

Identify and Analyze FTD Failover Events on FMC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Failover Events on FMC](#)

[Step 1. Health Policy Configuration](#)

[Step 2. Policy Assignment](#)

[Step 3. Failover Events Alerts](#)

[Step 4. Historical Failover Events](#)

[Step 5. High Availability Dashboard](#)

[Step 6. Threat Defense CLI](#)

[Related Information](#)

Introduction

This document describes how to identify and analyze failover events for Secure Firewall Threat Defense on Secure Firewall Management Center GUI.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- High Availability (HA) Setup for Cisco Secure Firewall Threat Defense (FTD)
- Basic Usability of the Cisco Firewall Management Center (FMC)

Components Used

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

- Cisco FMC v7.2.5
- Cisco Firepower 9300 Series v7.2.5

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 FMC is not only the administrative center for Firepower devices, beyond management, and configuration options, it also provides a graphical interface that helps to analyze logs and events in real and past time.

When speaking about failover, the interface has new improvements that help to analyze failover events in order to understand the failures.

Failover Events on FMC

Step 1. Health Policy Configuration

The module Cluster/HA Failure Status is enabled by default on the Health Policy but additionally, you can enable the Split-brain check option.

In order to enable the options for HA in the health policy, navigate to System > Health > Policy > Firewall Threat Defense Health Policy > High Availability.

This image describes the HA configuration of the Health Policy:

Firewall Management Center
System / Health / Policy

Overview Analysis Policies Devices Objects Integration

Initial_Health_Policy 2023-08-29 15:26:44
Initial Health Policy

Health Modules Run Time Intervals

Disk Usage

Monitors disk usage

Warning threshold % Critical threshold %

Warning Threshold (secondary HD) % Critical Threshold (secondary HD) %

High Availability

Cluster/HA Failure Status
Monitors cluster and HA members for their availability failure

Firewall Threat Defense HA (Split-brain check)
Monitors Firewall Threat Defense HA for split-brain (Both HA members are in active state)

