

# Comprensión de los Mensajes de Estado de Failover para FTD

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Mensajes de estado de failover](#)

[Caso práctico: enlace de datos inactivo sin conmutación por fallo](#)

[Caso práctico: falla de estado de la interfaz](#)

[Caso práctico: uso intensivo del disco](#)

[Caso práctico: seguimiento de Lina](#)

[Caso práctico: instancia de Snort caída](#)

[Caso práctico: fallo de hardware o alimentación](#)

[Caso práctico: fallo de latido MIO \(dispositivos de hardware\)](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo comprender los mensajes de estado de conmutación por error en Secure Firewall Threat Defence (FTD).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de alta disponibilidad (HA) para Cisco Secure FTD
- Uso básico de Cisco Firewall Management Center (FMC)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Descripción General de Failover Health Monitoring:

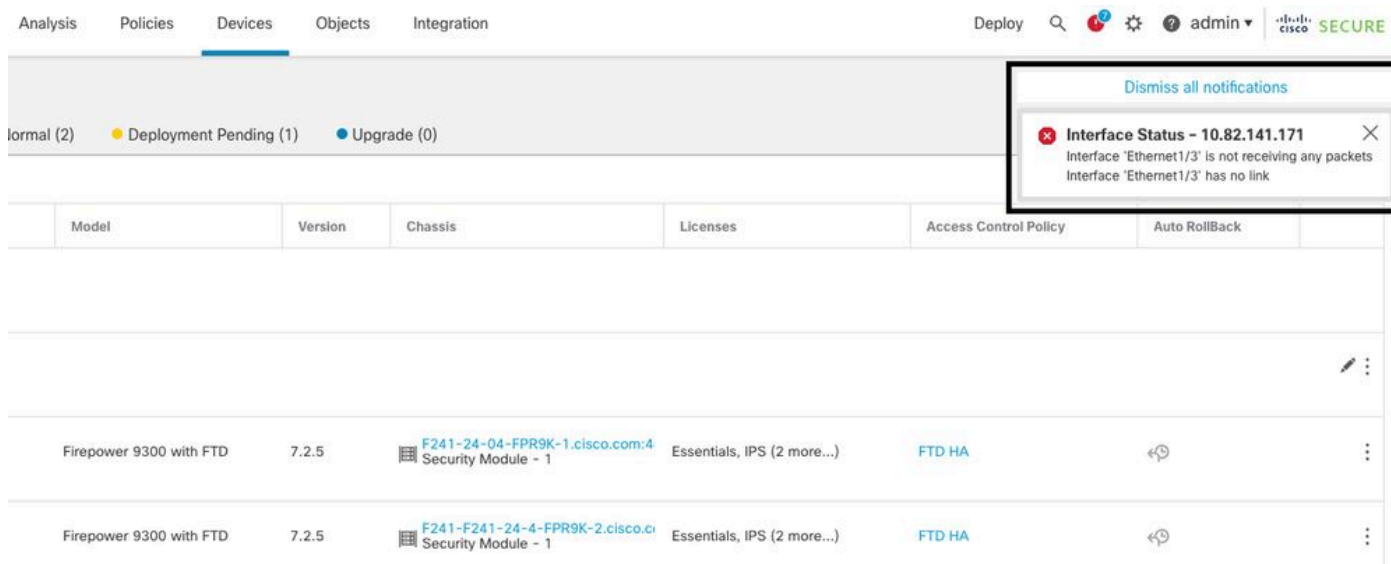
El dispositivo FTD monitorea cada unidad para ver el estado general y el estado de la interfaz. El FTD realiza pruebas para determinar el estado de cada unidad basándose en la supervisión del estado de la unidad y la supervisión de la interfaz. Cuando una prueba para determinar el estado de cada unidad en el par HA falla, se activan eventos de failover.

## Mensajes de estado de failover

Caso práctico: enlace de datos inactivo sin conmutación por fallo

Cuando la supervisión de la interfaz no está habilitada en el FTD HA y en caso de una falla del link de datos, no se activa un evento de failover ya que no se realizan las pruebas de supervisión de estado para las interfaces.

Esta imagen describe las alertas de una falla de link de datos pero no se disparan alertas de failover.



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 (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	

alerta de link caído

Para verificar el estado y el estado de los links de datos, utilice este comando:

- `show failover` - Muestra la información sobre el estado de failover de cada unidad e interfaz.

```

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)

```

Cuando el estado de la interfaz es 'En espera', significa que la interfaz está activa, pero aún no ha recibido un paquete de saludo de la interfaz correspondiente en la unidad de peer.

