

Vérification du mode Firepower, de l'instance, de la haute disponibilité et de la configuration évolutive

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Vérifier la configuration de haute disponibilité et d'évolutivité](#)

[Haute disponibilité FMC](#)

[Interface utilisateur FMC](#)

[CLI FMC](#)

[FMC REST-API](#)

[Fichier de dépannage FMC](#)

[Haute disponibilité FDM](#)

[Interface utilisateur FDM](#)

[FDM REST-API](#)

[CLI FTD](#)

[Sondage FTD SNMP](#)

[Fichier de dépannage FTD](#)

[Haute disponibilité et évolutivité FTD](#)

[CLI FTD](#)

[FTD SNMP](#)

[Fichier de dépannage FTD](#)

[Interface utilisateur FMC](#)

[API REST FMC](#)

[Interface utilisateur FDM](#)

[FDM REST-API](#)

[Interface utilisateur FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Fichier show-tech du châssis FXOS](#)

[Haute disponibilité et évolutivité ASA](#)

[CLI ASA](#)

[ASA SNMP](#)

[Fichier show-tech ASA](#)

[Interface utilisateur FCM](#)

[CLI FXOS](#)

[FXOS REST-API](#)

[Fichier show-tech du châssis FXOS](#)

[Vérification du mode pare-feu](#)

[Mode pare-feu FTD](#)

[CLI FTD](#)

[Fichier de dépannage FTD](#)

[Interface utilisateur FMC](#)

[FMC REST-API](#)

[Interface utilisateur FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Fichier show-tech du châssis FXOS](#)

[Mode pare-feu ASA](#)

[CLI ASA](#)

[Fichier show-tech ASA](#)

[Interface utilisateur FCM](#)

[CLI FXOS](#)

[FXOS REST-API](#)

[Fichier show-tech du châssis FXOS](#)

[Vérifier le type de déploiement d'instance](#)

[CLI FTD](#)

[Fichier de dépannage FTD](#)

[Interface utilisateur FMC](#)

[FMC REST-API](#)

[Interface utilisateur FCM](#)

[CLI FXOS](#)

[API REST FXOS](#)

[Fichier show-tech du châssis FXOS](#)

[Vérifier le mode de contexte ASA](#)

[CLI ASA](#)

[Fichier show-tech ASA](#)

[Vérification du mode Firepower 2100 avec ASA](#)

[CLI ASA](#)

[CLI FXOS](#)

[Fichier show-tech FXOS](#)

[Problèmes identifiés](#)

[Informations connexes](#)

Introduction

Ce document décrit la vérification de la configuration de Firepower haute disponibilité et évolutivité, du mode pare-feu et du type de déploiement d'instance.

Informations générales

Les étapes de vérification pour la configuration de haute disponibilité et d'évolutivité, le mode pare-feu et le type de déploiement d'instance sont indiquées sur l'interface utilisateur (UI), l'interface de ligne de commande (CLI), via les requêtes REST-API, SNMP et dans le fichier de dépannage.

Conditions préalables

Exigences

Connaissances de base sur les produits, REST-API, SNMP

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower 11xx
- Firepower 21xx
- Firepower 31xx
- Firepower 41xx
- Firepower Management Center (FMC) version 7.1.x
- Système d'exploitation extensible Firepower (FXOS) 2.11.1.x
- Firepower Device Manager (FDM) 7.1.x
- Défense contre les menaces Firepower 7.1.x
- ASA 9.17.x

Vérifier la configuration de haute disponibilité et d'évolutivité

La haute disponibilité fait référence à la configuration du basculement. La configuration de la haute disponibilité ou du basculement joint deux périphériques de sorte que si l'un des périphériques tombe en panne, l'autre périphérique peut prendre le relais.

L'évolutivité fait référence à la configuration du cluster. Une configuration de cluster vous permet de regrouper plusieurs noeuds FTD en un seul périphérique logique. Un cluster offre toutes les commodités d'un seul périphérique (gestion, intégration dans un réseau) et permet d'augmenter le débit et la redondance de plusieurs périphériques.

Dans ce document, ces expressions sont utilisées de façon interchangeable :

- haute disponibilité ou basculement
- évolutivité ou cluster

Dans certains cas, la vérification de la configuration ou de l'état de haute disponibilité et d'évolutivité n'est pas disponible. Par exemple, il n'existe aucune commande de vérification pour la configuration autonome FTD. Les modes de configuration autonome, de basculement et de cluster s'excluent mutuellement. Si un périphérique ne dispose pas de configuration de basculement et de

cluster, il est considéré comme fonctionnant en mode autonome.

Haute disponibilité FMC

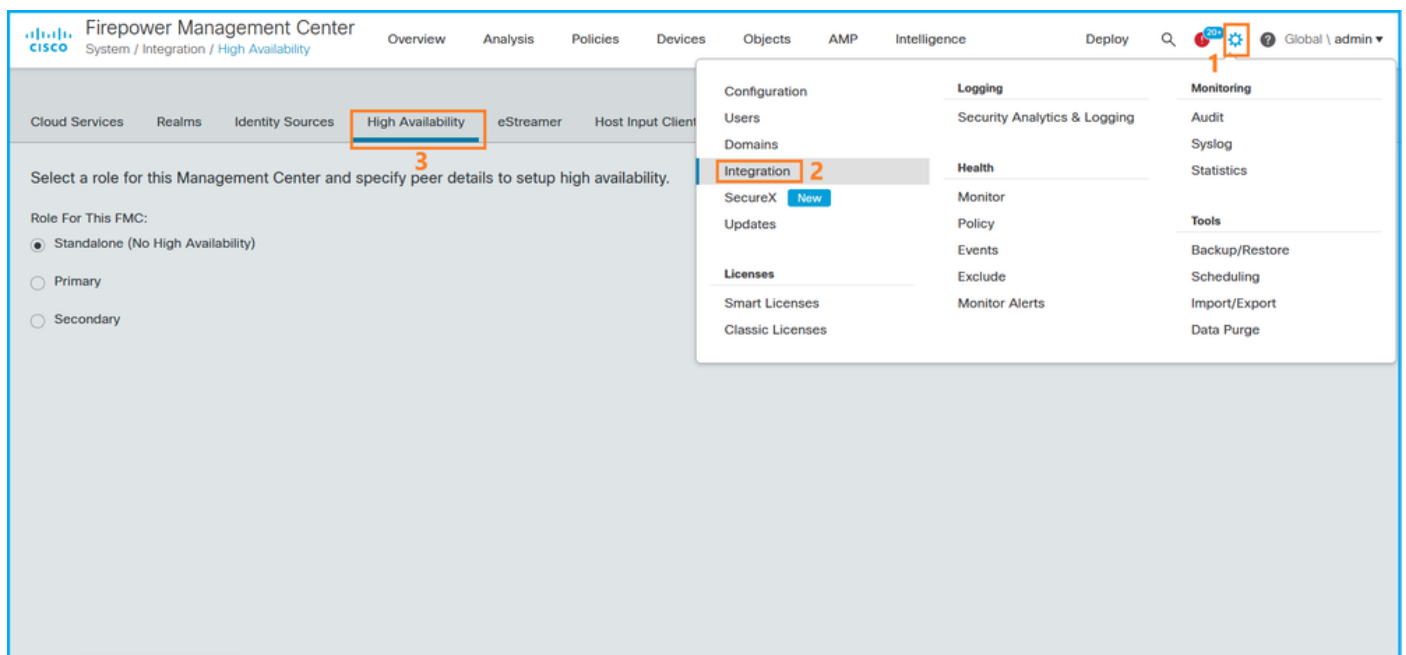
La configuration et l'état de la haute disponibilité du contrôleur FMC peuvent être vérifiés à l'aide des options suivantes :

- Interface utilisateur FMC
- CLI FMC
- Requête API REST
- Fichier de dépannage FMC

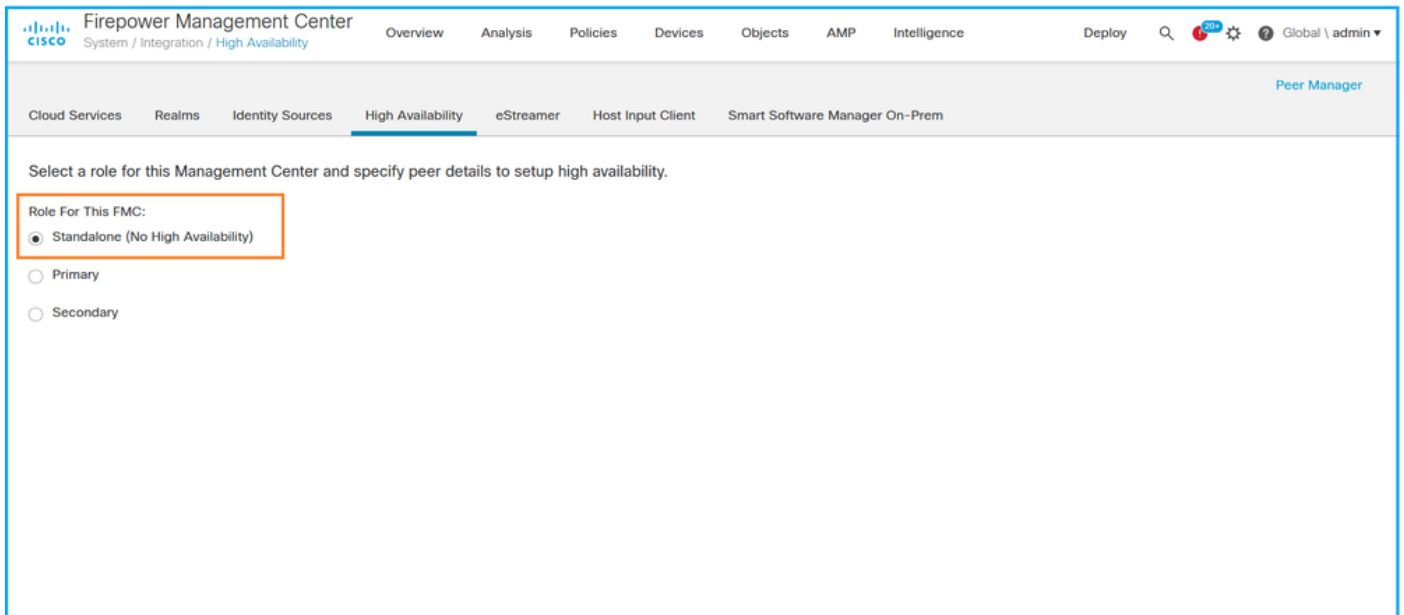
Interface utilisateur FMC

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité FMC sur l'interface utilisateur FMC :

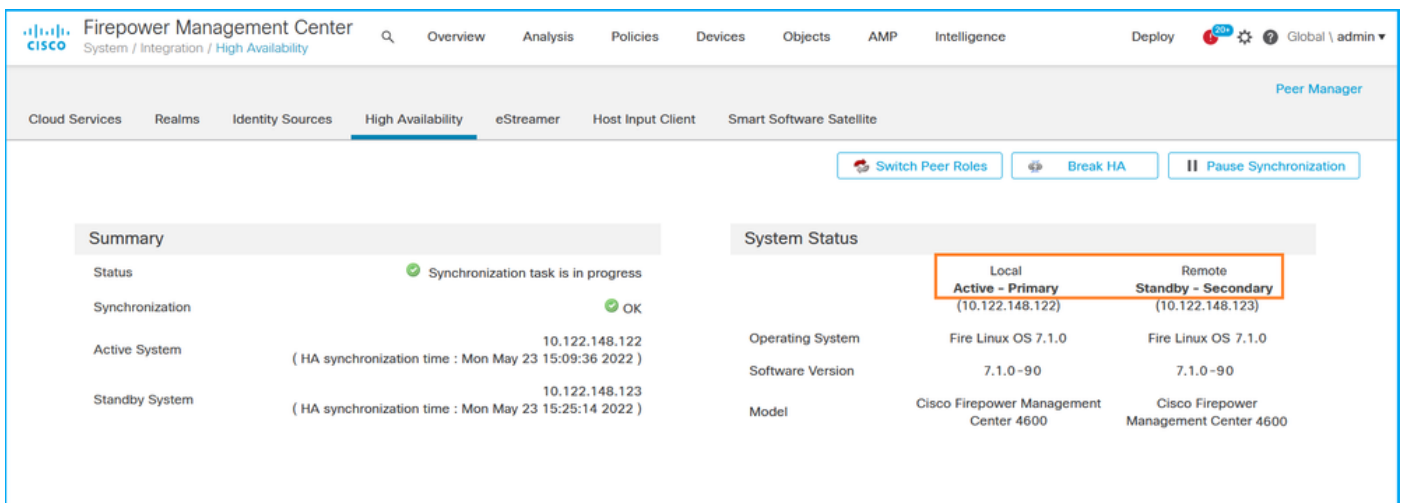
1. Choisissez System > Integration > High Availability :



2. Vérifiez le rôle du FMC. Dans ce cas, la haute disponibilité n'est pas configurée et FMC fonctionne dans une configuration autonome :



Si la haute disponibilité est configurée, les rôles locaux et distants sont affichés :



CLI FMC

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité FMC sur l'interface de ligne de commande FMC :

1. Accédez à FMC via SSH ou une connexion console.
2. Exécutez la commande expert, puis exécutez la commande sudo su :

```
<#root>
```

```
>
```

```
expert
```

```
admin@fmc1:~$
```

```
sudo su
```

Password:
Last login: Sat May 21 21:18:52 UTC 2022 on pts/0
fmc1:/Volume/home/admin#

3. Exécutez la commande `troubleshoot_HADC.pl` et sélectionnez l'option 1 Show HA Info Of FMC.
Si la haute disponibilité n'est pas configurée, ce résultat est affiché :

```
<#root>
fmc1:/Volume/home/admin#
troubleshoot_HADC.pl

***** Troubleshooting Utility *****

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

*****

Enter choice: 1

HA Enabled: No
```

Si la haute disponibilité est configurée, ce résultat est affiché :

```
<#root>
fmc1:/Volume/home/admin#
troubleshoot_HADC.pl

***** Troubleshooting Utility *****

1 Show HA Info Of FMC

2 Execute Sybase DBPing
3 Show Arbiter Status
4 Check Peer Connectivity
5 Print Messages of AQ Task
6 Show FMC HA Operations History (ASC order)
```

7 Dump To File: FMC HA Operations History (ASC order)

8 Help

0 Exit

Enter choice:

1

HA Enabled: Yes

This FMC Role In HA: Active - Primary

Status out put: vmsDbEngine (system,gui) - Running 29061

In vmsDbEngineStatus(): vmsDbEngine process is running at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize/

Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running)

Sybase Database Connectivity: Accepting DB Connections.

