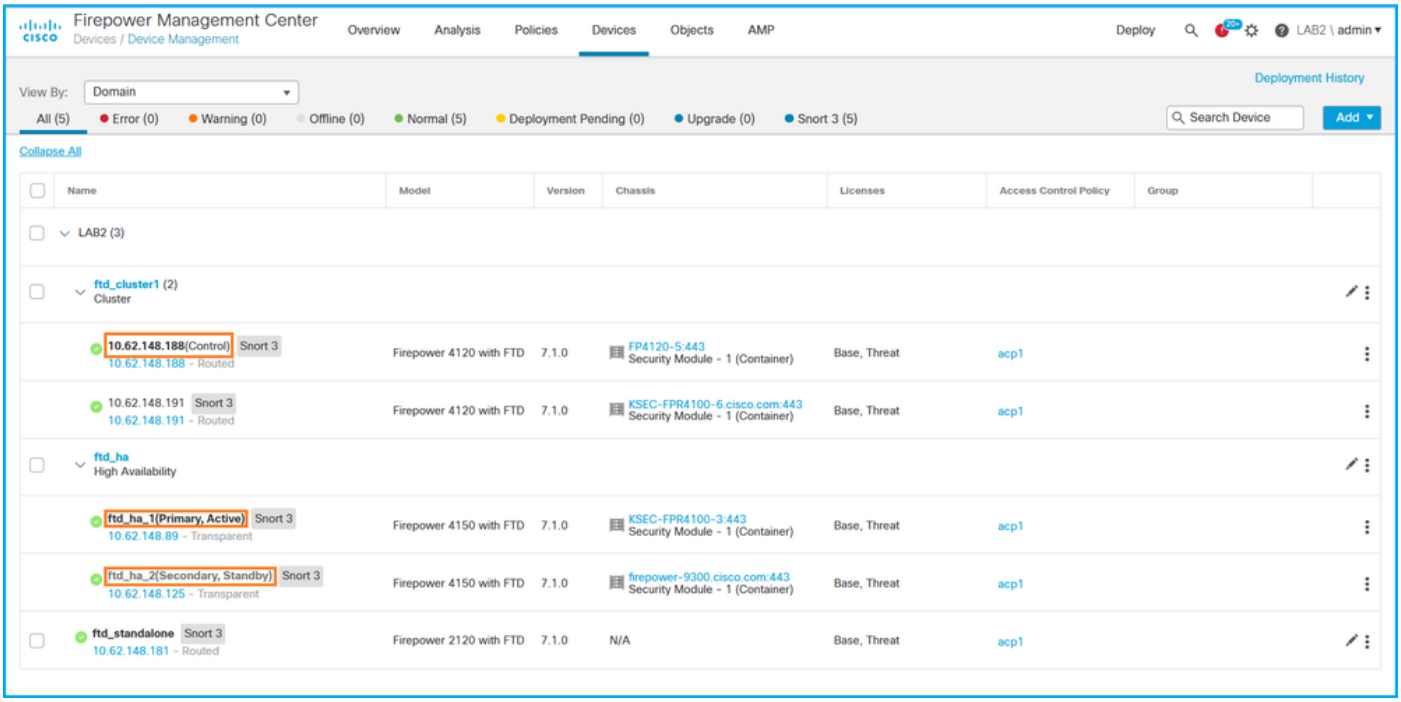
1. Scegliere **Dispositivi > Gestione dispositivi**:



2. Per verificare la configurazione dell'alta disponibilità e della scalabilità FTD, controllare le etichette **Alta disponibilità** o **Cluster**. Se non esistono, l'FTD viene eseguito in una configurazione autonoma:



3. Per verificare lo stato di elevata disponibilità e scalabilità FTD, controllare il ruolo dell'unità tra parentesi. Se un ruolo non esiste e l'FTD non fa parte di un cluster o di un failover, l'FTD viene eseguito in una configurazione autonoma:



Nota: Nel caso di un cluster, viene visualizzato solo il ruolo dell'unità di **controllo**.

API REST FMC

In questi output, **ftd_ha_1, ftd_ha_2, ftd_standalone, ftd_ha, ftc_cluster1** sono nomi di dispositivi configurabili dall'utente. Questi nomi non fanno riferimento alla configurazione o allo stato di elevata disponibilità e scalabilità effettivi.

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità FTD tramite l'API REST FMC. Utilizzare un client REST-API. Nell'esempio viene usato **il**

ricciolo:

1. Richiedi un token di autenticazione:

```
# 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. Identificare il dominio che contiene il dispositivo. Nella maggior parte delle query API REST il parametro **domain** è obbligatorio. Utilizzare il token in questa query per recuperare l'elenco dei domini:

```
# 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. Utilizzare l'UUID del dominio per eseguire una query sui **record** specifici del **dispositivo** e l'UUID specifico del dispositivo:

```
# 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. Per verificare la configurazione del failover, utilizzare l'UUID del dominio e l'UUID del dispositivo o del contenitore indicati nel passaggio 3 della seguente query:

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

```
            "name": "ftd_ha",
            "type": "DeviceHAPair"
        },
...
```

5. Per verificare lo stato del failover, utilizzare l'UUID del dominio e l'UUID di DeviceHAPair indicati nel passaggio 4 della presente query:

```
# 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. Per verificare la configurazione del cluster, utilizzare l'UUID del dominio e l'UUID del dispositivo o del contenitore indicati nel passaggio 3 della seguente query:

```
# 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. Per verificare lo stato del cluster, utilizzare l'UUID del dominio e l'UUID del dispositivo o del contenitore indicati nel passaggio 6 della seguente query:

```
# 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"
}
```


UI FDM

Seguire i passaggi descritti nella sezione.

FDM REST-API

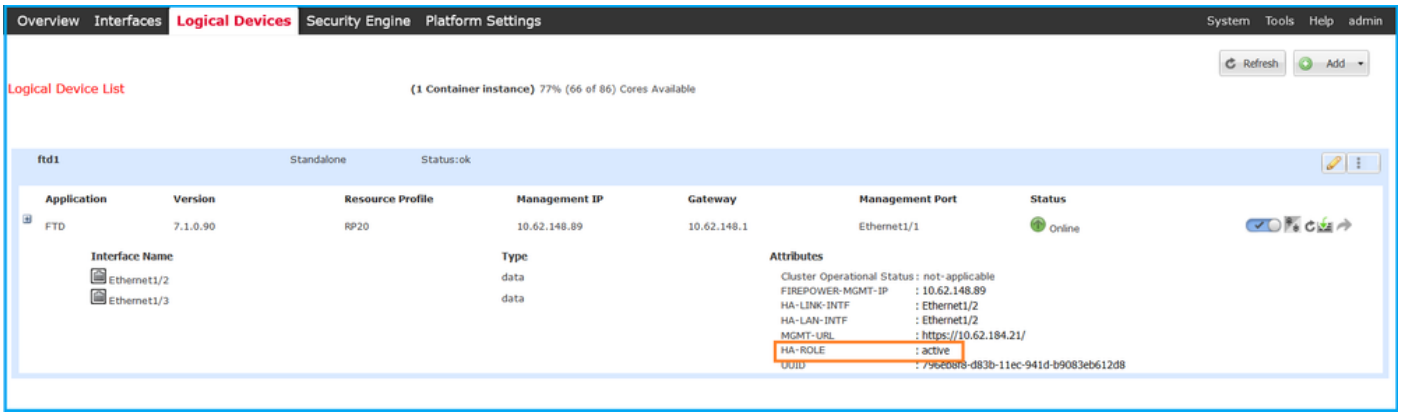
Seguire i passaggi descritti nella sezione.

UI FCM

FCM UI è disponibile su Firepower 4100/9300 e Firepower 2100 con ASA in modalità piattaforma.

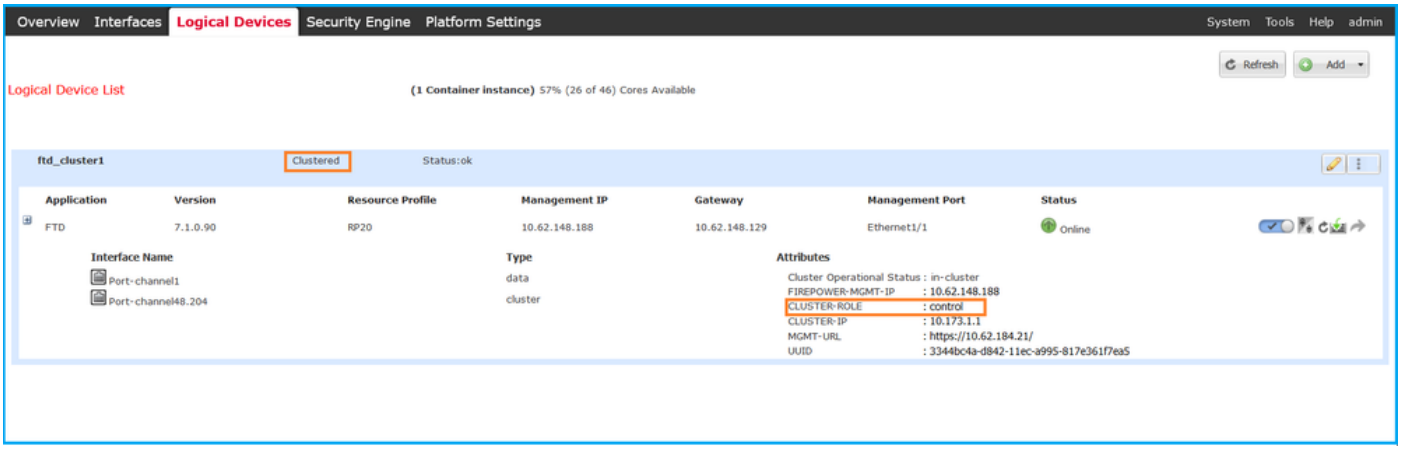
Per verificare lo stato di elevata disponibilità e scalabilità FTD sull'interfaccia utente di FCM, attenersi alla procedura descritta di seguito.

1. Per verificare lo stato di failover FTD, controllare il valore dell'attributo **HA-ROLE** nella pagina Dispositivi logici:



> **Nota:** L'etichetta **Standalone** accanto all'identificatore del dispositivo logico fa riferimento alla configurazione del dispositivo logico dello chassis, non alla configurazione di failover FTD.

2. Per verificare la configurazione e lo stato del cluster FTD, controllare l'etichetta **Clustered** e il valore dell'attributo **CLUSTER-ROLE** nella pagina Dispositivi logici:



CLI FXOS

La configurazione ad alta disponibilità e scalabilità FTD e la verifica dello stato sulla CLI di FXOS sono disponibili su Firepower 4100/9300.

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità FTD sulla CLI di FXOS:

1. Stabilire una connessione console o SSH allo chassis.

2. Per verificare lo stato di elevata disponibilità FTD, eseguire il comando **scope ssa**, quindi eseguire lo **slot <x>**di **ambito** per passare allo slot specifico in cui viene eseguito l'FTD ed eseguire il comando **show app-instance expand**:

```
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. Per verificare la configurazione e lo stato del cluster FTD, eseguire il comando **scope ssa**, eseguire il comando **show logical-device <name> detail expand**, dove name è il nome del

dispositivo logico, e il comando **show app-instance.** Controllare l'output per uno slot specifico:

```
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
```

API REST FXOS

FXOS REST-API è supportato su Firepower 4100/9300.

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità FTD tramite la richiesta FXOS REST-API. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedere un token di autenticazione:

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

2. Per verificare lo stato di failover FTD, utilizzare il token e l'ID dello slot in questa query:

```
# 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. Per verificare la configurazione del cluster FTD, utilizzare l'identificatore della periferica logica nella seguente query:

```
# 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. Per verificare lo stato del cluster FTD, utilizzare questa query:

```
# 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",
...
```

File show-tech per lo chassis FXOS

La configurazione e lo stato dell'FTD ad alta disponibilità e scalabilità possono essere verificati nel file show-tech dello chassis Firepower 4100/9300.

Seguire questi passaggi per verificare la configurazione e lo stato di elevata disponibilità e scalabilità nel file show-tech dello chassis FXOS:

1. Per FXOS versione 2.7 e successive, aprire il file **sam_techsupportinfo** in **<name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Per le versioni precedenti, aprire il file **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar.**

2. Per verificare lo stato del failover, controllare il valore dell'attributo **ha-role** nello slot specifico nella sezione **'show slot expand detail':**

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

# cat sam_techsupportinfo
...
`show slot expand detail`
Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
    Disk Format State: Ok
    Disk Format Status: 100%
    Clear Log Data: Available
    Error Msg:

    Application Instance:
        App Name: ftd
        Identifier: ftd1
        Admin State: Enabled
        Oper State: Online
        Running Version: 7.1.0.90
        Startup Version: 7.1.0.90
        Deploy Type: Container
        Turbo Mode: No
        Profile Name: RP20
        Hotfixes:
        Externally Upgraded: No
        Cluster State: Not Applicable
        Cluster Role: None
        Current Job Type: Start
        Current Job Progress: 100
        Current Job State: Succeeded
        Clear Log Data: Available
        Error Msg:
        Current Task:

        App Attribute:
```

```
            App Attribute Key: firepower-mgmt-ip
            Value: 10.62.148.89

            App Attribute Key: ha-lan-intf
            Value: Ethernet1/2

            App Attribute Key: ha-link-intf
            Value: Ethernet1/2

            App Attribute Key: ha-role
            Value: active

            App Attribute Key: mgmt-url
            Value: https://10.62.184.21/
```

3. Per verificare la configurazione del cluster FTD, controllare il valore dell'attributo **Mode** nello slot specifico nella sezione **'show logical-device detail expand':**

```
`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. Per verificare lo stato del cluster FTD, controllare il valore dei valori degli attributi **Stato cluster** e **Ruolo cluster** nello slot specifico nella sezione **'show slot expand detail':**

```
`show slot expand detail`

Slot:
    Slot ID: 1
    Log Level: Info
    Admin State: Ok
    Oper State: Online
```

```
Disk Format State: Ok
Disk Format Status:
Clear Log Data: Available
Error Msg:

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

ASA alta disponibilità e scalabilità

La configurazione e lo stato dell'ASA ad alta disponibilità e scalabilità possono essere verificati usando queste opzioni:

- ASA CLI
- Polling ASA SNMP
- File ASA show-tech
- UI FCM
- CLI FXOS
- API REST FXOS
- File show-tech dello chassis FXOS

ASA CLI

Per verificare la configurazione della disponibilità e della scalabilità elevate dell'ASA sulla CLI dell'ASA, attenersi alla procedura seguente:

1. Utilizzare queste opzioni per accedere alla CLI dell'ASA in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto telnet/SSH ad ASA su Firepower 1000/3100 e Firepower 2100 in modalità appliance
- Accesso dalla CLI della console FXOS su Firepower 2100 in modalità piattaforma e connessione all'ASA con il comando **connect asa**
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300): **connettere il modulo <x> [console|telnet],** dove x è l'ID dello slot, quindi **connettere un'appliance asa**

- Per le appliance ASA virtuali, accesso diretto SSH alle appliance ASA o accesso alla console dall'interfaccia utente dell'hypervisor o del cloud

2. Per verificare la configurazione e lo stato del failover dell'ASA, eseguire i comandi **show running-config failover** e **show failover state** sulla CLI dell'ASA.

Se il failover non è configurato, viene visualizzato questo output:

```
asa# show running-config failover
no failover
asa# show failover state
                State          Last Failure Reason      Date/Time
This host  -    Secondary
                Disabled       None
Other host -    Primary
                Not Detected   None
====Configuration State===
====Communication State==
```

Se il failover è configurato, viene visualizzato questo output:

```
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. Per verificare la configurazione e lo stato del cluster ASA, eseguire i comandi **show running-config cluster** e **show cluster info** sulla CLI.

Se il cluster non è configurato, viene visualizzato questo output:

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

Se il cluster è configurato, viene visualizzato questo output:

```
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

Per verificare la configurazione di elevata disponibilità e scalabilità dell'ASA tramite SNMP, attenersi alla procedura seguente:

1. Verificare che il protocollo SNMP sia configurato e abilitato.

2. Per verificare la configurazione e lo stato del failover, eseguire il polling a OID .1.3.6.1.4.1.9.9.147.1.2.1.1.1.

Se il failover non è configurato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.10 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit (this device)"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

Se il failover è configurato, viene visualizzato questo output:

```
# 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. Per verificare la configurazione e lo stato del cluster, eseguire il polling di OID 1.3.6.1.4.1.9.9.491.1.8.1.

Se il cluster non è configurato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
SNMPv2-SMI::enterprises.9.9.491.1.8.1.1.0 = INTEGER: 0
```

Se il cluster è configurato ma non abilitato, viene visualizzato questo output:

```
# snmpwalk -v2c -c cisco123 -On 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0              <-- Cluster status, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0              <-- Cluster unit state, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "asa_cluster1"  <-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"      <-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0 <-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1              <-- Cluster side ID
...
```

Se il cluster è configurato, abilitato e operativo, viene visualizzato questo output:

```
# 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
...
```

Per ulteriori informazioni sulle descrizioni degli OID, consultare il documento CISCO-UNIFIED-FIREWALL-MIB.

File ASA show-tech

1. Per verificare la configurazione e lo stato del failover dell'ASA, consultare la sezione **show failover**.

Se il failover non è configurato, viene visualizzato questo output:

```
------------------ show failover ------------------

Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1292 maximum
MAC Address Move Notification Interval not set
```

Se il failover è configurato, viene visualizzato questo output:

```
------------------ 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. Per verificare la configurazione e lo stato del cluster, controllare la sezione **show cluster info**.

Se il cluster non è configurato, viene visualizzato questo output:

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

Se il cluster è configurato e abilitato, viene visualizzato questo output:

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

UI FCM

Seguire i passaggi descritti nella sezione.

CLI FXOS

Seguire i passaggi descritti nella sezione.

API REST FXOS

Seguire i passaggi descritti nella sezione.

File show-tech per lo chassis FXOS

Seguire i passaggi descritti nella sezione.

Verificare la modalità Firewall

Modalità FTD Firewall

La modalità firewall fa riferimento a una configurazione firewall instradata o trasparente.

La modalità firewall FTD può essere verificata usando queste opzioni:

- CLI FTD
- FTD show-tech
- UI FMC
- API REST FMC
- UI FCM
- CLI FXOS
- API REST FXOS
- File show-tech dello chassis FXOS

Nota: FDM non supporta la modalità trasparente.

CLI FTD

Seguire questi passaggi per verificare la modalità firewall FTD sulla CLI FTD:

1. Utilizzare queste opzioni per accedere alla CLI FTD in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto SSH a FTD - tutte le piattaforme
- Accesso dalla CLI della console FXOS (Firepower 1000/2100/3100) tramite il comando **connect ftd**
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300): **connettere il modulo <x> [console|telnet],** dove x è l'ID dello slot e quindi

  connect ftd [instance], dove l'istanza è rilevante solo per la distribuzione a più istanze.

- Per i FTD virtuali, accesso diretto SSH al FTD o accesso alla console dall'interfaccia utente dell'hypervisor o del cloud

2. Per verificare la modalità firewall, eseguire il comando **show firewall** sulla CLI:

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

File di risoluzione dei problemi FTD

Seguire questi passaggi per verificare la modalità firewall FTD nel file di risoluzione dei problemi FTD:

1. Aprire il file per la risoluzione dei problemi e selezionare la cartella **<nomefile>-troubleshoot**

.tar/results-<data>—xxxxxx/command-outputs.

