

識別和分析FMC上的FTD故障轉移事件

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[FMC上的故障轉移事件](#)

[步驟 1. 運行狀況策略配置](#)

[步驟 2. 策略分配](#)

[步驟 3. 故障轉移事件警報](#)

[步驟 4. 歷史故障轉移事件](#)

[步驟 5. 高可用性儀表板](#)

[步驟 6. 威脅防禦CLI](#)

[相關資訊](#)

簡介

本文檔介紹如何識別和分析安全防火牆管理中心GUI上安全防火牆威脅防禦的故障轉移事件。

必要條件

需求

思科建議您瞭解以下主題：

- 適用於思科安全防火牆威脅防禦(FTD)的高可用性(HA)設定
- 思科防火牆管理中心(FMC)的基本可用性

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FMC不僅是Firepower裝置的管理中心，而且除了管理和配置選項之外，它還提供了一個圖形介面

，有助於即時分析日誌和事件。

當談到故障切換時，介面有了新的改進，有助於分析故障切換事件以瞭解故障。

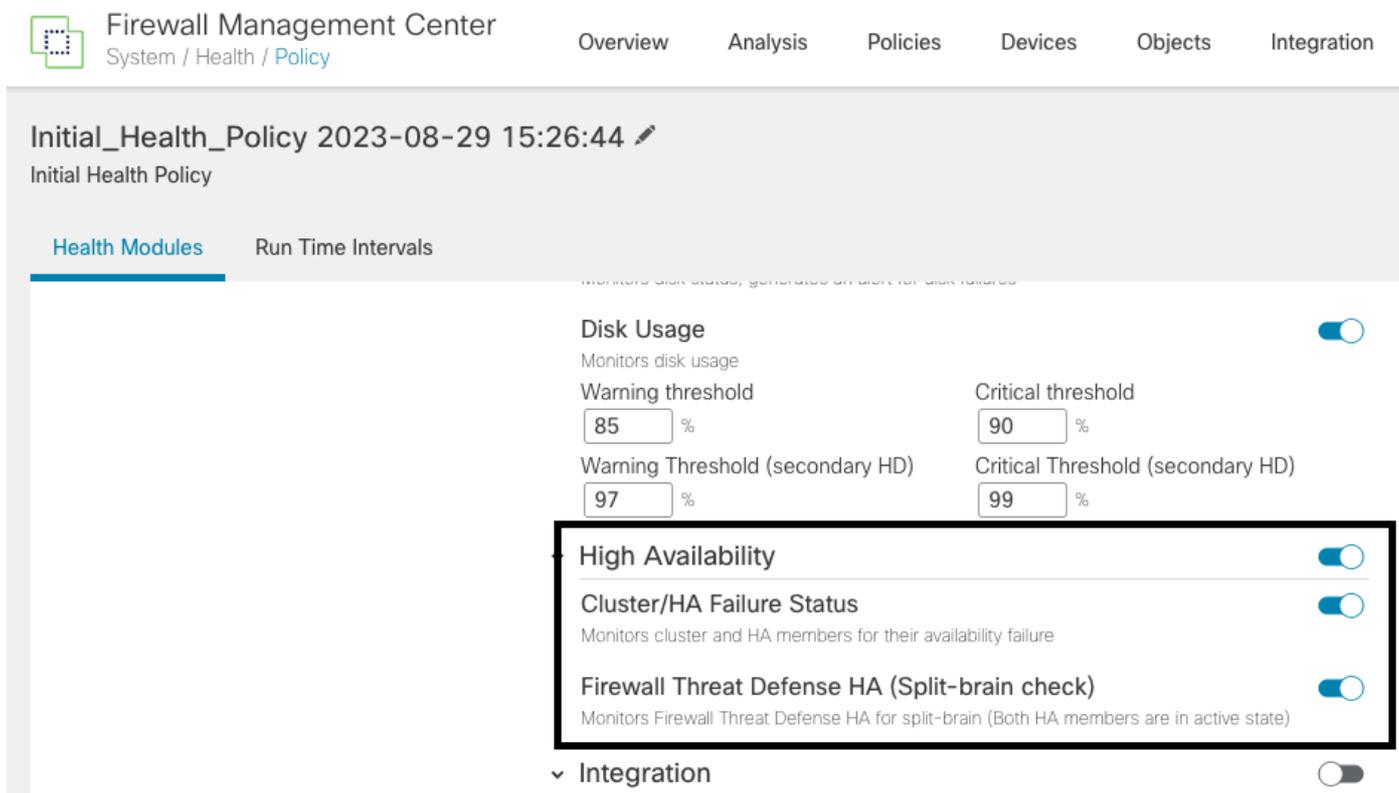
FMC上的故障轉移事件

步驟 1. 運行狀況策略配置

預設情況下，模組集群/HA Failure Status在運行狀況策略上啟用，但您也可以啟用Split-brain檢查選項。

若要啟用運行狀況策略中的HA選項，請導航至 [System > Health > Policy > Firewall Threat Defense Health Policy > High Availability](#)。