Sybase Database Name: csm_primary

Sybase Role: Active



Remarque : dans une configuration à haute disponibilité, le rôle FMC peut avoir un rôle principal ou secondaire, et un état actif ou en veille.

FMC REST-API

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FMC via FMC REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demandez un jeton d'authentification :

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: Basic Ym9keS10b290c0-cd742d3bd2eb:cm9udG90c0-cd742d3bd2eb'
```

...

< X-auth-access-token:

5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb

2. Utilisez le jeton dans cette requête pour trouver l'UUID du domaine global :

<#root>

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json' -H 'X-auth-access-token: 5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb'
```

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

```
    "name": "Global"
```

```

    '
      "type": "Domain",

"uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"

    },
    {
      "name": "Global/LAB2",
      "type": "Domain",
      "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
    },
    {
      "name": "Global/TEST1",
      "type": "Domain",
      "uuid": "ef0cf3e9-bb07-8f66-5c4e-000000000001"
    },
    {
      "name": "Global/TEST2",
      "type": "Domain",
      "uuid": "341a8f03-f831-c364-b751-000000000001"
    }
  ],
  "links": {
    "self": "https://192.0.2.1/api/fmc_platform/v1/info/domain?offset=0&limit=25"
  },
  "paging": {
    "count": 4,
    "limit": 25,
    "offset": 0,
    "pages": 1
  }
}

```

 Remarque : La partie « | python -m json.tool » de la commande est utilisé pour formater la sortie en style JSON et est optionnel.

3. Utilisez l'UUID de domaine global dans cette requête :

<#root>

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

Si la haute disponibilité n'est pas configurée, ce résultat est affiché :

```

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

```



```
}  
}
```

Si la haute disponibilité est configurée, ce résultat est affiché :

```
<#root>
```

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

Fichier de dépannage FMC

Procédez comme suit pour vérifier la configuration et l'état de haute disponibilité du FMC dans le fichier de dépannage FMC :

1. Ouvrez le fichier de dépannage et accédez au dossier <nom_fichier>.tar/results-<date>—xxxxxx/command-output

2. Ouvrez le fichier usr-local-sf-bin-troubleshoot_HADC.pl -a.output :

Si la haute disponibilité n'est pas configurée, ce résultat est affiché :

```
<#root>
```

```
#
```

```
pwd
```

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

```
#
```

```
cat "usr-local-sf-bin-troubleshoot_HADC.pl -a.output"
```

```
Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:
```

```
$VAR1 = [  
    'Mirror Server => csmEng',  
    {  
        'rcode' => 0,  
        'stderr' => undef,  
        'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745'  
    }  
];  
(system,gui) - Waiting
```

```
HA Enabled: No
```

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

```
Not In HA
```

Si la haute disponibilité est configurée, ce résultat est affiché :

<#root>

#

pwd

/var/tmp/results-05-06-2022--199172/command-outputs

#

cat "/usr/local/sf/bin/troubleshoot_HADC.pl -a.output

"

Output of /usr/local/sf/bin/troubleshoot_HADC.pl -a:

Status out put: vmsDbEngine (system,gui) - Running 9399

In vmsDbEngineStatus(): vmsDbEngine process is running at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize/

\$VAR1 = [

 'Mirror Server => csm_primary',

 {

 'stderr' => undef,

 'stdout' => 'SQL Anywhere Server Ping Utility Version 17.0.10.5745

Type	Property	Value
------	----------	-------

Database	MirrorRole	primary
----------	------------	---------

Database	MirrorState	synchronizing
----------	-------------	---------------

Database	PartnerState	connected
----------	--------------	-----------

Database	ArbiterState	connected
----------	--------------	-----------

Server	ServerName	csm_primary
--------	------------	-------------

Ping database successful.

'

 'rcode' => 0

 }

];

(system,gui) - Running 8185

...

HA Enabled: Yes

This FMC Role In HA: Active - Primary

Sybase Process: Running (vmsDbEngine, theSybase PM Process is Running)

Sybase Database Connectivity: Accepting DB Connections.

Sybase Database Name: csm_primary

Sybase Role: Active

Sybase Database Name: csm_primary

Arbiter Running On This FMC.

Peer Is Connected

Haute disponibilité FDM

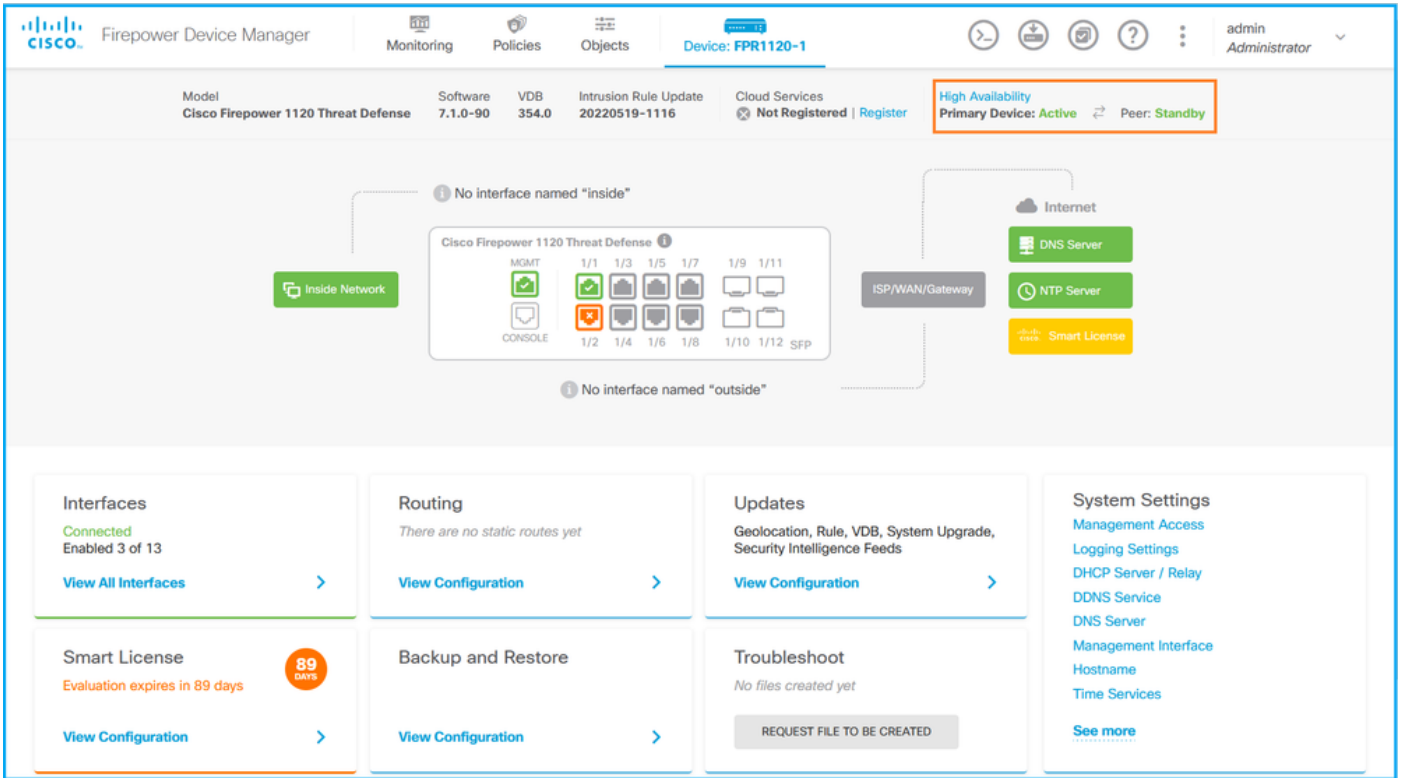
La configuration et l'état de la haute disponibilité de FDM peuvent être vérifiés à l'aide des options suivantes :

- Interface utilisateur FDM
- Demande d'API REST FDM
- CLI FTD
- Sondage FTD SNMP
- Fichier de dépannage FTD

Interface utilisateur FDM

Afin de vérifier la configuration et l'état de la haute disponibilité de FDM sur l'interface utilisateur de FDM, vérifiez la haute disponibilité sur la page principale. Si la haute disponibilité n'est pas configurée, la valeur High Availability est Not Configured :

Si la haute disponibilité est configurée, la configuration et les rôles de basculement de l'unité homologue locale et distante sont affichés :



FDM REST-API

Procédez comme suit pour vérifier la configuration et l'état de haute disponibilité de FDM via la demande FDM REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demandez un jeton d'authentification :

```
<#root>
```

```
#
```

```
curl -k -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ "grant_type": "password", "username": "admin", "password": "admin", "scope": "all" }' https://10.10.10.10:443/api/v1/aaa/authorize

{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlbnR1YiI6ImFkbWw1IiwianRpIjoimjI1YWRhZWMtZDlhYS0xMWVjLWE5MmM1LWUyOTQxNjksInN1YiI6ImFkbWw1IiwianRpIjoimGU0NGIx",
  "expires_in": 1800,
  "refresh_expires_in": 2400,
  "refresh_token": "eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJlbnR1YiI6ImFkbWw1IiwianRpIjoimGU0NGIx",
  "token_type": "Bearer"
}
```

2. Afin de vérifier la configuration de haute disponibilité, utilisez la valeur de jeton d'accès dans

Si la haute disponibilité est configurée, ce résultat est affiché :

```
<#root>
{
  "items": [
    {
      "version": "issgb3rw2lix",

      "name": "HA",

      "nodeRole": "HA_PRIMARY",

      "failoverInterface": {
        "version": "ezzafxo5ccti3",
        "name": "",
        "hardwareName": "Ethernet1/1",
        "id": "8d6c41df-3e5f-465b-8e5a-d336b282f93f",
        "type": "physicalinterface"
      },
    },
  ],
  ...
}
```

3. Afin de vérifier le statut de haute disponibilité, utilisez cette requête :

```
<#root>
#
curl -s -k -X GET -H 'Accept: application/json' -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJpYXQiOiJ1bnkifQ.eyJ1bnkifQ'
```

Si la haute disponibilité n'est pas configurée, ce résultat est affiché :

```
<#root>
{
  "nodeRole" : null,

  "nodeState" : "SINGLE_NODE",

  "peerNodeState" : "HA_UNKNOWN_NODE",

  "configStatus" : "UNKNOWN",
  "haHealthStatus" : "HEALTHY",
  "disabledReason" : "",
  "disabledTimestamp" : null,
  "id" : "default",
  "type" : "hastatus",
  "links" : {
```

```
    "self" : "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
  }
}
```

Si la haute disponibilité est configurée, ce résultat est affiché :

```
<#root>
```

```
{
  "nodeRole": "HA_PRIMARY",

  "nodeState": "HA_ACTIVE_NODE",

  "peerNodeState": "HA_STANDBY_NODE",

  "configStatus": "IN_SYNC",

  "haHealthStatus": "HEALTHY",

  "disabledReason": "",
  "disabledTimestamp": "",
  "id": "default",
  "type": "hastatus",
  "links": {
    "self": "https://192.0.2.3/api/fdm/v6/devices/default/operational/ha/status/default"
  }
}
```

CLI FTD

Suivez les étapes de la section.

Sondage FTD SNMP

Suivez les étapes de la section.

Fichier de dépannage FTD

Suivez les étapes de la section.

Haute disponibilité et évolutivité FTD

La configuration et l'état de la haute disponibilité et de l'évolutivité FTD peuvent être vérifiés à

l'aide des options suivantes :

- CLI FTD
- FTD SNMP
- Fichier de dépannage FTD
- Interface utilisateur FMC
- FMC REST-API
- Interface utilisateur FDM
- FDM REST-API
- Interface utilisateur FCM
- CLI FXOS
- FXOS REST-API
- Fichier show-tech du châssis FXOS

CLI FTD

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité du FTD sur l'interface de ligne de commande du FTD :

1. Utilisez ces options pour accéder à l'interface de ligne de commande FTD conformément à la plate-forme et au mode de déploiement :

- Accès SSH direct au FTD - toutes les plates-formes
- Accès à partir de la console FXOS CLI (Firepower 1000/2100/3100) via la commande `connect ftd`
- Accès à partir de l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :

connectez le module `<x>` [`console|telnet`], où `x` est l'ID de logement, puis connectez `ftd` [`instance`], où l'instance est pertinente uniquement pour le déploiement multi-instance

- Pour les FTD virtuels, accès SSH direct au FTD ou accès console à partir de l'hyperviseur ou de l'interface utilisateur du cloud

2. Afin de vérifier la configuration et l'état du basculement FTD, exécutez les commandes `show running-config failover` et `show failover state` sur l'interface de ligne de commande.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
>
```

```
show running-config failover
```

```
no failover
```

```
>
```

```
show failover state
```

```
                State          Last Failure Reason    Date/Time

This host

-      Secondary

      Disabled      None

Other host -      Primary
                Not Detected    None
====Configuration State====
====Communication State====
```

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

```
>
show running-config failover

failover

failover lan unit primary

failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 10.30.34.2 255.255.255.0 standby 10.30.34.3

>
show failover state

                State          Last Failure Reason    Date/Time

This host -      Primary
                Active          None

Other host -      Secondary
                Standby Ready    Comm Failure          09:21:50 UTC May 22 2022
====Configuration State====
      Sync Done
====Communication State====
      Mac set
```

3. Afin de vérifier la configuration et l'état du cluster FTD, exécutez les commandes show running-config cluster et show cluster info sur l'interface de ligne de commande.

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
>
```

```
show running-config cluster
```

```
>
```

```
show cluster info
```

```
Clustering is not configured
```

Si le cluster est configuré, ce résultat s'affiche :

```
<#root>
```

```
>
```

```
show running-config cluster
```

```
cluster group ftd_cluster1
```

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

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

```
cluster-interface Port-channel148.204 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
```

 Remarque : les rôles maître et contrôle sont identiques.

