

Begrijp de Berichten van de failoverstatus voor FTD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Statusberichten voor failover](#)

[Use Case - Data Link Down zonder failover](#)

[Use Case - Interface Health Failure](#)

[Use Case - gebruik op hoge schijf](#)

[Use Case - Lina Traceback](#)

[Use Case - Sort Instance Down](#)

[Use Case - hardware- of stroomuitval](#)

[Use Case - MIO-hartslagfalen \(hardwareapparaten\)](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de statusberichten van failover kunt begrijpen op Secure Firewall Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- High Availability (HA) Setup voor Cisco Secure 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

Overzicht van failover-gezondheidsbewaking:

Het FTD-apparaat bewaakt elke eenheid voor de algehele gezondheid en voor de interfacegezondheid. Het FTD voert tests uit om de status van elke eenheid te bepalen op basis van unit Health Monitoring and Interface Monitoring. Wanneer een test om de staat van elke eenheid in het HA-paar te bepalen mislukt, worden gebeurtenissen van failover geactiveerd.

Statusberichten voor failover

Use Case - Data Link Down zonder failover

Als de interface monitoring niet is ingeschakeld op de FTD HA en in het geval van een datalinkfout, wordt een failover-gebeurtenis niet geactiveerd omdat de tests van de gezondheidsmonitor voor de interfaces niet worden uitgevoerd.

In dit beeld worden de waarschuwingen voor een datalinkfout beschreven, maar er worden geen failover-waarschuwingen geactiveerd.

The screenshot shows the Cisco Secure FTD management console interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, notifications (with a red '2'), settings, help, and a user profile for 'admin'. Below the navigation, there are status indicators: 'normal (2)', 'Deployment Pending (1)', and 'Upgrade (0)'. A notification box is highlighted with a red border, containing the text: 'Dismiss all notifications', 'Interface Status - 10.82.141.171', and 'Interface 'Ethernet1/3' is not receiving any packets. Interface 'Ethernet1/3' has no link'. Below the notification, there is a table with columns: Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The table contains two rows of device information.

Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:4 Security Module - 1	Essentials, IPS (2 more...)	FTD HA	🔄
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.c Security Module - 1	Essentials, IPS (2 more...)	FTD HA	🔄

waarschuwing voor link omlaag

Gebruik deze opdracht om de status en de status van de datalink te controleren:

- show failover - Hier wordt de informatie weergegeven over de failover-status van elke eenheid en interface.

Monitored Interfaces 1 of 1291 maximum

```
...
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Waiting)
Interface INSIDE (172.16.10.1): No Link (Not-Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Waiting)
Interface INSIDE (172.16.10.2): Normal (Waiting)
Interface OUTSIDE (192.168.20.2): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
```

Wanneer de status van de interface 'Waiting' is, betekent dit dat de interface omhoog is, maar nog geen hello pakket heeft ontvangen van de betreffende interface op de peer unit.

Aan de andere kant betekent de staat 'No Link (Not-Monitored)' dat de fysieke link voor de interface is uitgeschakeld, maar niet wordt gecontroleerd door het failoverproces.

Om een stroomonderbreking te voorkomen, wordt ten zeerste aanbevolen de Interface Health Monitor in te schakelen voor alle gevoelige interfaces met de bijbehorende standby IP-adressen.

Om interfacebewaking in te schakelen, navigeer naar [Device > Device Management > High Availability > Monitored Interfaces](#).

Dit beeld toont het tabblad Gemonitorde interfaces:

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
DMZ	192.168.10.1	192.168.10.2				 
OUTSIDE	192.168.20.1	192.168.20.2				 
diagnostic						 
INSIDE	172.16.10.1	172.16.10.2				 

bewaakte interfaces

Om de status van de bewaakte interfaces en de standby IP-adressen te controleren, voert u deze opdracht uit:

- `show failover` - Hier wordt de informatie weergegeven over de failover-status van elke eenheid en interface.

Monitored Interfaces 3 of 1291 maximum

```
...
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Monitored)
```

```

Interface INSIDE (172.16.10.1): No Link (Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Monitored)
Interface INSIDE (172.16.10.2): Normal (Monitored)
Interface OUTSIDE (192.168.20.2): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)

```

Use Case - Interface Health Failure

Wanneer een eenheid gedurende 15 seconden geen hello-berichten op een bewaakte interface ontvangt en als de interfacetest in de ene eenheid mislukt maar in de andere eenheid werkt, wordt de interface geacht mislukt te zijn.