Integration

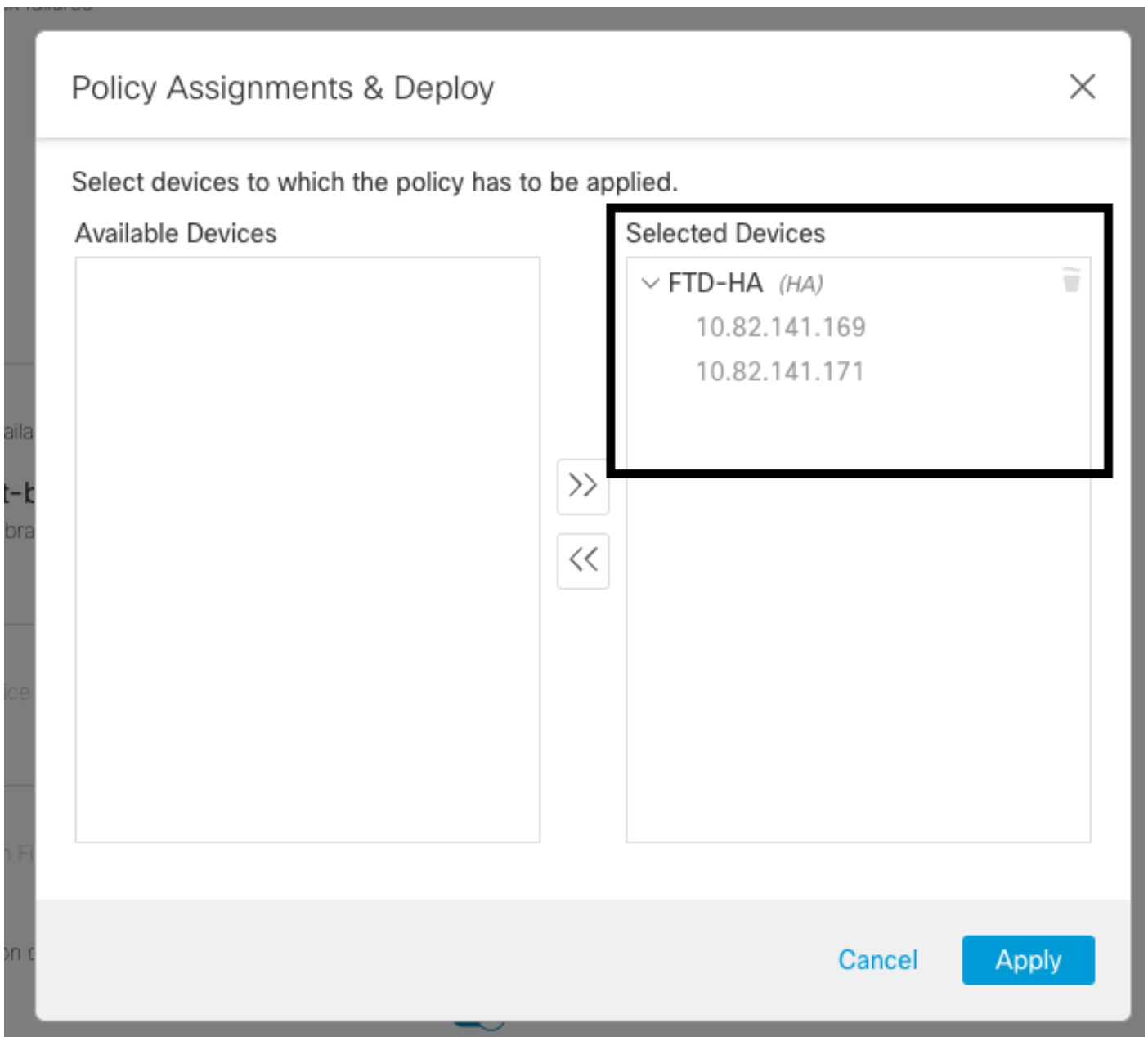
High Availability Health Settings

Step 2. Policy Assignment

Ensure the Health Policy is assigned to the HA pairs you want to monitor from the FMC.

In order to assign the policy, navigate to System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

This image shows how to assign the health policy to the HA pair:



HA assignment

Once the policy has been assigned and saved, automatically the FMC applies it to the FTD.

Step 3. Failover Events Alerts

Depending on the configuration of the HA, once a failover event is triggered, the pop-up alerts that describe the failover failure are shown.

This image shows the failover alerts generated:

Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco **SECURE**

0 Pending (0) ● Upgrade (0)

	Version	Chassis	Licenses	Access Control P
with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕
 SECONDARY (FLM1946BCEX)
 FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services-. Peer failed services-diskstatus))
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Check peer event for reason)

Cluster/Failover Status - 10.82.141.171 ✕
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Other unit wants me Standby)
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-))

Disk Usage - 10.82.141.171 ✕
 /ngfw using 98%: 186G (5.5G Avail) of 191G

Failover Alerts

You can also navigate to Notifications > Health in order to visualize the failover health alerts.

This image shows the failover alerts under notifications:

Firewall Management Center
Devices / Device Management Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco **SECURE**

View By: Group
 All (2) ● Error (2) ● Warning (0) ● Offline (0) ● Normal (0) ● Deployment Pending (0) ● Upgrade (0)

Collapse All

Name	Model	Version	Chassis
Ungrouped (1)			
FTD-HA High Availability			
10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1 Security Module - 1
10.82.141.171(Primary, Failed) 10.82.141.171 - Routed	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR Security Module - 1

Deployments Upgrades **Health** Tasks Show Notifications

20+ total 15 warnings 7 critical 0 errors Filter

- Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud
- URL Filtering Monitor URL Filtering registration failure

Devices

10.82.141.169

- Interface Status Interface 'Ethernet1/2' is not receiving any packets
Interface 'Ethernet1/3' is not receiving any packets
Interface 'Ethernet1/4' is not receiving any packets

10.82.141.171

- Disk Usage /ngfw using 98%: 186G (5.4G Avail) of 191G
- Interface Status Interface 'Ethernet1/2' is not receiving any packets
Interface 'Ethernet1/3' is not receiving any packets
Interface 'Ethernet1/4' is not receiving any packets

HA Notifications

Step 4. Historical Failover Events

The FMC provides a way to visualize failover events that occurred in the past. In order to filter the events, navigate to System > Health > Events > Edit Search and specify the **Module Name** as **Cluster/Failover Status**. Additionally, the filter can be applied based on the Status.

This image shows how to filter failover events:

General Information

Module Name	<input type="text" value="Cluster/Failover Status"/>	Disk Status, Interface Status
Value	<input type="text" value="25"/>	25
Description	<input type="text"/>	Sample Description
Units	<input type="text"/>	unit
Status	<input type="text" value="Warning"/>	Critical, Warning, Normal, Recovered
Device	<input type="text"/>	device1.example.com, *.example.com, 192.168.1.3

Failover filter messages

You can adjust the time settings in order to display the events for a specific date and time. In order to modify the time settings, navigate to System > Health > Events > Time.

This image shows how to edit the time settings:

The screenshot shows the Firewall Management Center interface. A modal window titled "Health Monitoring Time Window" is open, allowing users to adjust the time range for health events. The "Expanding Time Window" dropdown is selected. The "Start Time" is set to 2023-09-27 11:02 and the "End Time" is set to 2023-09-28 11:14. The "Presets" section shows "1 day" selected. The background table shows multiple rows of "Cluster/Failover Status" events for device 10.82.141.171.

