Probleemoplossing voor VCC - HA

Inhoud

Inleiding

In dit document wordt beschreven hoe u veelvoorkomende synchronisatieproblemen kunt oplossen in een High Availability (HA)-instelling voor Firepower Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de volgende onderwerpen:

- FMC - HA-configuratievereisten
- Basiskennis van Linux shell.

Gebruikte componenten

- FMCv voor VMware op versie 7.2.8.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De eerste configuratie van het voor dit document gebruikte laboratorium voldoet aan de eisen voor

de basisconfiguratie van de FMC-HA.

- Twee VCC's met dezelfde capaciteit of hardwareversie.
- Twee FMC's met dezelfde softwareversie, Inbraakregelupdate, Vulnerability Database en Lichtgewicht security pakket.
- twee VCC's met de bijbehorende vergunningen.

Voordat u begint

- Zorg ervoor dat de beheerder toegang heeft tot beide VCC's.
- Zorg ervoor dat de beheerder toegang heeft tot de FTD-apparaten die door het VCC worden beheerd.

Opdrachten voor probleemoplossing

Opdrachten voor FMC-probleemoplossing.

 Om de verbinding tussen FMC-apparaten te valideren, kan de gebruiker deze opdrachten uitvoeren.

<#root>

```
> expert

admin@firepower:~$
sudo su


root@firepower:/Volume/home/admin#
ping xx.xx.18.102


PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.533 ms
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.563 ms
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.431 ms
^C
--- xx.xx.18.102 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 59ms
rtt min/avg/max/mdev = 0.431/0.509/0.563/0.056 ms

root@firepower:/Volume/home/admin#
netstat -an | grep 8305


tcp 0 0 xx.xx.18.101:8305 0.0.0.0:* LISTEN
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.253:48759 ESTABLISHED
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:53875 ESTABLISHED
tcp 0 0 xx.xx.18.101:8305 xx.xx.18.254:49205 ESTABLISHED
tcp 0 0 xx.xx.18.101:60871 xx.xx.18.253:8305 ESTABLISHE
```
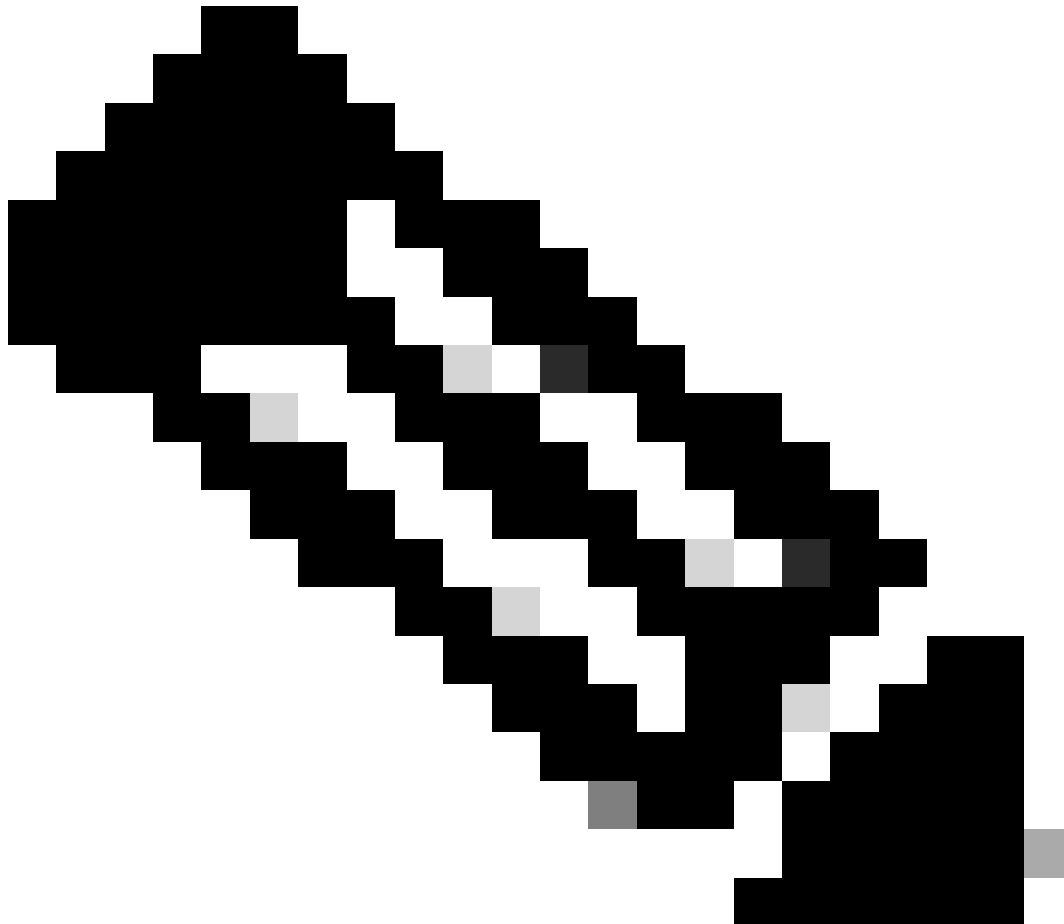
ping <peer-ip-adres> Deze opdracht kan worden gebruikt om de bereikbaarheid tussen beide apparaten te controleren.

