

# 识别和分析FMC上的FTD故障切换事件

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[FMC上的故障切换事件](#)

[步骤1:运行状况策略配置](#)

[第二步:策略分配](#)

[第三步:故障切换事件警报](#)

[第四步:历史故障切换事件](#)

[第五步:高可用性控制面板](#)

[第六步:威胁防御CLI](#)

[相关信息](#)

---

## 简介

本文档介绍如何在安全防火墙管理中心GUI上识别和分析安全防火墙威胁防御的故障转移事件。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御(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

FMC不仅是Firepower设备的管理中心，而且除了管理和配置选项之外，它还提供了一个图形界面

，有助于实时和以前分析日志和事件。

当谈到故障切换时，接口有了新的改进，有助于分析故障切换事件以便了解故障。

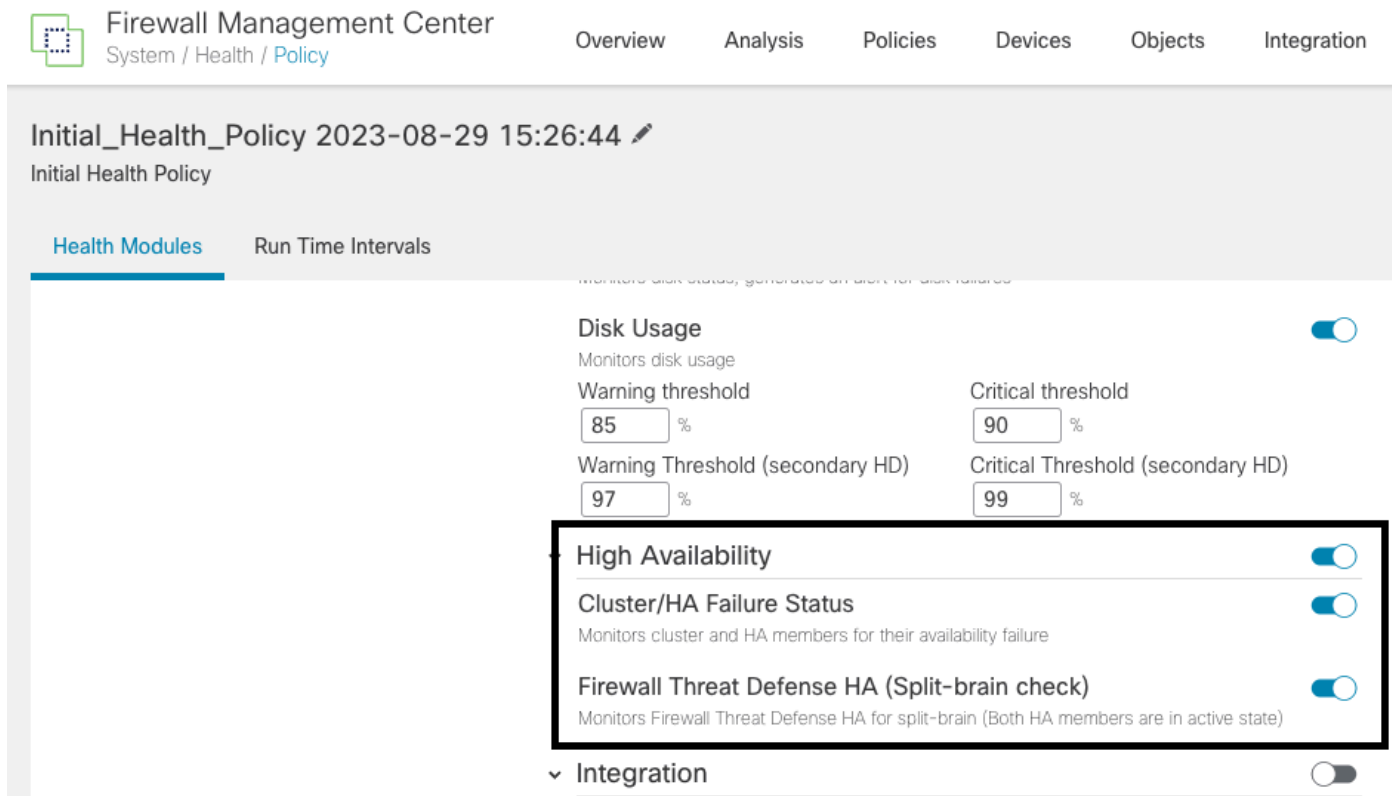
## FMC上的故障切换事件

### 步骤1:运行状况策略配置

默认情况下，模块Cluster/HA Failure Status在Health Policy上启用，但您也可以启用Split-brain检查选项。

要在运行状况策略中启用HA选项，请导航至 System > Health > Policy > Firewall Threat Defense Health Policy > High Availability.