Als aan de drempelwaarde die u definieert voor het aantal mislukte interfaces is voldaan en de actieve eenheid meer mislukte interfaces heeft dan de standby-eenheid, treedt een failover op.

Om de interfacedrempel te wijzigen, navigeer aan [Devices > Device Management > High Availability > Failover Trigger Criteria](#).

In dit beeld worden de waarschuwingen beschreven die bij een interfacestoornis zijn gegenereerd:

The screenshot shows the Cisco Secure Manager interface with a notification panel open. The notification panel contains three alerts:

- Cluster/Failover Status - 10.82.141.169**: A warning alert with a yellow triangle icon. The text includes: SECONDARY (FLM1946BCEX), FAILOVER_STATE_STANDBY_FAILED (Interface check), SECONDARY (FLM1946BCEX), FAILOVER_STATE_STANDBY (Interface check), SECONDARY (FLM1946BCEX), and FAILOVER_STATE_ACTIVE (Other unit wants me).
- Interface Status - 10.82.141.171**: A critical alert with a red 'X' icon. The text reads: Interface 'Ethernet1/4' has no link.
- Cluster/Failover Status - 10.82.141.171**: A warning alert with a yellow triangle icon. The text includes: SECONDARY (FLM1946BCEX), FAILOVER_STATE_STANDBY (Check peer event for reason), SECONDARY (FLM1946BCEX), FAILOVER_STATE_STANDBY (Check peer event for reason), and PRIMARY (FLM19389LQR).

The background shows a table of devices with columns for Model, Version, Chassis, Licenses, and Access Control. Two Firepower 9300 with FTD devices are listed.

failover-gebeurtenis met link down

Gebruik de volgende opdrachten om de reden van de fout te controleren:

- show failover state - Deze opdracht geeft de failover-status van beide eenheden en de laatst gemelde reden voor failover weer.

<#root>

firepower#

show failover state

```
This host - Primary
           Active      Ifc Failure      19:14:54 UTC Sep 26 2023
Other host - Secondary
           Failed      Ifc Failure      19:31:35 UTC Sep 26 2023
                                OUTSIDE: No Link
```

- `show failover history` - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen van de failover-status en de reden voor de wijziging van de status.

<#root>

firepower#

show failover history

```
=====
From State              To State          Reason
=====
19:31:35 UTC Sep 26 2023
Active                  Failed            Interface check
                                This host:1
                                single_vf: OUTSIDE
                                Other host:0
```

Use Case - gebruik op hoge schijf

Als de schijfruimte op de actieve eenheid meer dan 90% vol is, wordt een failover-gebeurtenis geactiveerd.

Dit beeld beschrijft de waarschuwingen die worden gegenereerd wanneer de schijf vol is:

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ admin | SECURE

Normal (2) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (2)

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:44 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.co Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕

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

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 (4.8G Avail) of 191G

failover met schijfgebruik

Gebruik de volgende opdrachten om de reden van de fout te controleren:

- `show failover history` - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen in de failover-status en de reden voor de wijzigingen in de status.

```
<#root>
```

```
firepower#
```

```
show failover history
```

```
=====
From State                To State                Reason
=====
20:17:11 UTC Sep 26 2023
Active                    Standby Ready           Other unit wants me Standby
                          Inspection engine in other unit ha
20:17:11 UTC Sep 26 2023.
Active                    Standby Ready           Failed Detect Inspection engine fa
                          due to disk failure
```

- `show failover` - Geeft de informatie weer over de failoverstatus van elke eenheid.

```
<#root>
```

```
firepower#
```

```
show failover | include host|disk
```

```
This host: Primary - Failed
           slot 2: diskstatus rev (1.0) status (down)
Other host: Secondary - Active
           slot 2: diskstatus rev (1.0) status (up)
```

- `df -h` - Hier wordt de informatie weergegeven over alle gekoppelde bestandssystemen, inclusief totale grootte, gebruikte ruimte, gebruikspercentage en het steunpunt.

```
<#root>
```

```
admin@firepower:/ngfw/Volume/home$
```