Por otro lado, el estado 'Sin link (no monitoreado)' significa que el link físico para la interfaz está inactivo pero no es monitoreado por el proceso de failover.

Para evitar una interrupción, se recomienda habilitar Interface Health Monitor en todas las interfaces sensibles con sus direcciones IP en espera correspondientes.

Para habilitar el Monitoreo de la Interfaz, navegue hasta `Device > Device Management > High Availability > Monitored Interfaces`.

Esta imagen muestra la ficha Interfaces supervisadas:

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				● /

interfaces supervisadas

Para verificar el estado de las interfaces monitoreadas y las direcciones IP en espera, ejecute este comando:

- `show failover` - Muestra la información sobre el estado de failover de cada unidad e interfaz.

```

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)

```

## Caso práctico: falla de estado de la interfaz

Cuando una unidad no recibe mensajes de saludo en una interfaz monitoreada durante 15 segundos y si la prueba de interfaz falla en una unidad pero funciona en la otra unidad, se considera que la interfaz ha fallado.

Si se alcanza el umbral definido para el número de interfaces fallidas y la unidad activa tiene más interfaces fallidas que la unidad standby, entonces ocurre una conmutación por fallas.

Para modificar el umbral de la interfaz, navegue hasta `Devices > Device Management > High Availability > Failover Trigger Criteria`.

Esta imagen describe las alertas generadas en una falla de interfaz:

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, and user profile (admin). Below the navigation, there are status indicators: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). A table lists two Firepower 9300 with FTD devices. The notification panel on the right shows three alerts:

- Cluster/Failover Status - 10.82.141.169**: Contains five entries for SECONDARY (FLM1946BCEX) with states: FAILOVER\_STATE\_STANDBY\_FAILED (Interface check), FAILOVER\_STATE\_STANDBY (Interface check), FAILOVER\_STATE\_STANDBY (Interface check), FAILOVER\_STATE\_ACTIVE (Other unit wants me).
- Interface Status - 10.82.141.171**: Interface 'Ethernet1/4' has no link.
- Cluster/Failover Status - 10.82.141.171**: Contains three entries for SECONDARY (FLM1946BCEX) with states: FAILOVER\_STATE\_STANDBY (Check peer event for reason), FAILOVER\_STATE\_STANDBY (Check peer event for reason), and PRIMARY (FLM19389LQR).

evento de falla con link inactivo

Para verificar la razón de la falla, utilice estos comandos:

- `show failover state` - Este comando muestra el estado de failover de ambas unidades y el último motivo reportado para el failover.

```
<#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** - Muestra el historial de fallas. El historial de conmutación por error muestra los cambios de estado de conmutación por error pasados y el motivo del cambio de estado.

<#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
```

## Caso práctico: uso intensivo del disco

En caso de que el espacio en disco de la unidad activa esté más del 90% lleno, se activa un evento de failover.

Esta imagen describe las alertas generadas cuando el disco está lleno:

The screenshot shows the Cisco Secure Management Center interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, and user profile (admin). Below the navigation, there is a summary bar showing: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). The main area contains a table with columns: Model, Version, Chassis, Licenses, and Access Control. Two rows of Firepower 9300 with FTD are visible. A notification panel is open on the right, displaying three alerts:

- Cluster/Failover Status - 10.82.141.169** (Warning): 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** (Warning): 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** (Error): /ngfw using 98%: 186G (4.8G Avail) of 191G

failover with disk usage

Para verificar la razón de la falla, utilice estos comandos:

- `show failover history` - Muestra el historial de fallas. El historial de failover muestra los cambios de estado de failover pasados y el motivo de los cambios de estado.

<#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` - Muestra la información sobre el estado de failover de cada unidad.

<#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` - Muestra la información sobre todos los sistemas de archivos montados, que incluye el tamaño total, el espacio utilizado, el porcentaje de uso y el punto de montaje.

