瞭解FTD的故障切換狀態訊息

目錄

簡介

本文說明如何理解安全防火牆威脅防禦(FTD)上的容錯移轉狀態訊息。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure 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

故障轉移運行狀況監控概述：

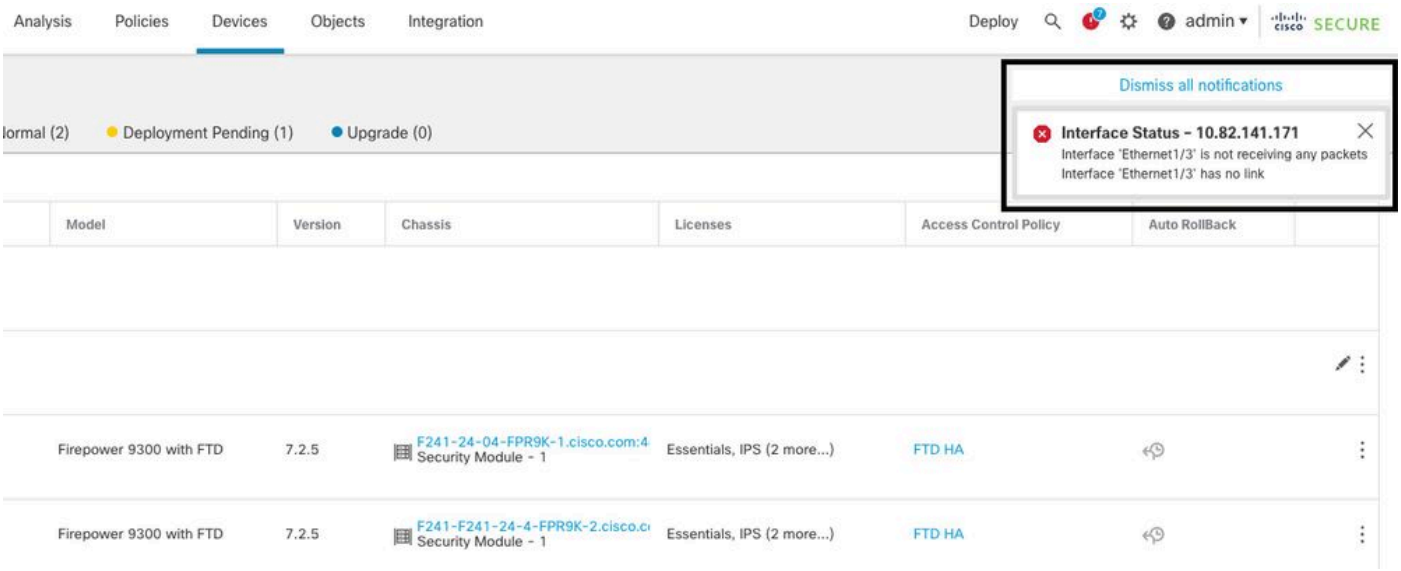
FTD裝置會監控每個裝置的整體健康狀況和介面健康狀況。FTD會執行測試，以根據裝置健康狀況監控和介面監控確定每個裝置的狀態。當用於確定HA對中每個單元的狀態的測試失敗時，將觸發故障切換事件。

故障切換狀態消息

使用案例 — 無故障切換的資料鏈路關閉

在FTD HA上未啟用介面監控時，以及在資料連結失敗的情況下，不會觸發容錯移轉事件，因為系統不會執行介面的健康監控測試。

此映像描述資料鏈路故障警報，但不觸發任何故障轉移警報。



鏈路關閉警報

若要驗證資料連結的狀態和狀態，請使用以下命令：

- show failover — 顯示有關每個裝置和介面的故障切換狀態的資訊。

```
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)
```

當介面的狀態為「正在等待」時，這意味著介面處於開啟狀態，但尚未從對等單元上的相應介面收到問候資料包。

另一方面，狀態「No Link(Not-Monitored)」表示介面的物理鏈路已關閉，但故障切換過程未對其進行監控。

為了避免中斷，強烈建議在具有其對應備用IP地址的所有敏感介面中啟用介面運行狀況監視器。

要啟用介面監控，請導航至Device > Device Management > High Availability > Monitored Interfaces.