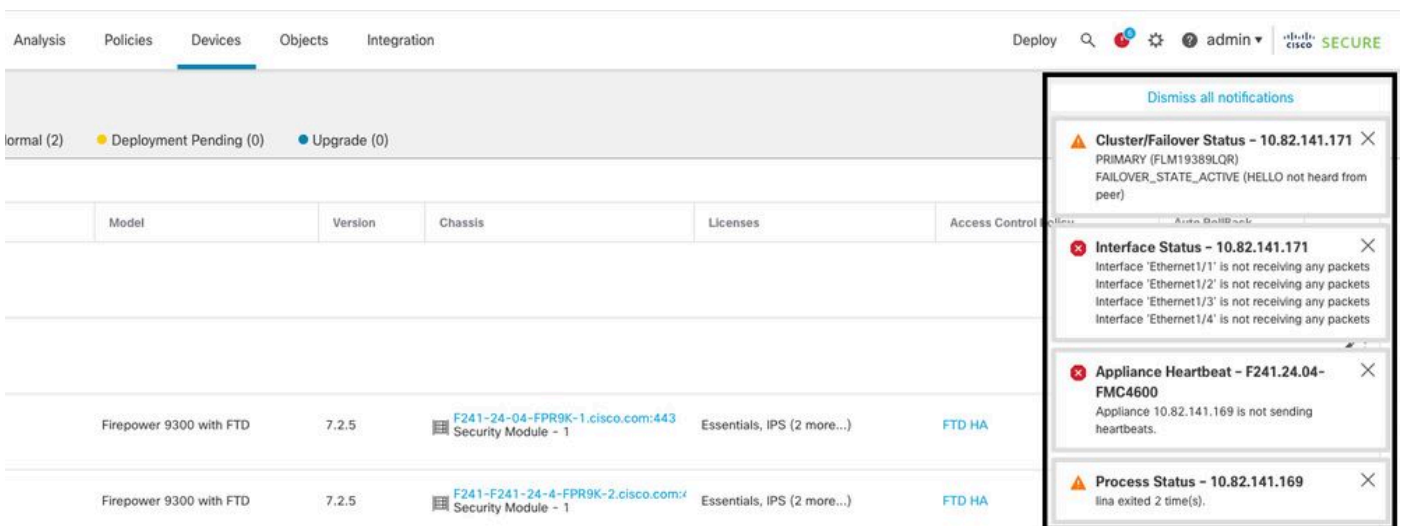
```
df -h /ngfw
```

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda6 191G 186G 4.8G 98% /ngfw
```

Use Case - Lina Traceback

In het geval van een lina traceback, kan een failover gebeurtenis worden geactiveerd.

Dit beeld beschrijft de waarschuwingen die bij lineaire traceback zijn gegenereerd:



failover met lina traceback

Gebruik de volgende opdrachten om de reden van de fout te controleren:

- `show failover history` - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen van de failover-status en de reden voor de statuswijziging.

```
<#root>
```

```
firepower#
```

```
show failover history
```

```
=====
From State          To State          Reason
=====
```

```
8:36:02 UTC Sep 27 2023
```

Standby Ready	Just Active	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Just Active	Active Drain	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Drain	Active Applying Config	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Config Applied	Active	HELLO not heard from peer (failover link up, no response from peer)

In het geval van lina traceback, gebruik deze opdrachten om de kernbestanden te vinden:

```
<#root>
```

```
root@firepower:/opt/cisco/csp/applications#
```

```
cd /var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 29016
```

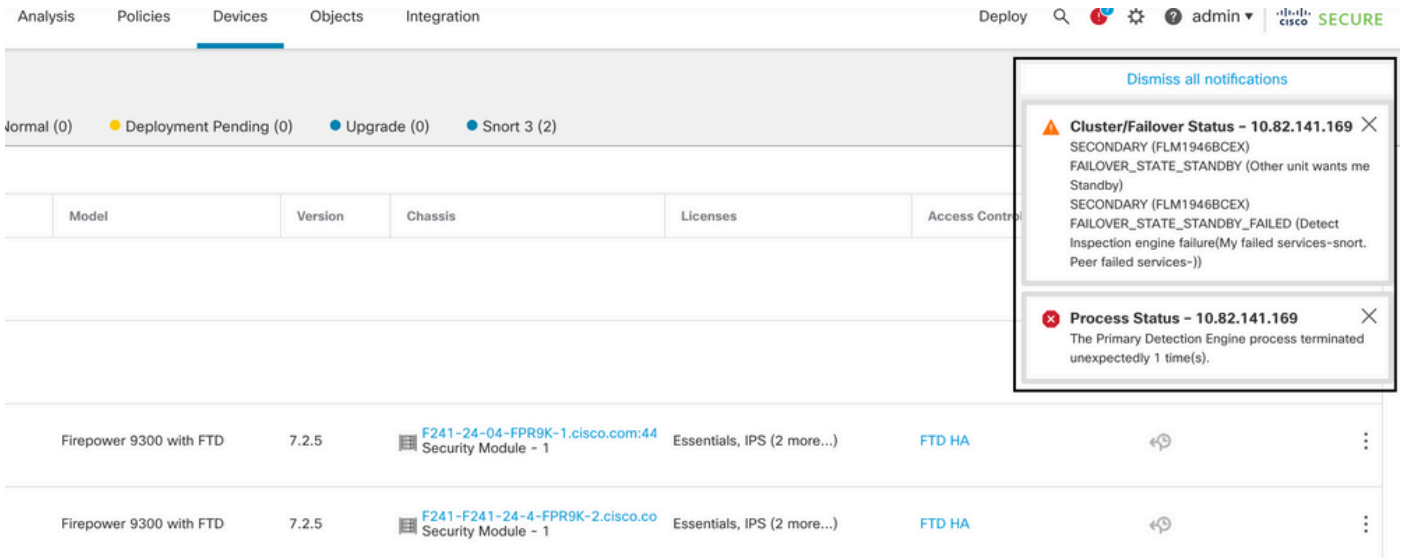
```
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

In het geval van lina traceback, is het sterk aanbevolen om de probleemoplossing bestanden te verzamelen, de Core-bestanden te exporteren en contact op te nemen met Cisco TAC.

Use Case - Sort Instance Down

Als meer dan 50% van de Snort-instanties op de actieve eenheid down zijn, wordt een failover geactiveerd.

In dit beeld worden de waarschuwingen beschreven die zijn gegenereerd bij een mislukte opdracht:



failover met snort traceback

Om controleer de reden voor de fout en gebruik de volgende opdrachten:

- show failover history - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen van de failover-status en de reden voor de statuswijziging.

```
<#root>
```

```
firepower#
```

```
show failover history
```

```
=====
```

From State	To State	Reason
21:22:03 UTC Sep 26 2023 Standby Ready	Just Active	Inspection engine in other unit has failed due to snort failure
21:22:03 UTC Sep 26 2023	Just Active	Active Drain Inspection engine in other unit due to snort failure
21:22:03 UTC Sep 26 2023	Active Drain	Active Applying Config Inspection engine in o due to snort failure
21:22:03 UTC Sep 26 2023	Active	Applying Config Active Config Applied Inspect due to snort failure

- show failover - Hier wordt informatie weergegeven over de failoverstatus van de unit.

```
<#root>
```

```
firepower#
```

```
show failover | include host|snort
```

```
This host: Secondart - Active  
slot 1: snort rev (1.0) status (up)  
Other host: Primary - Failed  
slot 1: snort rev (1.0) status (down)  
Firepower-module1#
```

In het geval van korte traceback, gebruik deze opdrachten om de crashinformatie of kernbestanden te vinden:

```
<#root>
```

```
For snort3:
```

```
root@firepower#
```

```
cd /ngfw/var/log/crashinfo/
```

```
root@firepower:/ngfw/var/log/crashinfo#
```

```
ls -l
```

```
total 4
```

```
-rw-r--r-- 1 root root 1052 Sep 27 17:37 snort3-crashinfo.1695836265.851283
```

```
For snort2:
```

```
root@firepower#
```

```
cd/var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -al
```

```
total 256912
```

```
-rw-r--r-- 1 root root 46087443 Apr 9 13:04 core.snort.24638.1586437471.gz
```

In het geval van snelle traceback, wordt het ten eerste aanbevolen om de probleemoplossing bestanden te verzamelen, de Core-bestanden te exporteren en contact op te nemen met Cisco TAC.