此映像描述運行狀況策略的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

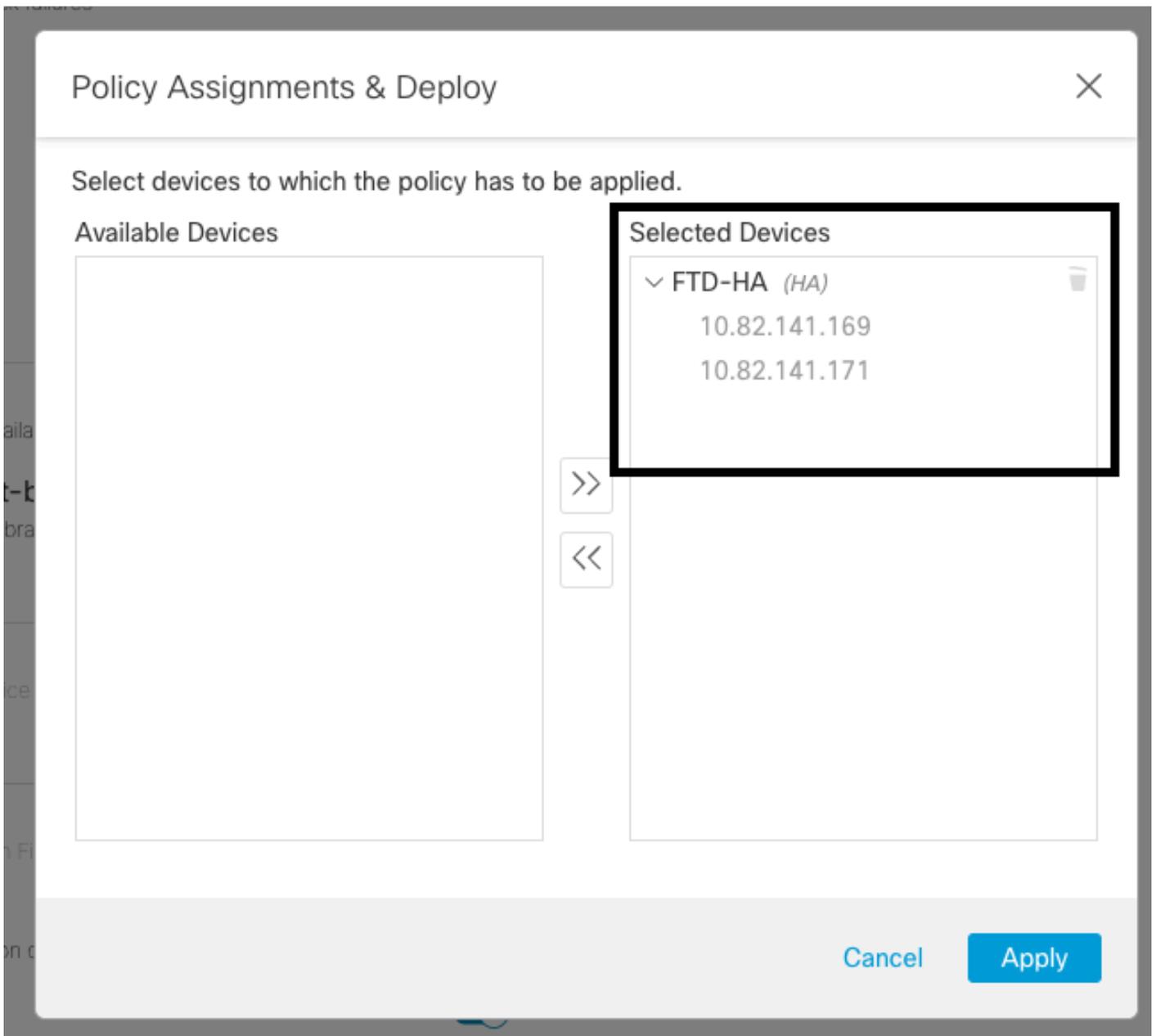
高可用性運行狀況設定

步驟 2. 策略分配

確保將運行狀況策略分配給要從FMC監控的HA對。

要分配策略，請導航至 [System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy](#)。

此圖顯示如何將運行狀況策略分配給HA配對：