netstat -an | grep 8305 Deze opdracht geeft de met poort 8305 verbonden apparaten weer.

> Opmerking: de poort 8305 is de standaardpoort die op de FirePOWER-apparaten is geconfigureerd om het communicatiekanaal met het VCC te creëren.

Om de FMC-HA setup configuratie te valideren, kan de gebruiker ook het script troubleshoot_HADC.pl. Dit is met name nuttig in deze scenario's:

- Wanneer de FMC-HA integratiestatus verslechtert.
- Indien de toegang tot de grafische gebruikersinterface (GUI) van het VCC ontbreekt, maar de toegang van het VCC-CLI nog werkt en toegankelijk is.

<#root>

```
> expert


admin@firepower:~$

sudo su


root@firepower:/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 Get Remote Stale Sync AQ Info
14 Help
0 Exit


**************************************************************
Enter choice:
```

Opdrachten voor FTD-probleemoplossing

Probleemoplossing voor de connectiviteit van de FTD naar de FMC-HA stelt de gebruiker in staat om de connectiviteit te valideren van apparaten die moeten worden geregistreerd op zowel de FMC's als bij een verslechterde HA, en geeft de waarschuwing "Degraded - Synchronization incomplete (This Management Center heeft minder apparaten geregistreerd)" weer.

 Op FTD-niveau kan de gebruiker deze opdrachten uitvoeren om de communicatie met het FMC te valideren.