Use Case - hardware- of stroomuitval

Het FTD-apparaat bepaalt de gezondheid van de andere eenheid door de failover-link met hello-berichten te bewaken. Wanneer een eenheid niet drie opeenvolgende hello-berichten op de failover-link ontvangt en de tests op de bewaakte interfaces mislukken, kan een failover-gebeurtenis worden geactiveerd.

In dit beeld worden de waarschuwingen beschreven die worden gegenereerd bij een stroomuitval:

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

Model	Version	Chassis	Licenses	Access Cor
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.cor Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisc Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Interface Status - 10.82.141.171 ✕
Interface 'Ethernet1/1' has no link
Interface 'Ethernet1/2' has no link

Cluster/Failover Status - 10.82.141.171 ✕
CLUSTER_STATE_GENERAL_FAILURE (Failover Stateful link down)
CLUSTER_STATE_GENERAL_FAILURE (Failover LAN link down)
PRIMARY (FLM19389LQR)
FAILOVER_STATE_ACTIVE (HELLO not heard from peer)

failover met stroomuitval

Om controleer de reden voor de fout en gebruik de volgende opdrachten:

- `show failover history` - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen van de failover-status en de reden voor de statuswijziging.

<#root>

firepower#

`show failover history`

```

=====
From State                To State                Reason
=====
22:14:42 UTC Sep 26 2023
Standby Ready            Just Active             HELLO not heard from peer
                           (failover link down)
22:14:42 UTC Sep 26 2023
Just Active              Active Drain            HELLO not heard from peer
                           (failover link down)
22:14:42 UTC Sep 26 2023
Active Drain             Active Applying Config  HELLO not heard from peer
                           (failover link down)
22:14:42 UTC Sep 26 2023
Active Applying Config   Active Config Applied   HELLO not heard from peer
                           (failover link down)
22:14:42 UTC Sep 26 2023
Active Config Applied    Active                  HELLO not heard from peer
                           (failover link down)

```

- `show failover state` - Deze opdracht geeft de failover-status van beide eenheden en de laatst gemelde reden voor failover weer.

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Failed	Comm Failure	22:14:42 UTC Sep 26 2023

Use Case - MIO-hartslagfalen (hardwareapparaten)

De applicatie stuurt periodiek een overstap naar de toezichhouder. Wanneer de hearbeat-responsen niet worden ontvangen, kan een failover-gebeurtenis worden geactiveerd.

Om controleer de reden voor de fout en gebruik de volgende opdrachten:

- `show failover history` - Toont de failover-geschiedenis. De failover geschiedenis toont de wijzigingen van de failover-status en de reden voor de statuswijziging.

<#root>

firepower#

show failover history

```
=====
From State                To State                Reason
=====
02:35:08 UTC Sep 26 2023
Active                    Failed                   MIO-blade heartbeat failure
02:35:12 UTC Sep 26 2023
Failed                    Negotiation              MIO-blade heartbeat recovered
.
.
.
02:37:02 UTC Sep 26 2023
Sync File                 System Bulk Sync         Detected an Active mate
02:37:14 UTC Sep 26 2023
Bulk Sync                 Standby Ready            Detected an Active mate
```

Wanneer MIO-hearbeat faalt, is het sterk aanbevolen om de probleemoplossing bestanden te verzamelen, technische logboeken van FXOS te tonen en contact op te nemen met Cisco TAC.

Verzamel voor Firepower 4100/9300 het showtech-support chassis en toon tech-support module.

Verzamel voor FPR1000/2100 en Secure Firewall 3100/4200 het formulier voor technische

ondersteuning van het programma.

Gerelateerde informatie

- [Hoge beschikbaarheid voor FTD](#)
- [Hoge beschikbaarheid van FTD op Firepower-applicaties configureren](#)
- [Procedures voor het genereren van Firepower-bestanden oplossen](#)
- [Video - Hoe kan ik bestanden voor technische ondersteuning genereren op FXOS?](#)
- [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.