2. Aprire il file **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'
```

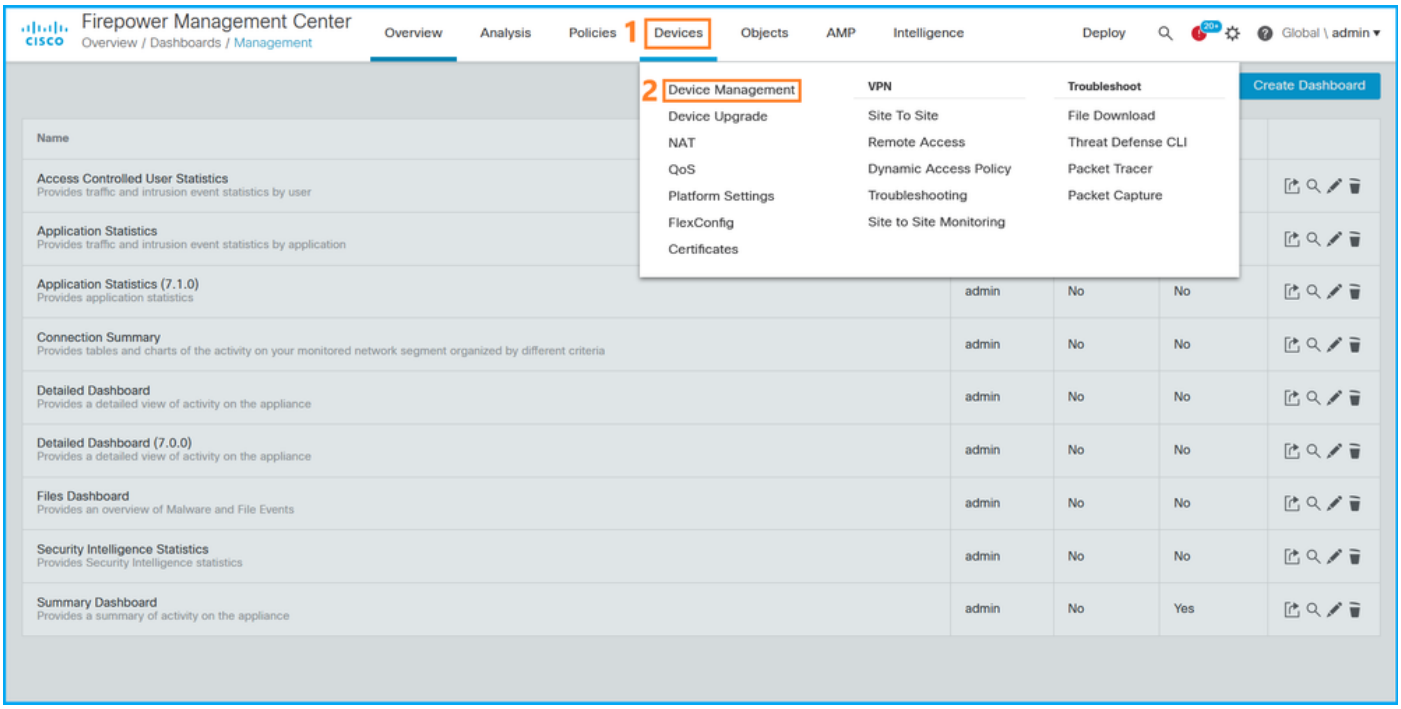
3. Per verificare la modalità firewall FTD, controllare la sezione **show firewall**:

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

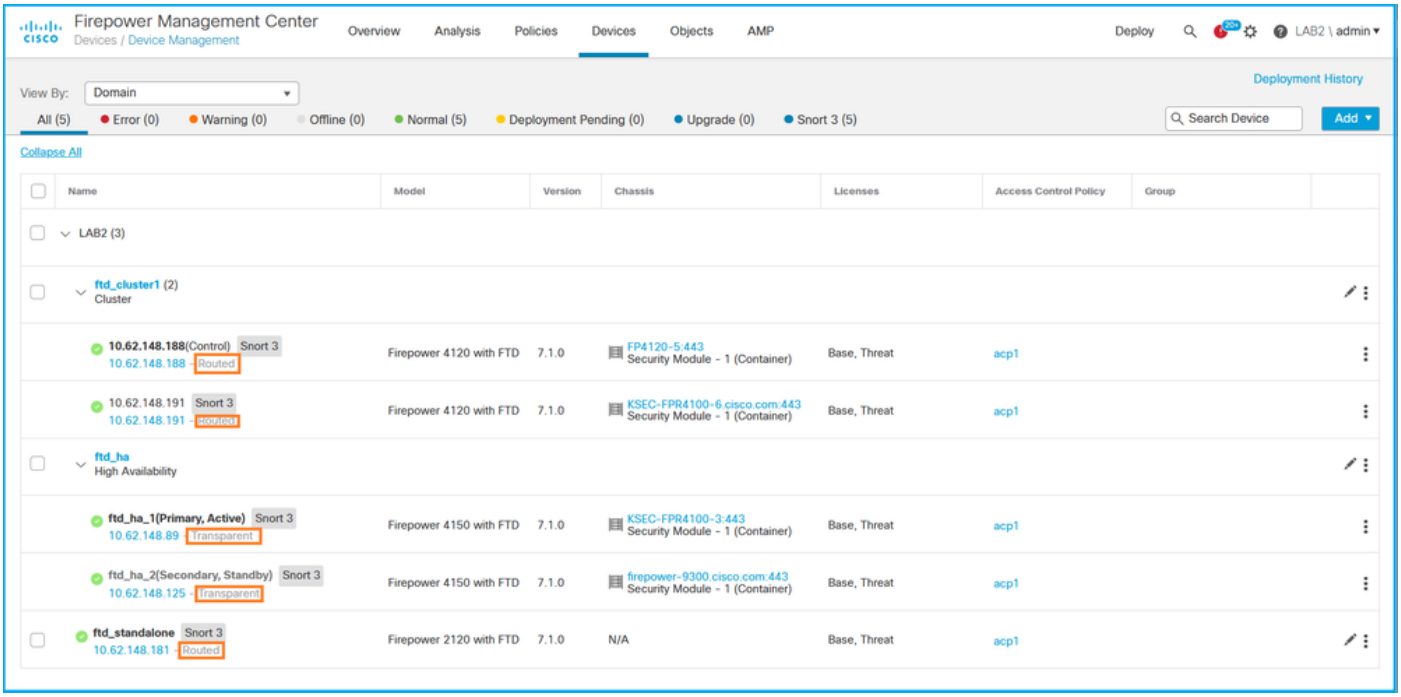
UI FMC

Per verificare la modalità firewall FTD nell'interfaccia utente di FMC, eseguire la procedura seguente:

1. Scegliere **Dispositivi > Gestione dispositivi**:



2. Selezionare le etichette **Stesura** o **Trasparente**:



API REST FMC

Seguire questi passaggi per verificare la modalità firewall FTD tramite FMC REST-API. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedi un token di autenticazione:

```
# 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. Identificare il dominio che contiene il dispositivo. Nella maggior parte delle query API REST il parametro **domain** è obbligatorio. Utilizzare il token in questa query per recuperare l'elenco dei domini:

```
# 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. Utilizzare l'UUID del dominio per eseguire una query sui **record** specifici del **dispositivo** e l'UUID specifico del dispositivo:

```
# 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. Utilizzare l'UUID del dominio e l'UUID del dispositivo/contenitore del passaggio 3 in questa query e controllare il valore di **ftdMode**:

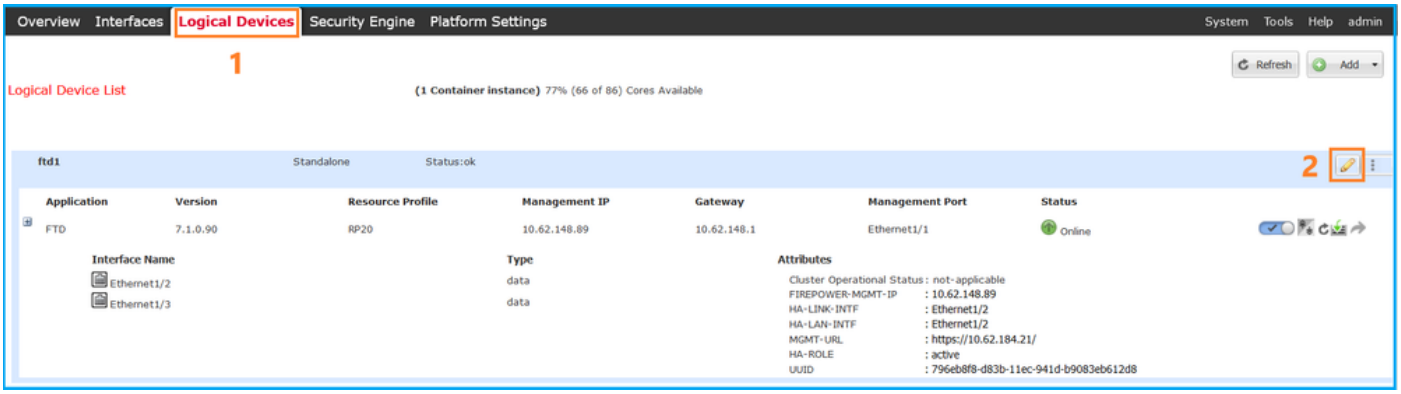
```
# curl -s -k -X 'GET'  'https://192.0.2.1./api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8' -H 'accept: application/json'  -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb' | python -m json.tool
...
{
    "accessPolicy":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

UI FCM

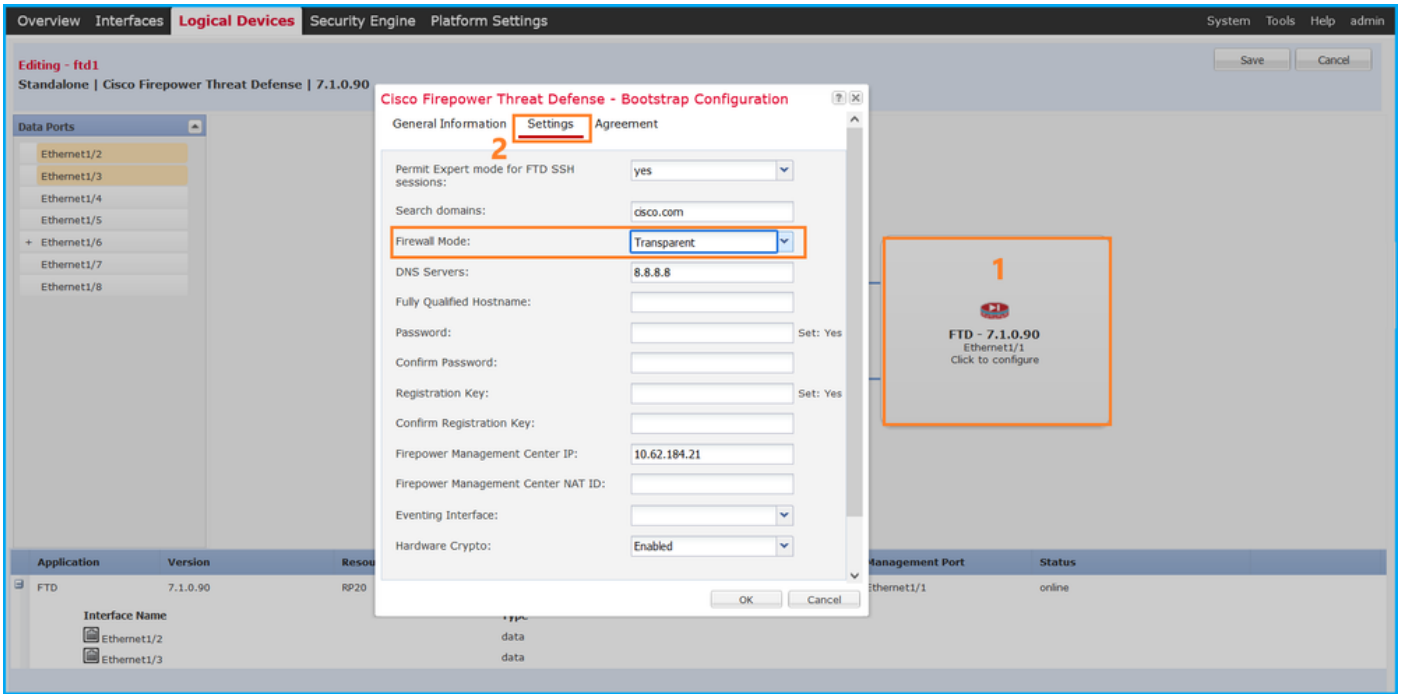
La modalità firewall può essere verificata per FTD su Firepower 4100/9300.

Per verificare la modalità firewall FTD sull'interfaccia utente di FCM, eseguire la procedura seguente:

1. Modificare la periferica logica nella pagina **Periferiche logiche**:



2. Fare clic sull'icona dell'applicazione e controllare la **modalità firewall** nella scheda **Impostazioni**:



CLI FXOS

La modalità firewall può essere verificata per FTD su Firepower 4100/9300.

Seguire questi passaggi per verificare la modalità firewall FTD sulla CLI di FXOS:

1. Stabilire una connessione console o SSH allo chassis.
2. Passare all'ambito ssh, passare alla **periferica logica** specifica, eseguire il comando **show mgmt-bootstrap expand** e verificare il valore dell'attributo **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
...
```

API REST FXOS

FXOS REST-API è supportato su Firepower 4100/9300.