<#root>

>

ping system xx.xx.18.102


```
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.595 ms
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.683 ms
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.642 ms
64 bytes from xx.xx.18.102: icmp_seq=4 ttl=64 time=24.4 ms
64 bytes from xx.xx.18.102: icmp_seq=5 ttl=64 time=11.4 ms
```

```
^C
--- xx.xx.18.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 128ms
rtt min/avg/max/mdev = 0.595/7.545/24.373/9.395 ms


> show managers


Type : Manager
Host : xx.xx..18.101
Display name : xx.xx..18.101
Version : 7.2.8 (Build 25)
Identifier : fc3e3572-xxxx-xxxx-xxxx-39e0098c166c
Registration : Completed
Management type : Configuration and analytics

Type : Manager
Host : xx.xx..18.102
Display name : xx.xx..18.102
Version : 7.2.8 (Build 25)
Identifier : bb333216-xxxx-xxxx-xxxx-c68c0c388b44
Registration : Completed
Management type : Configuration and analytics



> sftunnel-status


SFTUNNEL Start Time: Mon Oct 14 21:29:16 2024

Both IPv4 and IPv6 connectivity is supported
Broadcast count = 5
Reserved SSL connections: 0
Management Interfaces: 2
eth0 (control events) xx.xx..18.254,
tap_nlp (control events) 169.254.1.2,fd00:0:0:1::2

***********************

**RUN STATUS****xx.xx..18.102**************
Key File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-key.pem
Cert File = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-cert.pem
CA Cert = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/cacert.pem
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.102' Start Time: Tue Oct 15 00:38:43 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.102' via Primary ip/host 'xx.xx..18.102'

PEER INFO:
sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.102,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.102' via 'xx.xx..18

***********************
```

```
**RUN STATUS****xx.xx..18.101*************
Key File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-key.pem
Cert File = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-cert.pem
CA Cert = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/cacert.pem
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelA Connected: Yes, Interface eth0
Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
ChannelB Connected: Yes, Interface eth0
Registration: Completed.
IPv4 Connection to peer 'xx.xx..18.101' Start Time: Mon Oct 14 21:29:15 2024 UTC
IPv4 Last outbound connection to peer 'xx.xx..18.101' via Primary ip/host 'xx.xx..18.101'

PEER INFO:

sw_version 7.2.8
sw_build 25
Using light registration
Management Interfaces: 1
eth0 (control events) xx.xx..18.101,
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to 'xx.xx..18.101' via 'xx.xx..18

***********************
**RPC STATUS****xx.xx..18.102*************
'uuid' => 'bb333216-xxxx-xxxx-xxxx-c68c0c388b44',
'uuid_gw' => '',
'last_changed' => 'Wed Oct 9 07:00:11 2024',
'active' => 1,
'name' => 'xx.xx..18.102',
'ip' => 'xx.xx..18.102',
'ipv6' => 'IPv6 is not configured for management'

**RPC STATUS****xx.xx..18.101*************
'uuid_gw' => '',
'uuid' => 'fc3e3572-xxxx-xxxx-xxxx-39e0098c166c',
'last_changed' => 'Mon Jun 10 18:59:54 2024',
'active' => 1,
'ip' => 'xx.xx..18.101',
'ipv6' => 'IPv6 is not configured for management',
'name' => 'xx.xx..18.101'

Check routes:
No peers to check
```

ping-systeem <fmc-IP> Volg de FTD-beheerinterface om een ICMP te genereren.

show managers Dit commando geeft de informatie van de managers waar het apparaat is geregistreerd.

sftunnel-status Deze opdracht valideert het communicatiekanaal dat tussen de apparaten is ingesteld. Dit kanaal krijgt de naam sftunnel.

De opdrachten voor het controleren van de connectiviteit op het basisniveau van het FTD zijn dezelfde als het FMC. Het FTD bevat geen script dat de communicatie met het FMC kan valideren, maar het is mogelijk de tijdens het registratieproces verkregen informatie te controleren

in het /ngfw/var/log/action.log.

Verificatie

Voor de volgende topologie kan de communicatie tussen de FMC-HA peers en de FTD01 gevalideerd worden met behulp van de eerder beschreven opdrachten.