此圖顯示Monitored Interfaces頁籤：

受監控介面

若要確認受監控介面和備用IP位址的狀態，請執行以下命令：

- show failover — 顯示有關每個裝置和介面的故障切換狀態的資訊。

```
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)
```

用例 — 介面運行狀況故障

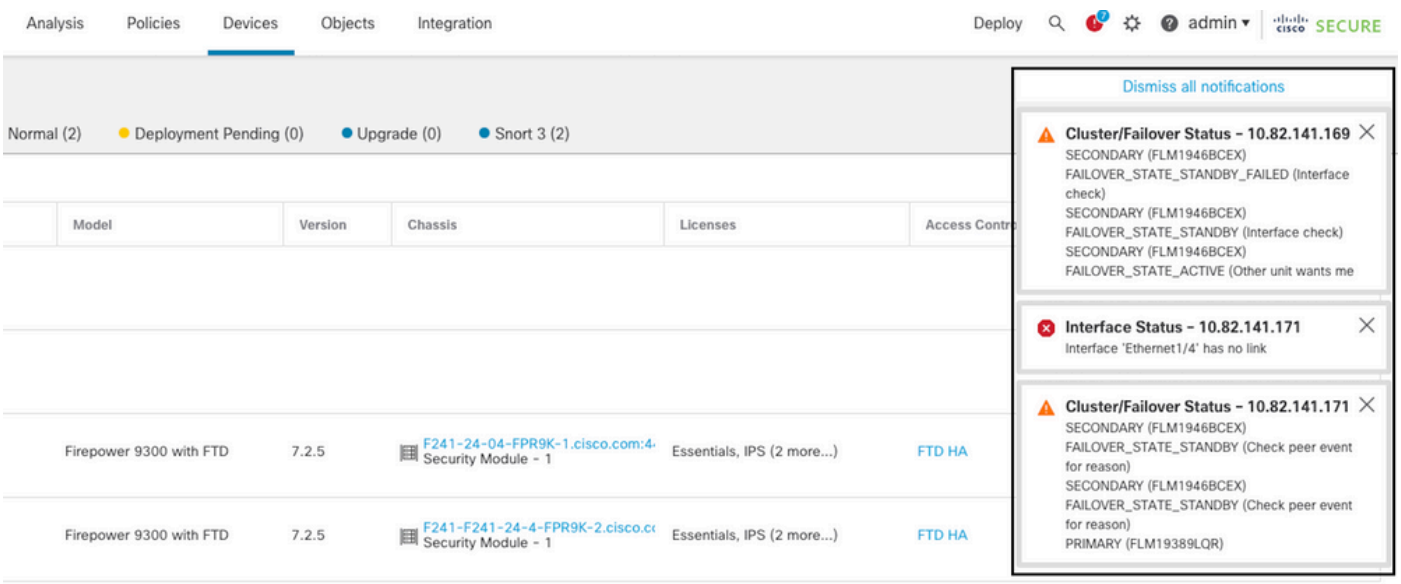
當某台裝置在受監控的介面上未收到hello消息15秒鐘，並且如果某台裝置的介面測試失敗，但在另

一台裝置上工作，則介面被視為失敗。

如果滿足為故障介面數量定義的閾值，並且主用裝置的故障介面多於備用裝置，則會發生故障轉移。

要修改介面閾值，請導航至 Devices > Device Management > High Availability > Failover Trigger Criteria.