此映像描述运行状况策略的HA配置：



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

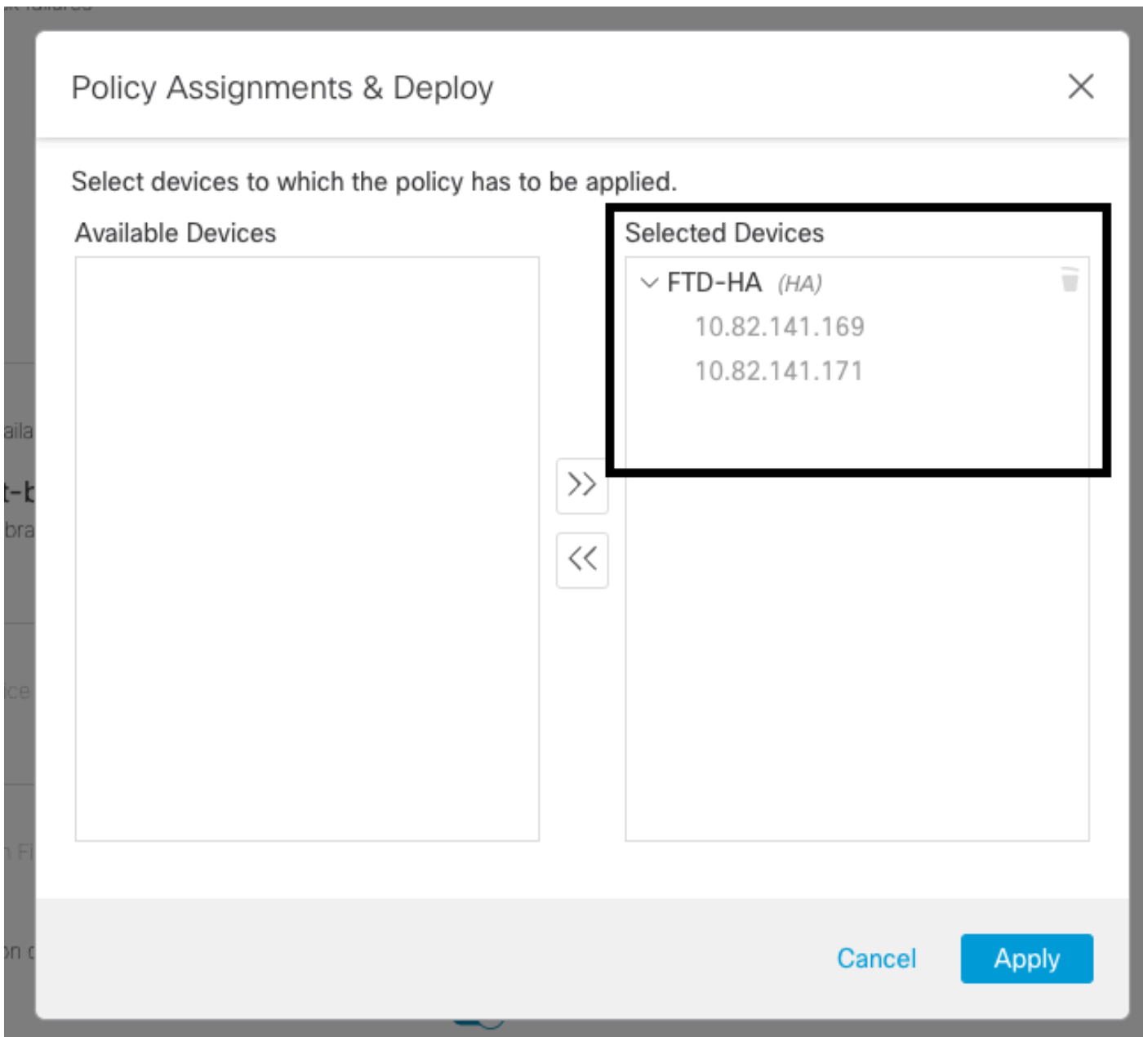
高可用性运行状况设置

### 第二步：策略分配

确保将运行状况策略分配给要从FMC监控的HA对。

要分配策略，请导航至 System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

此图显示如何将运行状况策略分配给HA对：



HA分配

分配并保存策略后，FMC会自动将其应用到FTD。

### 第三步：故障切换事件警报

根据HA的配置，一旦触发了故障切换事件，将显示描述故障切换故障的弹出警报。

下图显示生成的故障切换警报：

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

t Pending (0)    ● Upgrade (0)