FMC - Active

FMC - Standby

xx.xx.18.101

xx.xx.18.102

FTD01

FTD02

xx.xx.18.253

xx.xx.18.254
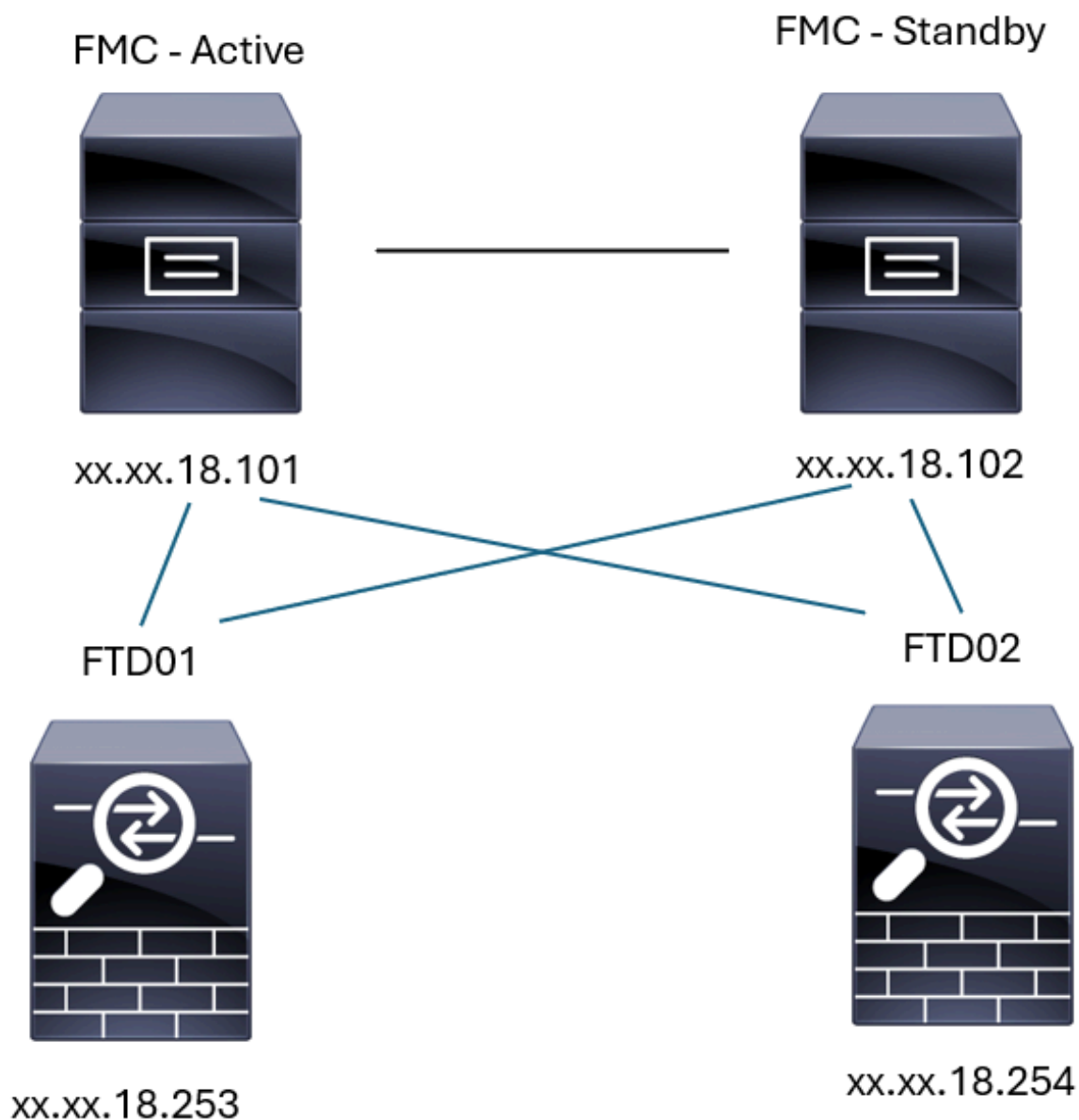
FMC-HA-topologie

FMC - HA-validering

Voor deze validatie kunnen de basisrichtlijnen voor het instellen van een FMC-HA ook worden gevalideerd met behulp van de opdrachtshow versie.

