

了解FTD的故障切换状态消息

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[故障切换状态消息](#)

[使用案例 — 数据链路断开，无故障切换](#)

[使用案例 — 接口运行状况故障](#)

[使用案例 — 高磁盘使用率](#)

[使用案例 — Lina Traceback](#)

[使用案例 — Snort实例关闭](#)

[使用案例 — 硬件或电源故障](#)

[使用案例 — MIO-Heartbeat故障 \(硬件设备 \)](#)

[相关信息](#)

简介

本文档介绍如何理解安全防火墙威胁防御(FTD)上的故障切换状态消息。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure FTD的高可用性(HA)设置
- 思科防火墙管理中心(FMC)的基本可用性

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FMC v7.2.5
- Cisco Firepower 9300系列v7.2.5

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

故障切换运行状况监控概述：

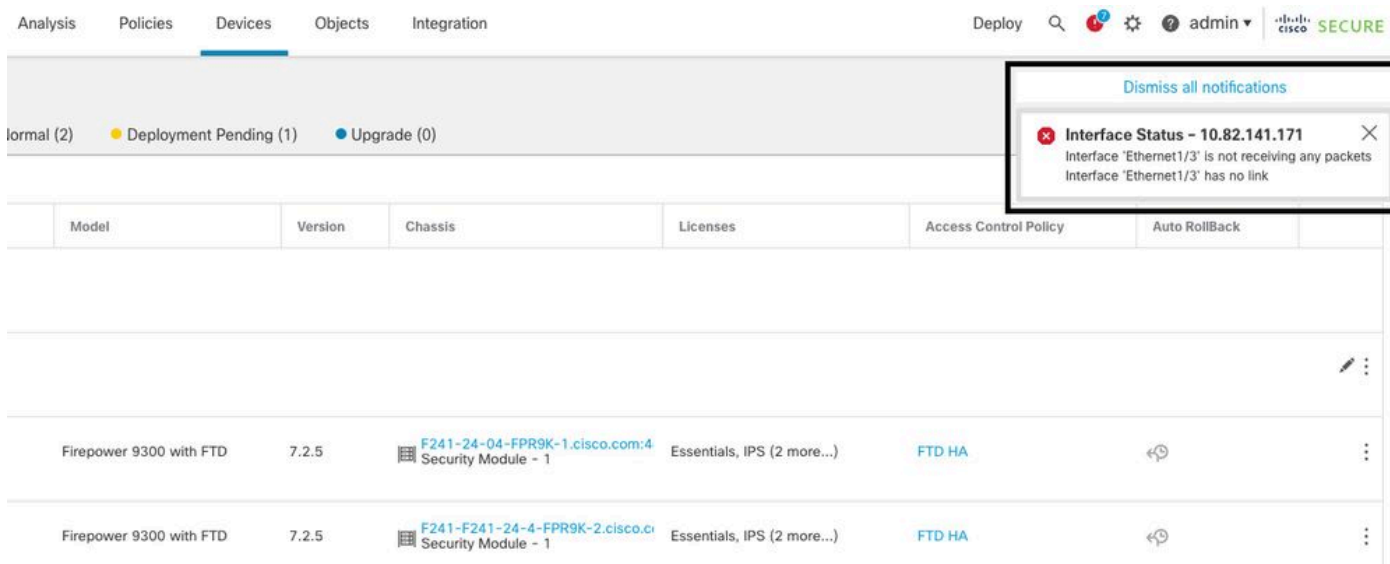
FTD设备监控每台设备的整体运行状况和接口运行状况。FTD执行测试，以便根据设备运行状况监控和接口监控确定每台设备的状态。当用于确定HA对中每台设备状态的测试失败时，会触发故障切换事件。

故障切换状态消息

使用案例 — 数据链路断开，无故障切换

在FTD HA上未启用接口监控时，如果出现数据链路故障，则不会触发故障切换事件，因为未执行接口的运行状况监控测试。

此映像描述数据链路故障警报，但不触发故障转移警报。



The screenshot shows the Cisco Secure Manager 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 dot), 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: 'Interface Status - 10.82.141.171', 'Interface 'Ethernet1/3' is not receiving any packets', and '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 data for Firepower 9300 with FTD devices.