FTD SNMP

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FTD via SNMP :

1. Assurez-vous que SNMP est configuré et activé. Pour les FTD gérés par FDM, référez-vous à [Configurer et dépanner SNMP sur Firepower FDM](#) pour les étapes de configuration. Pour les FTD gérés par FMC, référez-vous à [Configurer SNMP sur les appareils NGFW Firepower](#) pour les étapes de configuration.
2. Afin de vérifier la configuration et l'état du basculement FTD, interrogez l'OID `.1.3.6.1.4.1.9.9.147.1.2.1.1.1`.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
#
```

```
snmpwalk -v2c -c cisco123 -On 192.0.2.5 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
```

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit (this device)"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured"

SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"

SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

```

#
snmpwalk -v2c -c cisco123 -On
192.0.2.5 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING:
"Primary unit (this device)" <-- This device is primary
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 9
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 10
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "fover Ethernet1/2"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING:
"Active unit" <-- Primary device is active
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Standby unit"

```

3. Pour vérifier la configuration et l'état du cluster, interrogez l'OID 1.3.6.1.4.1.9.9.491.1.8.1.

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

```

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

```

Si le cluster est configuré, mais pas activé, le résultat suivant s'affiche :

```

<#root>
#
snmpwalk -v2c -c cisco123 -On 192.0.2.7 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0
<-- Cluster status, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0
<-- Cluster unit state, disabled
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11

```

```

.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "ftd_cluster1"

<-- Cluster group name
.
1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"

<-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0 <-- Cluster unit ID

.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1 <-- Cluster side ID
...

```

Si le cluster est configuré, activé et opérationnel, ce résultat est affiché :

```

<#root>
#
snmpwalk -v2c -c cisco123 -On 192.0.2.7 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 1

<-- Cluster status, enabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 16
    <-- Cluster unit state, control unit
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 10
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "ftd_cluster1"
<-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"
<-- Cluster unit name
.
1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0
<-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1
<-- Cluster side ID
...

```

Pour plus d'informations sur les descriptions OID, reportez-vous à la [MIB CISCO-UNIFIED-FIREWALL](#).

Fichier de dépannage FTD

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité du FTD dans le fichier de dépannage du FTD :

1. Ouvrez le fichier de dépannage et accédez au dossier <nom du fichier>-troubleshoot.tar/results-<date>—xxxxxx/command-output.
2. Ouvrez le fichier usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output :

```
<#root>
```

```
# pwd
```

```
/ngfw/var/common/results-05-22-2022--102758/command-outputs
```

```
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

3. Afin de vérifier la configuration et l'état du basculement, vérifiez la section show failover.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

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

```
Failover Off
```

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

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

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

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: fover Ethernet1/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.17(1), Mate 9.17(1)
Serial Number: Ours FLM2006EN9UR93, Mate FLM2006EQFWAGG
Last Failover at: 13:45:46 UTC May 20 2022
```

```
This host: Primary - Active
```

```
Active time: 161681 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)
Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

```
Other host: Secondary - Standby Ready
```

```
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)
Interface diagnostic (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)...
```

4. Afin de vérifier la configuration et l'état du cluster FTD, vérifiez la section show cluster info.

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

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

```
Clustering is not configured
```

Si le cluster est configuré et activé, le résultat suivant s'affiche :

```
<#root>
```

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

```
Cluster ftd_cluster1: On
```


Interface mode: spanned
Cluster Member Limit : 16

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

ID : 0
Site ID : 1
Version : 9.17(1)
Serial No.: FLM1949C5RR6HE
CCL IP : 10.173.1.1
CCL MAC : 0015.c500.018f
Module : FPR4K-SM-24
Resource : 20 cores / 44018 MB RAM
Last join : 13:53:52 UTC May 20 2022
Last leave: N/A

Other members in the cluster:

Unit "unit-2-1" in state SLAVE

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

Interface utilisateur FMC

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FTD sur l'interface utilisateur FMC :

1. Choisissez Périphériques > Gestion des périphériques :

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', '1 Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. The 'Devices' menu is open, showing '2 Device Management' selected, along with other options like 'VPN', 'Troubleshoot', 'Device Upgrade', 'NAT', 'QoS', 'Platform Settings', 'FlexConfig', 'Certificates', 'Site To Site', 'Remote Access', 'Dynamic Access Policy', 'Troubleshooting', 'Site to Site Monitoring', 'File Download', 'Threat Defense CLI', 'Packet Tracer', and 'Packet Capture'. The main content area displays a table of various dashboards:

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

2. Afin de vérifier la configuration de la haute disponibilité et de l'évolutivité du FTD, vérifiez les étiquettes Haute disponibilité ou Cluster. Si aucun des deux n'existe, le FTD s'exécute dans une configuration autonome :

The screenshot shows the Firepower Management Center interface. The 'Devices' tab is active, displaying a list of devices. The 'View By' dropdown is set to 'Domain'. The status bar shows 5 Normal devices, 0 Errors, 0 Warnings, 0 Offline, 0 Deployment Pending, 0 Upgrade, and 5 Snort 3. The table below shows the configuration for a cluster and high availability setup.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
ftd_cluster1 (2) Cluster						
10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5.443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha High Availability						
ftd_ha_1(Primary, Active) Snort 3 10.62.148.89 - Transparent	Firepower 4150 with FTD	7.1.0	KSEC-FPR4100-3.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha_2(Secondary, Standby) Snort 3 10.62.148.125 - Transparent	Firepower 4150 with FTD	7.1.0	firepower-9300.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_standalone Snort 3 10.62.148.181 - Routed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1	

3. Afin de vérifier l'état de haute disponibilité et d'évolutivité du FTD, vérifiez le rôle de l'unité entre parenthèses. Si un rôle n'existe pas et que le FTD ne fait pas partie d'un cluster ou d'un basculement, le FTD s'exécute dans une configuration autonome :

The screenshot shows the Firepower Management Center interface. The 'Devices' tab is active, displaying a list of devices. The 'View By' dropdown is set to 'Domain'. The status bar shows 5 Normal devices, 0 Errors, 0 Warnings, 0 Offline, 0 Deployment Pending, 0 Upgrade, and 5 Snort 3. The table below shows the configuration for a cluster and high availability setup, with roles highlighted in red boxes.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Group
ftd_cluster1 (2) Cluster						
10.62.148.188(Control) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.1.0	FP4120-5.443 Security Module - 1 (Container)	Base, Threat	acp1	
10.62.148.191 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.1.0	KSEC-FPR4100-6.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha High Availability						
ftd_ha_1(Primary, Active) Snort 3 10.62.148.89 - Transparent	Firepower 4150 with FTD	7.1.0	KSEC-FPR4100-3.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_ha_2(Secondary, Standby) Snort 3 10.62.148.125 - Transparent	Firepower 4150 with FTD	7.1.0	firepower-9300.cisco.com.443 Security Module - 1 (Container)	Base, Threat	acp1	
ftd_standalone Snort 3 10.62.148.181 - Routed	Firepower 2120 with FTD	7.1.0	N/A	Base, Threat	acp1	



Remarque : dans le cas d'un cluster, seul le rôle de l'unité de contrôle est affiché.

Dans ces sorties, ftd_ha_1, ftd_ha_2, ftd_standalone, ftd_ha, ftc_cluster1 sont des noms de périphériques configurables par l'utilisateur. Ces noms ne font pas référence à la configuration ou à l'état réel de la haute disponibilité et de l'évolutivité.

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FTD via FMC REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demander un jeton d'authentification :

```
<#root>
```

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

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

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

2. Identifiez le domaine qui contient le périphérique. Dans la plupart des requêtes de l'API REST, le paramètre domain est obligatoire. Utilisez le jeton dans cette requête pour récupérer la liste des domaines :

```
<#root>
```

```
#
```

```
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
  "items":
  [
    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
```

```
"name": "Global/LAB2",
```

```
"type": "Domain",
```

```
"uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
```

```
},
```

```
...
```

3. Utilisez l'UUID de domaine pour interroger les enregistrements spécifiques des périphériques et l'UUID spécifique des périphériques :

```
<#root>
#
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/d
{
  "items": [
    {

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

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

      "name": "ftd_ha_1",

      "type": "Device"
    },
    ...
  ]
}
```

4. Afin de vérifier la configuration de basculement, utilisez l'UUID de domaine et l'UUID de périphérique/conteneur de l'étape 3 dans cette requête :

```
<#root>
#
curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/devic
...
  "containerDetails": {
    "id": "eec3ddfc-d842-11ec-a15e-986001c83f2f",

    "name": "ftd_ha",

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

5. Afin de vérifier l'état de basculement, utilisez l'UUID de domaine et l'UUID DeviceHAPair de l'étape 4 dans cette requête :

```
<#root>
```

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

"primaryStatus": {
    "currentStatus": "Active",
    "device": {
        "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8",
        "keepLocalEvents": false,

"name": "ftd_ha_1"
    }
},
"secondaryStatus": {
    "currentStatus": "Standby",
    "device": {
        "id": "e60ca6d0-d83d-11ec-b407-cdc91a553663",
        "keepLocalEvents": false,

"name": "ftd_ha_2"
    }
}
...

```

6. Afin de vérifier la configuration du cluster, utilisez l'UUID de domaine et l'UUID de périphérique/conteneur de l'étape 3 dans cette requête :

<#root>

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/dev
...
    "containerDetails": {
        "id": "
8e6188c2-d844-11ec-bdd1-6e8d3e226370
",
        "links": {
            "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000
        },

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

```

7. Afin de vérifier l'état du cluster, utilisez l'UUID de domaine et l'UUID de périphérique/conteneur de l'étape 6 dans cette requête :

```
<#root>
```

```
# curl -s -k -X GET 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/dev
{
  "controlDevice": {
    "deviceDetails": {
      "
id": "3344bc4a-d842-11ec-a995-817e361f7ea5",
      "name": "10.62.148.188",
      "type": "Device"
    }
  },
  "dataDevices": [
    {
      "deviceDetails": {
id": "a7ba63cc-d842-11ec-be51-f3efcd7cd5e5",
      "name": "10.62.148.191",
      "type": "Device"
    }
  ],
  "id": "8e6188c2-d844-11ec-bdd1-6e8d3e226370",

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

Interface utilisateur FDM

Suivez les étapes de la section.

FDM REST-API

Suivez les étapes de la section.

Interface utilisateur FCM

L'interface utilisateur FCM est disponible sur Firepower 4100/9300 et Firepower 2100 avec ASA en mode plate-forme.

Procédez comme suit pour vérifier l'état de haute disponibilité et d'évolutivité du FTD sur l'interface utilisateur du FCM :

1. Afin de vérifier l'état de basculement FTD, vérifiez la valeur de l'attribut HA-ROLE sur la page Logical Devices :

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

Interface Name	Type
Ethernet1/2	data
Ethernet1/3	data

Attributes
Cluster Operational Status : not-applicable
FIREPOWER-MGMT-IP : 10.62.148.89
HA-LBWK-INTF : Ethernet1/2
HA-LAN-INTF : Ethernet1/2
MGMT-URL : https://10.62.184.21/
HA-ROLE : active
UUID : 79626898-d83b-11ec-941d-b9083eb612d8

Remarque : l'étiquette Autonome en regard de l'identificateur de périphérique logique fait référence à la configuration du périphérique logique du châssis, et non à la configuration de basculement FTD.

2. Afin de vérifier la configuration et l'état du cluster FTD, vérifiez l'étiquette Clustered et la valeur de l'attribut CLUSTER-ROLE sur la page Logical Devices :

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

Interface Name	Type
port-channel1	data
port-channel48.204	cluster

Attributes
Cluster Operational Status : in-cluster
FIREPOWER-MGMT-IP : 10.62.148.188
CLUSTER-ROLE : control
CLUSTER-IP : 10.173.1.1
MGMT-URL : https://10.62.184.21/
UUID : 3344bc4a-d842-11ec-9955-817e3617ea5

CLI FXOS

La configuration et la vérification de l'état de la haute disponibilité et de l'évolutivité FTD sur l'interface de ligne de commande FXOS sont disponibles sur Firepower 4100/9300.

Procédez comme suit pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FTD sur l'interface de ligne de commande FXOS :

- Établissez une connexion de console ou SSH au châssis.
- Afin de vérifier l'état de haute disponibilité du FTD, exécutez la commande `scope ssa`, puis exécutez `scope slot <x>` pour basculer vers le logement spécifique où le FTD s'exécute et exécutez la commande `show app-instance expand` :

<#root>

```
firepower #
scope ssa
firepower /ssa #
scope slot 1
firepower /ssa/slot #
show app-instance expand
```

Application Instance:

```
App Name: ftd
Identifier: ftd1
Admin State: Enabled
Oper State: Online
Running Version: 7.1.0.90
Startup Version: 7.1.0.90
Deploy Type: Container
Turbo Mode: No
Profile Name: RP20
Cluster State: Not Applicable
Cluster Role: None
```

App Attribute:

App Attribute Key	Value
firepower-mgmt-ip	192.0.2.5
ha-lan-intf	Ethernet1/2
ha-link-intf	Ethernet1/2

```
ha-role          active
mgmt-url         https://192.0.2.1/
uuid             796eb8f8-d83b-11ec-941d-b9083eb612d8
...
```

3. Afin de vérifier la configuration et l'état du cluster FTD, exécutez la commande `scope ssa`, exécutez la commande `show logical-device <name> detail expand`, où le nom est le nom du périphérique logique, et la commande `show app-instance`. Vérifiez la sortie d'un logement spécifique :

<#root>

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

Logical Device:

```
Name: ftd_cluster1
```


Description:
Slot ID: 1

Mode: Clustered

Oper State: Ok
Template Name: ftd
Error Msg:
Switch Configuration Status: Ok
Sync Data External Port Link State with FTD: Disabled
Current Task:

...
firepower /ssa #

show app-instance

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version	Deploy Ty
ftd							
ftd_cluster1							
1	Enabled	Online	7.1.0.90	7.1.0.90	Container	No	RP20

In Cluster

Master

API REST FXOS

FXOS REST-API est pris en charge sur Firepower 4100/9300.

Suivez ces étapes pour vérifier la configuration et l'état de la haute disponibilité et de l'évolutivité FTD via la demande FXOS REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demandez un jeton d'authentification :

<#root>

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

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

2. Afin de vérifier l'état de basculement FTD, utilisez le jeton et l'ID de slot dans cette requête :

```
<#root>
```

```
#
```

```
curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453c
```

```
...
```

```
{  
  "smAppInstance": [  
    {  
      "adminState": "enabled",  
      "appDn": "sec-svc/app-ftd-7.1.0.90",  
      "appInstId": "ftd_001_JAD201200R43VLP1G3",  
      "appName": "ftd",  
      "clearLogData": "available",  
      "clusterOperationalState": "not-applicable",  
      "clusterRole": "none",  
      "currentJobProgress": "100",  
      "currentJobState": "succeeded",  
      "currentJobType": "start",  
      "deployType": "container",  
      "dn": "slot/1/app-inst/ftd-ftd1",  
      "errorMsg": "",  
      "eventMsg": "",  
      "executeCmd": "ok",  
      "externallyUpgraded": "no",  
      "fsmDescr": "",  
      "fsmProgr": "100",  
      "fsmRmtInvErrCode": "none",  
      "fsmRmtInvErrDescr": "",  
      "fsmRmtInvRslt": "",  
      "fsmStageDescr": "",  
      "fsmStatus": "nop",  
      "fsmTry": "0",  
      "hotfix": "",  
  
      "identifiant": "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-i
        "value": "Ethernet1/2"
    },
    {
        "key": "mgmt-url",
        "rn": "app-attribute-mgmt-url",
        "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-mgmt-ur
        "value": "https://192.0.2.1/"
    },
    {
        "key": "ha-role",

        "rn": "app-attribute-ha-role",
        "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-ha-role"

        "value": "active"
    },
    {
        "key": "uuid",
        "rn": "app-attribute-uuid",
        "urllink": "https://192.0.2.100/api/slot/1/app/inst/ftd-ftd1/app/attribute-uuid",
        "value": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
    }
],
...

