

Identificeren en analyseren van FTD-failover-gebeurtenissen op FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[failover-gebeurtenissen op FMC](#)

[Stap 1. Configuratie van het gezondheidsbeleid](#)

[Stap 2. Beleidstoewijzing](#)

[Stap 3. Waarschuwingen voor failover-gebeurtenissen](#)

[Stap 4. Historische failover-gebeurtenissen](#)

[Stap 5. Dashboard met hoge beschikbaarheid](#)

[Stap 6. Threat Defense CLI](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u failover-gebeurtenissen kunt identificeren en analyseren voor Secure Firewall Threat Defence op Secure Firewall Management Center GUI.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- High Availability (HA) Setup voor Cisco Secure Firewall Threat Defence (FTD)
- Basisbruikbaarheid van Cisco Firewall Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

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

Het VCC is niet alleen het beheercentrum voor FirePOWER-apparaten, naast beheer- en configuratieopties, het biedt ook een grafische interface die logbestanden en gebeurtenissen in real en past helpt analyseren.

Wanneer het spreken over failover, heeft de interface nieuwe verbeteringen die helpen om failover gebeurtenissen te analyseren om de mislukkingen te begrijpen.

failover-gebeurtenissen op FMC

Stap 1. Configuratie van het gezondheidsbeleid

De module Cluster/HA Failure Status is standaard ingeschakeld op het Health Policy, maar daarnaast kunt u de optie Split-brain check inschakelen.

Om de opties voor HA in het gezondheidsbeleid mogelijk te maken, gaat u naar `System > Health > Policy > Firewall Threat Defense Health Policy > High Availability`.

Dit beeld beschrijft de HA-configuratie van het gezondheidsbeleid:

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

Gezondheidsinstellingen voor hoge beschikbaarheid

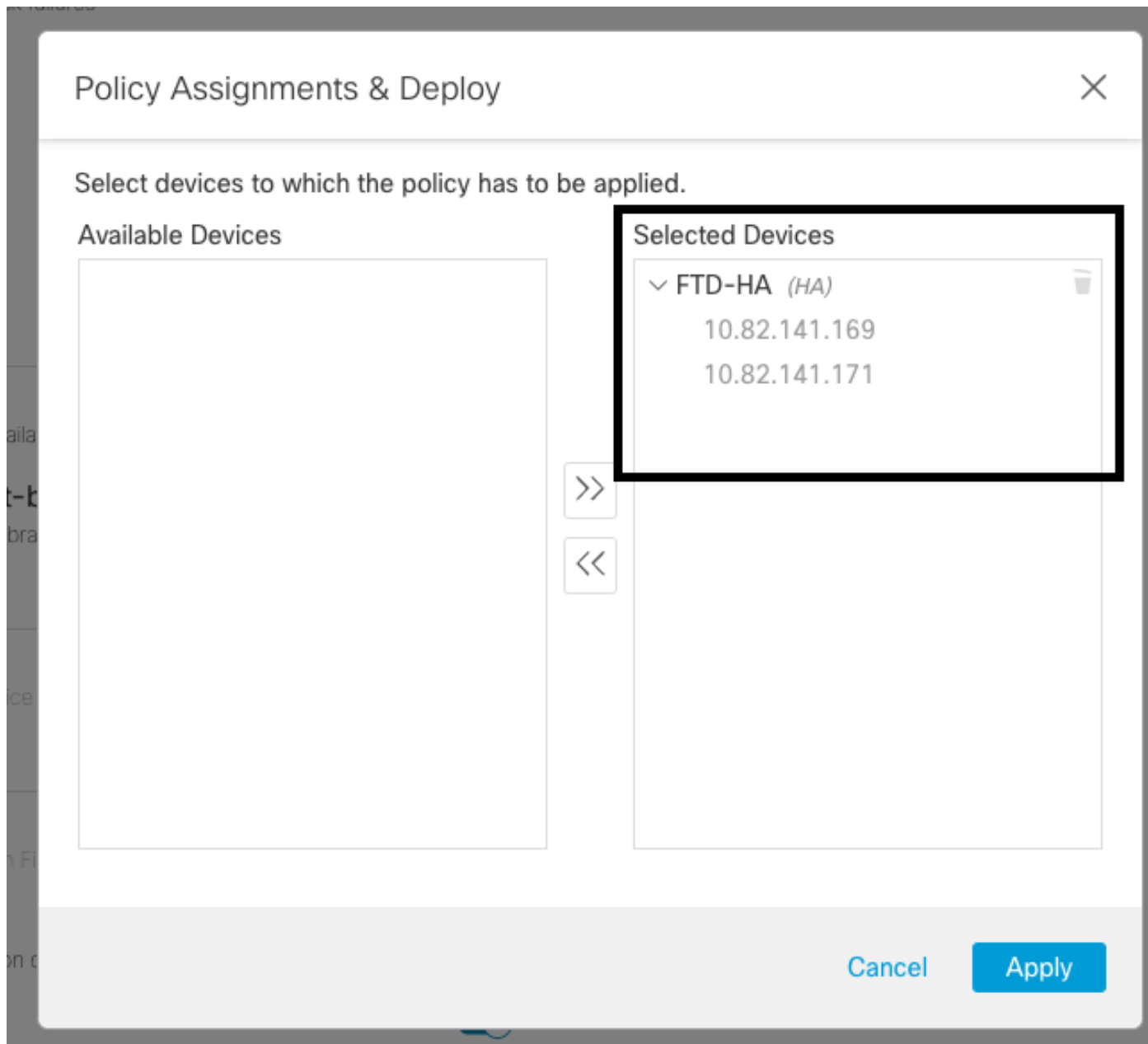
Stap 2. Beleidstoeijzing

Zorg ervoor dat het gezondheidsbeleid is toegewezen aan de HA-paren die u vanaf het VCC wilt

bewaken.

Ga om het beleid toe te wijzen naar System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

Deze afbeelding laat zien hoe het gezondheidsbeleid aan het HA-paar kan worden toegewezen:



Toewijzing HA

Zodra het beleid is toegewezen en opgeslagen, past het VCC het automatisch toe op het FTD.

Stap 3. Waarschuwingen voor failover-gebeurtenissen

Afhankelijk van de configuratie van de HA, zodra een failover-gebeurtenis wordt geactiveerd, worden de pop-upwaarschuwingen die de failover-fout beschrijven weergegeven.

Dit beeld toont de gegenereerde failover-waarschuwingen:

Devices Objects Integration Deploy 🔍 ⚙️ 🔔 admin | cisco SECURE

t 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

Waarschuwingen voor failover

U kunt ook navigeren naar [Notifications > Health](#) om de failover-gezondheidswaarschuwingen te visualiseren.

Dit beeld toont de failover waarschuwingen onder meldingen:

Firewall Management Center 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)

Collaps 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-meldingen

Stap 4. Historische failover-gebeurtenissen

Het VCC biedt een manier om de failover-gebeurtenissen in het verleden te visualiseren. Om de gebeurtenissen te filteren, navigeer naar [System > Health > Events > Edit Search](#) en specificeer de modulenaam als Cluster/failover-status. Bovendien kan het filter worden toegepast op basis van de status.

Dit beeld toont hoe failover-gebeurtenissen te filteren:

General Information

Module Name	<input type="text" value="Cluster/Failover Status"/>	Disk Status, Interface Status
Value	<input type="text"/>	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

Berichten over failover-filters

U kunt de tijdstellingen aanpassen om de gebeurtenissen voor een bepaalde datum en tijd weer te geven. Als u de tijdstellingen wilt wijzigen, navigeert u naar System > Health > Events > Time.

Deze afbeelding toont hoe u de tijdstellingen kunt bewerken:

The screenshot shows the Firewall Management Center interface. The main content area displays a 'Table View of Health Events' with a list of events for 'Cluster/Failover Status'. A modal window titled 'Health Monitoring Time Window' is open, allowing the user to adjust the time range for the 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' list includes options like '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month'. The 'Current' preset is 'Day'. The 'Last' preset is '1 hour'. The 'Events Time Window' is selected. The 'Table View of Health Events' shows a list of events for 'Cluster/Failover Status' with columns for 'Module Name X', 'Test Name X', 'Status X', and 'Device X'.

Tijdfilter

Zodra de gebeurtenissen zijn geïdentificeerd, om de reden voor de gebeurtenis te bevestigen, richt de cursor onder Beschrijving.

Dit beeld toont hoe de reden voor failover kan worden gezien.

Module Name X	Test Name X	Time X	Description X	Value X	Units X	Status X	Device X
Cluster/Failover Status	Cluster/Failover Status	2023-09-28 11:41:52	PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAIL... PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-)).	0		🚨	10.82.141.171