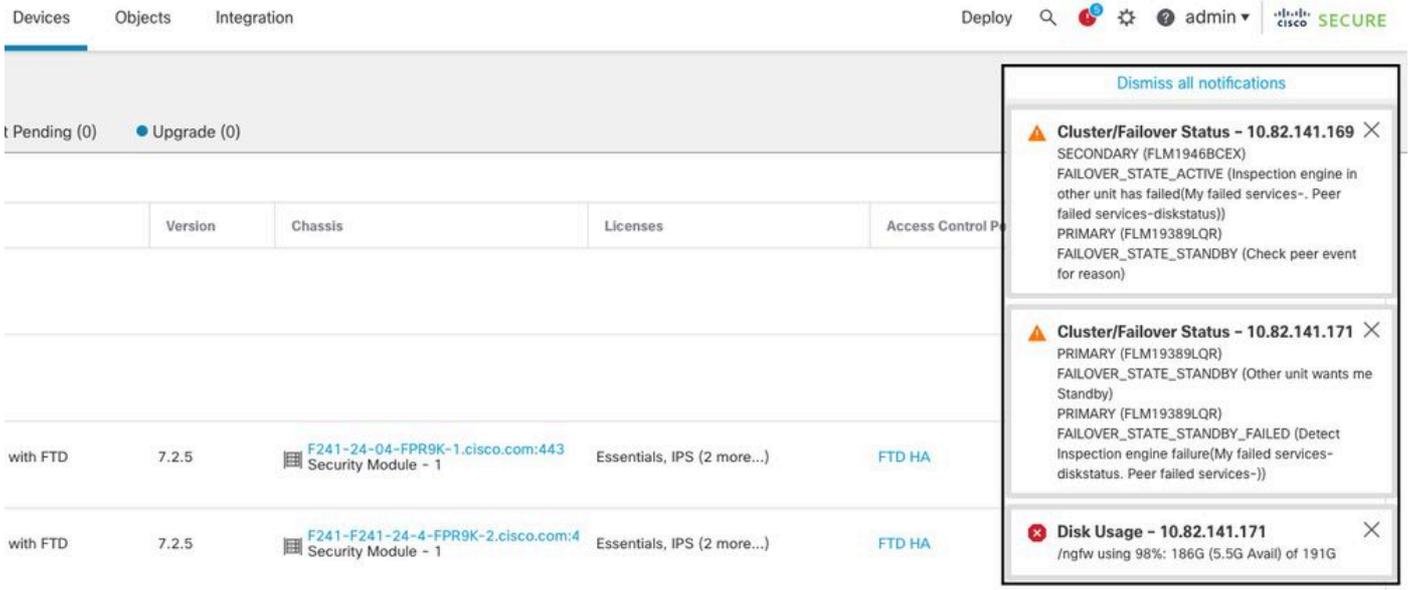
HA分配

分配並儲存策略後，FMC會自動將其應用到FTD。

步驟 3.故障轉移事件警報

根據HA的配置，一旦觸發了故障切換事件，將顯示描述故障切換故障的彈出警報。

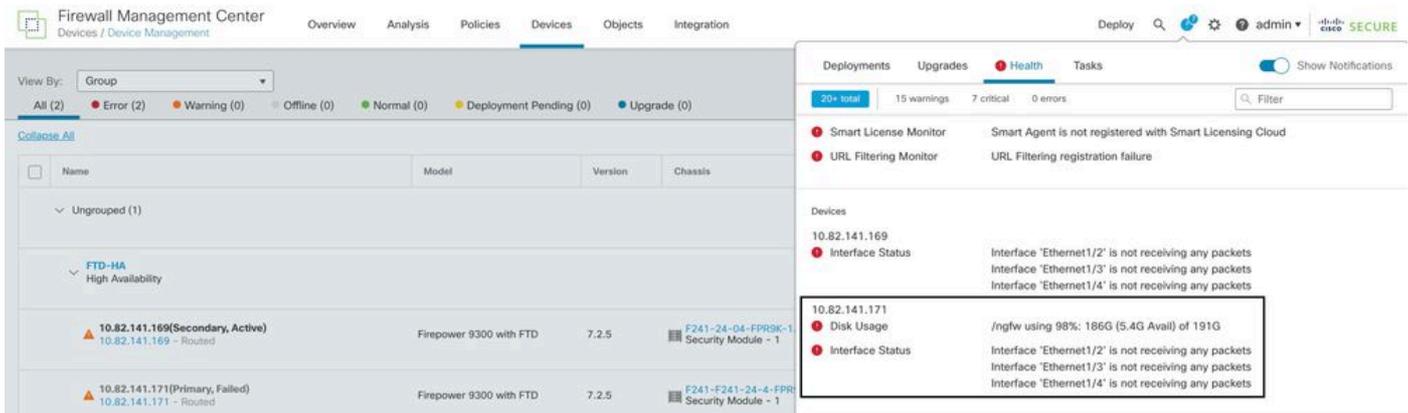
此圖顯示生成的故障切換警報：



故障切換警報

您也可以導航至 [Notifications > Health](#) 以便視覺化故障切換運行狀況警報。

此圖顯示了通知下的故障切換警報：



HA通知

步驟 4. 歷史故障轉移事件