```

3. Afin de vérifier la configuration du cluster FTD, utilisez l'identificateur de périphérique logique dans cette requête :

```
<#root>
```

```

# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da445
{
  "smLogicalDevice": [
    {
      "description": "",
      "dn": "ld/ftd_cluster1",
      "errorMsg": "",
      "fsmDescr": "",
      "fsmProgr": "100",
      "fsmRmtInvErrCode": "none",
      "fsmRmtInvErrDescr": "",
      "fsmRmtInvRslt": "",
      "fsmStageDescr": "",
      "fsmStatus": "nop",
      "fsmTaskBits": "",
      "fsmTry": "0",

      "ldMode": "clustered",

      "linkStateSync": "disabled",

      "name": "ftd_cluster1",

      "operationalState": "ok",

```

```

"slotId": "1",
"smClusterBootstrap": [
  {
    "cc1Network": "10.173.0.0",
    "chassisId": "1",
    "gatewayv4": "0.0.0.0",
    "gatewayv6": "::",
    "key": "",
    "mode": "spanned-etherchannel",
    "name": "ftd_cluster1",
    "netmaskv4": "0.0.0.0",
    "poolEndv4": "0.0.0.0",
    "poolEndv6": "::",
    "poolStartv4": "0.0.0.0",
    "poolStartv6": "::",
    "prefixLength": "",
    "rn": "cluster-bootstrap",
    "siteId": "1",
    "supportCc1Subnet": "supported",
    "updateTimestamp": "2022-05-20T13:38:21.872",
    "urlLink": "https://192.0.2.101/api/1d/ftd_cluster1/cluster-bootstrap",
    "virtualIPv4": "0.0.0.0",
    "virtualIPv6": "::"
  }
],
...

```

4. Afin de vérifier l'état du cluster FTD, utilisez cette requête :

```
<#root>
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da444'
```

```

{
  "smAppInstance": [
    {
      "adminState": "enabled",
      "appDn": "sec-svc/app-ftd-7.1.0.90",
      "appInstId": "ftd_001_JAD19500BABIYA30058",
      "appName": "ftd",
      "clearLogData": "available",

      "clusterOperationalState": "in-cluster",

      "clusterRole": "master",

      "currentJobProgress": "100",
      "currentJobState": "succeeded",
      "currentJobType": "start",
      "deployType": "container",
      "dn": "slot/1/app-inst/ftd-ftd_cluster1",
      "errorMsg": "",
      "eventMsg": "",
      "executeCmd": "ok",
      "externallyUpgraded": "no",
      "fsmDescr": "",
      "fsmProgr": "100",
      "fsmRmtInvErrCode": "none",
      "fsmRmtInvErrDescr": "",

```

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

"identifiant": "ftd_cluster1",

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

Fichier show-tech du châssis FXOS

La configuration et l'état de la haute disponibilité et de l'évolutivité du FTD peuvent être vérifiés dans le fichier show-tech du châssis Firepower 4100/9300.

Procédez comme suit pour vérifier la configuration et l'état de haute disponibilité et d'évolutivité dans le fichier show-tech du châssis FXOS :

1. Pour FXOS versions 2.7 et ultérieures, ouvrez le fichier sam_techsupportinfo dans <name>_BC1_all.tar/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Pour les versions antérieures, ouvrez le fichier sam_techsupportinfo dans FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar.

2. Afin de vérifier l'état de basculement, vérifiez la valeur de l'attribut ha-role sous le logement spécifique dans la section « show slot expand detail » :

```
<#root>
```

```
# pwd
```

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

```
# cat sam_techsupportinfo
```

```
...
```

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

```
Slot:
```

```
slot ID: 1
```

```
Log Level: Info
Admin State: Ok
Oper State: Online
Disk Format State: Ok
Disk Format Status: 100%
Clear Log Data: Available
Error Msg:
```

Application Instance:

App Name: ftd

Identifier: ftd1

Admin State: Enabled

Oper State: Online

Running Version: 7.1.0.90

Startup Version: 7.1.0.90

Deploy Type: Container

Turbo Mode: No

Profile Name: RP20

Hotfixes:

Externally Upgraded: No

Cluster State: Not Applicable

Cluster Role: None

Current Job Type: Start

Current Job Progress: 100

Current Job State: Succeeded

Clear Log Data: Available

Error Msg:

Current Task:

App Attribute:

App Attribute Key: firepower-mgmt-ip

Value: 10.62.148.89

App Attribute Key: ha-lan-intf

Value: Ethernet1/2

App Attribute Key: ha-link-intf

Value: Ethernet1/2

App Attribute Key: ha-role

Value: active

App Attribute Key: mgmt-url

Value: https://10.62.184.21/

3. Afin de vérifier la configuration du cluster FTD, vérifiez la valeur de l'attribut Mode sous le logement spécifique dans la section `show logical-device detail expand` :

<#root>

`show logical-device detail expand`

Logical Device:

Name: ftd_cluster1

Description:

Slot ID: 1

Mode: Clustered

Oper State: Ok
Template Name: ftd
Error Msg:
Switch Configuration Status: Ok
Sync Data External Port Link State with FTD: Disabled
Current Task:

Cluster Bootstrap:
Name of the cluster: ftd_cluster1
Mode: Spanned Etherchannel
Chassis Id: 1
Site Id: 1
Key:
Cluster Virtual IP: 0.0.0.0
IPv4 Netmask: 0.0.0.0
IPv4 Gateway: 0.0.0.0
Pool Start IPv4 Address: 0.0.0.0
Pool End IPv4 Address: 0.0.0.0
Cluster Virtual IPv6 Address: ::
IPv6 Prefix Length:
IPv6 Gateway: ::
Pool Start IPv6 Address: ::
Pool End IPv6 Address: ::
Last Updated Timestamp: 2022-05-20T13:38:21.872
Cluster Control Link Network: 10.173.0.0

...

4. Afin de vérifier l'état du cluster FTD, vérifiez la valeur des valeurs d'attribut État du cluster et Rôle du cluster sous le logement spécifique dans la section `show slot expand detail` :

<#root>

`show slot expand detail`

Slot:

slot ID: 1

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

Application Instance:
App Name: ftd

Identifiant: 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:

Haute disponibilité et évolutivité ASA

La configuration et l'état de la haute disponibilité et de l'évolutivité de l'ASA peuvent être vérifiés à l'aide des options suivantes :

- CLI ASA
- Sondage SNMP ASA
- Fichier show-tech ASA
- Interface utilisateur FCM
- CLI FXOS
- FXOS REST-API
- Fichier show-tech du châssis FXOS

CLI ASA

Procédez comme suit pour vérifier la configuration de la haute disponibilité et de l'évolutivité ASA sur l'interface de ligne de commande ASA :

1. Utilisez ces options pour accéder à l'interface de ligne de commande ASA en fonction de la plate-forme et du mode de déploiement :

- Accès Telnet/SSH direct à ASA sur Firepower 1000/3100 et Firepower 2100 en mode appliance
- Accès à partir de l'ILC de la console FXOS sur Firepower 2100 en mode plate-forme et connexion à ASA via la commande `connect asa`
- Accès depuis l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :

connectez le module `<x>` [`console|telnet`], où `x` est l'ID du logement, puis connectez `asa`

- Pour l'ASA virtuel, un accès SSH direct à l'ASA ou un accès console à partir de l'hyperviseur ou de l'interface utilisateur cloud

2. Afin de vérifier la configuration et l'état du basculement ASA, exécutez les commandes `show running-config failover` et `show failover state` sur l'interface de ligne de commande ASA.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
asa#
```

```
show running-config failover
```

```
no failover
```

```
asa#
```

```
show failover state
```

State	Last Failure Reason	Date/Time
-------	---------------------	-----------

This host

- Secondary

Disabled	None	
----------	------	--

Other host - Primary
Not Detected None

====Configuration State====

====Communication State====

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

```
asa#
```

```
show running-config failover
```

```
failover
```

```
failover lan unit primary
```

```
failover lan interface failover-link Ethernet1/1
```

```
failover replication http
```

```
failover link failover-link Ethernet1/1
```

```
failover interface ip failover-link 10.30.35.2 255.255.255.0 standby 10.30.35.3
```

```
#
```

```
show failover state
```

State	Last Failure Reason	Date/Time
-------	---------------------	-----------

This host - Primary

Active	None	
--------	------	--

Other host - Secondary
Standby Ready Comm Failure

19:42:22 UTC May 21 2022

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

3. Afin de vérifier la configuration et l'état du cluster ASA, exécutez les commandes `show running-config cluster` et `show cluster info` sur l'interface de ligne de commande.

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
asa#
```

```
show running-config cluster
```

```
asa#
```

```
show cluster info
```

```
Clustering is not configured
```

Si le cluster est configuré, ce résultat s'affiche :

```
<#root>
```

```
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

Procédez comme suit pour vérifier la configuration de la haute disponibilité et de l'évolutivité de l'ASA via SNMP :

1. Assurez-vous que SNMP est configuré et activé.
2. Afin de vérifier la configuration de basculement et l'état, interrogez l'OID
.1.3.6.1.4.1.9.9.147.1.2.1.1.1.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

```
#
```

```
snmpwalk -v2c -c cisco123 -On 192.0.2.10 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
```

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING: "Primary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit (this device)"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 3
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "not Configured"
```

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING: "Failover Off"
```

```
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Failover Off"
```

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

```
#
```

```
snmpwalk -v2c -c cisco123 -On
```

```
192.0.2.10 .1.3.6.1.4.1.9.9.147.1.2.1.1.1
```

```

SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.4 = STRING: "Failover LAN Interface"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.6 = STRING:

"Primary unit (this device)"      <-- This device is primary

SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.2.7 = STRING: "Secondary unit"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.4 = INTEGER: 2
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.6 = INTEGER: 9
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.3.7 = INTEGER: 10
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.4 = STRING: "fover Ethernet1/2"
SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.6 = STRING:

"Active unit"                    <-- Primary device is active

SNMPv2-SMI::enterprises.9.9.147.1.2.1.1.1.4.7 = STRING: "Standby unit"

```

3. Afin de vérifier la configuration et l'état du cluster, interrogez l'OID 1.3.6.1.4.1.9.9.491.1.8.1.

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

```

<#root>

# snmpwalk -v2c -c cisco123 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1

SNMPv2-SMI::enterprises.9.9.491.1.8.1.1.0 = INTEGER:
0

```

Si le cluster est configuré, mais pas activé, le résultat suivant s'affiche :

```

<#root>

#

snmpwalk -v2c -c cisco123 -On 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1

.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 0

<-- Cluster status, disabled

.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1

.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 0

<-- Cluster unit state, disabled

.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 11

.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "asa_cluster1"

<-- Cluster group name

```

```

.
1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"
<-- Cluster unit name
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0          <-- Cluster unit ID

.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1          <-- Cluster side ID
...

```

Si le cluster est configuré, activé et opérationnel, ce résultat est affiché :

```

<#root>
#
snmpwalk -v2c -c cisco123 -On 192.0.2.12 .1.3.6.1.4.1.9.9.491.1.8.1
.1.3.6.1.4.1.9.9.491.1.8.1.1.0 = INTEGER: 1
<-- Cluster status, enabled
.1.3.6.1.4.1.9.9.491.1.8.1.2.0 = INTEGER: 1
.1.3.6.1.4.1.9.9.491.1.8.1.3.0 = INTEGER: 16
      <-- Cluster unit state, control unit
.1.3.6.1.4.1.9.9.491.1.8.1.4.0 = INTEGER: 10
.1.3.6.1.4.1.9.9.491.1.8.1.5.0 = STRING: "asa_cluster1"
<-- Cluster group name
.1.3.6.1.4.1.9.9.491.1.8.1.6.0 = STRING: "unit-1-1"
<-- Cluster unit name
.
.1.3.6.1.4.1.9.9.491.1.8.1.7.0 = INTEGER: 0
<-- Cluster unit ID
.1.3.6.1.4.1.9.9.491.1.8.1.8.0 = INTEGER: 1
      <-- Cluster side ID
...

```

Pour plus d'informations sur les descriptions OID, reportez-vous à la [MIB CISCO-UNIFIED-FIREWALL](#).

Fichier show-tech ASA

1. Afin de vérifier la configuration et l'état du basculement ASA, vérifiez la section show failover.

Si le basculement n'est pas configuré, le résultat suivant s'affiche :

```
<#root>
```

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

```
Failover Off
```

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

Si le basculement est configuré, le résultat suivant s'affiche :

```
<#root>
```

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

```
Failover On
```

```
Failover unit Primary
```

```
Failover LAN Interface: fover Ethernet1/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.17(1), Mate 9.17(1)
Serial Number: Ours FLM2006EN9AB11, Mate FLM2006EQZY02
Last Failover at: 13:45:46 UTC May 20 2022
```

```
This host: Primary - Active
```

```
Active time: 161681 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)
```

```
Other host: Secondary - Standby Ready
```

```
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.17(1)) status (Up Sys)
```

```
...
```

2. Afin de vérifier la configuration et l'état du cluster, vérifiez la section show cluster info .

Si le cluster n'est pas configuré, le résultat suivant s'affiche :

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

Clustering is not configured
```

Si le cluster est configuré et activé, le résultat suivant s'affiche :

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

Cluster asa_cluster1: On
    Interface mode: spanned
    Cluster Member Limit : 16

