FMC故障排除- HA

目录

简介

本文档介绍如何对Firepower管理中心(FMC)的高可用性(HA)设置中的常见同步问题进行故障排除。

先决条件

要求

Cisco建议您了解以下主题：

- FMC - HA配置要求
- Linux shell基础知识。

使用的组件

- FMCv for VMware（版本7.2.8）。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档所用实验室的初始设置遵循基本FMC-HA初始配置的要求。

- 两个具有相同容量或硬件版本的FMC。
- 两个运行相同软件版本的FMC：入侵规则更新、漏洞数据库和轻量级安全包。

- 两个FMC及相应的许可证。

开始使用前

- 确保管理员有权访问两个FMC。
- 确保管理员有权访问FMC管理的FTD设备。

故障排除命令

FMC故障排除命令。

要验证FMC设备之间的连接，用户可以运行以下命令。

```
<#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
```
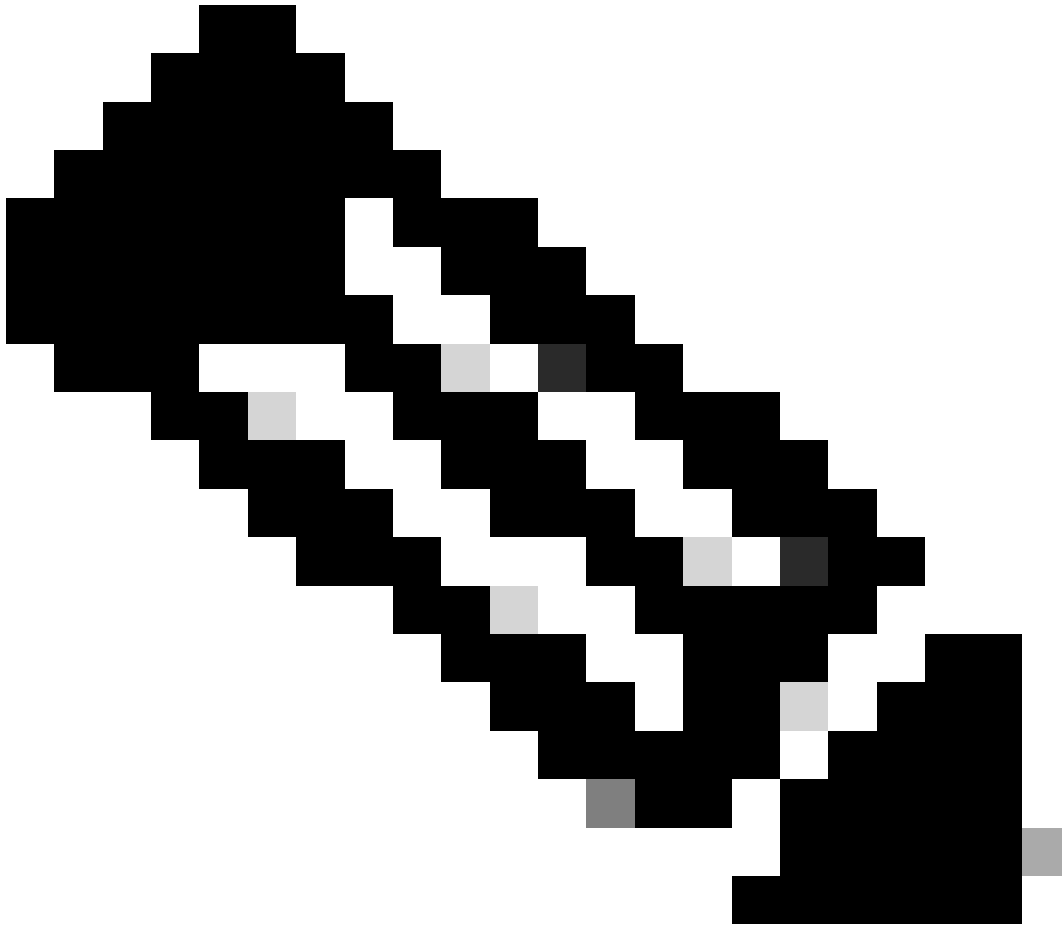
ping <peer-ip-address>此命令可用于检查两台设备之间的可接通性。

