Troubleshoot Firepower Threat Defense High Availability Issues

Contents

Introduction

This document describes the operation, verification, and troubleshooting procedures for High Availability (HA) on Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- FTD and ASA platforms
- Packet captures on FTD appliances

It is highly recommended that the Firepower Configuration Guide Configure FTD High Availability on Firepower Appliances is read to better comprehend the concepts described in this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco FTD
- Cisco Firepower Management Center (FMC)

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The information and the examples are based on FTD, but most of the concepts are also fully applicable to Adaptive Security Appliance (ASA).

An FTD supports two main management modes:

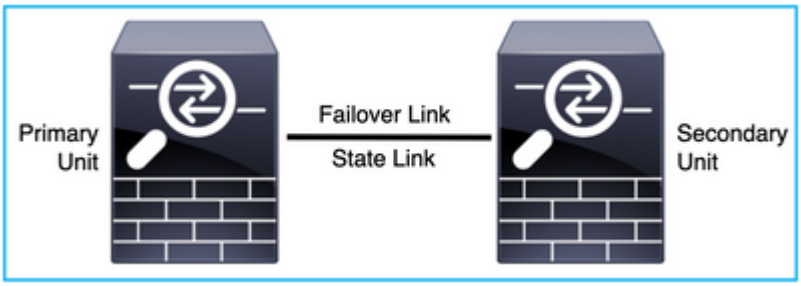
- Off-box via FMC - also known as remote management
- On-box via Firepower Device Manager (FDM) - also known as local management

---

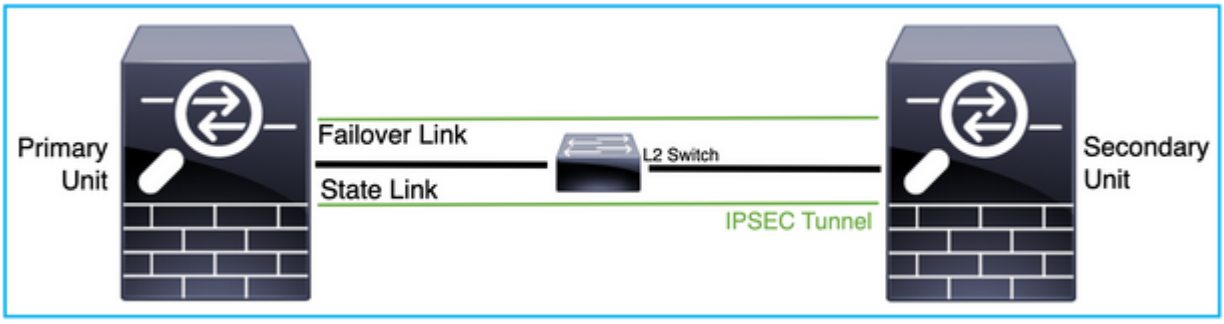
Note: FTD managed via FDM can be added in High Availability from Firepower version code v6.3.0 onwards.

Design Options

From a design point of view of the FTD, it can be directly connected, as shown in this image:



Or, it can be connected via Layer 2 (L2) switch, as shown in this image:



HA Terminology

Active	The active ASA receives all traffic flows and filters all network traffic. The configuration changes are made on the active ASA.
HA Link	The two units in a failover pair constantly communicate over a failover link to determine the operating status of each unit and to synchronize configuration changes. The information shared over the link is: • The unit state (active or standby) • Hello messages (keep-alive) • Network link status • MAC address exchange • Configuration replication and synchronization
Primary	This is the unit that is usually configured first when you create an HA. The significance of this is that if both the devices of an ASA HA were to come up together at the exact same instant, the primary assumes the active role.
Secondary	This is the unit that is usually configured second when you create an HA. The significance of this is that, if both the devices of an ASA HA were to come up together at the exact same instant, the secondary assumes the standby role.
Standby	The standby ASA does not handle any live traffic, it syncs the connections and the configuration from the active device, and takes up the active role in case of a failover.
State Link	The active unit uses the state link to pass connection state information to the standby device. Therefore, the standby unit can maintain certain types of connections and it does not affect you. This information helps the standby unit to maintain the connections that exist when a failover occurs. NB: When you use the same link for failover and stateful failover, you conserve interfaces the best. However, you must consider a dedicated interface for the state link and failover link, if you have a large configuration and a high traffic network. We recommend that the bandwidth of the stateful failover link must match the largest bandwidth of the data interfaces on the device.

HA States

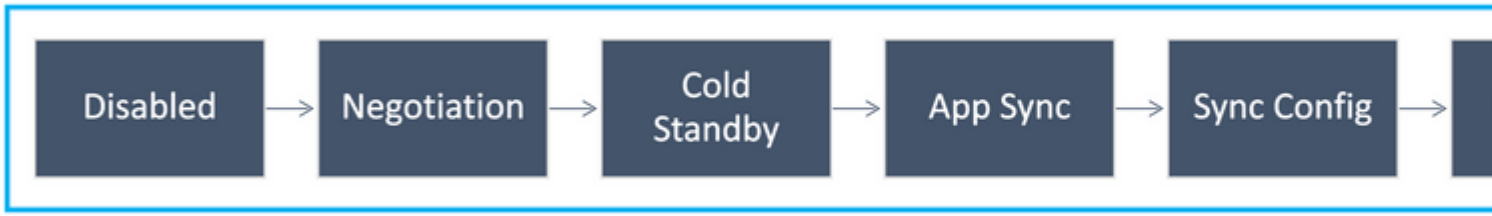
Active	The device currently handles the live traffic on the network, and all the configuration changes that need to be done are to be performed on this device.
App Sync	The device in this state synchronizes the configuration from the active device.