<#root>

FMC Active


```
>

show version


------------------[ firepower ]-------------------
Model                   : Secure Firewall Management Center for VMware (66) Version 7.2.8 (Build 25)
UUID                    : fc3e3572-xxxx-xxxx-xxxx-39e0098c166c
Rules update version    : 2023-11-29-001-vrt
LSP version             : lsp-rel-20231129-1200
VDB version             : 395
---------------------------------------------------

> expert


admin@firepower:~$

sudo su



root@firepower:/Volume/home/admin#

ping xx.xx.18.102


PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=0.433 ms
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.606 ms
64 bytes from xx.xx.18.102: icmp_seq=4 ttl=64 time=0.480 ms
64 bytes from xx.xx.18.102: icmp_seq=5 ttl=64 time=0.524 ms
^C
--- xx.xx.18.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 84ms
rtt min/avg/max/mdev = 0.385/0.485/0.606/0.079 ms

root@firepower:/Volume/home/admin#

netstat -an | grep 8305


tcp        0        0 xx.xx.18.101:8305      xx.xx.18.254:53875      ESTABLISHED
tcp        0        0 xx.xx.18.101:8305      xx.xx.18.102:38239      ESTABLISHED ------ communication es
tcp        0        0 xx.xx.18.101:8305      xx.xx.18.254:49205      ESTABLISHED
tcp        0        0 xx.xx.18.101:8305      xx.xx.18.253:34865      ESTABLISHED
tcp        0        0 xx.xx.18.101:60871     xx.xx.18.253:8305       ESTABLISHED
tcp        0        0 xx.xx.18.101:8305      xx.xx.18.102:42253      ESTABLISHED ------ communication es

root@firepower:/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   Get Remote Stale Sync AQ Info
 14   Help
  0   Exit
**************************************************************
Enter choice: 1

HA Enabled: Yes
This FMC Role In HA: Active - Primary
Status out put: vmsDbEngine (system,gui) - Running 5093
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


****************  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   Get Remote Stale Sync AQ Info
 14   Help
  0   Exit
**************************************************************
Enter choice: 4
Peer UUID [Enter 'Return' For HA Peer(no UUID required)]:

Peer Is Connected
$VAR1 = {
          'vip' => '',
          'model_id' => 'E',
          'ip' => 'xx.xx.18.102',
          'persistent' => 0,
          'sw_version' => '7.2.8',
          'last_changed' => 1728457211,
          'active' => 1,
          'uuid' => 'bb333216-xxxx-xxxx-xxxx-c68c0c388b44',
          'upgrade_version' => '',
          'reg_state' => 0,
          'model_number' => '66',
          'primary_mgr' => 0,
          'name' => 'xx.xx.18.102',
          'uuid_gw' => '',
          'ipv6' => undef,
          'vip_local' => '',
          'priority' => 0,
          'reg_key' => '',
```

```
            'vnet' => undef,
            'role' => 0,
            'mgmt_mac_address' => '00:50:56:B3:D1:07'
          };

*************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
***************************************************************
Enter choice: 8

------------------------- Last periodic sync time details -----------------------------------

Last successful sync completed at: Wed Oct 16 16:44:23 2024 UTC
Current time: Wed Oct 16 16:46:34 2024 UTC
Last successful sync completed '2 minutes 11 seconds' ago.

------------------------- Last periodic sync time details end -------------------------------

*************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
***************************************************************
Enter choice: 9

SYNC_ACTIVE: 1 at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 494, <STDIN> line 5.
Sybase state :  at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 701.
Sybase state :  at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 801.
Sync status : at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 802.
------------------------- FMC HA status messages start -------------------------------

Status: Healthy

------------------------- FMC HA status messages end -------------------------------
*************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
****************************************************************
Enter choice: 10

Fetching standby missing device information...
Devices are in sync.

*************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
****************************************************************
Enter choice: 0
Thank you
```

<#root>

FMC Standby

```
>
```

show version

```
-------------------[ firepower ]-------------------
Model                    : Secure Firewall Management Center for VMware (66) Version 7.2.8 (Build 25)
UUID                     : bb333216-xxxx-xxxx-xxxx-c68c0c388b44
Rules update version     : 2023-11-29-001-vrt
LSP version              : lsp-rel-20231129-1200
VDB version              : 395
---------------------------------------------------
```