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

故障切换警报

您也可以导航至 [Notifications > Health](#) 以便可视化故障切换运行状况警报。

下图显示通知下的故障切换警报：

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

View By: Group

All (2)    ● Error (2)    ● Warning (0)    ● Offline (0)    ● Normal (0)    ● Deployment Pending (0)    ● Upgrade (0)

**Health**    Deployments    Upgrades    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通知

## 第四步：历史故障切换事件

FMC提供了一种可视化过去发生的故障切换事件的方式。要过滤事件，请导航至 [System > Health > Events > Edit Search](#) 并将Module Name指定为Cluster/Failover Status。此外，可以根据状态应用过滤器。

此图显示如何过滤故障切换事件：

## 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 |

故障切换过滤器消息

您可以调整时间设置以显示特定日期和时间的事件。要修改时间设置，请导航至 System > Health > Events > Time.

此图显示如何编辑时间设置：

The screenshot shows the Firewall Management Center interface. The 'Health Monitoring Time Window' dialog is open, allowing users to configure 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 2023-09-28 11:14. The 'Presets' section shows '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month' options. The 'Current' preset is 'Day'. The 'Synchronize with' options are 'Audit Log Time Window' and 'Events Time Window'. The 'Apply' button is highlighted.

时间过滤器

确定事件后，为了确认事件的原因，请将光标指向Description下。

此图显示如何查看故障切换的原因。

The screenshot shows the Firewall Management Center interface. The 'Table View of Health Events' is displayed. The table has columns for Module Name, Test Name, Time, Description, Value, Units, Status, and Device. The 'Description' column is expanded, showing the event details: 'PRIMARY (FLM19389LOR) FAILOVER\_STATE\_STANDBY\_FAIL...' and 'PRIMARY (FLM19389LOR) FAILOVER\_STATE\_STANDBY\_FAILED (Detect inspection engine failure:My failed services-diskstatus. Peer failed services-)).' The 'Status' column shows a warning icon.

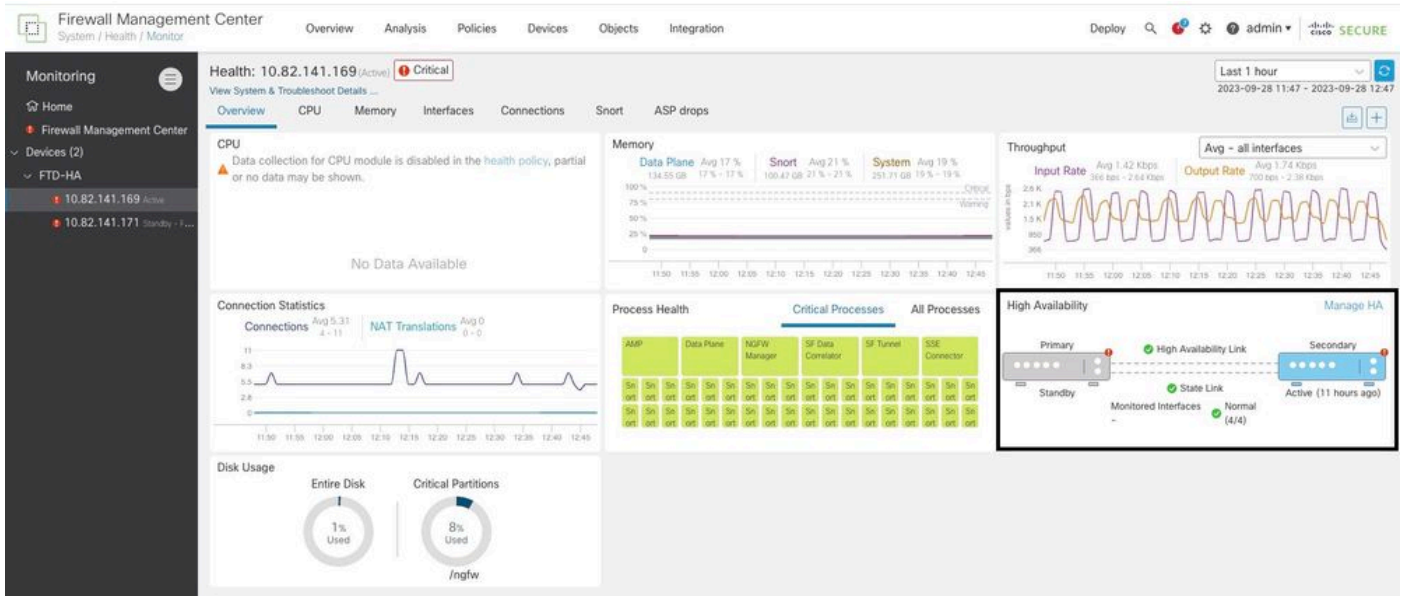
故障切换详细信息

## 第五步：高可用性控制面板

监控故障转移的另一种方法位于 `System > Health Monitor > Select Active or Standby Unit`.