Bulk Sync	The device in this state synchronizes the configuration from the active device.
Disabled	The failover on the unit has been disabled (command: no failover).
Negotiation	The device checks for the availability of the active device and takes the active role if the active device is not found to be standby ready.
Standby Ready	The device currently does not handle traffic but takes on the active role if the active device shows any health check issues.
Sync Configuration	The configuration is replicated from the active device to the standby device.
Cold Standby	The device takes over as active on failover but does not replicate the connection events.

HA State Flow Diagram

Primary (without any connected peer):

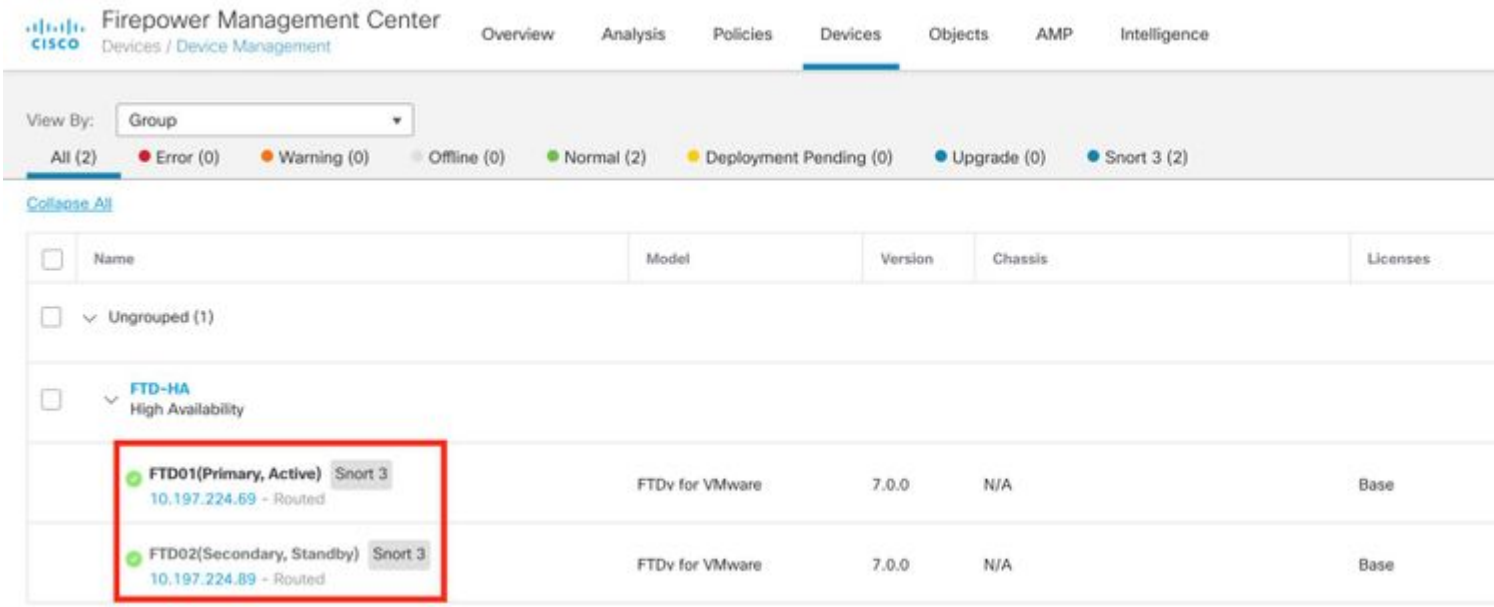
Secondary (with an Active connected peer):