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

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

```

Interface utilisateur FCM

Suivez les étapes de la section.

CLI FXOS

Suivez les étapes de la section.

FXOS REST-API

Suivez les étapes de la section.

Fichier show-tech du châssis FXOS

Suivez les étapes de la section.

Vérification du mode pare-feu

Mode pare-feu FTD

Le mode pare-feu fait référence à une configuration de pare-feu routé ou transparent.

Le mode pare-feu FTD peut être vérifié à l'aide des options suivantes :

- CLI FTD
- FTD show-tech
- Interface utilisateur FMC
- FMC REST-API
- Interface utilisateur FCM
- CLI FXOS
- FXOS REST-API
- Fichier show-tech du châssis FXOS



Remarque : FDM ne prend pas en charge le mode transparent.

CLI FTD

Procédez comme suit pour vérifier le mode de pare-feu FTD sur l'interface de ligne de commande FTD :

1. Utilisez ces options pour accéder à l'interface de ligne de commande FTD conformément à la plate-forme et au mode de déploiement :

- Accès SSH direct au FTD - toutes les plates-formes
- Accès à partir de la console FXOS CLI (Firepower 1000/2100/3100) via la commande `connect ftd`
- Accès à partir de l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :

connectez le module `<x>` [`console|telnet`], où `x` est l'ID du logement, puis

connectez `ftd` [`instance`], où l'instance ne concerne que le déploiement multi-instance.

- Pour les FTD virtuels, accès SSH direct au FTD ou accès console à partir de l'hyperviseur ou de l'interface utilisateur du cloud

2. Afin de vérifier le mode de pare-feu, exécutez la commande `show firewall` sur l'interface de ligne de commande :

```
<#root>
```

```
>
```

```
show firewall
```


Firewall mode: Transparent

Fichier de dépannage FTD

Procédez comme suit pour vérifier le mode de pare-feu FTD dans le fichier de dépannage FTD :

1. Ouvrez le fichier de dépannage et accédez au dossier <nom du fichier>-troubleshoot .tar/results-<date>—xxxxxx/command-output.

2. Ouvrez le fichier usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output :

```
<#root>
```

```
# pwd
```

```
/ngfw/var/common/results-05-22-2022--102758/command-outputs
```

```
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

3. Afin de vérifier le mode de pare-feu FTD, vérifiez la section show firewall :

```
<#root>
```

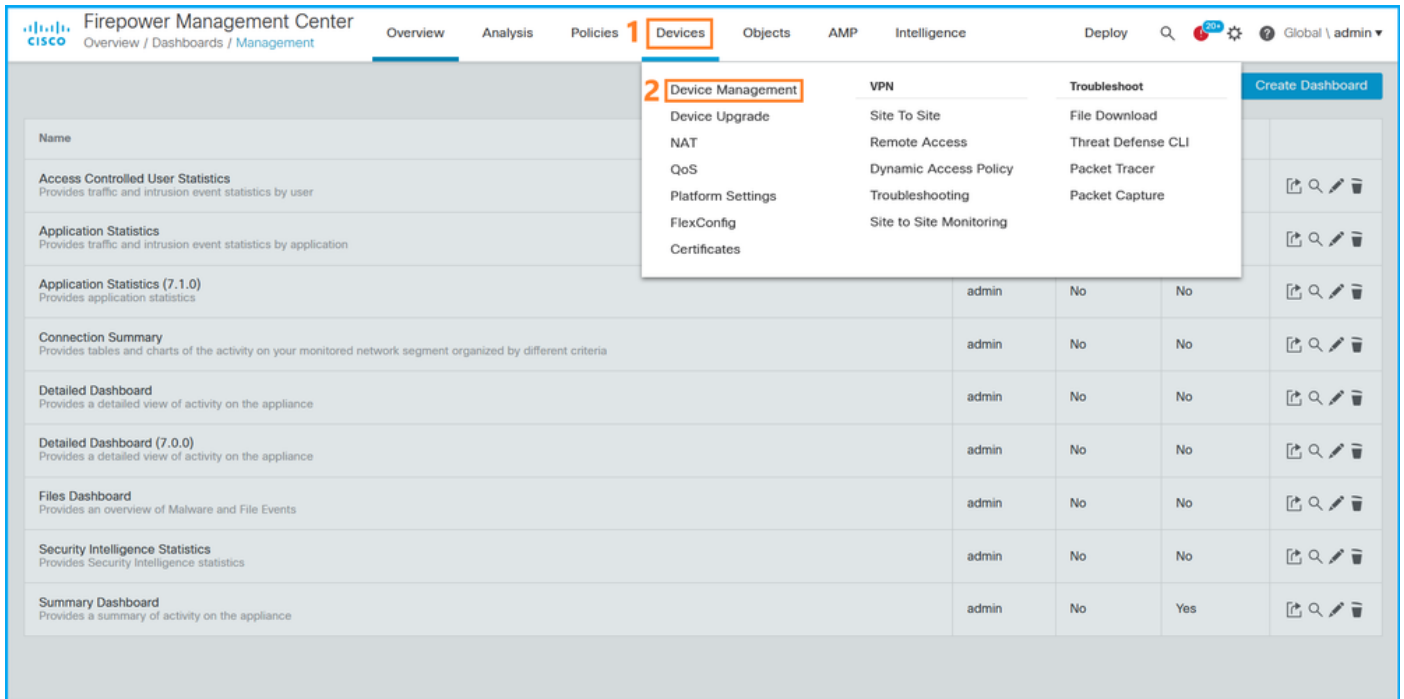
```
----- show firewall -----
```

```
Firewall mode: Transparent
```

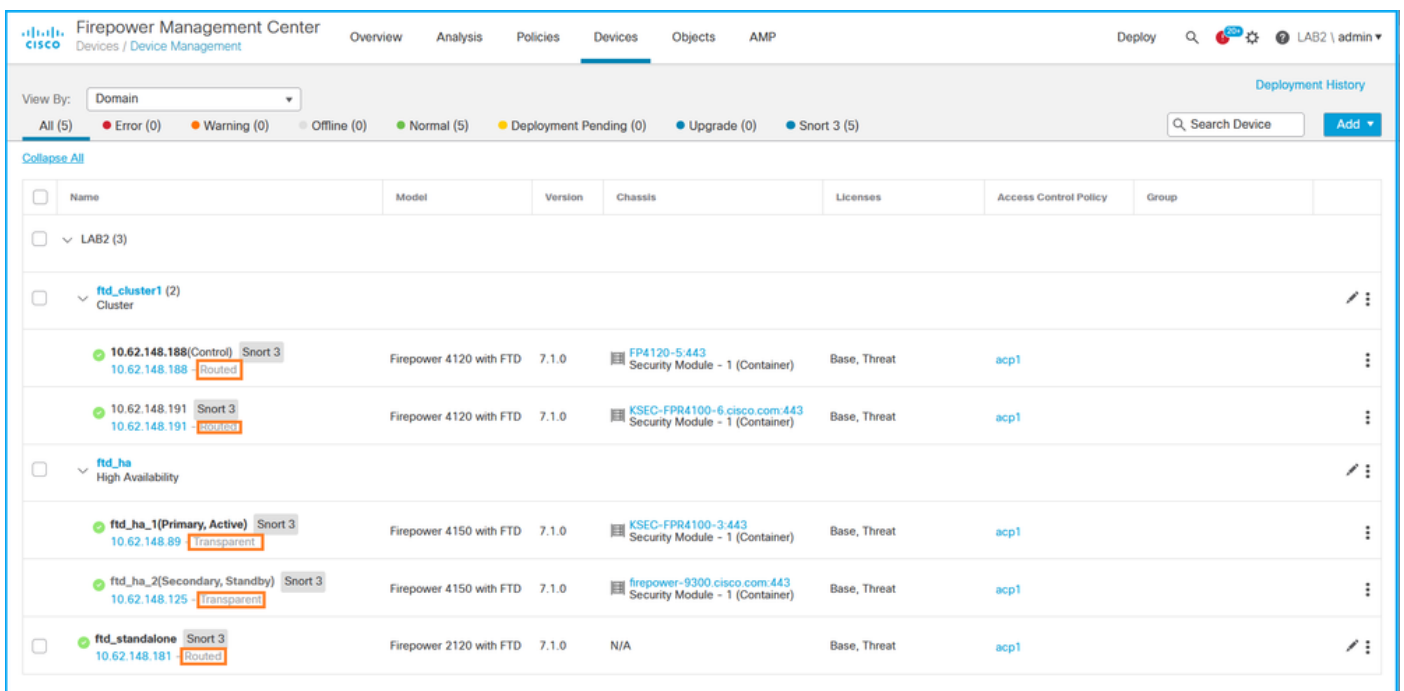
Interface utilisateur FMC

Procédez comme suit pour vérifier le mode de pare-feu FTD sur l'interface utilisateur FMC :

1. Choisissez Périphériques > Gestion des périphériques :



2. Vérifiez les étiquettes Routed ou Transparent :



FMC REST-API

Procédez comme suit pour vérifier le mode de pare-feu FTD via FMC REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demander un jeton d'authentification :

```
<#root>
```

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

< X-auth-access-token:

5d817ef7-f12f-4dae-b0c0-cd742d3bd2eb

2. Identifiez le domaine qui contient le périphérique. Dans la plupart des requêtes de l'API REST, le paramètre domain est obligatoire. Utilisez le jeton dans cette requête pour récupérer la liste des domaines :

<#root>

#

```
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
  "items":
  [
    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
      "name": "Global/LAB2",
      "type": "Domain",
      "uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
    },
    ...
  ],
  ...
}
```

3. Utilisez l'UUID de domaine pour interroger les enregistrements spécifiques des périphériques et l'UUID spécifique des périphériques :

<#root>

#

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

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

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

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

4. Utilisez l'UUID de domaine et l'UUID de périphérique/conteneur de l'étape 3 dans cette requête, et vérifiez la valeur de ftdMode :

<#root>

```
# curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000'  
...  
{  
  "accessPolicy": {  
    "id": "00505691-3a23-0ed3-0006-536940224514",  
    "name": "acp1",  
    "type": "AccessPolicy"  
  },  
  "advanced": {  
    "enableOGS": false  
  },  
  "description": "NOT SUPPORTED",  
  
  "ftdMode": "ROUTED",  
  
  ...  
}
```

Interface utilisateur FCM

Le mode pare-feu peut être vérifié pour FTD sur Firepower 4100/9300.

Procédez comme suit pour vérifier le mode de pare-feu FTD sur l'interface utilisateur FCM :

1. Modifiez le périphérique logique sur la page Périphériques logiques :

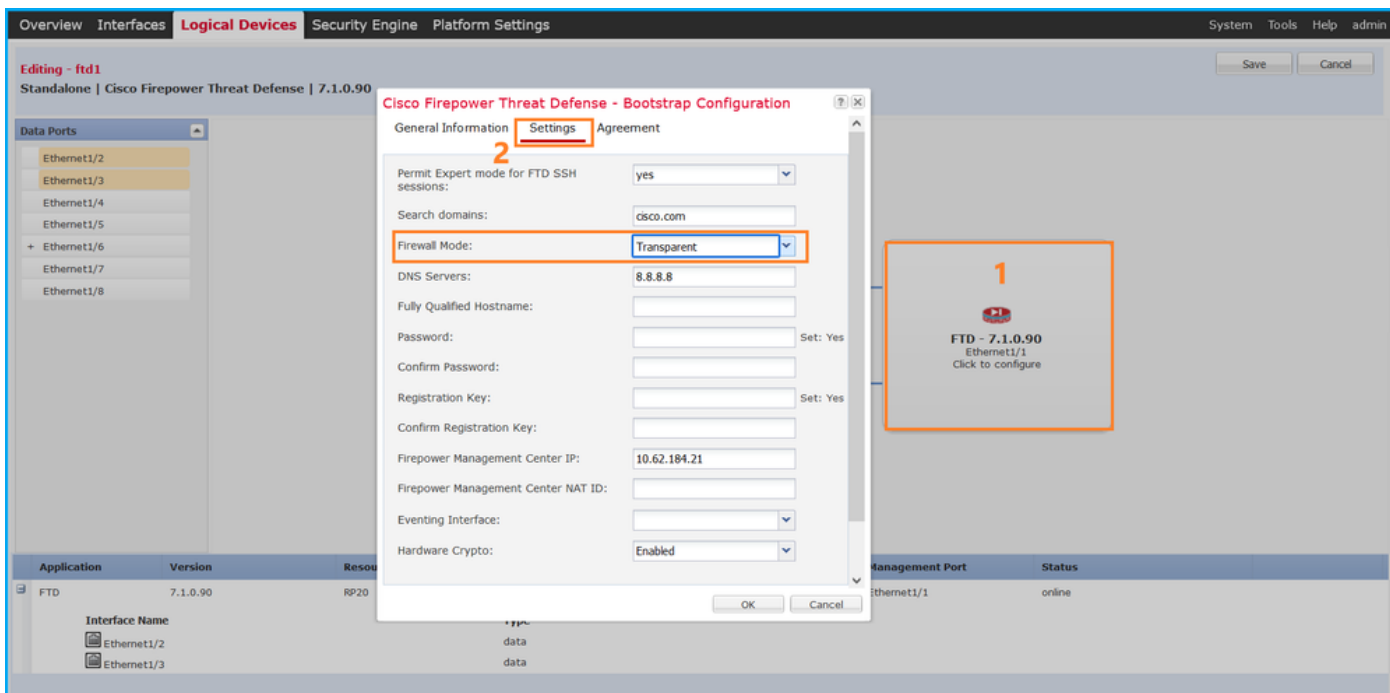
The screenshot shows the 'Logical Devices' page in the FCM interface. A red box highlights the 'Logical Devices' tab. A large orange '1' is placed above the page title. Below the title, there is a table with columns: Application, Version, Resource Profile, Management IP, Gateway, Management Port, and Status. The first row shows 'FTD' with version '7.1.0.90', resource profile 'RP20', management IP '10.62.148.89', gateway '10.62.148.1', management port 'Ethernet1/1', and status 'Online'. A red box highlights the 'Attributes' section for the selected device, which includes: Cluster Operational Status: not-applicable, FIREPOWER-MGMT-IP: 10.62.148.89, HA-LINK-INTF: Ethernet1/2, HA-LAN-INTF: Ethernet1/2, MGMT-URL: https://10.62.184.21/, HA-ROLE: active, and UUID: 796eb8f8-d83b-11ec-941d-b9083eb612d8. A red box with the number '2' highlights the 'Attributes' section.

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

Attributes

- Cluster Operational Status: not-applicable
- FIREPOWER-MGMT-IP: 10.62.148.89
- HA-LINK-INTF: Ethernet1/2
- HA-LAN-INTF: Ethernet1/2
- MGMT-URL: https://10.62.184.21/
- HA-ROLE: active
- UUID: 796eb8f8-d83b-11ec-941d-b9083eb612d8

2. Cliquez sur l'icône de l'application, et vérifiez le Mode pare-feu dans l'onglet Paramètres :



CLI FXOS

Le mode pare-feu peut être vérifié pour FTD sur Firepower 4100/9300.