链路关闭警报

要验证数据链路的状态和状态，请使用以下命令：

- show failover — 显示有关每个设备和接口的故障切换状态的信息。

```
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)

```

当接口的状态为“Waiting”时，这意味着接口处于启用状态，但尚未收到来自对等设备上相应接口的hello数据包。

另一方面，状态“No Link(Not-Monitored)”意味着该接口的物理链路已关闭，但故障切换过程未对其进行监控。

为了避免中断，强烈建议在所有敏感接口上启用接口运行状况监控器及其相应的备用IP地址。

要启用接口监控，请导航至Device > Device Management > High Availability > Monitored Interfaces.

此图显示Monitored Interfaces选项卡：

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				● /

监控接口

要验证受监控接口和备用IP地址的状态，请运行以下命令：

- show failover — 显示有关每个设备和接口的故障切换状态的信息。

```

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)

```

使用案例 — 接口运行状况故障

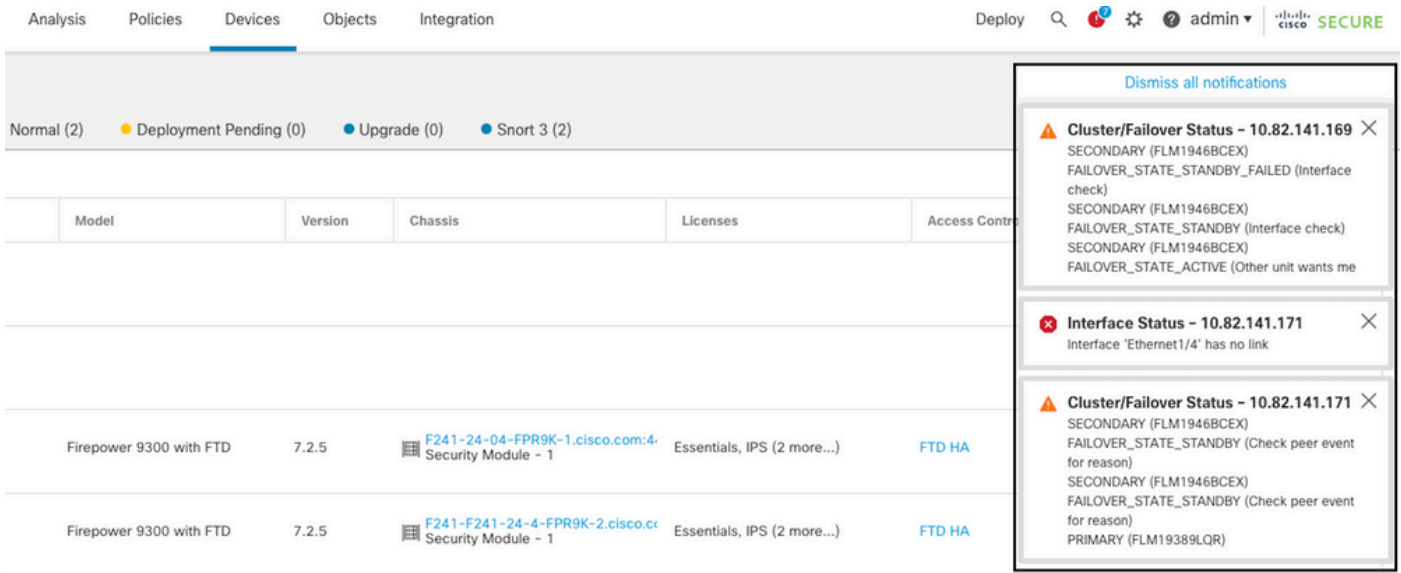
如果设备在受监控接口上未收到hello消息15秒，并且如果一台设备的接口测试失败，但在另一台设