UI Verification

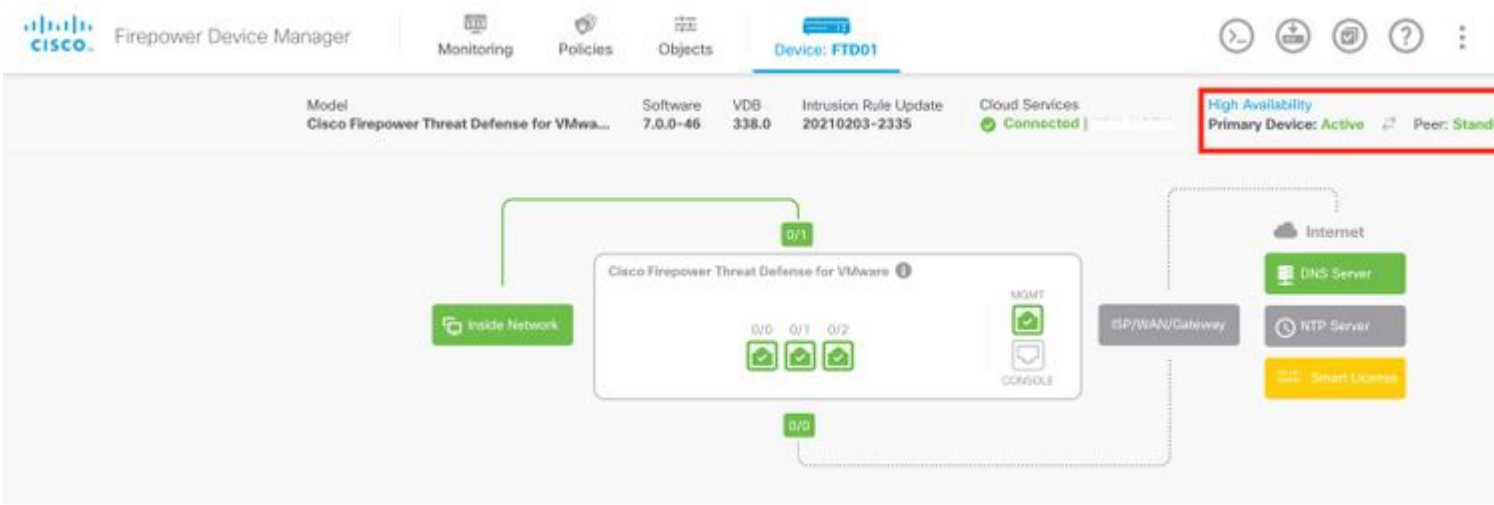
Firepower Management Center Managed FTD HA

The FTD HA state can be checked from FMC UI when you navigate to **Device > Device Management**, as shown in this image:

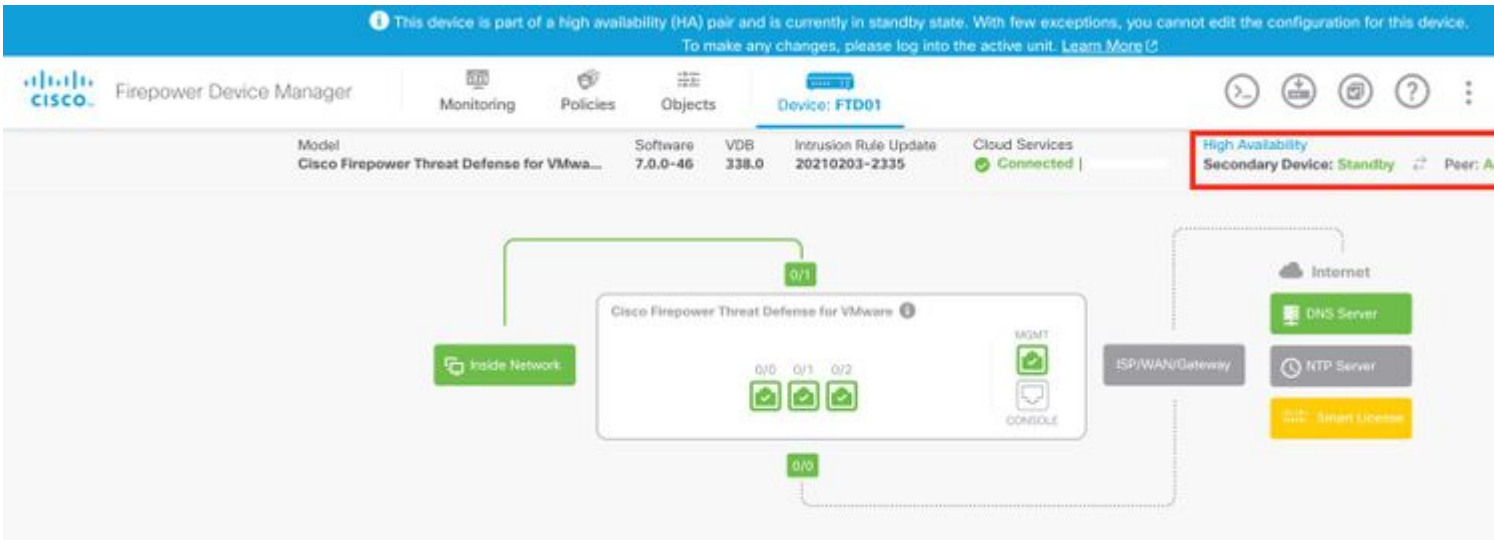


FDM Managed FTD HA

Primary FDM Overview page:

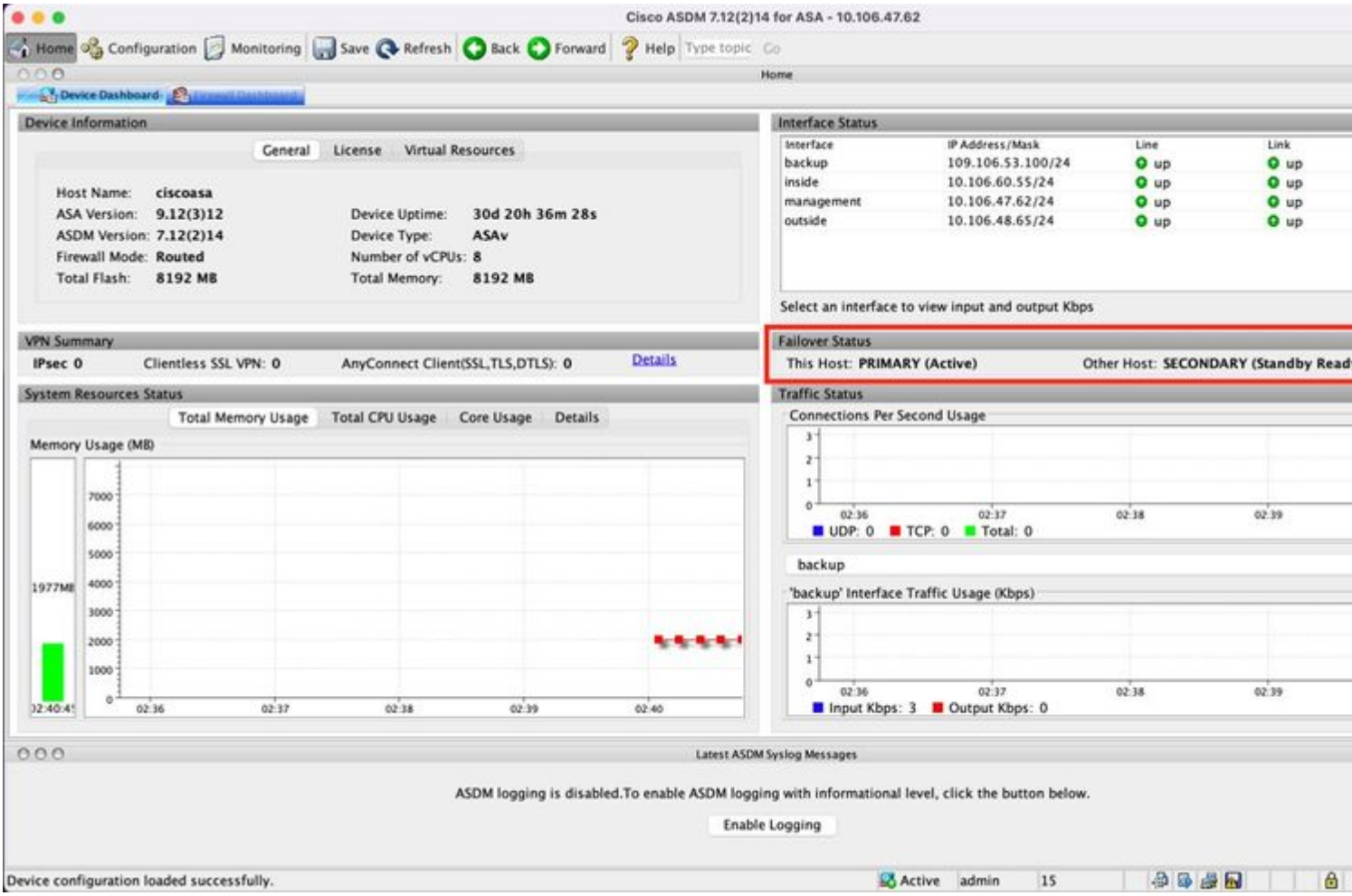


Secondary FDM Overview page:

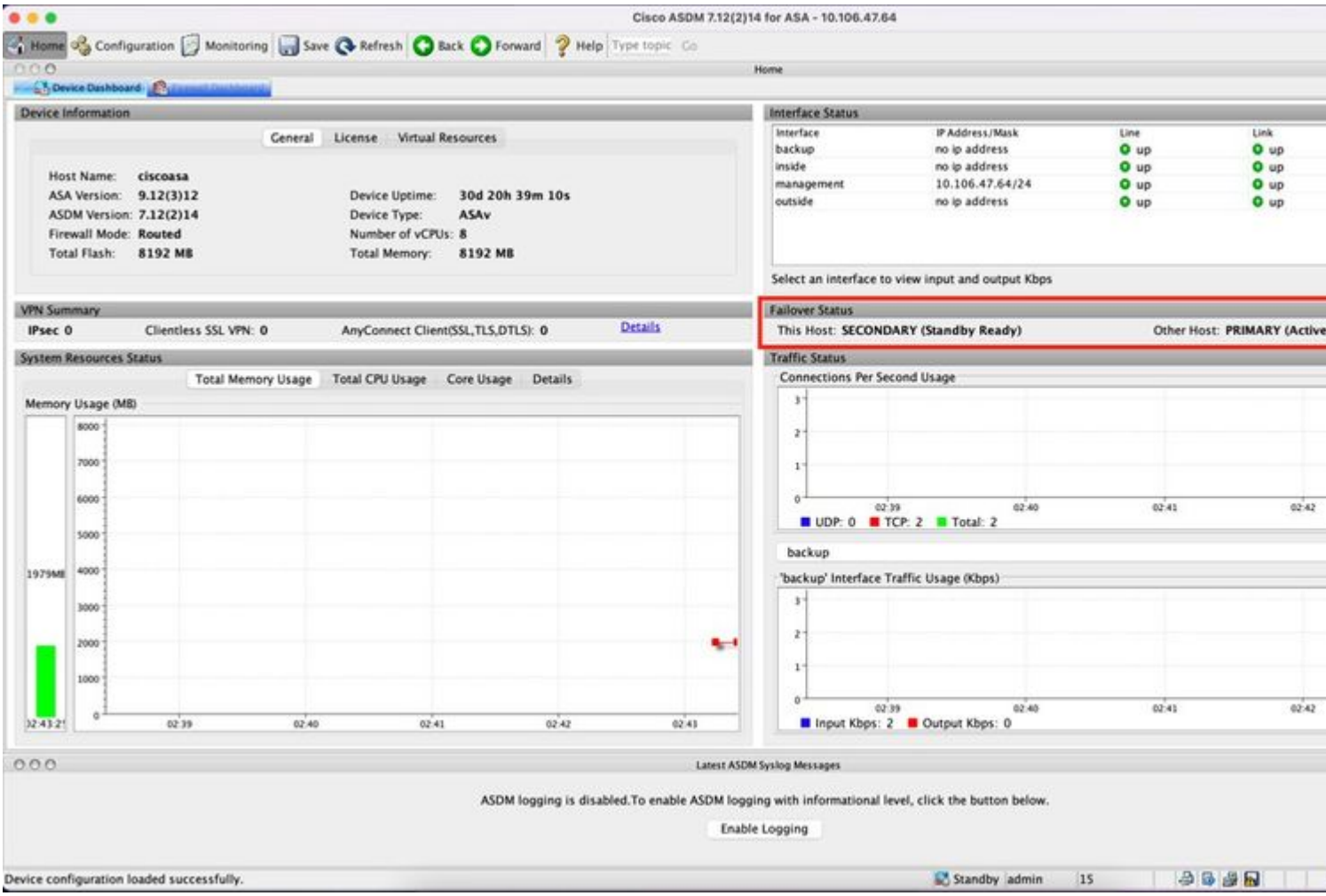


ASDM Managed ASA HA

ASDM Home page to Primary ASA:

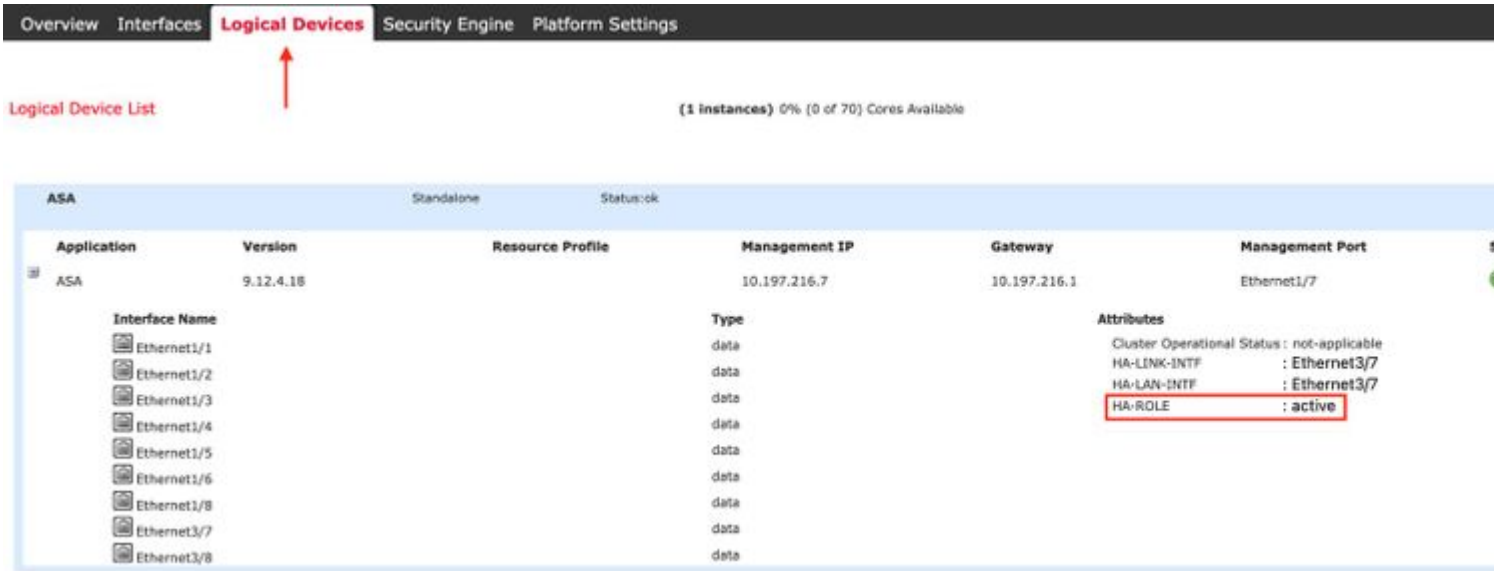


ASDM Home page to Secondary ASA:

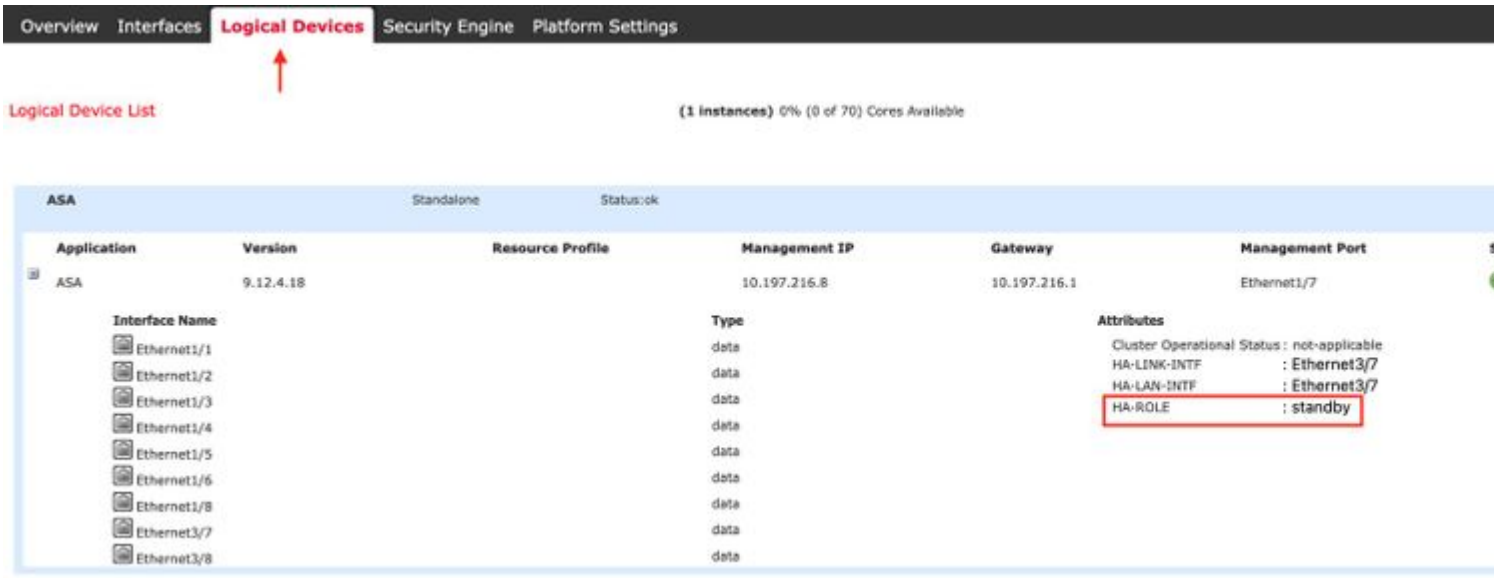


Firepower Chassis Manager for 4100/9300 Running FTD/ASA HA

Primary FCM Logical Device page:



Secondary FCM Logical Device page:



Verify CLI

<#root>

>

show running-config failover

```
failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

The important points to consider in this are:

failover
failover lan unit secondary --> whether the unit is primary or secondary
failover lan interface failover-link GigabitEthernet0/2 --> failover link physical interface on the device
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 --> primary and the standby device failover link ip addresses.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (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 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.2): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)
    Other host: Primary - Active
        Active time: 707216 (sec)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.1): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
    Link : failover-link GigabitEthernet0/2 (up)
    Stateful Obj        xmit       xerr          rcv          rerr
    General             95752       0           115789          0
    sys cmd             95752       0            95752          0
    up time               0         0              0            0
    RPC services          0         0              0            0
    TCP conn              0         0              0            0
    UDP conn              0         0              0            0
    ARP tbl               0         0            20036          0
    Xlate_Timeout         0         0              0            0
    IPv6 ND tbl           0         0              0            0
    VPN IKEv1 SA          0         0              0            0
    VPN IKEv1 P2          0         0              0            0
    VPN IKEv2 SA          0         0              0            0
    VPN IKEv2 P2          0         0              0            0
    VPN CTCP upd          0         0              0            0
    VPN SDI upd           0         0              0            0
    VPN DHCP upd          0         0              0            0
    SIP Session           0         0              0            0
    SIP Tx                0         0              0            0
    SIP Pinhole           0         0              0            0
    Route Session         0         0              0            0
    Router ID             0         0              0            0
    User-Identity         0         0              1            0
    CTS SGTNAME           0         0              0            0
    CTS PAC               0         0              0            0
    TrustSec-SXP          0         0              0            0
    IPv6 Route            0         0              0            0
    STS Table             0         0              0            0
    Rule DB B-Sync        0         0              0            0
    Rule DB P-Sync        0         0              0            0
    Rule DB Delete        0         0              0            0

    Logical Update Queue Information
       Cur   Max    Total
Recv Q: 0     5     504656
```

```
Xmit Q: 0     1     95752
```

Failover On: Failover is Enabled or Disabled.