Time filter

Once the events have been identified, in order to confirm the reason for the event, point the cursor under Description.

This image shows how the reason for the failover can be seen.

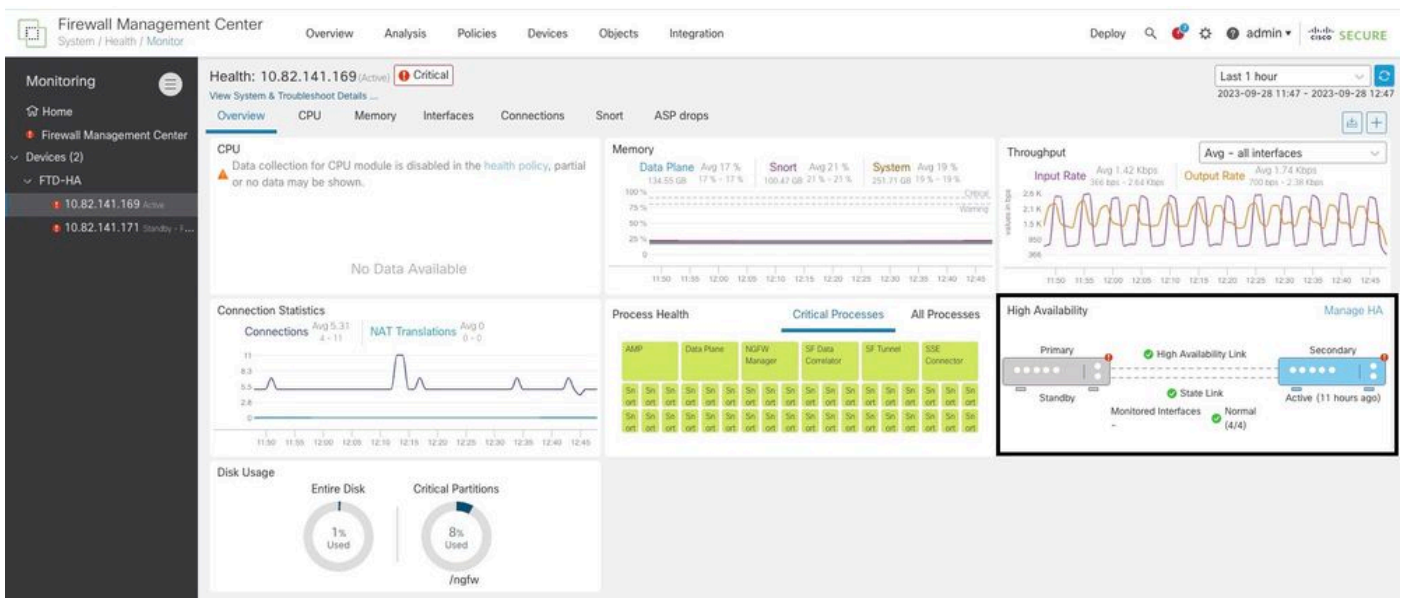
The screenshot shows the Firewall Management Center interface. A table of health events is displayed. The "Description" column is highlighted, showing the reason for the failover: "PRIMARY (FLM19389LQR) FAILOVER_STATE_STANDBY_FAIL...". The "Status" column shows a warning icon.

Step 5. High Availability Dashboard

Another way to monitor the failover can be found under System > Health Monitor > Select Active or Standby Unit.