> expert

```
admin@firepower:~$

sudo su


root@firepower:/Volume/home/admin#

ping xx.xx.18.101


PING xx.xx.18.101 (xx.xx.18.101) 56(84) bytes of data.
64 bytes from xx.xx.18.101: icmp_seq=1 ttl=64 time=0.402 ms
64 bytes from xx.xx.18.101: icmp_seq=2 ttl=64 time=0.482 ms
64 bytes from xx.xx.18.101: icmp_seq=3 ttl=64 time=0.452 ms
64 bytes from xx.xx.18.101: icmp_seq=4 ttl=64 time=0.490 ms
64 bytes from xx.xx.18.101: icmp_seq=5 ttl=64 time=0.519 ms
^C
--- xx.xx.18.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 123ms
rtt min/avg/max/mdev = 0.402/0.469/0.519/0.039 ms

root@firepower:/Volume/home/admin#

netstat -an | grep 8305


tcp        0        0 xx.xx.18.102:8305        xx.xx.18.254:50373        ESTABLISHED
tcp        0        0 xx.xx.18.102:8305        xx.xx.18.253:42083        ESTABLISHED
tcp        0        0 xx.xx.18.102:59439        xx.xx.18.254:8305        ESTABLISHED
tcp        0        0 xx.xx.18.102:36751        xx.xx.18.253:8305        ESTABLISHED
tcp        0        0 xx.xx.18.102:38239        xx.xx.18.101:8305        ESTABLISHED ------ communication es
tcp        0        0 xx.xx.18.102:42253        xx.xx.18.101:8305        ESTABLISHED ------ communication es

root@firepower:/Volume/home/admin#

root@firepower:/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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
****************************************************************
Enter choice: 1

HA Enabled: Yes
This FMC Role In HA: Standby - Secondary
Status out put: vmsDbEngine (system,gui) - Running 29652
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_secondary
Sybase Role: Standby

**************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
******************************************************************
Enter choice: 4
Peer UUID [Enter 'Return' For HA Peer(no UUID required)]:

Peer Is Connected
$VAR1 = {
          'vnet' => undef,
          'upgrade_version' => '',
          'uuid_gw' => '',
          'name' => 'xx.xx.18.101',
          'primary_mgr' => 1,
          'sw_version' => '7.2.8',
          'persistent' => 0,
          'model_number' => '66',
          'last_changed' => 1718045994,
          'reg_key' => '',
          'active' => 1,
          'reg_state' => 0,
          'model_id' => 'E',
          'vip' => '',
          'mgmt_mac_address' => '00:50:56:B3:E1:57',
          'vip_local' => '',
          'ip' => 'xx.xx.18.101',
          'priority' => 0,
          'uuid' => 'fc3e3572-xxxx-xxxx-xxxx-39e0098c166c',
          'role' => 0,
          'ipv6' => undef
        };

**************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
**************************************************************
Enter choice: 8

------------------------- Last periodic sync time details ---------------------------------

Last successful sync completed at: Wed Oct 16 16:46:06 2024 UTC
Current time: Wed Oct 16 16:47:35 2024 UTC
Last successful sync completed '1 minute 29 seconds' ago.

------------------------- Last periodic sync time details end ---------------------------------

**************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
**************************************************************
Enter choice: 9

SYNC_ACTIVE: 1 at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 494, <STDIN> line 5.
Found running Synchronization task: Initializing at /usr/local/sf/lib/perl/5.24.4/SF/Transaction/HADC.pm
Sybase state :  at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 701.
Sybase state :  at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line 801.
Sync status :Synchronization Task In-progress  at /usr/local/sf/lib/perl/5.24.4/SF/Synchronize.pm line
Found running Synchronization task: Initializing at /usr/local/sf/lib/perl/5.24.4/SF/Transaction/HADC.pm

------------------------- FMC HA status messages start ---------------------------------

Status: Synchronization Task In-progress

------------------------- FMC HA status messages end ---------------------------------

**************** 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 Get Remote Stale Sync AQ Info
14 Help
```

```
0 Exit
*****************************************************************
Enter choice: 10

Fetching standby missing device information...
Devices are in sync.

*************** 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 Get Remote Stale Sync AQ Info
14 Help
0 Exit
*****************************************************************
Enter choice: 0
Thank you
```