This host: Secondary - Standby Ready. The role of this device and the states of the interfaces.

Other hosts: Primary - Active. The other device is in an Active state and communicates with the current device.

<#root>

>

show failover history

```
==========================================================================
From State                 To State                       Reason
==========================================================================
01:18:14 UTC Nov 25 2021
Not Detected               Negotiation                    No Error

01:18:27 UTC Nov 25 2021
Negotiation                Just Active                    No Active unit found

01:18:27 UTC Nov 25 2021
Just Active                Active Drain                   No Active unit found

01:18:27 UTC Nov 25 2021
Active Drain               Active Applying Config         No Active unit found

01:18:27 UTC Nov 25 2021
Active Applying Config     Active Config Applied          No Active unit found

01:18:27 UTC Nov 25 2021
Active Config Applied         Active                      No Active unit found
==========================================================================
```

Use this to check the historic states of the devices and the reasons for those state changes:

<#root>

>

show failover state

```
              State              Last Failure Reason      Date/Time
This host -   Secondary
              Standby Ready          None
Other host -  Primary
              Active                 None

====Configuration State===
    Sync Done - STANDBY
```

```
====Communication State===
    Mac set
```

Check the current states of the devices and the reason for the last failover:

Field	Description
Configuration State	Displays the state of configuration synchronization. Possible configuration states for the standby unit: • Config Syncing - STANDBY â€” Set while the synchronized configuration is executed. • Interface Config Syncing - STANDBY • Sync Done - STANDBY â€” Set when the standby unit has completed a configuration synchronization from the active unit. Possible configuration states for the active unit: • Config Syncing â€” Set on the active unit when it performs a configuration synchronization to the standby unit. • Interface Config Syncing • Sync Done â€”Set when the active unit has completed a successful configuration synchronization to the standby unit. • Ready for Config Sync â€”Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • Mac set â€”The MAC addresses have been synchronized from the peer unit to this unit. • Updated Mac â€”Used when a MAC address is updated and needs to be synchronized to the other unit. Also used at the time of transition where the unit updates the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
Last Failure Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs. Possible failure reasons: • Interface Failure â€” The number of interfaces that failed met the failover criteria

Field	Description
	and caused failover. • Comm Failure â€" The failover link failed or the peer is down. • Backplane Failure
State	Displays the Primary/Secondary and Active/Standby status for the unit.
This host/Other hosts	This host indicates information for the device upon which the command was executed. Another host indicates information for the other device in the failover pair.

<#root>

>

show failover descriptor

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

Troubleshoot

Debugs

<#root>

>

debug fover ?

```
cable         Failover LAN status
cmd-exec      Failover EXEC command execution
fail          Failover internal exception
fmsg          Failover message
ifc           Network interface status trace
open          Failover device open
rx            Failover Message receive
rxdmp         Failover recv message dump (serial console only)
rxip          IP network failover packet recv
snort         Failover NGFW mode snort processing
switch        Failover Switching status
sync          Failover config/command replication
tx            Failover Message xmit
txdmp         Failover xmit message dump (serial console only)
txip          IP network failover packet xmit
verify        Failover message verify
```

Captures:

Failover interface captures:

You can refer to this capture to determine if the failover hello packets are sent on the failover link at the rate at which they are sent.

<#root>

>

show capture

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
```

>

show capture capfail

```
15 packets captured

1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

ARP capture on the failover link:

You can take this capture to see if the peers have Mac entries in the ARP table.

<#root>

>

show capture

```
capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
```

>

show capture caparp

```
22 packets captured

1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

Scenarios

If the peer unit fails to join the HA group or fails while you deploy changes from the active unit, log into the failed unit, navigate to the High Availability page, and click the Failover History link.

APP-SYNC Failure

If the show failover history output indicates an App Sync failure, then there was a problem at the time of the HA validation phase, where the system checks that the units can function correctly as a high availability group.

The message â€œAll validation passedâ€ when the From State is App Sync appears, and the node moves to the Standby Ready state.

Any validation failure transitions the peer to the Disabled (Failed) state. Resolve the problems to make the peers function as a high availability group again.

Note that if you fix an App Sync error and make changes to the active unit, you must deploy them and then resume HA for the peer node to join.

The messages indicate failures, with an explanation of how you can resolve the issues. These errors can happen on node join and on each subsequent deployment.

At the time of a node join, the system performs a check against the last deployed configuration on the active unit.

Standby Node Fails to Join HA with "CD App Sync error is App Config Apply Failed"

On the Standby FTD command line, **/ngfw/var/log/action_queue.log** must have the reason for configuration failure.
Remediation: On identification of the configuration error, post-making required changes, HA can be resumed.
See Cisco bug IDCSCvu15611.

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
15:10:16 CDT Sep 28 2021
Not Detected                Disabled                    No Error
15:10:18 CDT Sep 28 2021
Disabled                    Negotiation                 Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation                 Cold Standby                Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby                App Sync                    Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync                    Disabled
```