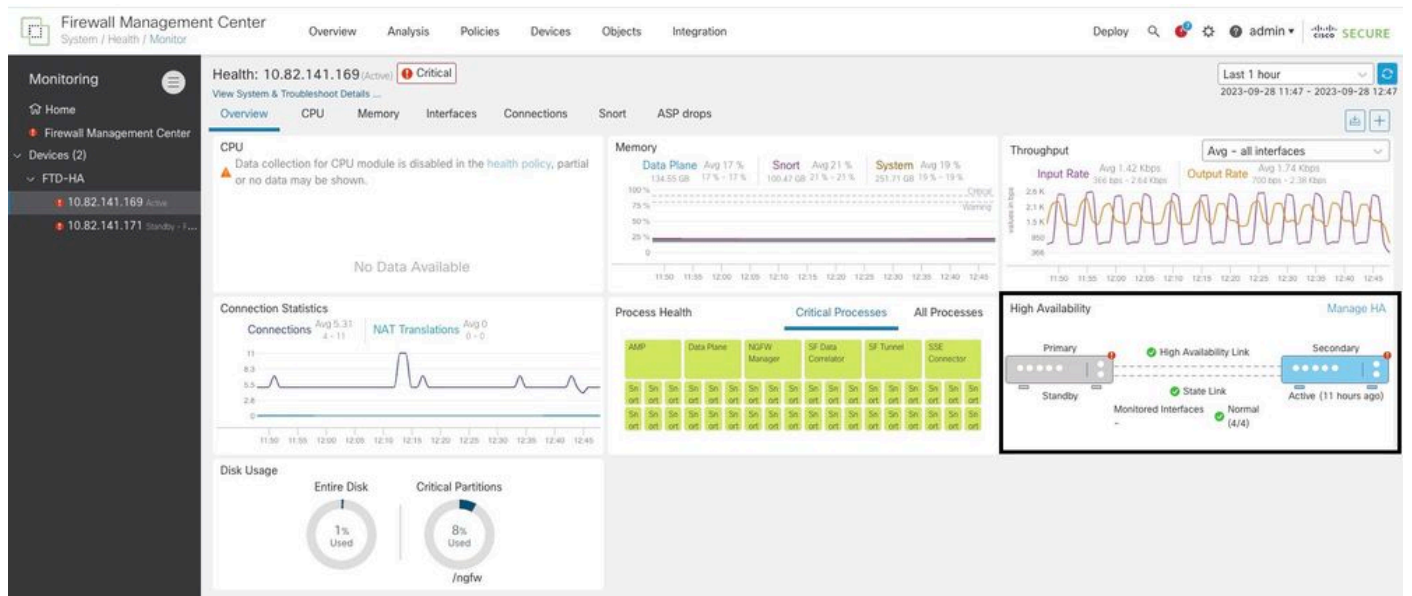
failover-gegevens

Stap 5. Dashboard met hoge beschikbaarheid

Een andere manier om de failover te bewaken is te vinden onder System > Health Monitor > Select Active or Standby Unit.

De HA-monitor biedt informatie over de status van de HA en State Link, bewaakte interfaces, ROL en de status van de waarschuwingen op elke eenheid.

Deze afbeelding toont de HA-monitor:



Afbeeldingen over gezondheid

Blader naar om de waarschuwingen te visualiseren. System > Health Monitor > Select Active or Standby Unit > Select the Alerts.

Firewall Management Center
System / Health / Monitor

Overview Analysis Policies Devices Ob

Monitoring

- Home
- Firewall Management Center
- Devices (2)
 - FTD-HA
 - 10.82.141.169 Active
 - 10.82.141.171 Standby - F...

Health: 10.82.141.171 (Standby - Failed) **Critical**

View System & Troubleshoot Det

Overview CPU

CPU

Data collection for CPU or no data may be show

FTD-HA (HA-Standby - Failed)
10.82.141.171 - Critical
Alerts: 2 | 0 | 17

Top 5 Alerts

- Disk Usage
- Interface Status
- Firewall Threat Defense HA (Split-brain check)
- Snort Identity Memory Usage
- Configuration Resource Utilization

[View all alerts](#)

No Data Available

Waarschuwing

Kies voor meer informatie over de waarschuwingen [View all alerts > see more.](#)

Dit beeld toont de diskstatus die de failover heeft veroorzaakt:

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 Runas Status

Sep 28, 2023 12:47 PM

Stap 6. Threat Defense CLI

Ten slotte kunt u voor het verzamelen van aanvullende informatie over VCC navigeren naar **Devices** > **Troubleshoot** > **Threat Defense CLI**. Configureer de parameters zoals **Apparaat** en de opdracht die moet worden uitgevoerd en klik **Execute**.

Deze afbeelding toont een voorbeeld van de opdracht `show failover history` die kunnen worden uitgevoerd op het VCC waar u de storing van failover kunt vaststellen.

The screenshot shows the Firewall Management Center interface. The breadcrumb navigation is **Devices / Troubleshoot / Threat Defense CLI**. The main navigation tabs are **Overview**, **Analysis**, **Policies**, **Devices**, **Objects**, and **Integration**. The **Devices** tab is selected.

The configuration section shows:

- Device:** 10.82.141.169
- Command:** show
- Parameter:** failover history

The **Output** section displays the following text:

```

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
    
```

At the bottom of the configuration area, there are **Back** and **Execute** buttons.

failover-geschiedenis

Gerelateerde informatie

- [Hoge beschikbaarheid voor FTD](#)
- [Hoge beschikbaarheid van FTD op Firepower-applicaties configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.