Communicatie van FTD naar FMC-HA-validering

<#root>

```
>

 show version


------------------[ firepower ]-------------------
Model                    : Cisco Firepower Threat Defense for VMware (75) Version 7.2.4 (Build 165)
UUID                     : 7064913a-xxxx-xxxx-xxxx-803aefd05d2c
LSP version              : lsp-rel-20231129-1200
VDB version              : 395
--------------------------------------------------


>

ping system xx.xx.18.101

------ ping to FMC-Active
PING xx.xx.18.101 (xx.xx.18.101) 56(84) bytes of data.
64 bytes from xx.xx.18.101: icmp_seq=1 ttl=64 time=14.1 ms
64 bytes from xx.xx.18.101: icmp_seq=2 ttl=64 time=27.8 ms
64 bytes from xx.xx.18.101: icmp_seq=3 ttl=64 time=26.1 ms
64 bytes from xx.xx.18.101: icmp_seq=6 ttl=64 time=55.7 ms
64 bytes from xx.xx.18.101: icmp_seq=7 ttl=64 time=39.9 ms
64 bytes from xx.xx.18.101: icmp_seq=8 ttl=64 time=38.9 ms
^C
--- xx.xx.18.101 ping statistics ---
```

```
8 packets transmitted, 6 received, 25% packet loss, time 76ms
rtt min/avg/max/mdev = 14.081/33.733/55.658/13.069 ms


>

ping system xx.xx.18.102

------ ping to FMC-Active
PING xx.xx.18.102 (xx.xx.18.102) 56(84) bytes of data.
64 bytes from xx.xx.18.102: icmp_seq=1 ttl=64 time=23.9 ms
64 bytes from xx.xx.18.102: icmp_seq=2 ttl=64 time=23.10 ms
64 bytes from xx.xx.18.102: icmp_seq=3 ttl=64 time=0.425 ms
64 bytes from xx.xx.18.102: icmp_seq=4 ttl=64 time=6.88 ms
64 bytes from xx.xx.18.102: icmp_seq=5 ttl=64 time=10.5 ms
^C
--- xx.xx.18.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 70ms
rtt min/avg/max/mdev = 0.425/13.131/23.969/9.380 ms


>

show managers


Type                    : Manager
Host                    : xx.xx.18.101
Display name            : xx.xx.18.101
Version                 : 7.2.8 (Build 25)
Identifier              : fc3e3572-xxxx-xxxx-xxxx-39e0098c166c
Registration            : Completed
Management type         : Configuration and analytics

Type                    : Manager
Host                    : xx.xx.18.102
Display name            : xx.xx.18.102
Version                 : 7.2.8 (Build 25)
Identifier              : bb333216-xxxx-xxxx-xxxx-c68c0c388b44
Registration            : Completed
Management type         : Configuration and analytics


>

sftunnel-status


SFTUNNEL Start Time: Mon Oct 14 21:29:16 2024
        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 17
        Reserved SSL connections: 0
        Management Interfaces: 2
        eth0 (control events) xx.xx.18.254,
        tap_nlp (control events) 169.254.1.2,fd00:0:0:1::2
***********************

**RUN STATUS****xx.xx.18.102************* ------------------------------------- sftunnel information
        Key File    = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-key.pem
        Cert File   = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/sftunnel-cert.pem
        CA Cert     = /var/sf/peers/bb333216-xxxx-xxxx-xxxx-c68c0c388b44/cacert.pem
        Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface eth0
        Registration: Completed.
        IPv4 Connection to peer 'xx.xx.18.102' Start Time: Wed Oct 16 15:06:23 2024 UTC
```

```
        IPv4 Last outbound connection to peer 'xx.xx.18.102' via Primary ip/host 'xx.xx.18.102'

PEER INFO:
        sw_version 7.2.8
        sw_build 25
        Using light registration
        Management Interfaces: 1
        eth0 (control events) xx.xx.18.102,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to 'xx.xx.18.102' via
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to 'xx.xx.18.102' via 'x:

***********************

**RUN STATUS****xx.xx.18.101************* ------------------------------------- sftunnel information o
        Key File    = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-key.pem
        Cert File   = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/sftunnel-cert.pem
        CA Cert     = /var/sf/peers/fc3e3572-xxxx-xxxx-xxxx-39e0098c166c/cacert.pem
        Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        Cipher used = TLS_AES_256_GCM_SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface eth0
        Registration: Completed.
        IPv4 Connection to peer 'xx.xx.18.101' Start Time: Mon Oct 14 21:29:15 2024 UTC

PEER INFO:
        sw_version 7.2.8
        sw_build 25
        Using light registration
        Management Interfaces: 1
        eth0 (control events) xx.xx.18.101,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to 'xx.xx.18.101' via
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to 'xx.xx.18.101' via 'x:

***********************

**RPC STATUS****xx.xx.18.101*************
  'name' => 'xx.xx.18.101',
  'last_changed' => 'Mon Jun 10 18:59:54 2024',
  'uuid_gw' => '',
  'ip' => 'xx.xx.18.101',
  'ipv6' => 'IPv6 is not configured for management',
  'active' => 1,
  'uuid' => 'fc3e3572-xxxx-xxxx-xxxx-39e0098c166c'

**RPC STATUS****xx.xx.18.102*************
  'name' => 'xx.xx.18.102',
  'last_changed' => 'Wed Oct  9 07:00:11 2024',
  'uuid_gw' => '',
  'ip' => 'xx.xx.18.102',
  'ipv6' => 'IPv6 is not configured for management',
  'active' => 1,
  'uuid' => 'bb333216-xxxx-xxxx-xxxx-c68c0c388b44'

Check routes:
No peers to check
```