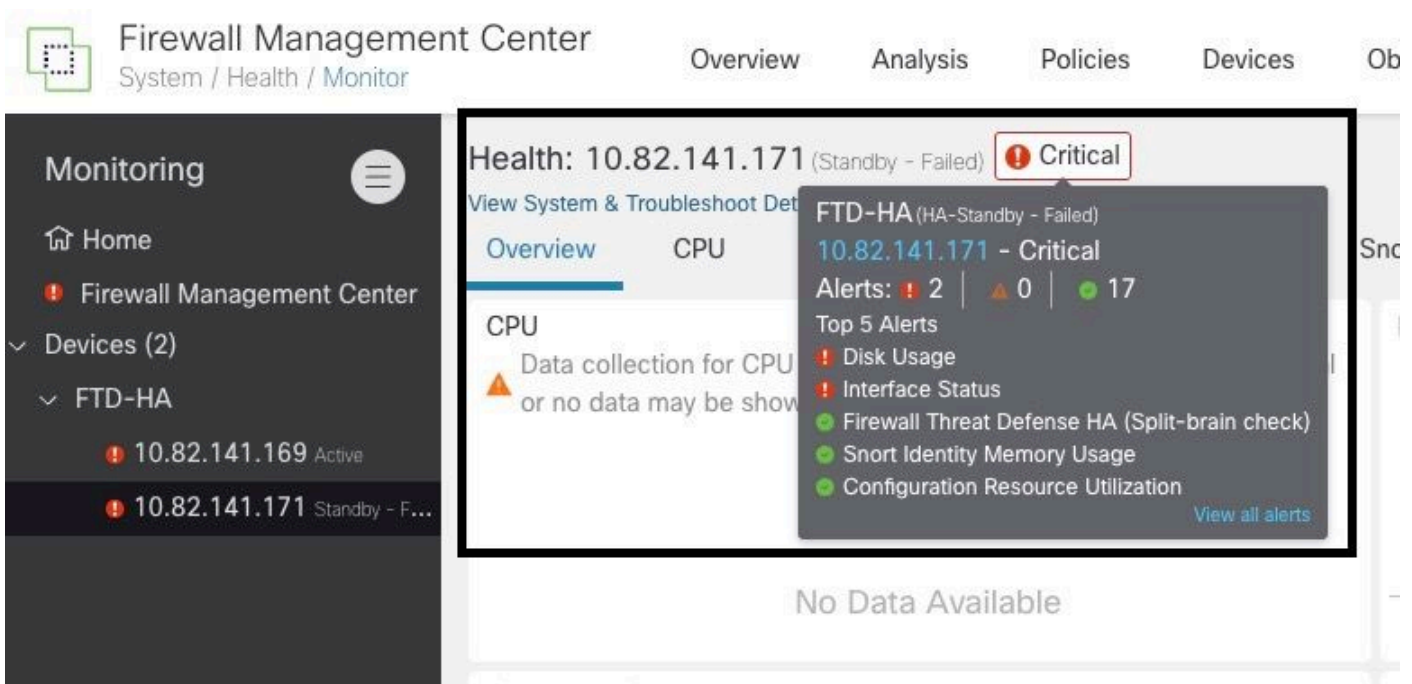
The HA monitor provides information about the status of the HA and State Link, Monitored Interfaces, ROL, and the status of the alerts on each unit.

This image shows the HA Monitor:



Health graphics

In order to visualize the alerts, navigate to System > Health Monitor > Select Active or Standby Unit > Select the Alerts.



Alerts

In order to get more details of the alerts, choose View all alerts > see more.

This image shows the disk status that caused the failover:

Health Alerts - 10.82.141.171

19 total 2 critical 0 warnings 7 normal Export Run All

Sep 28, 2023 12:47 PM

Disk Usage
/ngfw using 98%: 186G (5.4G Avail) of 191G see less

Local Disk Partition Status

Mount	Size	Free	Used	Percent
/mnt/boot	7.5G	7.3G	208M	3%
/opt/cisco/config	1.9G	1.8G	3.4M	1%
/opt/cisco/platform/logs	4.6G	4.3G	19M	1%
/var/data/cores	46G	43G	823M	2%
/opt/cisco/csp	684G	498G	187G	28%
/ngfw	191G	5.4G	186G	98%

Interface Status
Interface 'Ethernet1/2' is not receiving any packets
Interface 'Ethernet1/3' is not receiving any packets
Interface 'Ethernet1/4' is not receiving any packets see more

Appliance Heartbeat
All appliances are sending heartbeats correctly.

Automatic Application Bypass Status

Sep 28, 2023 12:47 PM

alert details

Step 6. Threat Defense CLI

Finally, in order to collect additional information on FMC, you can navigate to Devices > Troubleshoot > Threat Defense CLI. Configure the parameters like Device and the command to be executed and click Execute.

This image shows an example of the command `show failover history` that can be executed on the FMC where you can identify the failure of failover.

Firewall Management Center
 Devices / Troubleshoot / Threat Defense CLI

Overview Analysis Policies **Devices** Objects Integration

Device: 10.82.141.169

Command: show Parameter: failover history

Output

```

other unit has failed
                                due to disk failure

05:28:05 UTC Sep 28 2023
Active Drain                    Active Applying Config  Inspection engine in
other unit has failed
                                due to disk failure

05:28:05 UTC Sep 28 2023
Active Applying Config          Active Config Applied    Inspection engine in
other unit has failed
                                due to disk failure

05:28:05 UTC Sep 28 2023
Active Config Applied           Active                   Inspection engine in
other unit has failed
                                due to disk failure

```

Back Execute

failover history

Related Information

- [High Availability for FTD](#)
- [Configure FTD High Availability on Firepower Appliances](#)
- [Technical Support & Documentation - Cisco Systems](#)