设备上运行，则认为该接口发生故障。

如果达到您为故障接口数量定义的阈值，并且主用设备的故障接口多于备用设备，则会发生故障切换。

要修改接口阈值，请导航至 [Devices > Device Management > High Availability > Failover Trigger Criteria](#)。

此映像描述接口故障时生成的警报：



链路关闭时的故障切换事件

要验证故障原因，请使用以下命令：

- `show failover state` — 此命令显示两个设备的故障切换状态和上次报告的故障切换原因。

```
<#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` — 显示故障切换历史记录。故障切换历史记录显示过去的故障切换状态更改以及状态更改的原因。

```
<#root>
```

```
firepower#
```


20:17:11 UTC Sep 26 2023.
Active

Standby Ready

Failed Detect Inspection engine fa
due to disk failure

- `show failover` — 显示有关每台设备的故障切换状态的信息。

<#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` — 显示所有已装载文件系统的相关信息，包括总大小、已用空间、使用百分比和装载点。

<#root>

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

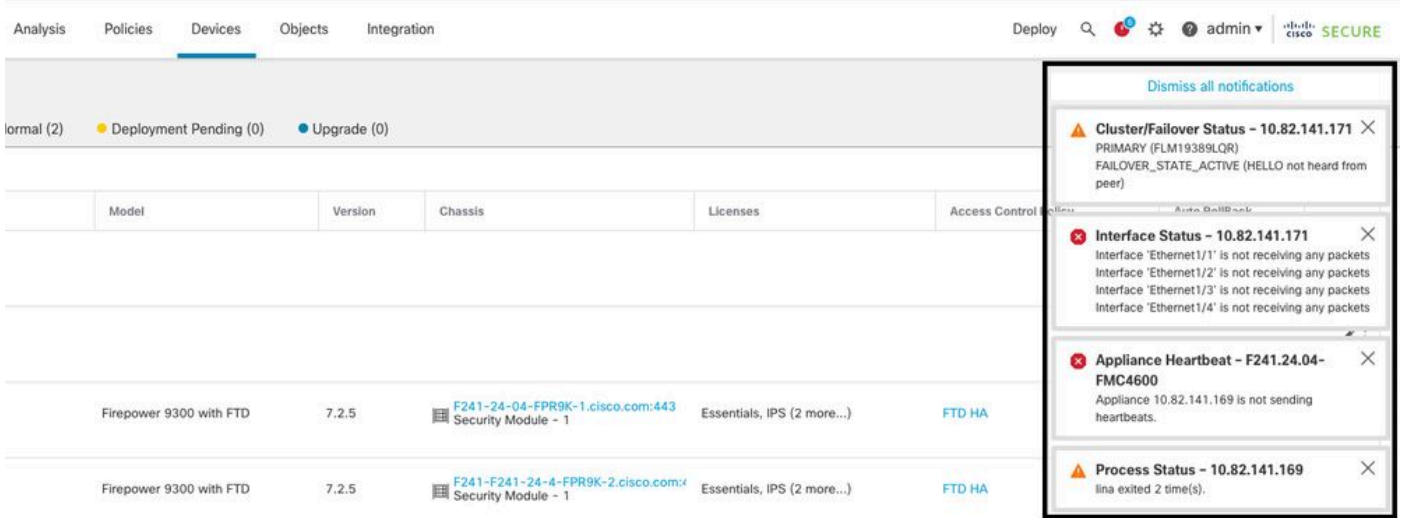
```
df -h /ngfw
```

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

使用案例 — Lina Traceback

如果为lina回溯，可能会触发故障切换事件。

此图像描述在lina traceback情况下生成的警报：



使用lina traceback进行故障切换

要验证故障原因，请使用以下命令：

- show failover history — 显示故障切换历史记录。故障切换历史记录显示过去的故障切换状态更改以及状态更改的原因。

<#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)

```

如果是lina traceback，请使用以下命令查找核心文件：

<#root>

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

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

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

```
ls -l
```

```
total 29016
```