Seguire questi passaggi per verificare la modalità firewall FTD tramite la richiesta FXOS REST-API. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedi un token di autenticazione:

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

2. Utilizzare l'identificatore di periferica logica nella query e controllare il valore della chiave **FIREWALL_MODE**:

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token:
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d'
https://192.0.2.100/api/ld/ftd_cluster1
...                         {                             "key": "FIREWALL_MODE",
                            "rn": "key-FIREWALL_MODE",
                            "updateTimestamp": "2022-05-20T13:28:37.093",
                            "urllink": "https://192.0.2.100/api/ld/ftd_cluster1/mgmt-
bootstrap/ftd/key/FIREWALL_MODE",
                            "value": "routed"
                        },
...
```

File show-tech per lo chassis FXOS

La modalità firewall per FTD può essere verificata nel file show-tech di Firepower 4100/9300.

Seguire questi passaggi per verificare la modalità firewall FTD nel file show-tech dello chassis FXOS:

1. Per FXOS versione 2.7 e successive, aprire il file **sam_techsupportinfo** in **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

   Per le versioni precedenti, aprire il file **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Controllare la sezione **`show logical-device detail expand`** sotto l'identificatore specifico e lo slot:

```
# 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
...
```

Modalità ASA Firewall

La modalità firewall dell'ASA può essere verificata usando queste opzioni:

- ASA CLI
- ASA show-tech
- UI FCM
- CLI FXOS
- API REST FXOS
- File show-tech dello chassis FXOS

ASA CLI

Per verificare la modalità firewall dell'ASA sulla CLI dell'ASA, attenersi alla procedura seguente:

1. Utilizzare queste opzioni per accedere alla CLI dell'ASA in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto telnet/SSH ad ASA su Firepower 1000/3100 e Firepower 2100 in modalità appliance
- Accesso dalla CLI della console FXOS su Firepower 2100 in modalità piattaforma e connessione all'ASA con il comando **connect asa**
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300): **connettere il modulo <x> [console|telnet],** dove x è l'ID dello slot, quindi **connettere un'appliance asa**

- Per le appliance ASA virtuali, accesso diretto SSH alle appliance ASA o accesso alla console

dall'interfaccia utente dell'hypervisor o del cloud

2. Eseguire il comando **show firewall** sulla CLI:

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

File ASA show-tech

Per verificare la modalità firewall ASA, controllare la sezione **show firewall**:

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

UI FCM

Seguire i passaggi descritti nella sezione.

CLI FXOS

Seguire i passaggi descritti nella sezione.

API REST FXOS

Seguire i passaggi descritti nella sezione.

File show-tech per lo chassis FXOS

Seguire i passaggi descritti nella sezione.

Verifica tipo di distribuzione istanza

Esistono due tipi di distribuzione dell'istanza dell'applicazione:

- Istanza nativa: un'istanza nativa utilizza tutte le risorse (CPU, RAM e spazio su disco) del modulo/motore di sicurezza, pertanto è possibile installare una sola istanza nativa.
- Istanza contenitore: un'istanza contenitore utilizza un sottoinsieme di risorse del modulo di sicurezza o del motore di sicurezza. la capacità a più istanze è supportata solo per l'FTD gestito dal CCP; non è supportata per l'ASA o l'FTD gestito da FDM.

La configurazione dell'istanza della modalità contenitore è supportata solo per FTD su Firepower 4100/9300.

Èpossibile verificare il tipo di distribuzione dell'istanza utilizzando le opzioni seguenti:

- CLI FTD
- FTD Show-tech
- UI FMC
- API REST FMC

- UI FCM
- CLI FXOS
- API REST FXOS
- File show-tech dello chassis FXOS

CLI FTD

Per verificare il tipo di distribuzione dell'istanza FTD nella CLI FTD, attenersi alla procedura descritta di seguito.

1. Utilizzare queste opzioni per accedere alla CLI FTD in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto SSH a FTD - tutte le piattaforme
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300):

connettere il modulo <x> [console|telnet], dove x è l'ID dello slot, quindi **connettere ftd [istanza],** dove l'istanza è rilevante solo per la distribuzione a più istanze.

2. Eseguire il comando **show version system** e controllare la riga con la stringa **SSP Slot Number**. Se il **Container** esiste in questa riga, l'FTD viene eseguito in modalità container:

```
> 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)
…
```

File di risoluzione dei problemi FTD

Seguire questi passaggi per verificare il tipo di distribuzione dell'istanza FTD nel file di risoluzione dei problemi FTD:

1. Aprire il file per la risoluzione dei problemi e selezionare la cartella **<nomefile>-troubleshoot .tar/results-<data>—xxxxxx/command-outputs.**
2. Aprire il file **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'
```

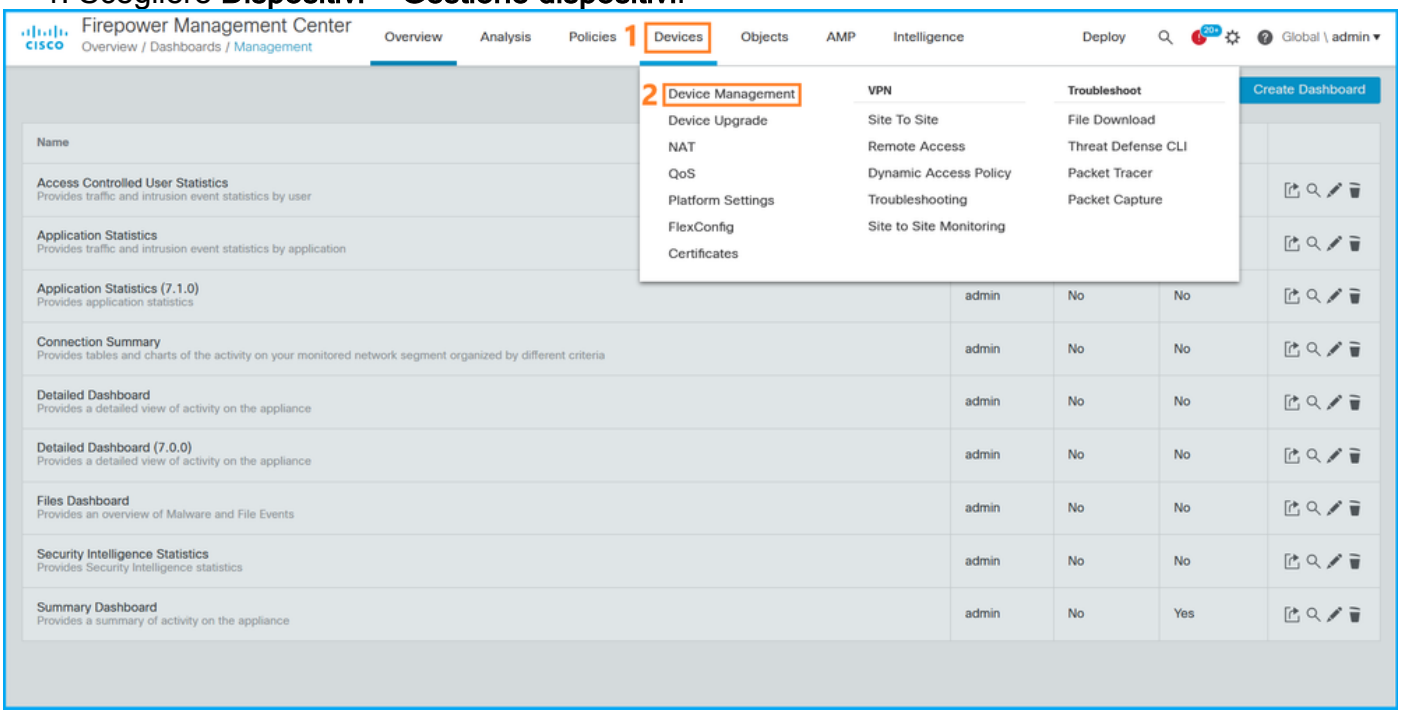
3. Controllare la riga con la stringa **SSP Slot Number** (Numero slot SSP). Se il **Container** esiste in questa riga, l'FTD viene eseguito in modalità container:

```
-------------------[ 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)
…
```