Procédez comme suit pour vérifier le mode de pare-feu FTD sur l'interface de ligne de commande de FXOS :

1. Établissez une connexion de console ou SSH au châssis.
2. Basculez vers la portée ssa, puis basculez vers le périphérique logique spécifique, exécutez la commande `show mgmt-bootstrap expand` et vérifiez la valeur de l'attribut `FIREWALL_MODE` :

```
<#root>
```

```
firepower#
```

```
scope ssa
```

```
firepower /ssa #
```

```
scope logical-device ftd_cluster1
```

```
firepower /ssa/logical-device #
```

```
show mgmt-bootstrap expand
```

```
Management Configuration:
```

```
App Name: ftd
```

```
Secret Bootstrap Key:
```

```
Key Value
```

```
-----  
PASSWORD
```

REGISTRATION_KEY

IP v4:

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

Bootstrap Key:

Key	Value
DNS_SERVERS	192.0.2.250
FIREPOWER_MANAGER_IP	10.62.184.21

```
FIREWALL_MODE          routed
PERMIT_EXPERT_MODE     yes
SEARCH_DOMAINS         cisco.com
...
```

API REST FXOS

FXOS REST-API est pris en charge sur Firepower 4100/9300.

Procédez comme suit pour vérifier le mode de pare-feu FTD via la requête FXOS REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demander un jeton d'authentification :

```
<#root>
```

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

2. Utilisez l'identificateur de périphérique logique dans cette requête et vérifiez la valeur de la clé FIREWALL_MODE :

```
<#root>
```

```
# curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d' https://192.0.2.100/api/ld/ftd_cluster1
...
{
```

```

"key": "FIREWALL_MODE",
    "rn": "key-FIREWALL_MODE",
    "updateTimestamp": "2022-05-20T13:28:37.093",
    "urlLink": "https://192.0.2.100/api/1d/ftd_cluster1/mgmt-bootstrap/ftd/key/

"value": "routed"
    },
...

```

Fichier show-tech du châssis FXOS

Le mode pare-feu pour FTD peut être vérifié dans le fichier show-tech de Firepower 4100/9300.

Procédez comme suit pour vérifier le mode de pare-feu FTD dans le fichier show-tech du châssis FXOS :

1. Pour FXOS versions 2.7 et ultérieures, ouvrez le fichier sam_techsupportinfo dans <name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Pour les versions antérieures, ouvrez le fichier sam_techsupportinfo dans FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Vérifiez la section `show logical-device detail expand` sous l'identificateur spécifique et le logement :

```

<#root>

# 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

...

Mode pare-feu ASA

Le mode pare-feu ASA peut être vérifié à l'aide des options suivantes :

- CLI ASA
- ASA show-tech
- Interface utilisateur FCM
- CLI FXOS
- FXOS REST-API
- Fichier show-tech du châssis FXOS

CLI ASA

Procédez comme suit pour vérifier le mode pare-feu ASA sur l'interface de ligne de commande ASA :

1. Utilisez ces options pour accéder à l'interface de ligne de commande ASA en fonction de la plate-forme et du mode de déploiement :

- Accès Telnet/SSH direct à ASA sur Firepower 1000/3100 et Firepower 2100 en mode appliance
- Accès à partir de l'ILC de la console FXOS sur Firepower 2100 en mode plate-forme et connexion à ASA via la commande connect asa
- Accès depuis l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :

connectez le module <x> [console|telnet], où x est l'ID du logement, puis connectez asa

- Pour l'ASA virtuel, un accès SSH direct à l'ASA ou un accès console à partir de l'hyperviseur ou de l'interface utilisateur cloud

2. Exécutez la commande show firewall sur l'interface de ligne de commande :


```
<#root>
```

```
asa#
```

```
show firewall
```

```
Firewall mode: Routed
```

Fichier show-tech ASA

Afin de vérifier le mode pare-feu ASA, vérifiez la section show firewall :

```
<#root>
```

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

Interface utilisateur FCM

Suivez les étapes de la section.

CLI FXOS

Suivez les étapes de la section.

FXOS REST-API

Suivez les étapes de la section.

Fichier show-tech du châssis FXOS

Suivez les étapes de la section.

Vérifier le type de déploiement d'instance

Il existe 2 types de déploiement d'instance d'application :

- Instance native : une instance native utilise toutes les ressources (processeur, mémoire vive et espace disque) du module/moteur de sécurité. Vous ne pouvez donc installer qu'une seule instance native.
- Instance de conteneur - Une instance de conteneur utilise un sous-ensemble de ressources du module/moteur de sécurité. La fonctionnalité multi-instance est uniquement prise en charge pour le FTD géré par FMC ; elle n'est pas prise en charge pour l'ASA ou le FTD géré par FDM.

La configuration d'instance en mode conteneur est prise en charge uniquement pour FTD sur Firepower 4100/9300.

Le type de déploiement d'instance peut être vérifié à l'aide des options suivantes :

- CLI FTD
- FTD Show-tech
- Interface utilisateur FMC
- FMC REST-API
- Interface utilisateur FCM
- CLI FXOS
- FXOS REST-API
- Fichier show-tech du châssis FXOS

CLI FTD

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD sur l'interface de ligne de commande FTD :

1. Utilisez ces options pour accéder à l'interface de ligne de commande FTD en fonction de la plate-forme et du mode de déploiement :

- Accès SSH direct au FTD - toutes les plates-formes
- Accès à partir de l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :

connectez le module <x> [console|telnet], où x est l'ID de logement, puis connectez ftd [instance], où l'instance ne concerne que le déploiement multi-instance.

2. Exécutez la commande `show version system` et vérifiez la ligne avec la chaîne SSP Slot Number. Si le conteneur existe dans cette ligne, le FTD s'exécute dans un mode conteneur :

```
<#root>
```

```
>
```

```
show version system
```

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

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

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

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

SSP Slot Number: 1 (Container)

...

Fichier de dépannage FTD

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD dans le fichier de dépannage FTD :

1. Ouvrez le fichier de dépannage et accédez au dossier <nom du fichier>-troubleshoot.tar/results-<date>—xxxxxx/command-output.
2. Ouvrez le fichier usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output :

```
<#root>
```

```
# pwd
```

```
/ngfw/var/common/results-05-22-2022--102758/command-outputs
```

```
# cat 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'
```

3. Vérifiez la ligne avec la chaîne SSP Slot Number. Si le conteneur existe dans cette ligne, le FTD s'exécute dans un mode conteneur :

```
<#root>
```

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

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

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

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

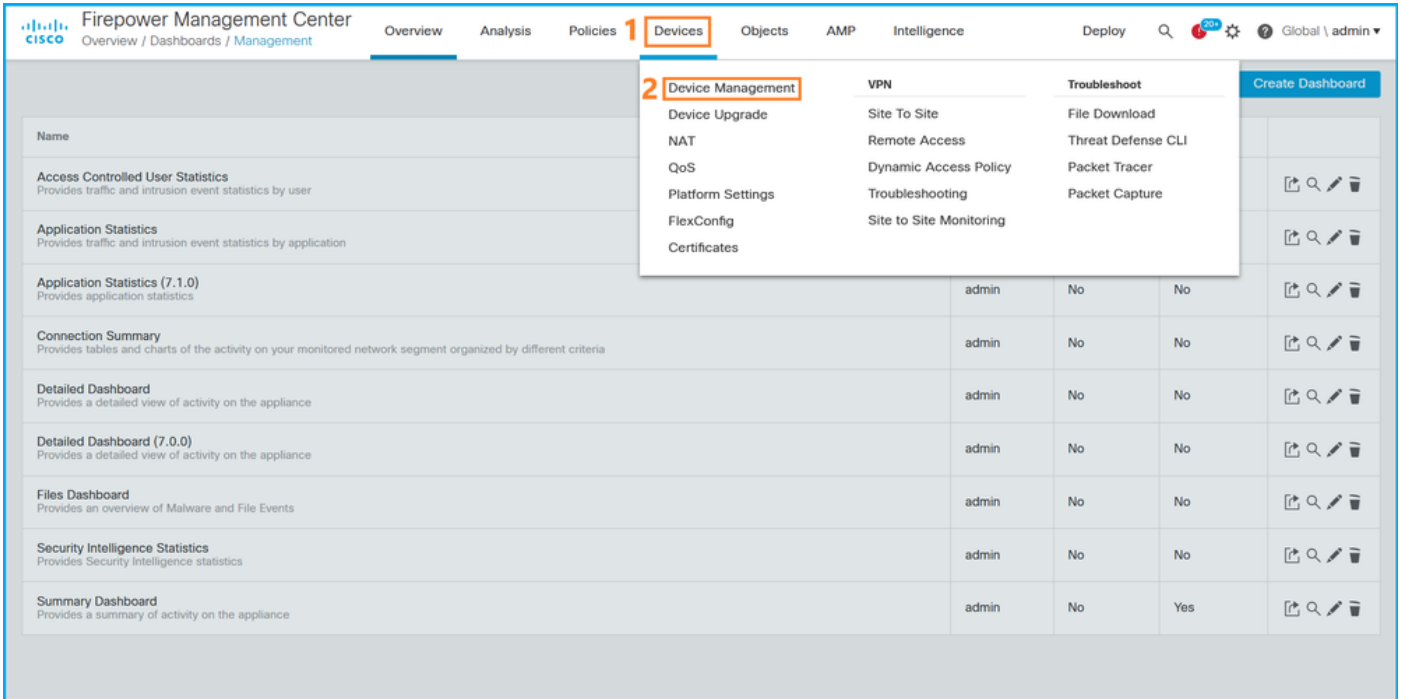
```
SSP Slot Number: 1 (Container)
```

...

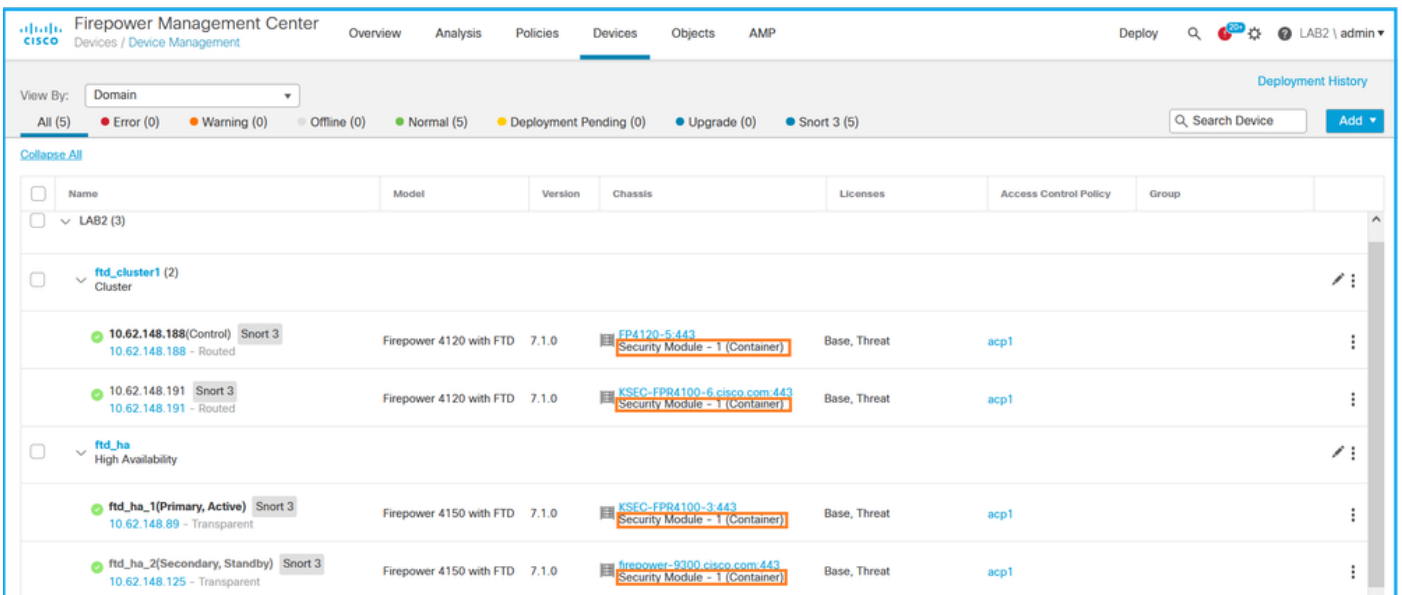
Interface utilisateur FMC

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD sur l'interface utilisateur FMC :

1. Choisissez Devices > Device Management :



2. Vérifiez la colonne Châssis. Si le conteneur existe dans la ligne, alors FTD s'exécute en mode conteneur.



FMC REST-API

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD via FMC REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demander un jeton d'authentification :

<#root>

```
# curl -s -k -v -X POST 'https://192.0.2.1/api/fmc_platform/v1/auth/generatetoken' -H 'Authentication: Basic YWVhbnQ6Ym9keS00'
```

< X-auth-access-token:

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

2. Identifiez le domaine qui contient le périphérique. Dans la plupart des requêtes de l'API REST, le paramètre domain est obligatoire. Utilisez le jeton dans cette requête pour récupérer la liste des domaines :

<#root>

```
#
```

```
curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_platform/v1/info/domain' -H 'accept: application/json'
```

```
{
  "items":
  [
    {
      "name": "Global",
      "type": "Domain",
      "uuid": "e276abec-e0f2-11e3-8169-6d9ed49b625f"
    },
    {
```

```
"name": "Global/LAB2",
```

```
"type": "Domain",
```

```
"uuid": "84cc4afe-02bc-b80a-4b09-000000000000"
```

```
},
```

```
...
```

3. Utilisez l'UUID de domaine pour interroger les enregistrements spécifiques des périphériques et l'UUID spécifique des périphériques :

<#root>

```
#
```

```

curl -s -k -X 'GET' 'https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000/d
{
  "items": [
    {
      "id": "796eb8f8-d83b-11ec-941d-b9083eb612d8"
    },
    {
      "links": {
        "self": "https://192.0.2.1/api/fmc_config/v1/domain/84cc4afe-02bc-b80a-4b09-000000000000
      },
      "name": "ftd_ha_1",
      "type": "Device"
    },
    ...
  ]
}

```

4. Utilisez l'UUID de domaine et l'UUID de périphérique/conteneur de l'étape 3 dans cette requête et vérifiez la valeur de isMultiInstance :

<#root>