netstat -an | grep 8305此命令显示连接到端口8305的设备。

注意：端口8305是Firepower设备上配置的默认端口，用于建立与FMC的通信信道。

要验证FMC-HA设置配置，用户还可以运行脚本troubleshoot_HADC.pl。 这在以下情况下尤其有用
：

- 当FMC-HA集成运行状况降级时。
- 如果缺少对其中一台设备的FMC图形用户界面(GUI)的访问，但是FMC-CLI访问仍在运行并可访问。

<#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:
```

FTD故障排除命令

通过排除从FTD到FMC-HA的连接故障，用户可以验证需要在两个FMC上注册或在HA降级时注册设备的连接，并显示警告"已降级-同步未完成（此管理中心注册的设备较少）"。

从FTD清除级别，用户可以运行这些命令来验证与FMC的通信。

<#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 system <fmc-IP>要生成ICMP，请从FTD管理接口执行操作。

show managers -此命令列出注册设备的管理器的信息。

sftunnel-status 此命令用于验证设备之间建立的通信信道。此信道接收名称sftunnel。

在FTD上检查根级别连接的命令与FMC相同。在FTD的情况下，它不包含允许验证与FMC的通信的脚本，但可以在/ngfw/var/log/action.log中检查注册过程中生成的信息。

确认

对于下一个拓扑，可以使用前面介绍的命令验证FMC-HA对等体和FTD01之间的通信。

FMC - Active   FMC - Standby

xx.xx.18.101   xx.xx.18.102

FTD01   FTD02

xx.xx.18.253   xx.xx.18.254
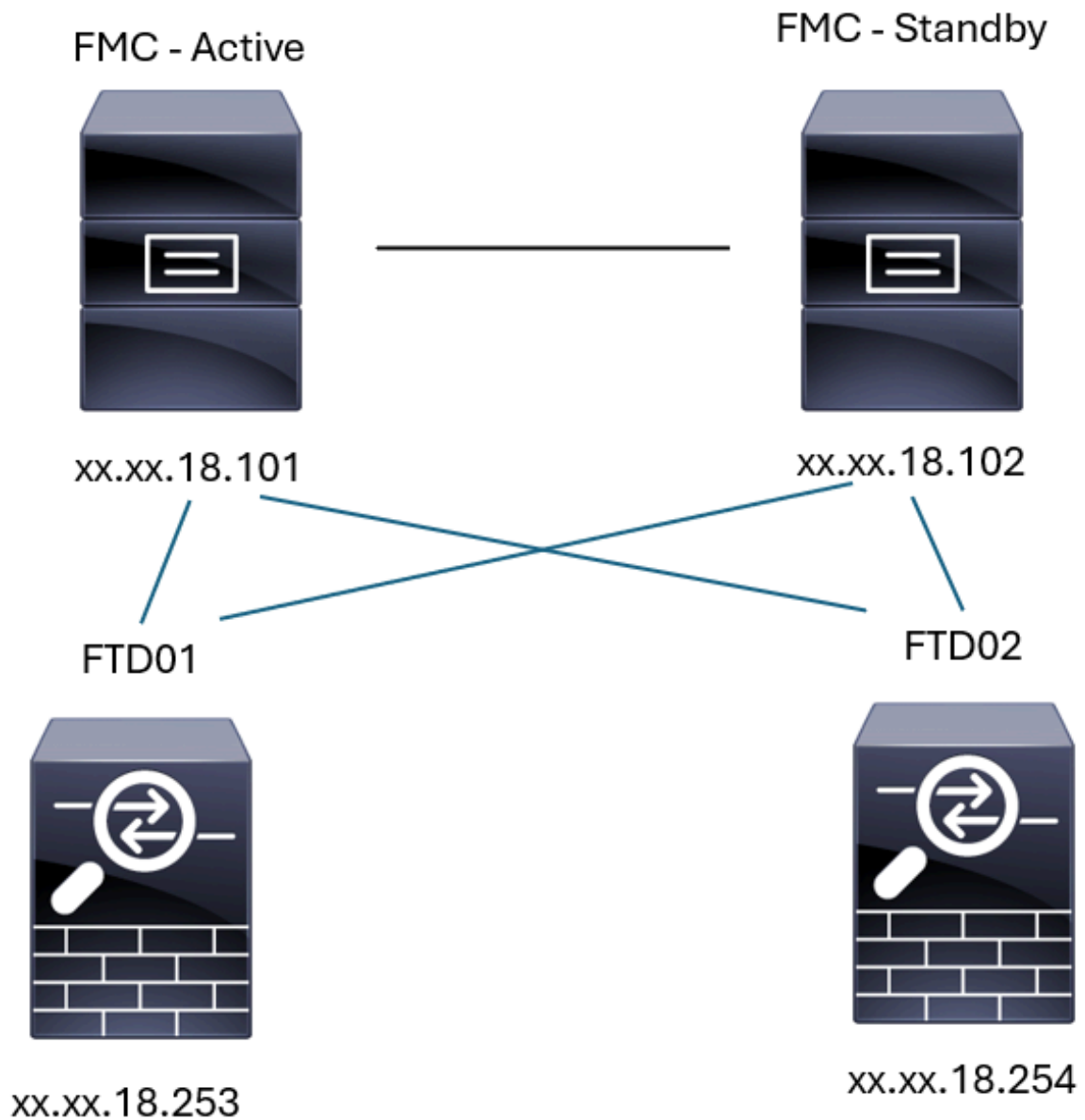
FMC-HA拓扑

FMC - HA验证

对于此验证，还可以使用命令show version验证设置FMC-HA的基本指南。

<#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/I
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
```

从FTD到FMC-HA验证的通信

<#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
```

注意：如果某个FMC的sftunnel信息丢失，这可能表明与管理器的通信受到危害

<#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
```