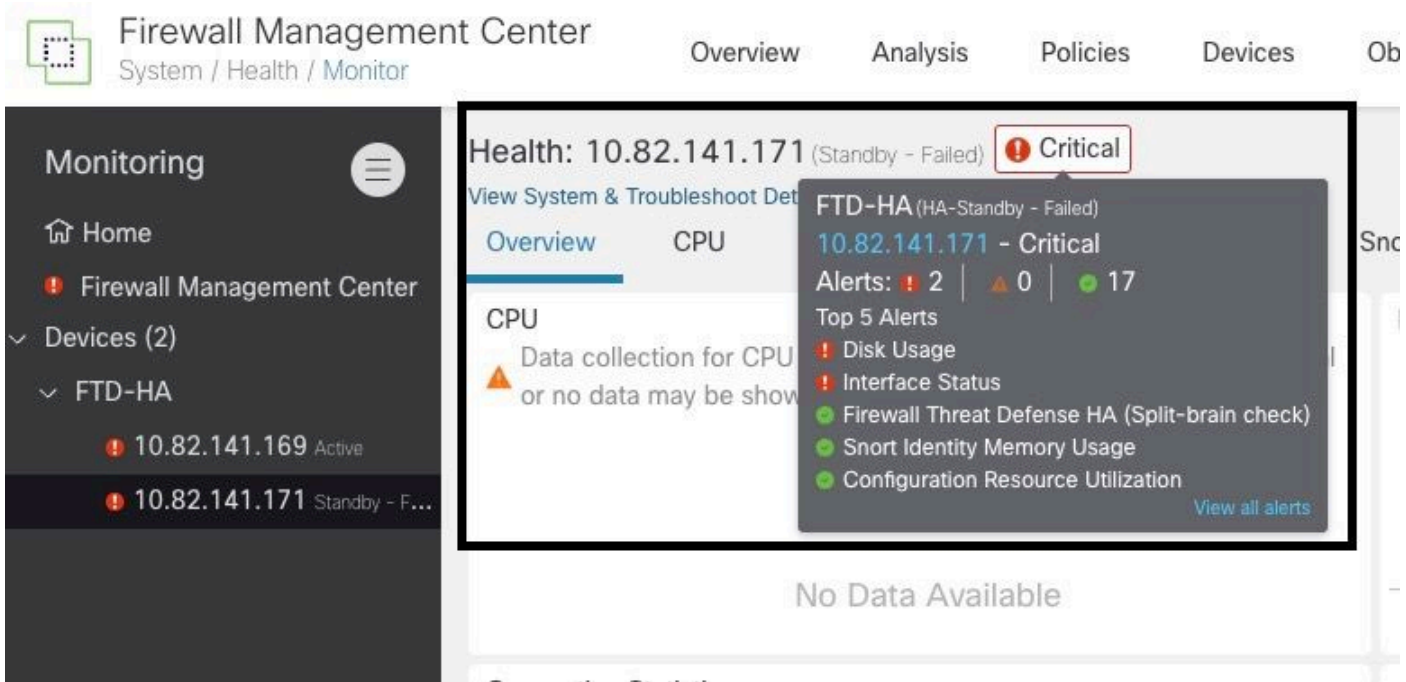
HA监视器提供有关HA和状态链路、受监控接口、ROL的状态以及每台设备上警报状态的信息。

此图显示HA监视器：



运行状况图形

要将警报可视化，请导航至 `System > Health Monitor > Select Active or Standby Unit > Select the Alerts`.



风险通告

要获取警报的更多详细信息，请选择 `View all alerts > see more`.

此映像显示导致故障切换的磁盘状态：

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**      Sep 28, 2023 12:47 PM  
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**      Sep 28, 2023 12:47 PM  
All appliances are sending heartbeats correctly.

**Automatic Application Bypass Status**      Sep 28, 2023 12:47 PM

提示详情

## 第六步：威胁防御CLI

最后，为了收集有关FMC的其他信息，您可以导航至 `Devices > Troubleshoot > Threat Defense CLI`。配置要执行的参数（如设备和命令），然后单击 `Execute`。

下图显示了命令的示例 `show failover history` 可在FMC上执行，您可以在其中识别故障切换故障。

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

故障切换历史记录

## 相关信息

- [FTD的高可用性](#)
- [在 Firepower 设备上配置 FTD 高可用性](#)
- [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）。