```

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

"name": "ftd_cluster1"
,
  "isMultiInstance": true,
...

```

Interface utilisateur FCM

Afin de vérifier le type de déploiement de l'instance FTD, vérifiez la valeur de l'attribut Profil de ressource dans Périphériques logiques. Si la valeur n'est pas vide, le FTD s'exécute en mode conteneur :

The screenshot shows the 'Logical Devices' section of the FCM interface. At the top, there are navigation tabs: Overview, Interfaces, Logical Devices (selected), Security Engine, and Platform Settings. Below the tabs, there's a 'Logical Device List' section with a sub-header '(1 Container Instance) 57% (26 of 46) Cores Available'. A table lists the logical devices. The first entry is 'ftd_cluster1', which is 'Clustered' and has a 'Status: ok'. Below this, a detailed table shows the configuration for the 'FTD' application:

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

CLI FXOS

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD sur l'interface de ligne de commande FXOS :

1. Établissez une connexion de console ou SSH au châssis.
2. Passez à la portée ssa et exécutez la commande show app-instance , puis vérifiez la colonne Deploy Type du FTD spécifique en fonction du slot et de l'identificateur :

```
<#root>
```

```
firepower #
```

```
scope ssa
```

```
firepower /ssa #
```

```
show app-instance
```

App Name	Identifiant	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

Procédez comme suit pour vérifier le type de déploiement de l'instance FTD via une demande FXOS REST-API. Utilisez un client REST-API. Dans cet exemple, curl est utilisé :

1. Demander un jeton d'authentification :

```
<#root>
```

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

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

```
3dba916cdfb850c204b306a138cde9659ba997da4453cdc0c37ffb888816c94d
```

```
"  
}
```

2. Spécifiez le jeton, l'ID d'emplacement dans cette requête et vérifiez la valeur de deployType :

```
<#root>
```

```
#
```

```
curl -s -k -X GET -H 'Accept: application/json' -H 'token: 3dba916cdfb850c204b306a138cde9659ba997da4453c
```

```
...  
{
```

```
  "smAppInstance": [  
    {
```

```
      "adminState": "enabled",  
      "appDn": "sec-svc/app-ftd-7.1.0.90",  
      "appInstId": "ftd_001_JAD201200R43VLP1G3",  
      "appName": "ftd",  
      "clearLogData": "available",  
      "clusterOperationalState": "not-applicable",  
      "clusterRole": "none",  
      "currentJobProgress": "100",  
      "currentJobState": "succeeded",  
      "currentJobType": "start",  
  
      "deployType": "container",
```

```
...  
}
```

Fichier show-tech du châssis FXOS

Procédez comme suit pour vérifier le mode de pare-feu FTD dans le fichier show-tech du châssis FXOS :

1. Pour FXOS versions 2.7 et ultérieures, ouvrez le fichier sam_techsupportinfo dans <name>_BC1_all.tar/ FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar

Pour les versions antérieures, ouvrez le fichier sam_techsupportinfo dans FPRM_A_TechSupport.tar.gz/ FPRM_A_TechSupport.tar.

2. Vérifiez la section `show slot expand detail` pour le logement spécifique et l'identificateur :

```
<#root>
```

```
# pwd
```

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



```
# cat sam_techsupportinfo
...
~show slot expand detail~
```

Slot:

slot ID: 1

```
Log Level: Info
Admin State: Ok
Oper State: Online
Disk Format State: Ok
Disk Format Status: 100%
Clear Log Data: Available
Error Msg:
```

```
Application Instance:
  App Name: ftd
```

Identifiant: ftd_cluster1

```
Admin State: Enabled
Oper State: Online
Running Version: 7.1.0.90
Startup Version: 7.1.0.90
```

Deploy Type: Container

Vérifier le mode de contexte ASA

ASA prend en charge les modes à contexte unique et à contexte multiple. FTD ne prend pas en charge le mode multicontexte.

Le type de contexte peut être vérifié à l'aide des options suivantes :

- CLI ASA
- ASA show-tech

CLI ASA

Procédez comme suit pour vérifier le mode de contexte ASA sur l'interface de ligne de commande ASA :

1. Utilisez ces options pour accéder à l'interface de ligne de commande ASA en fonction de la plate-forme et du mode de déploiement :
 - Accès Telnet/SSH direct à ASA sur Firepower 1000/3100 et Firepower 2100 en mode appliance
 - Accès à partir de l'ILC de la console FXOS sur Firepower 2100 en mode plate-forme et connexion à ASA via la commande connect asa

- Accès depuis l'interface de ligne de commande FXOS via des commandes (Firepower 4100/9300) :
connectez le module <x> [console|telnet], où x est l'ID du logement, puis connectez asa
- Pour l'ASA virtuel, un accès SSH direct à l'ASA ou un accès console à partir de l'hyperviseur ou de l'interface utilisateur cloud

2. Exécutez la commande show mode sur l'interface de ligne de commande :

```
<#root>
```

```
ASA#
```

```
show mode
```

```
Security context mode:
```

```
multiple
```

```
ASA#
```

```
show mode
```

```
Security context mode:
```

```
single
```

Fichier show-tech ASA

Procédez comme suit pour vérifier le mode de contexte ASA dans le fichier show-tech ASA :

1. Vérifiez la section show context detail dans le fichier show-tech. Dans ce cas, le mode de contexte est multiple puisqu'il y a plusieurs contextes :

```
<#root>
```

```
----- show context detail -----
```

```
Context "system"
```

```
, is a system resource
```

```
Config URL: startup-config
```

```
Real Interfaces:
```

```
Mapped Interfaces: Ethernet1/1, Ethernet1/10, Ethernet1/11,  
Ethernet1/12, Ethernet1/13, Ethernet1/14, Ethernet1/15,  
Ethernet1/16, Ethernet1/2, Ethernet1/3, Ethernet1/4, Ethernet1/5,  
Ethernet1/6, Ethernet1/7, Ethernet1/8, Ethernet1/9, Ethernet2/1,  
Ethernet2/2, Ethernet2/3, Ethernet2/4, Ethernet2/5, Ethernet2/6,  
Ethernet2/7, Ethernet2/8, Internal-Data0/1, Internal-Data1/1,
```

```
Management1/1
Class: default, Flags: 0x00000819, ID: 0

Context "admin"
, has been created
Config URL: disk0:/admin.cfg
Real Interfaces: Ethernet1/1, Ethernet1/2, Management1/1
Mapped Interfaces: Ethernet1/1, Ethernet1/2, Management1/1
Real IPS Sensors:
Mapped IPS Sensors:
Class: default, Flags: 0x00000813, ID: 1

Context "null", is a system resource
Config URL: ... null ...
Real Interfaces:
Mapped Interfaces:
Real IPS Sensors:
Mapped IPS Sensors:
Class: default, Flags: 0x00000809, ID: 507
```

Vérification du mode Firepower 2100 avec ASA

Firepower 2100 avec ASA peut fonctionner dans l'un des modes suivants :

- Mode plate-forme : les paramètres de fonctionnement de base et les paramètres de l'interface matérielle sont configurés dans FXOS. Ces paramètres incluent la modification de l'état admin des interfaces, la configuration EtherChannel, NTP, la gestion des images, etc. L'interface Web FCM ou l'interface de ligne de commande FXOS peuvent être utilisées pour la configuration FXOS.
- Mode appliance (par défaut) : ce mode permet aux utilisateurs de configurer toutes les stratégies dans l'ASA. Seules les commandes avancées sont disponibles dans l'interface de ligne de commande FXOS.

Le mode Firepower 2100 avec ASA peut être vérifié à l'aide des options suivantes :

- CLI ASA
- CLI FXOS
- show-tech FXOS

CLI ASA

Procédez comme suit pour vérifier le mode Firepower 2100 avec ASA sur l'interface de ligne de commande ASA :

1. Utilisez telnet/SSH pour accéder à l'ASA sur Firepower 2100.
2. Exécutez la commande show fxos mode sur l'interface de ligne de commande :

<#root>

```
ciscoasa(config)#
```

```
show fxos mode
```

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


Mode appareil :

```
<#root>
```

```
ciscoasa(config)#
```

```
show fxos mode
```

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

 Remarque : en mode multicontexte, la commande show fxos mode est disponible dans le système ou le contexte admin.

CLI FXOS

Procédez comme suit pour vérifier le mode Firepower 2100 avec ASA sur l'interface de ligne de commande FXOS :

1. Utilisez telnet/SSH pour accéder à l'ASA sur Firepower 2100.
2. Exécutez la commande connect fxos :

```
<#root>
```

```
ciscoasa/admin(config)#
```

```
connect fxos
```

```
Configuring session.
```

```
.  
Connecting to FXOS.
```

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

 Remarque : en mode multicontexte, la commande connect fxos est disponible dans le contexte admin.

3. Exécutez la commande show fxos-mode :

```
<#root>
```

```
firepower-2140#
```

```
show fxos mode
```

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

Mode appareil :

```
<#root>
```

```
firepower-2140#
```

```
show fxos mode
```

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

Fichier show-tech FXOS

Procédez comme suit pour vérifier le mode Firepower 2100 avec ASA dans le fichier show-tech du châssis FXOS :

1. Ouvrez le fichier tech_support_brief dans <name>_FPRM.tar.gz/<name>_FPRM.tar
2. Consultez la section `show fxos-mode` :

```
<#root>
```

```
# pwd
```

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

```
# cat tech_support_brief
```

```
...
```

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

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

Mode appareil :

```
<#root>
```

```
# pwd
```

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

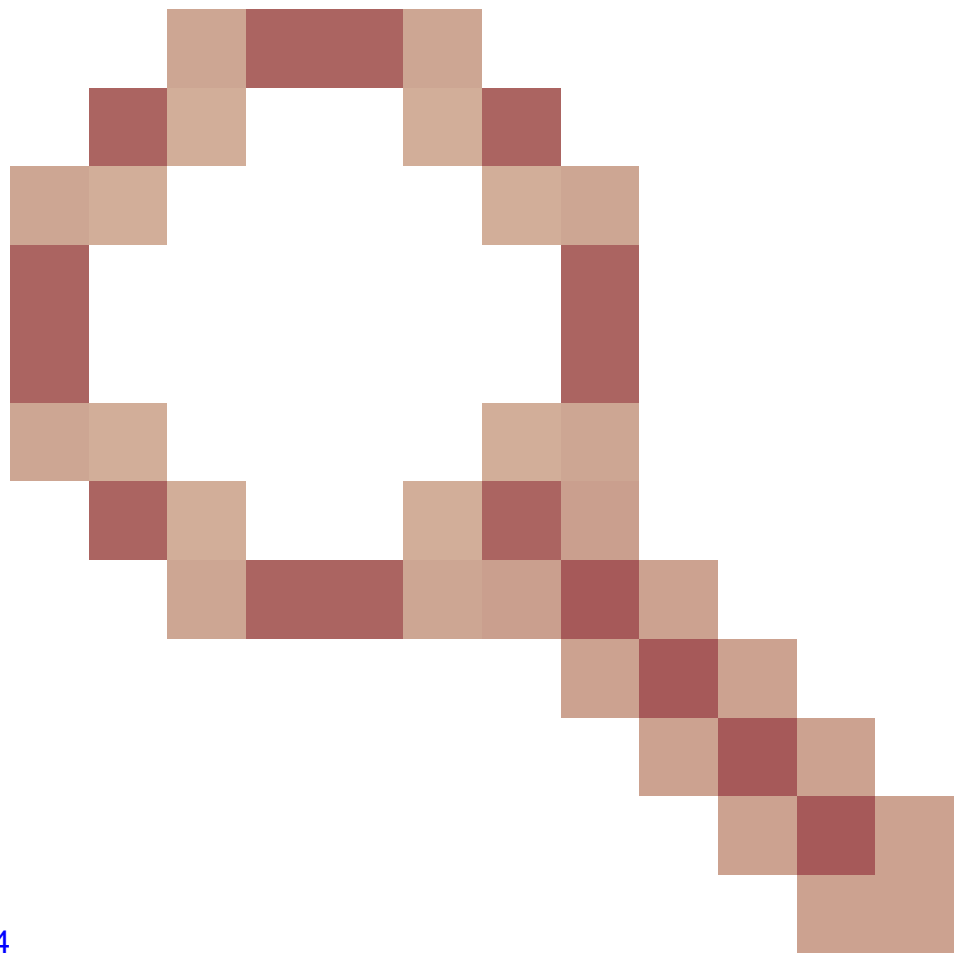
```
# cat tech_support_brief
```