此圖說明發生介面故障時生成的警報：



鏈路關閉時的故障切換事件

若要驗證失敗的原因，請使用以下命令：

- show failover state — 此命令顯示兩台裝置的故障切換狀態和上次報告的故障切換原因。

```
<#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** — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

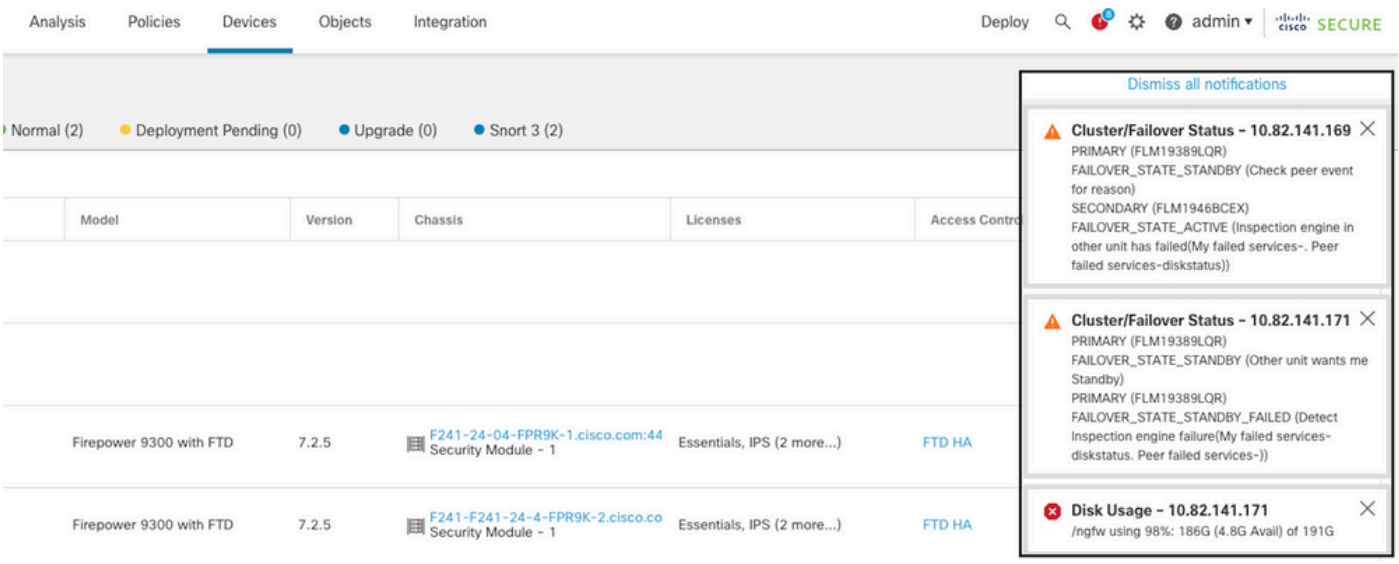
```
<#root>

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
```

使用案例 — 高磁碟使用率

如果主用裝置上的磁碟空間超過90%已滿，將觸發故障轉移事件。

此映像描述磁碟已滿時生成的警報：



使用磁碟進行故障切換

若要驗證失敗的原因，請使用以下命令：

- show failover history — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

```
<#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.          Standby Ready                    Failed Detect Inspection engine fa
Active                                                              due to disk failure
```

- show failover — 顯示有關每台裝置的故障切換狀態的資訊。

<#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 — 顯示所有已裝載檔案系統的相關資訊，包括總大小、已用空間、使用百分比和裝載點。

<#root>

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

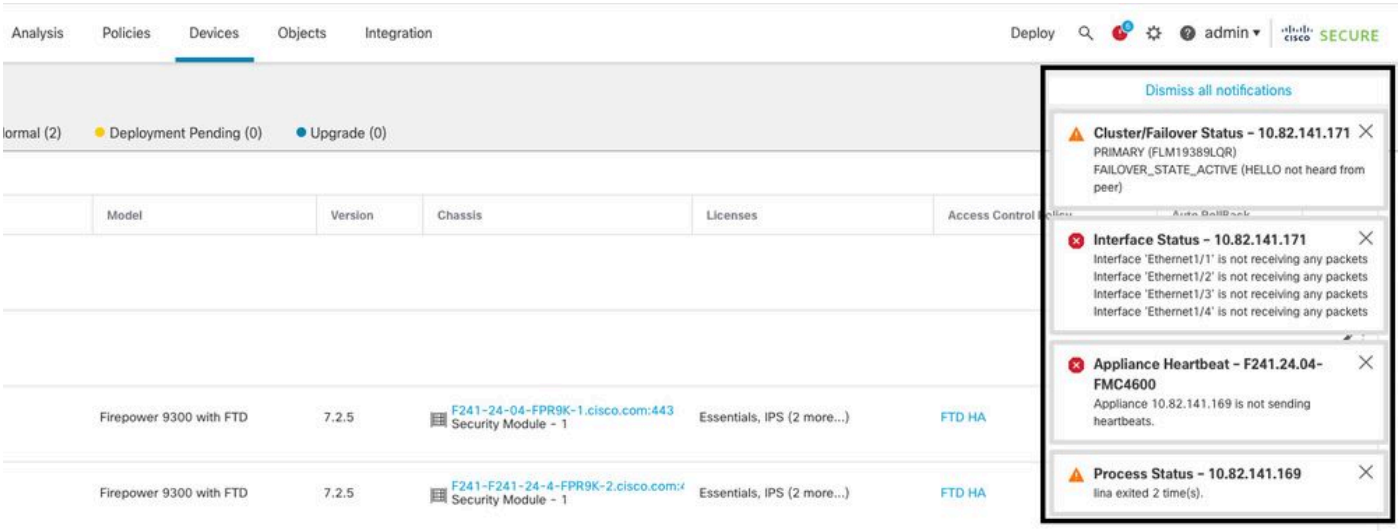
df -h /ngfw

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

使用案例 — Lina Traceback

在lina追蹤的情況下，可能會觸發容錯移轉事件。

此圖說明lina追蹤時產生的警示：



使用lina追蹤的容錯移轉

若要驗證失敗的原因，請使用以下命令：

- show failover history — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

<#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 pee
18:36:02 UTC Sep 27 2023
Just Active                    Active Drain                   HELLO not heard from peer
                                                              (failover link up, no response from pee

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

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

18:36:02 UTC Sep 27 2023
Active Config Applied           Active                        HELLO not heard from peer
                                                              (failover link up, no response from pee
```