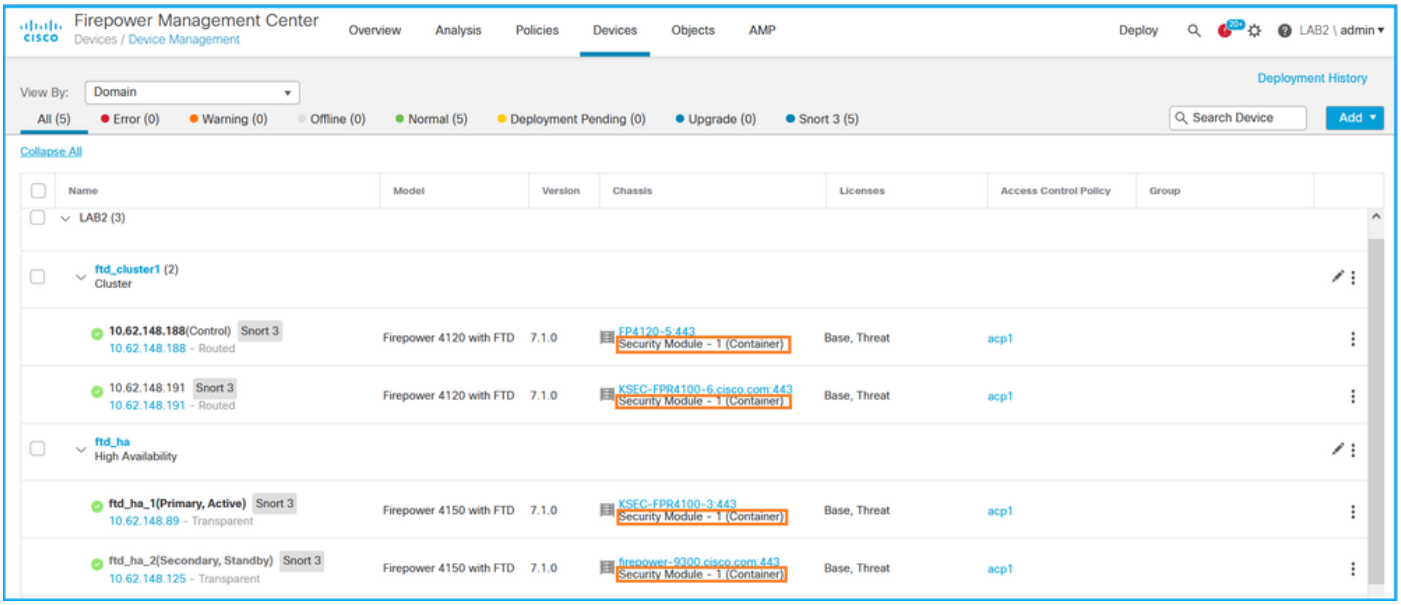
UI FMC

Per verificare il tipo di distribuzione dell'istanza FTD nell'interfaccia utente di FMC, eseguire la procedura seguente:

1. Scegliere **Dispositivi > Gestione dispositivi**:



2. Controllare la colonna **Chassis**. Se il **container** esiste nella linea, FTD viene eseguito in modalità container.



API REST FMC

Per verificare il tipo di distribuzione dell'istanza FTD tramite REST-API di FMC, eseguire la procedura seguente. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedi un token di autenticazione:

```
# 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. Identificare il dominio che contiene il dispositivo. Nella maggior parte delle query API REST il parametro **domain** è obbligatorio. Utilizzare il token in questa query per recuperare l'elenco dei domini:

```
# 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. Utilizzare l'UUID del dominio per eseguire una query sui **record** specifici del **dispositivo** e l'UUID specifico del dispositivo:

```
# 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
```

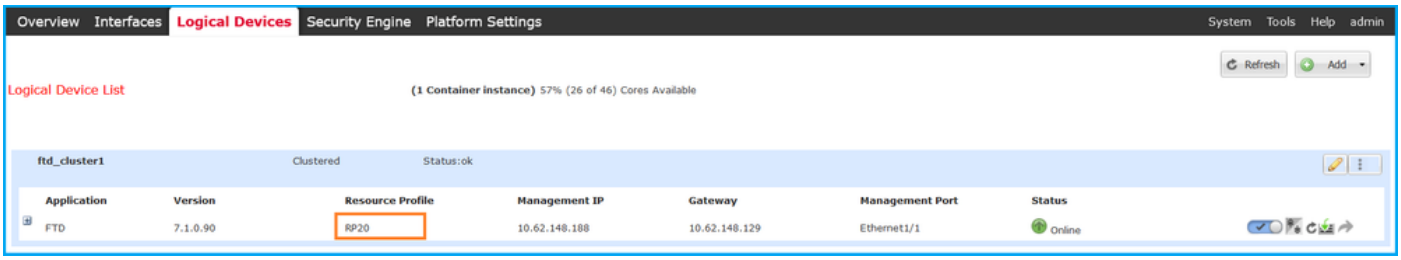
```
{
    "items": [
        {
            "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
            "links": {
                "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-
000000000000/devices/devicerecords/796eb8f8-d83b-11ec-941d-b9083eb612d8"
            },
       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

4. Utilizzare l'UUID del dominio e l'UUID del dispositivo/contenitore del passaggio 3 in questa query e controllare il valore di **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,
...
```