FMC提供了一種顯示過去發生的故障切換事件的方式。要過濾事件，請導航至 [System > Health > Events > Edit Search](#) 並指定Module Name為Cluster/Failover Status。此外，還可以根據狀態應用過濾器。

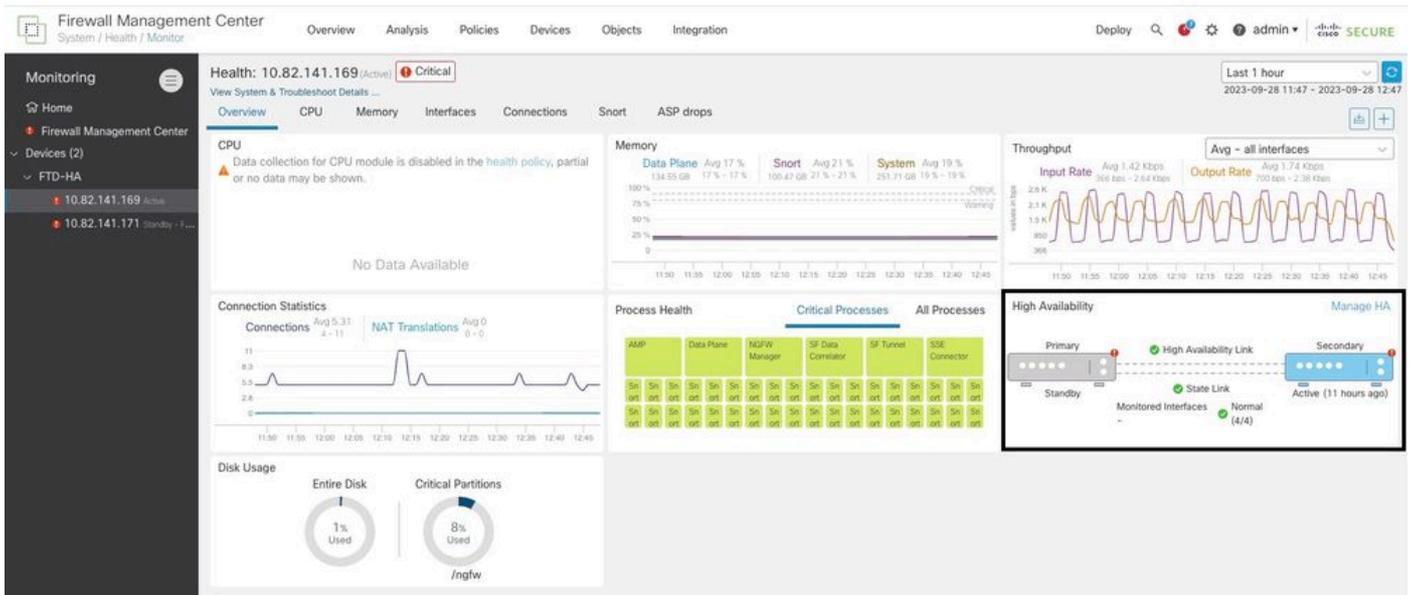
此圖顯示如何過濾故障轉移事件：

步驟 5.高可用性儀表板

監視故障轉移的另一種方法位於 [System > Health Monitor > Select Active or Standby Unit](#).