<#root>

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

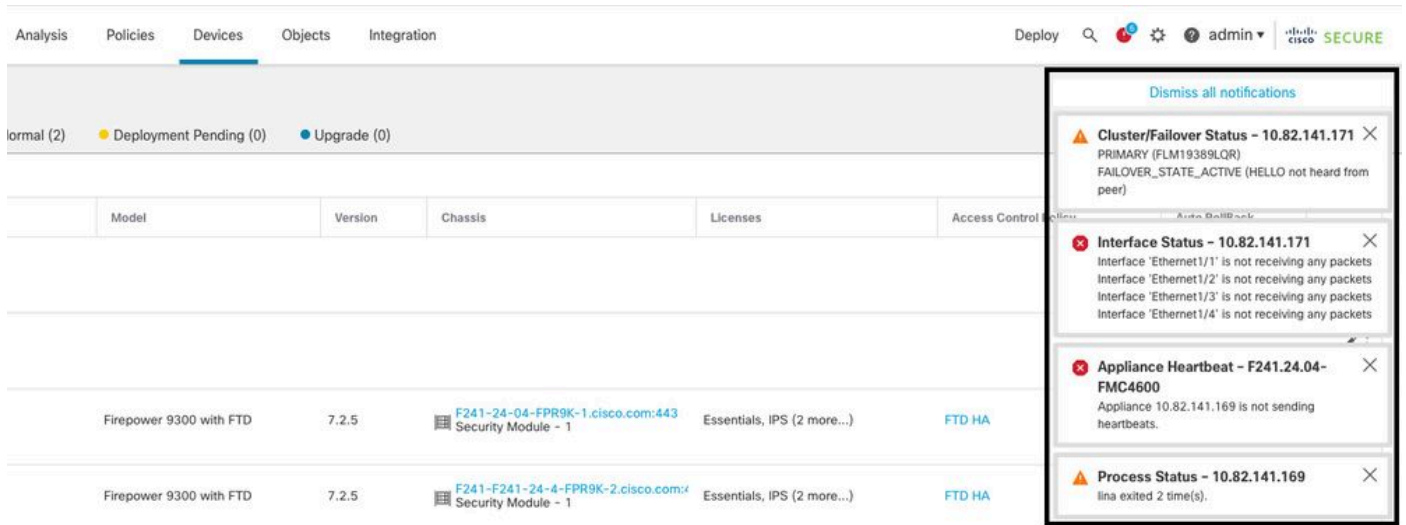
`df -h /ngfw`

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

## Caso práctico: seguimiento de Lina

En el caso de un seguimiento de línea, se puede activar un evento de failover.

Esta imagen describe las alertas generadas en el caso de seguimiento de línea:



failover with lina traceback

Para verificar la razón de la falla, utilice estos comandos:

- `show failover history` - Muestra el historial de fallas. El historial de conmutación por fallas muestra los cambios de estado de conmutación por fallas pasados y la razón del cambio de estado.

```
<#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)
```

En el caso de una traceback, utilice estos comandos para localizar los archivos de núcleo:

```
<#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
```

En el caso del rastreo de líneas, se recomienda encarecidamente recopilar los archivos de troubleshooting, exportar los archivos Core y comunicarse con el TAC de Cisco.

## Caso práctico: instancia de Snort caída

En caso de que más del 50% de las instancias de Snort en la unidad activa estén inactivas, se activa un failover.

Esta imagen describe las alertas generadas cuando falla el snort:

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. Below the navigation bar, there are status indicators for 'Normal (0)', 'Deployment Pending (0)', 'Upgrade (0)', and 'Snort 3 (2)'. A table below shows a list of devices with columns for Model, Version, Chassis, Licenses, and Access Control. Two devices are listed: 'Firepower 9300 with FTD' with version 7.2.5 and chassis 'F241-24-04-FPR9K-1.cisco.com:44 Security Module - 1'. A notification window is open on the right side, titled 'Cluster/Failover Status - 10.82.141.169'. The notification contains the following text: 'SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY (Other unit wants me Standby)', 'SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY\_FAILED (Detect Inspection engine failure(My failed services-snort. Peer failed services-))', and 'Process Status - 10.82.141.169 The Primary Detection Engine process terminated unexpectedly 1 time(s)'. There is also a 'Dismiss all notifications' link at the top of the notification window.

failover con snort traceback

Para poder verificar la razón de la falla, utilice estos comandos:

- show failover history - Muestra el historial de fallas. El historial de conmutación por fallas muestra los cambios de estado de conmutación por fallas pasados y la razón del cambio de estado.

```
<#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` - Muestra la información sobre el estado de failover de la unidad.