在lina追蹤的情況下，使用以下命令來定位核心檔案：

<#root>

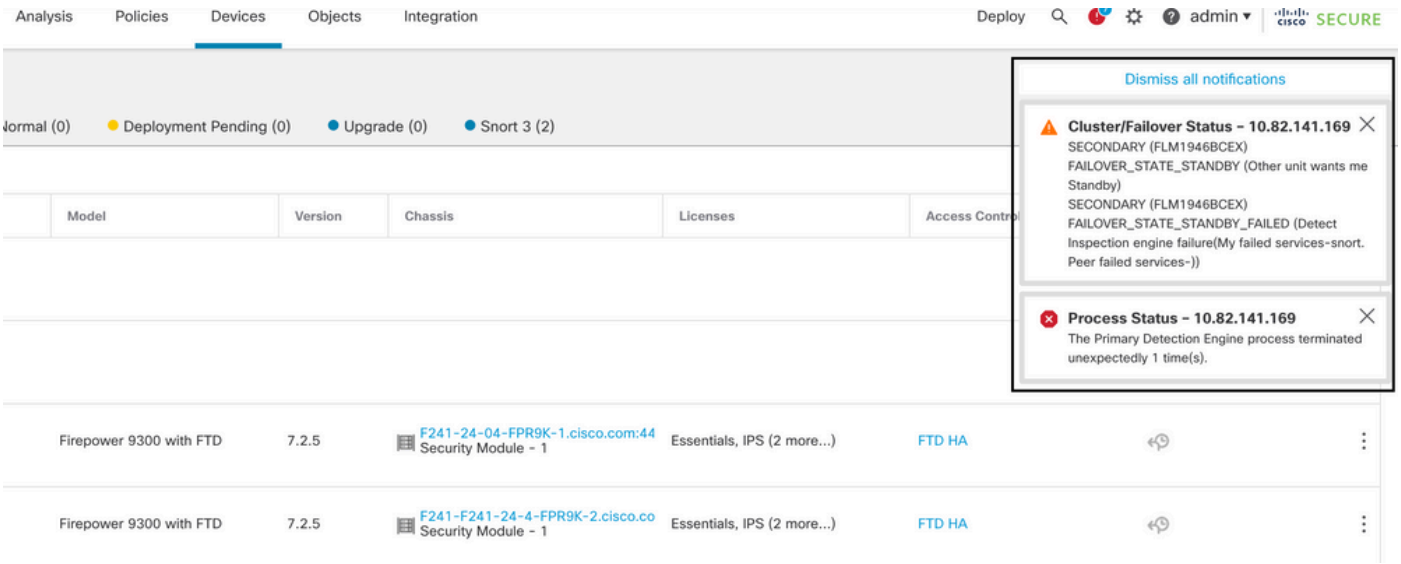
```
root@firepower:/opt/cisco/csp/applications#
cd /var/data/cores

root@firepower:/var/data/cores#
ls -l

total 29016
-rw------- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

在lina追蹤的情況下，強烈建議收集疑難排解檔案、匯出核心檔案並與Cisco TAC聯絡。

用例 — Snort例項關閉

如果主用裝置上50%以上的Snort例項出現故障，則觸發故障切換。

此圖說明當snort失敗時生成的警報：



使用snort回溯進行容錯移轉

為了 驗證失敗的原因，使用以下命令：

- show failover history — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

<#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 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 — 顯示有關裝置的故障切換狀態的資訊。

<#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#
```