UI FCM

Per verificare il tipo di distribuzione dell'istanza FTD, controllare il valore dell'attributo **Profilo risorsa** in Dispositivi logici. Se il valore non è vuoto, l'FTD viene eseguito in modalità contenitore:



CLI FXOS

Per verificare il tipo di distribuzione dell'istanza FTD nella CLI di FXOS, attenersi alla procedura seguente:

1. Stabilire una connessione console o SSH allo chassis.
2. Passare all'**ambito ssa** ed eseguire il comando **show app-instance**, quindi controllare la colonna **Deploy Type** dell'FTD specifico in base allo slot e all'identificatore:

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

API REST FXOS

Seguire questi passaggi per verificare il tipo di distribuzione dell'istanza FTD tramite una richiesta REST-API FXOS. Utilizzare un client REST-API. Nell'esempio viene usato **il ricciolo**:

1. Richiedi un token di autenticazione:

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

2. Specificare il token, l'ID slot in questa query e controllare il valore di **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",
...
```

File show-tech per lo chassis FXOS

Seguire questi passaggi per verificare la modalità firewall FTD nel file show-tech dello chassis FXOS:

1. Per FXOS versione 2.7 e successive, aprire il file **sam_techsupportinfo** in **<name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar**

Per le versioni precedenti, aprire il file **sam_techsupportinfo** in **FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.**

2. Controllare la sezione **`show slot expand detail`** per lo slot e l'identificatore specifici:

```
# 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
```

Verifica della modalità contesto ASA

ASA supporta modalità a contesto singolo e multiplo. FTD non supporta la modalità multi-contesto.

Èpossibile verificare il tipo di contesto utilizzando le opzioni seguenti:

- ASA CLI
- ASA show-tech

ASA CLI

Per verificare la modalità di contesto ASA sulla CLI dell'ASA, attenersi alla procedura seguente:

1. Utilizzare queste opzioni per accedere alla CLI dell'ASA in base alla piattaforma e alla modalità di distribuzione:

- Accesso diretto telnet/SSH ad ASA su Firepower 1000/3100 e Firepower 2100 in modalità appliance
- Accesso dalla CLI della console FXOS su Firepower 2100 in modalità piattaforma e connessione all'ASA con il comando **connect asa**
- Accesso dalla CLI di FXOS tramite comandi (Firepower 4100/9300): **connettere il modulo <x> [console|telnet],** dove x è l'ID dello slot, quindi **connettere un'appliance asa**

- Per le appliance ASA virtuali, accesso diretto SSH alle appliance ASA o accesso alla console dall'interfaccia utente dell'hypervisor o del cloud

2. Eseguire il comando **show mode** dalla CLI:

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

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

File ASA show-tech

Per verificare la modalità di contesto ASA nel file show-tech ASA, attenersi alla procedura seguente:

1. Controllare la sezione **show context detail** nel file show-tech. In questo caso, la modalità contesto è multipla poiché esistono più contesti:

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

Verificare la modalità Firepower 2100 con ASA

Firepower 2100 con ASA può essere eseguito in una delle seguenti modalità:

- Modalità piattaforma: i parametri operativi di base e le impostazioni dell'interfaccia hardware sono configurati in FXOS. Queste impostazioni includono la modifica dello stato di amministrazione delle interfacce, la configurazione di EtherChannel, NTP, gestione delle immagini e altro ancora. Per la configurazione di FXOS è possibile utilizzare l'interfaccia Web di FCM o la CLI di FXOS.
- Modalità accessorio (predefinita): la modalità accessorio consente agli utenti di configurare tutti i criteri nell'appliance ASA. Dalla CLI di FXOS sono disponibili solo comandi avanzati.

La modalità Firepower 2100 con ASA può essere verificata usando queste opzioni:

- ASA CLI
- CLI FXOS
- FXOS show-tech

ASA CLI

Per verificare la modalità Firepower 2100 con ASA sulla CLI dell'appliance ASA, attenersi alla procedura seguente:

1. Utilizzare telnet/SSH per accedere all'appliance ASA su Firepower 2100.

2. Eseguire il comando **show fxos mode** sulla CLI:

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

Modalità accessorio:

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

> **Nota:** In modalità multi-contesto, il comando **show fax mode** è disponibile nel **sistema** o nel contesto **admin**.

CLI FXOS

Seguire questa procedura per verificare la modalità Firepower 2100 con ASA sulla CLI di FXOS:

1. Utilizzare telnet/SSH per accedere all'appliance ASA su Firepower 2100.

2. Eseguire il comando **connect fxos**:

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

> **Nota:** In modalità multi-contesto, il comando **connect fxos** è disponibile nel contesto **admin**.

3. Eseguire il comando **show fxos-mode**:

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

Modalità accessorio:

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

File FXOS show-tech

Seguire questa procedura per verificare la modalità Firepower 2100 con ASA nel file show-tech dello chassis FXOS:

1. Aprire il file **tech_support_brief** in **<nome>_FPRM.tar.gz/<nome>_FPRM.tar**

2. Controllare la sezione **`show fxos-mode`**:

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

Modalità accessorio:

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

Problemi noti

ID bug Cisco CSCwb94424 ENH: Aggiungere un comando CLISH per la verifica della configurazione HA di FMC

ID bug Cisco CSCvn3162 ENH: Aggiungi OID SNMP FXOS per eseguire il polling della configurazione di dispositivi logici e istanze dell'app

ID bug Cisco CSCwb97767 ENH: Aggiungi OID per la verifica del tipo di distribuzione dell'istanza FTD

ID bug Cisco CSCwb97772 ENH: Includere l'output del comando 'show fax mode' in show-tech dell'appliance ASA su Firepower 2100

ID bug Cisco CSCwb97751 OID 1.3.6.1.4.1.9.9.491.1.6.1.1 per la verifica in modalità firewall trasparente non disponibile

Informazioni correlate

- Guida rapida all'API REST di Secure Firewall Management Center, versione 7.1
- Configurazione di SNMP su appliance Firepower NGFW
- Guida API REST Cisco Firepower Threat Defense
- Guida di riferimento all'API REST Cisco FXOS
- Compatibilità Cisco ASA
- Versioni di Firepower 1000/2100 e Secure Firewall 3100 ASA e FXOS Bundle
- Componenti in bundle
- Procedure di generazione file di Firepower
- Guida introduttiva a Cisco Firepower 2100
- Guida alla compatibilità di Cisco Firepower Threat Defense