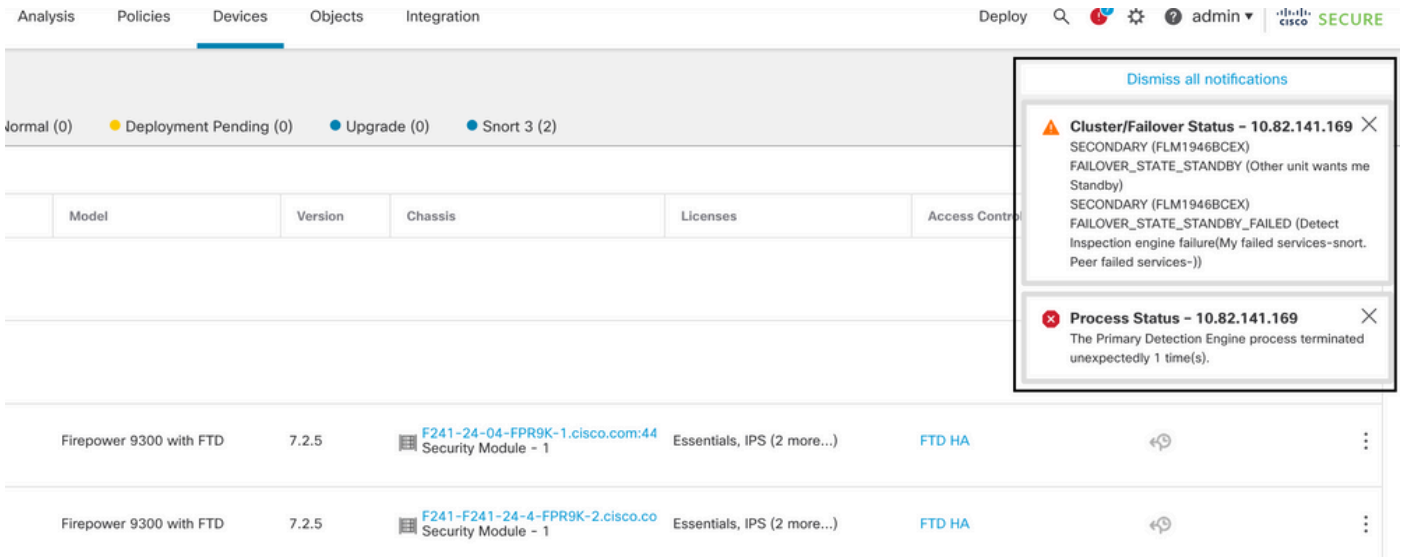
```
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

如果使用lina回溯，强烈建议收集故障排除文件、导出核心文件并联系思科TAC。

使用案例 — Snort实例关闭

如果主用设备上超过50%的Snort实例发生故障，则会触发故障切换。

此映像描述当snort失败时生成的警报：



使用snort回溯进行故障切换

为了验证故障原因，请使用以下命令：

- show failover history — 显示故障切换历史记录。故障切换历史记录显示过去的故障切换状态更改以及状态更改的原因。

```
<#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 due to snort failure
21:22:03 UTC Sep 26 2023	Active	Applying Config Active Config Applied Inspect due to snort failure

- `show failover` — 显示有关设备的故障切换状态的信息。

```
<#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#
```