在snort回溯的情況下，使用以下命令查詢crashinfo或core檔案：

<#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

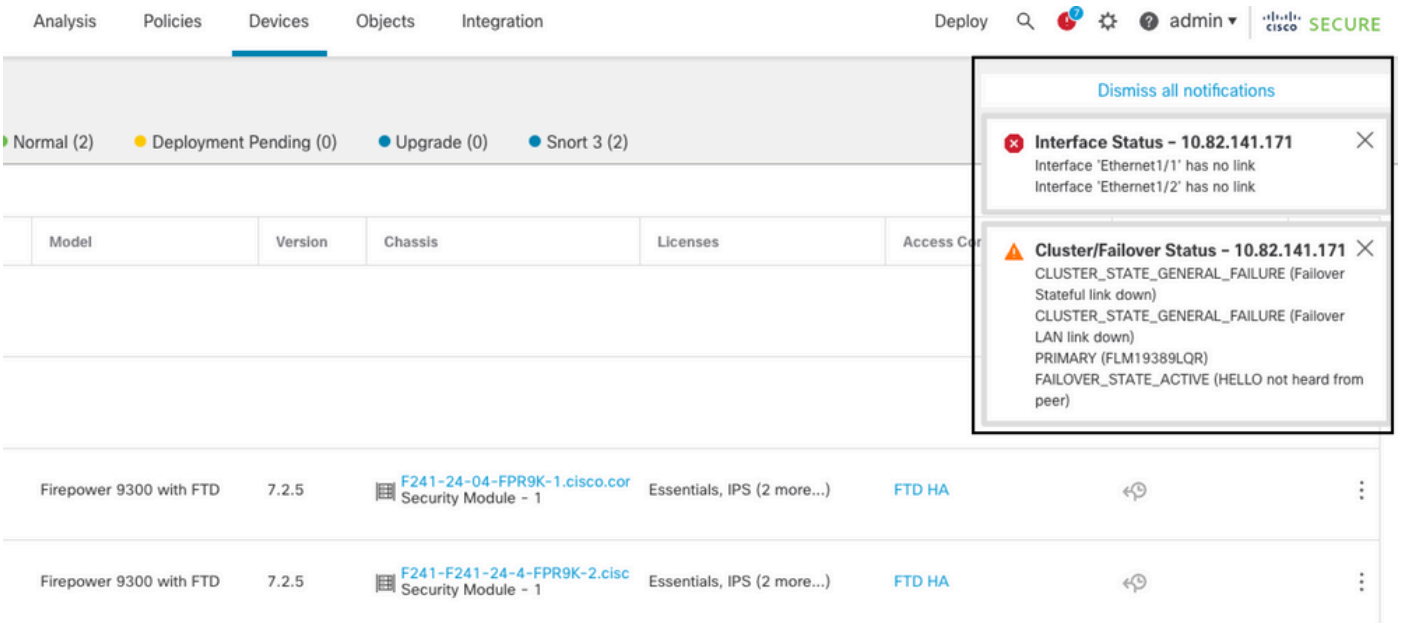
```
total 256912
-rw-r--r-- 1 root root  46087443 Apr  9 13:04 core.snort.24638.1586437471.gz
```

若使用Snort追蹤功能，強烈建議收集疑難排解檔案、匯出核心檔案，並與Cisco TAC聯絡。

使用案例 — 硬體或電源故障

FTD裝置透過使用hello訊息監控容錯移轉連結來判斷另一個裝置的健康狀況。 當裝置在故障切換鏈路上未收到連續三條hello消息，並且在受監控介面上的測試失敗時，可能會觸發故障切換事件。

此圖說明發生電源故障時生成的警報：



發生電源故障時的故障切換

為了 驗證失敗的原因，使用以下命令：

- show failover history — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

```
<#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 — 此命令顯示兩台裝置的故障切換狀態和上次報告的故障切換原因。

<#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（硬體裝置）

應用程式例項定期向主管傳送心跳訊號。當未收到心跳響應時，可以觸發故障轉移事件。

為了 驗證失敗的原因，使用以下命令：

- show failover history — 顯示故障切換歷史記錄。故障切換歷史記錄顯示過去的故障切換狀態更改以及狀態更改的原因。

<#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
```

```
02:37:14 UTC Sep 26 2023
Bulk Sync                       Standby Ready          Detected an Active mate
```

當MIO-hearbeat失敗時，強烈建議收集故障排除檔案，顯示FXOS的技術日誌，然後與Cisco TAC聯絡。

對於Firepower 4100/9300，請收集show tech-support機箱和show tech-support模組。

對於FPR1000/2100和安全防火牆3100/4200，請收集show tech-support表格。

相關資訊

- FTD的高可用性
- 在 Firepower 設備上設定 FTD 高可用性
- 排除Firepower檔案生成過程故障
- 影片 — 如何在FXOS上生成顯示技術支援檔案
- 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）。