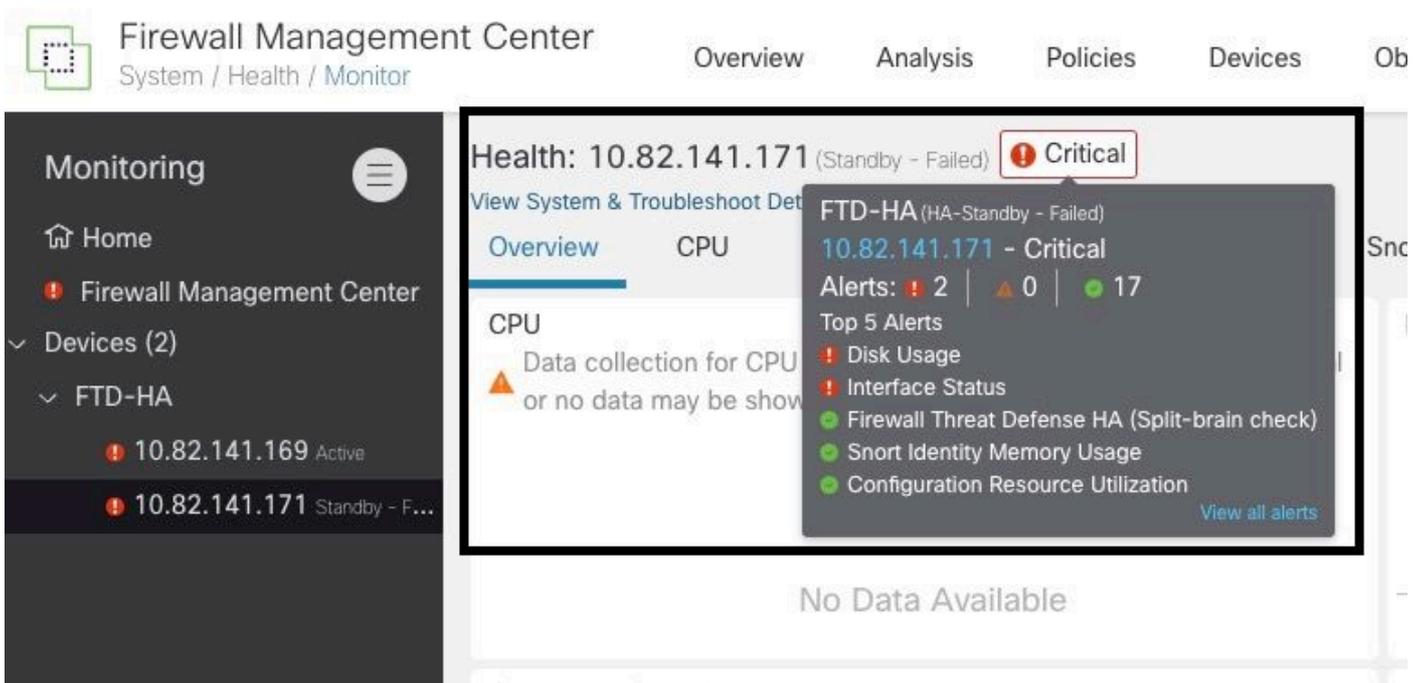
HA監控器會提供有關HA和狀態連結、受監控介面、ROL的狀態以及每個裝置上的警報狀態的資訊

此圖顯示HA監控器：



運行狀況圖形

要直觀顯示警報，請導航至 [System > Health Monitor > Select Active or Standby Unit > Select the Alerts](#).



警報

要獲取警報的更多詳細資訊，請選擇 [View all alerts > see more.](#)

此映像顯示導致故障切換的磁碟狀態：

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

[警報詳細資訊](#)

步驟 6. 威脅防禦CLI

最後，為了收集有關FMC的其他資訊，您可以導航至 [Devices > Troubleshoot > Threat Defense CLI](#). 配置引數 (如裝置和要執行的命令)，然後按一下 [Execute](#).

此圖顯示命令範例 `show failover history` 可以在FMC上執行，您可以在其中識別故障切換故障。

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

故障切換歷史記錄

相關資訊

- [FTD的高可用性](#)
- [在 Firepower 設備上設定 FTD 高可用性](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。