如果是snort回溯，请使用以下命令查找crashinfo或core文件：

```
<#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

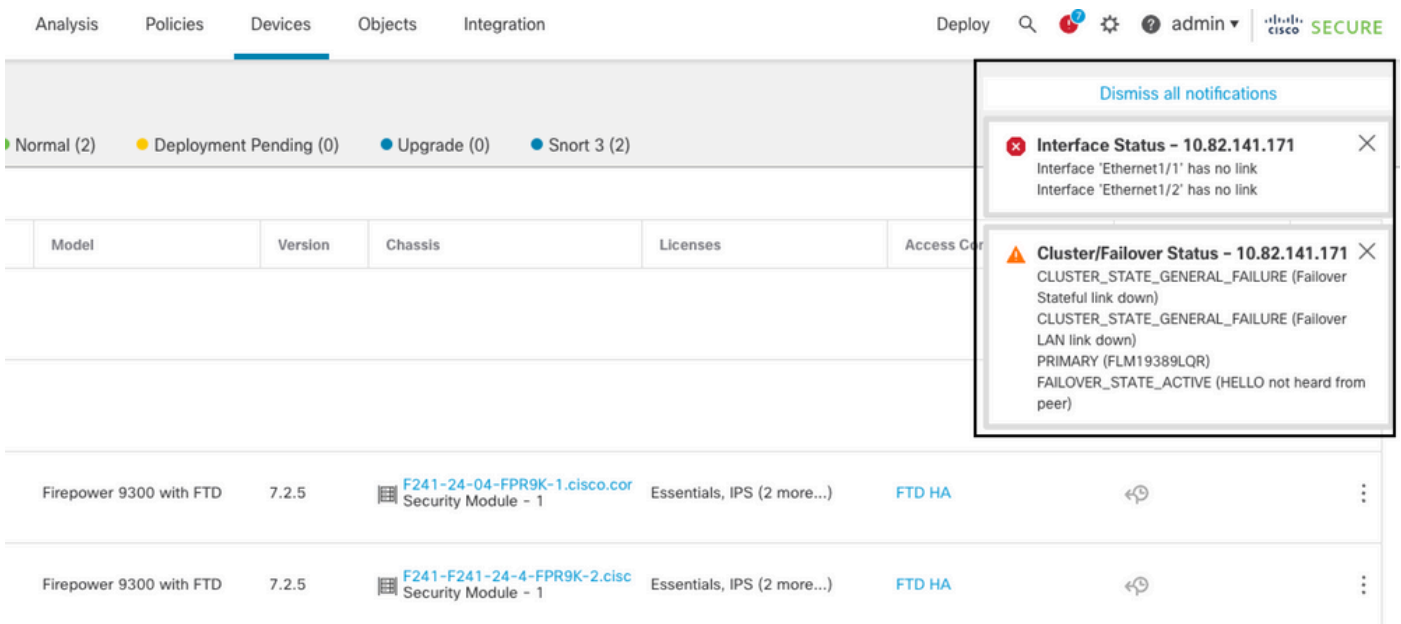
-rw-r--r-- 1 root root 46087443 Apr 9 13:04 core.snort.24638.1586437471.gz

对于snort回溯，强烈建议收集故障排除文件、导出核心文件，并联系思科TAC。

使用案例 — 硬件或电源故障

FTD设备通过使用hello消息监控故障转移链路来确定另一设备的运行状况。当设备在故障切换链路上未收到连续的三条hello消息，并且受监控接口上的测试失败时，可能会触发故障切换事件。

此映像介绍发生电源故障时生成的警报：



发生电源故障时的故障切换

为了验证故障原因，请使用以下命令：

- show failover history — 显示故障切换历史记录。故障切换历史记录显示过去的故障切换状态更改以及状态更改的原因。

<#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` — 此命令显示两个设备的故障切换状态和上次报告的故障切换原因。

```
<#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

使用案例 — MIO-Hearbeat故障 (硬件设备)

应用程序实例定期向主管发送心跳信号。当未收到心跳响应时，可能会触发故障切换事件。

为了验证故障原因，请使用以下命令：

- `show failover history` — 显示故障切换历史记录。故障切换历史记录显示过去的故障切换状态更改以及状态更改的原因。

```
<#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

```

当MIO-heartbeat出现故障时，强烈建议收集故障排除文件，显示FXOS的技术日志，并与思科TAC联系。

对于Firepower 4100/9300，请收集show tech-support chassis和show tech-support module。

对于FPR1000/2100和安全防火墙3100/4200，请收集show tech-support表格。

相关信息

- [FTD的高可用性](#)
- [在 Firepower 设备上配置 FTD 高可用性](#)
- [排除Firepower文件生成过程故障](#)
- [视频 — 如何在FXOS上生成Show Tech-Support文件](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。