Opmerking: Als de informatie over de sftunnels van een van de VCC's ontbreekt, kan dit erop wijzen dat de communicatie met de beheerder in gevaar is

<#root>

FTD root level troubleshoot

> expert

admin@firepower:~$

sudo su

root@firepower:/home/admin#

netstat -an | grep 8305

```
tcp       0        0 xx.xx.18.254:8305        xx.xx.18.102:59439      ESTABLISHED ------ communication es
tcp       0        0 xx.xx.18.254:49205       xx.xx.18.101:8305       ESTABLISHED ------ communication es
tcp       0        0 xx.xx.18.254:50373       xx.xx.18.102:8305       ESTABLISHED ------ communication es
tcp       0        0 xx.xx.18.254:53875       xx.xx.18.101:8305       ESTABLISHED ------ communication es

root@firepower:/home/admin#

cat /ngfw/var/log/action_queue.log | less


Oct 16 15:06:50 firepower ActionQueueScrape.pl[4166]: Waiting for light registration to complete on dev
erl/5.24.4/SF/PeerManager/RegistrationCL.pm line 1805.
Oct 16 15:06:50 firepower ActionQueueScrape.pl[4166]: Found Registered peer with name xx.xx.18.102 (bb3
Oct 16 15:06:50 firepower ActionQueueScrape.pl[4166]: Found peer with name xx.xx.18.102 - update DB at
Oct 16 15:06:50 firepower ActionQueueScrape.pl[4166]: Found Registered peer with name xx.xx.18.101 (fc3
```