CD App Sync error is App Config Apply Failed

```
================================================================================
```

Standby Node Fails to Join HA with "HA state progression failed due to APP SYNC timeout"

On the Standby FTD command line, **/ngfw/var/log/ngfwmanager.log** must have the reason for the app-sync timeout.
At this stage, policy deployments also fail because the active unit thinks app sync is still in progress.
Policy deployment throws the error - "since newNode join/AppSync process is in progress, Configuration Changes are not allowed, and hence rejects the deployment request. Please retry deployment after some time"
Remediation: Sometimes, when you resume high availability on the Standby node, it can resolve the issue.
See Cisco bug ID CSCvt48941
See Cisco bug ID CSCvx11636

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
19:07:01 EST MAY 31 2021
Not Detected                Disabled                    No Error
19:07:04 EST MAY 31 2021
Disabled                    Negotiation                 Set by the config command
19:07:06 EST MAY 31 2021
Negotiation                 Cold Standby                Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby                App Sync                    Detected an Active mate
```

```
21:11:18 EST Jun 30 2021
App Sync                    Disabled
```

HA state progression failed due to APP SYNC timeout

```
================================================================================
```

Standby Node Fails to Join HA with "CD App Sync error is Failed to apply SSP config on standby"

On the Standby FTD command line, **/ngfw/var/log/ngfwmanager.log** must have the exact reason for the failure.

Remediation: Sometimes, when you resume high availability on the Standby node, it can resolve the issue.

See Cisco bug ID CSCvy04965

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
04:15:15 UTC Apr 17 2021
Not Detected                Disabled                    No Error
04:15:24 UTC Apr 17 2021
Disabled                    Negotiation                 Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation                 Cold Standby                Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby                App Sync                    Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync                    Disabled
```

CD App Sync error is Failed to apply SSP config on standby

```
================================================================================
```

Health Check Failure

"HELLO not heard from mate" means the mate is offline or the failover link does not communicate the HELLO keepalive messages.

Try to log in to the other device, if SSH does not work, get the console access and check if the device is operational or offline.

If operational, identify the cause of the failure with the command, **show failover state.**

If not operational, try a graceful reboot and check if you see any boot logs on the console, otherwise, the device can be considered hardware faulty.

<#root>

```
================================================================================
```

```
From State                 To State                   Reason
================================================================================
04:53:36 UTC Feb 6 2021
Failed                     Standby Ready
```

Interface check

```
02:12:46 UTC Jul 11 2021
Standby Ready              Just Active                HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied      Active                     HELLO not heard from mate
================================================================================
```

Snort Down or Disk Failure

If the FTD gives this error, "Detect Inspection engine failure due to disk failure", there are 2 possibilities.

The Detection Engine (SNORT Instance) is Down

This can be validated with the command on the Linux side, **pmtool status | grep -i de,**

Remediation: If any of the instances is down, check for **/ngfw/var/log/messages** and identify the cause.

The Device Shows High Disk Utilization

This can be validated with the command on the Linux side, **df -Th**.

Remediation: Identify the directory which consumes most of the disk and contact TAC to delete the unwanted files.

<#root>

```
================================================================================
From State                 To State                   Reason
================================================================================
Active Config Applied      Active                     No Active unit found
16:07:18 UTC Dec 5 2020
Active                     Standby Ready              Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready              Failed
```

Detect Inspection engine failure due to disk failure

```
16:07:29 UTC Dec 5 2020
Failed                     Standby Ready              My Inspection engine is as good as peer due to dis
================================================================================
```

Service Card Failure

Such issues are generally reported because of Firepower module failure on ASA 5500-X devices. Please check the sanity of the module via **show module sfr details**.

Remediation: Collect ASA Syslog around the time of the failure, and these can contain details like control or data plane failure.

That can be due to various reasons in the SFR module. It is recommended to open TAC to find the root cause of this issue on the IPS.

<#root>

```
==========================================================================
From State                 To State                   Reason
==========================================================================
21:48:19 CDT Aug 1 2021
Active                     Standby Ready              Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready              Just Active

Service card in other unit has failed


21:48:19 CDT Aug 1 2021
Active Config Applied      Active                     Service card in other unit has failed
==========================================================================
```

MIO Heartbeat Failure

Firepower Threat Defense/ASA reports failure due to "MIO-blade heartbeat failure" on FPR1K, 2K, 4K, 9K.

See Cisco bug ID CSCvy14484
See Cisco bug ID CSCvh26447

<#root>

```
==========================================================================
From State                 To State                   Reason
==========================================================================
20:14:45 EDT Apr 14 2021
Active Config Applied      Active                     No Active unit found
20:15:18 EDT Apr 14 2021
Active                     Failed

MIO-blade heartbeat failure


20:15:19 EDT Apr 14 2021
Failed                     Negotiation                MIO-blade heartbeat recovered
==========================================================================
```

Related Information

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-

fdm-ha.html#id_72185

- **Technical Support & Documentation - Cisco Systems**