```
<#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#
```

En el caso de snort traceback, utilice estos comandos para localizar los archivos crashinfo o core:

```
<#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

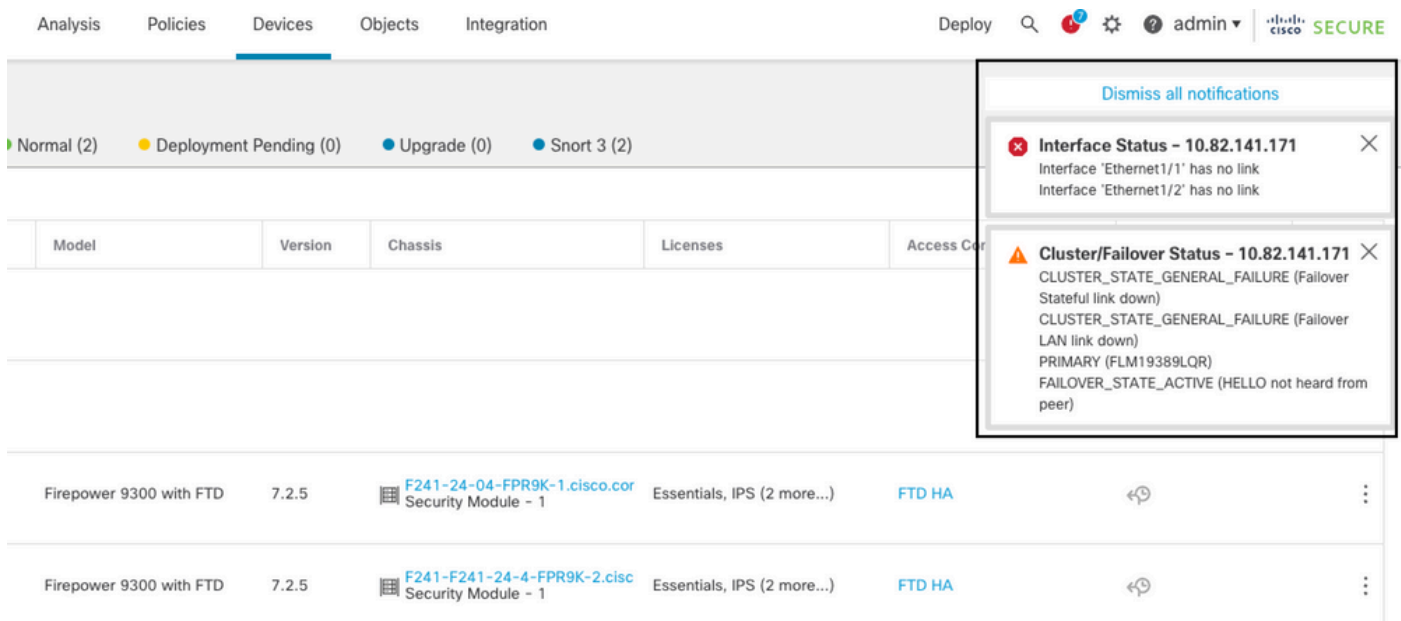
```

En el caso del seguimiento de snort, se recomienda recopilar los archivos de solución de problemas, exportar los archivos de núcleo y ponerse en contacto con el TAC de Cisco.

### Caso práctico: fallo de hardware o alimentación

El dispositivo FTD determina el estado de la otra unidad monitoreando el link de failover con los mensajes hello. Cuando una unidad no recibe tres mensajes hello consecutivos en el link de failover, y las pruebas fallan en las interfaces monitoreadas, se puede activar un evento de failover.

Esta imagen describe las alertas generadas cuando hay una falla de energía:



falla con falla de energía

Para poder verifique la razón de la falla, utilice estos comandos:

- show failover history - Muestra el historial de fallas. El historial de conmutación por fallas muestra los cambios de estado de conmutación por fallas pasados y la razón del cambio de estado.

<#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` - Este comando muestra el estado de failover de ambas unidades y el último motivo reportado para el failover.

```
<#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

## Caso práctico: fallo de latido MIO (dispositivos de hardware)

La instancia de la aplicación envía periódicamente latidos al supervisor. Cuando no se reciben las respuestas de latido, se puede activar un evento de failover.

Para poder verificar la razón de la falla, utilice estos comandos:

- `show failover history` - Muestra el historial de fallas. El historial de conmutación por fallas muestra los cambios de estado de conmutación por fallas pasados y la razón del cambio de estado.

```
<#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

Cuando MIO-HeartBeat falla, se recomienda recopilar los archivos de solución de problemas, mostrar los registros técnicos de FXOS y ponerse en contacto con el TAC de Cisco.

Para Firepower 4100/9300, recopile el chasis show tech-support y el módulo show tech-support.

Para FPR1000/2100 y Secure Firewall 3100/4200, recopile el formulario show tech-support.

## Información Relacionada

- [Alta disponibilidad para FTD](#)
- [Configuración de alta disponibilidad de FTD en dispositivos Firepower](#)
- [Solucionar problemas de procedimientos de generación de archivos Firepower](#)
- [Vídeo: Cómo generar archivos de soporte técnico de Show en FXOS](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).