```
...
```

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

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

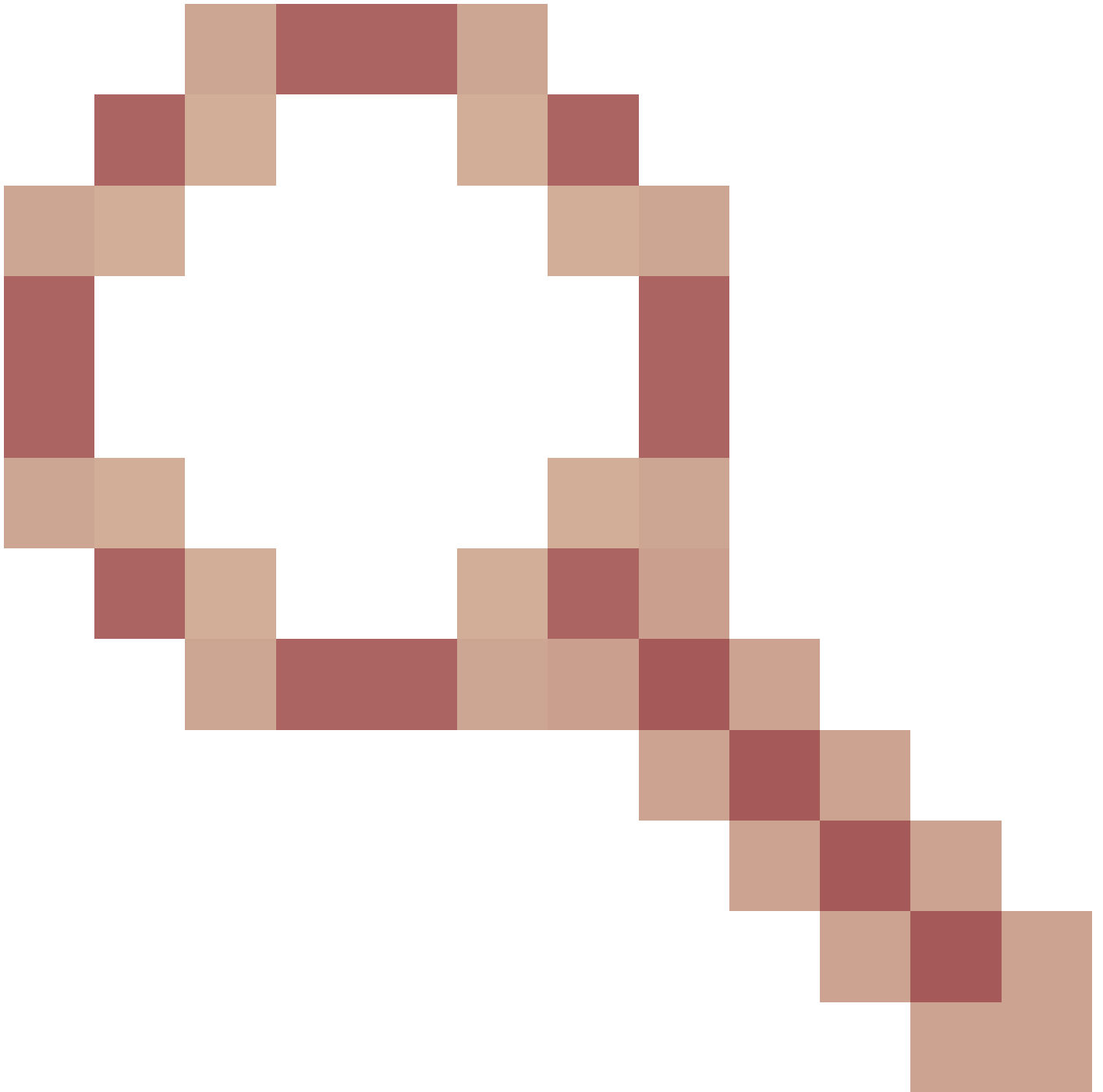
Problèmes identifiés



ID de bogue Cisco [CSCwb9424](#)

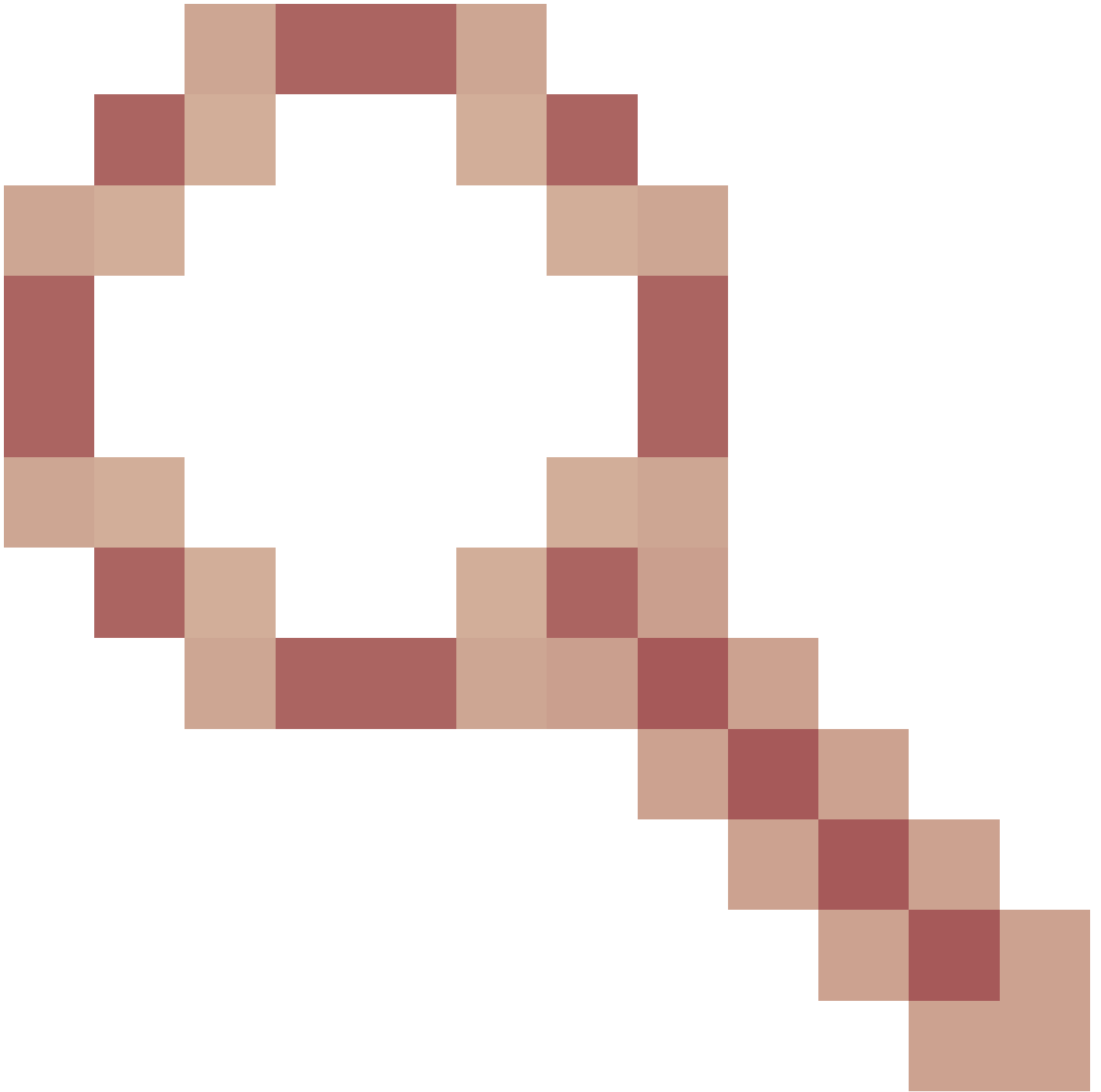
ENH : ajouter une commande CLISH pour la vérification de la configuration FMC HA

ID de bogue Cisco [CSCvn31622](#)



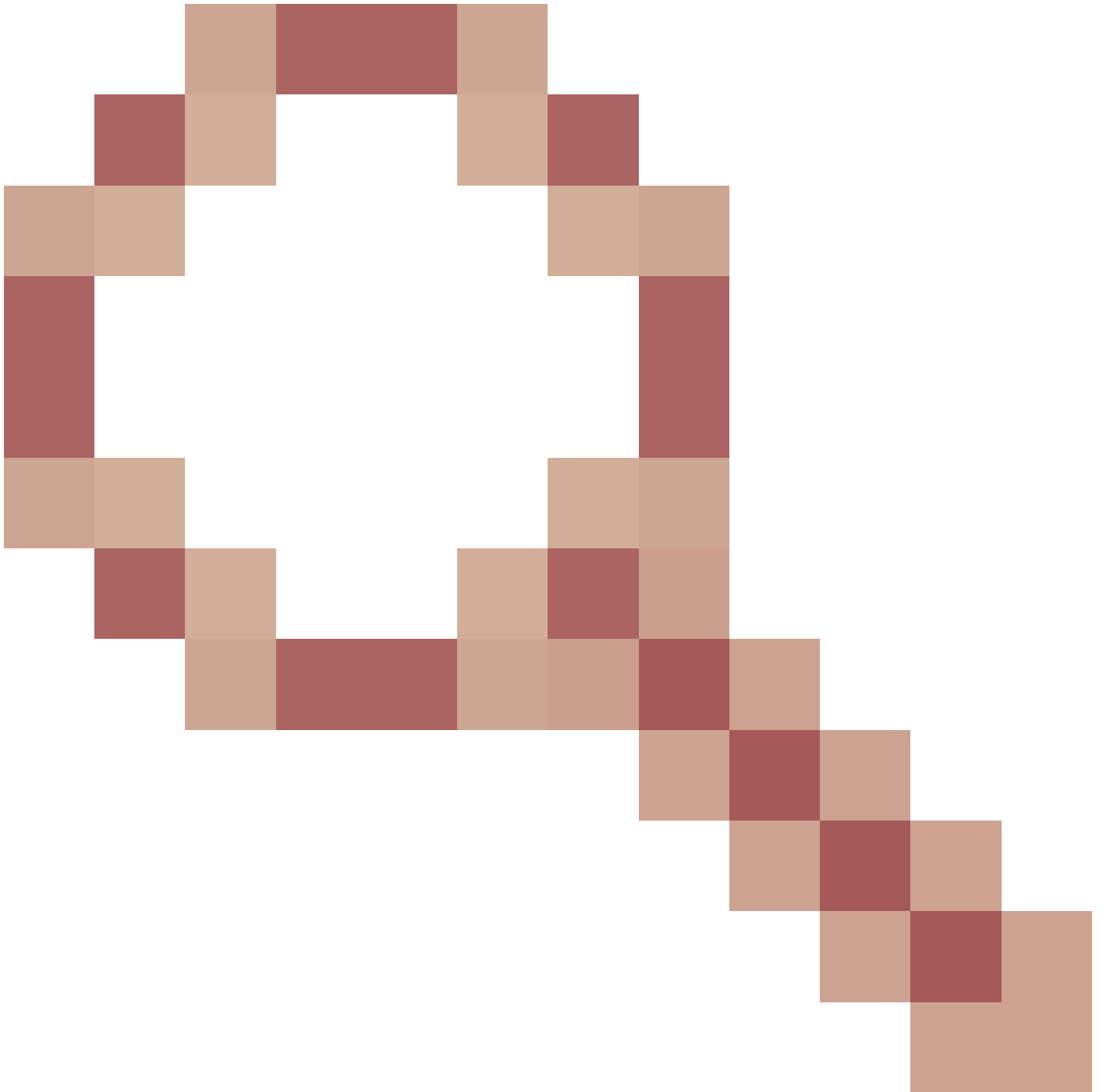
ENH : ajout d'OID SNMP FXOS pour interroger la configuration des périphériques logiques et des instances d'applications

ID de bogue Cisco [CSCwb97767](https://www.cisco.com/cisco/webbugtool/show_bug.do?bugID=CSCwb97767)



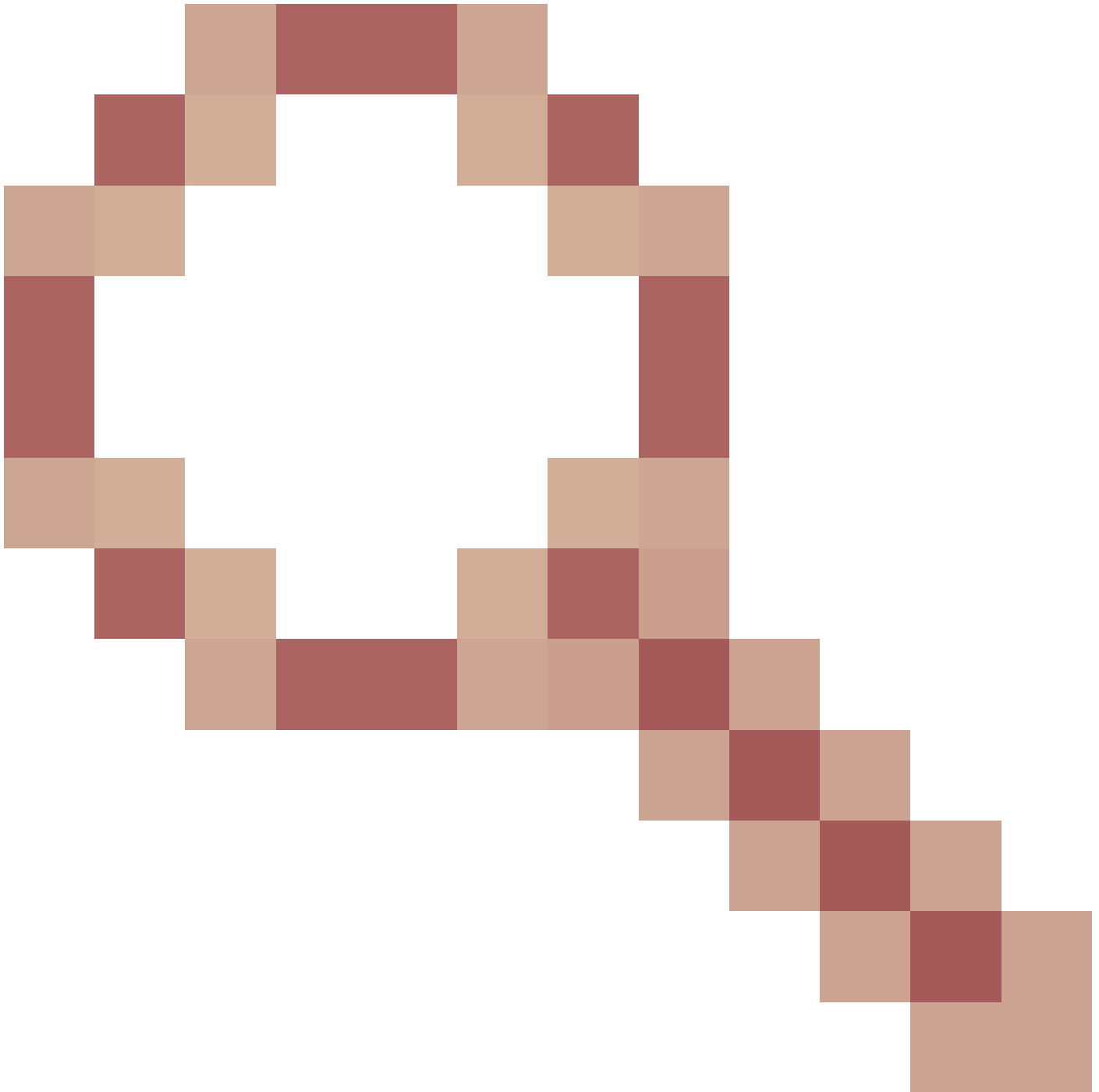
ENH : ajouter un OID pour la vérification du type de déploiement d'instance FTD

ID de bogue Cisco [CSCwb9772](#)



ENH : inclure la sortie de « show fxos mode » dans show-tech de l'ASA sur Firepower 2100

L'ID de bogue Cisco [CSCwb97751](https://tools.cisco.com/bugcenter/bug/?bugID=CSCwb97751)



OID 1.3.6.1.4.1.9.9.491.1.6.1.1 pour la vérification du mode pare-feu transparent n'est pas disponible

Informations connexes

- [Guide de démarrage rapide de l'API REST de Secure Firewall Management Center, version 7.1](#)
- [Configuration du protocole SNMP sur les pare-feu de nouvelle génération Firepower](#)
- [Guide de l'API REST de Cisco Firepower Threat Defense](#)
- [Référence API REST Cisco FXOS](#)
- [Compatibilité Cisco ASA](#)
- [Versions de l'offre groupée ASA et FXOS Firepower 100/2100 et Secure Firewall 3100](#)
- [Composants groupés](#)

- [Firepower Dépanner Les Procédures De Génération De Fichiers](#)
- [Guide de démarrage de Cisco Firepower 2100](#)
- [Guide de compatibilité de Cisco Firepower Threat Defense](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.