

# Identificación y análisis de eventos de conmutación por fallo de FTD en FMC

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Eventos de conmutación por fallo en FMC](#)

[Paso 1. Configuración de directiva de mantenimiento](#)

[Paso 2. Asignación de políticas](#)

[Paso 3. Alertas de eventos de failover](#)

[Paso 4. Eventos históricos de failover](#)

[Paso 5. Panel de alta disponibilidad](#)

[Paso 6. CLI de Threat Defence](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe cómo identificar y analizar eventos de failover para Secure Firewall Threat Defence en la GUI de Secure Firewall Management Center.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de alta disponibilidad (HA) para Cisco Secure Firewall Threat Defence (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

El FMC no es solo el centro administrativo de los dispositivos Firepower, más allá de las opciones de gestión y configuración, sino que también proporciona una interfaz gráfica que ayuda a analizar los registros y los eventos en tiempo real y pasado.

Cuando se habla de failover, la interfaz tiene nuevas mejoras que ayudan a analizar los eventos de failover para comprender los fallos.

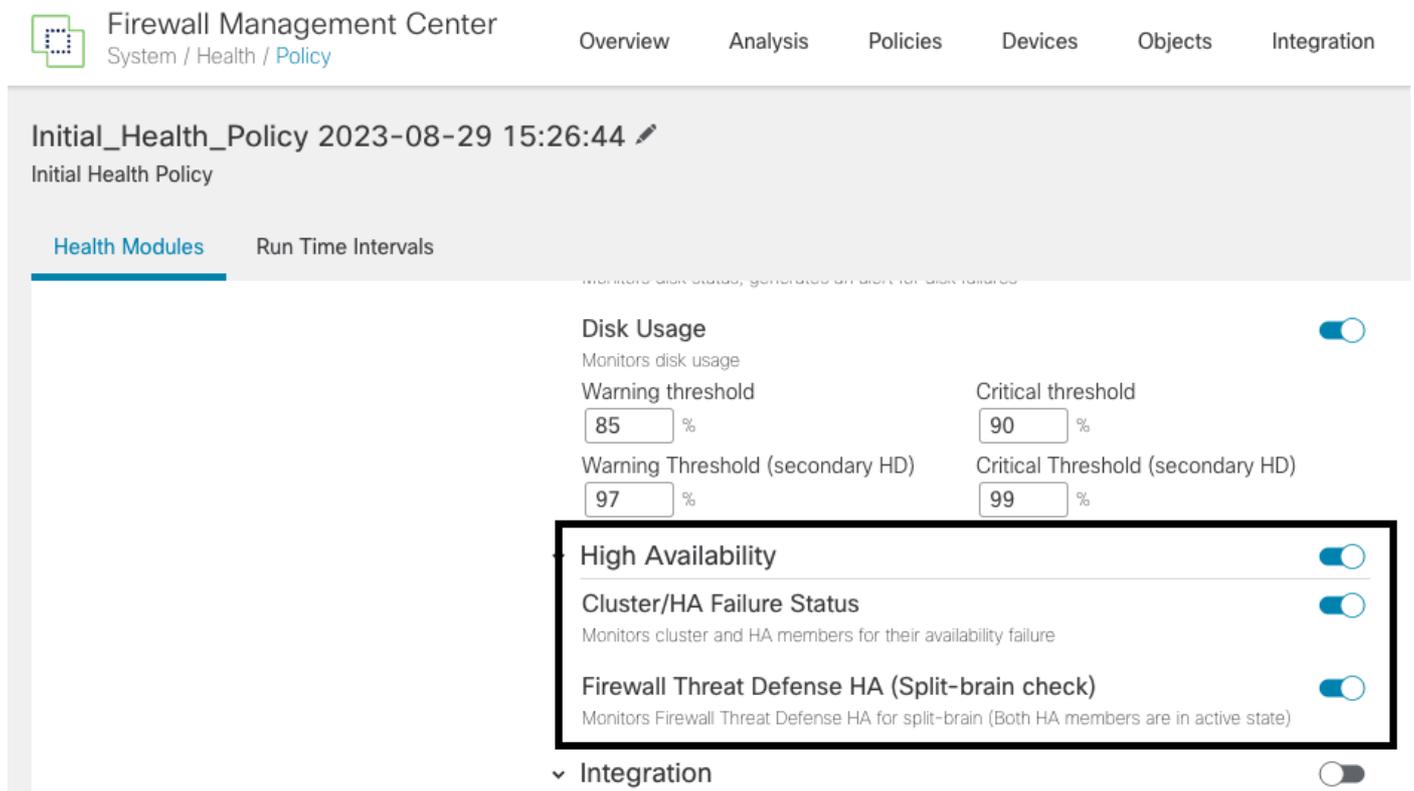
## Eventos de conmutación por fallo en FMC

### Paso 1. Configuración de directiva de mantenimiento

El módulo Cluster/HA Failure Status (Estado de fallos de HA/clúster) está activado de forma predeterminada en la Health Policy (Política de estado), pero también puede activar la opción Split-brain check (Verificación por cerebro dividido).

Para habilitar las opciones para HA en la política sanitaria, navegue hasta `System > Health > Policy > Firewall Threat Defense Health Policy > High Availability`.

Esta imagen describe la configuración HA de la política de salud:



The screenshot shows the Firewall Management Center interface. The breadcrumb navigation is `System / Health / Policy`. The main heading is `Initial_Health_Policy 2023-08-29 15:26:44`. Under `Health Modules`, there are two tabs: `Health Modules` and `Run Time Intervals`. The `Health Modules` tab is active. The `Disk Usage` module is shown with a description: "Monitors disk status, generates an alert for disk failures". It has a toggle switch turned on. Below it are four input fields for thresholds: `Warning threshold` (85%), `Critical threshold` (90%), `Warning Threshold (secondary HD)` (97%), and `Critical Threshold (secondary HD)` (99%). A red box highlights the `High Availability` section, which includes three modules, all with their toggle switches turned on: `High Availability`, `Cluster/HA Failure Status` (with description: "Monitors cluster and HA members for their availability failure"), and `Firewall Threat Defense HA (Split-brain check)` (with description: "Monitors Firewall Threat Defense HA for split-brain (Both HA members are in active state)"). Below this is the `Integration` section, which is currently turned off.

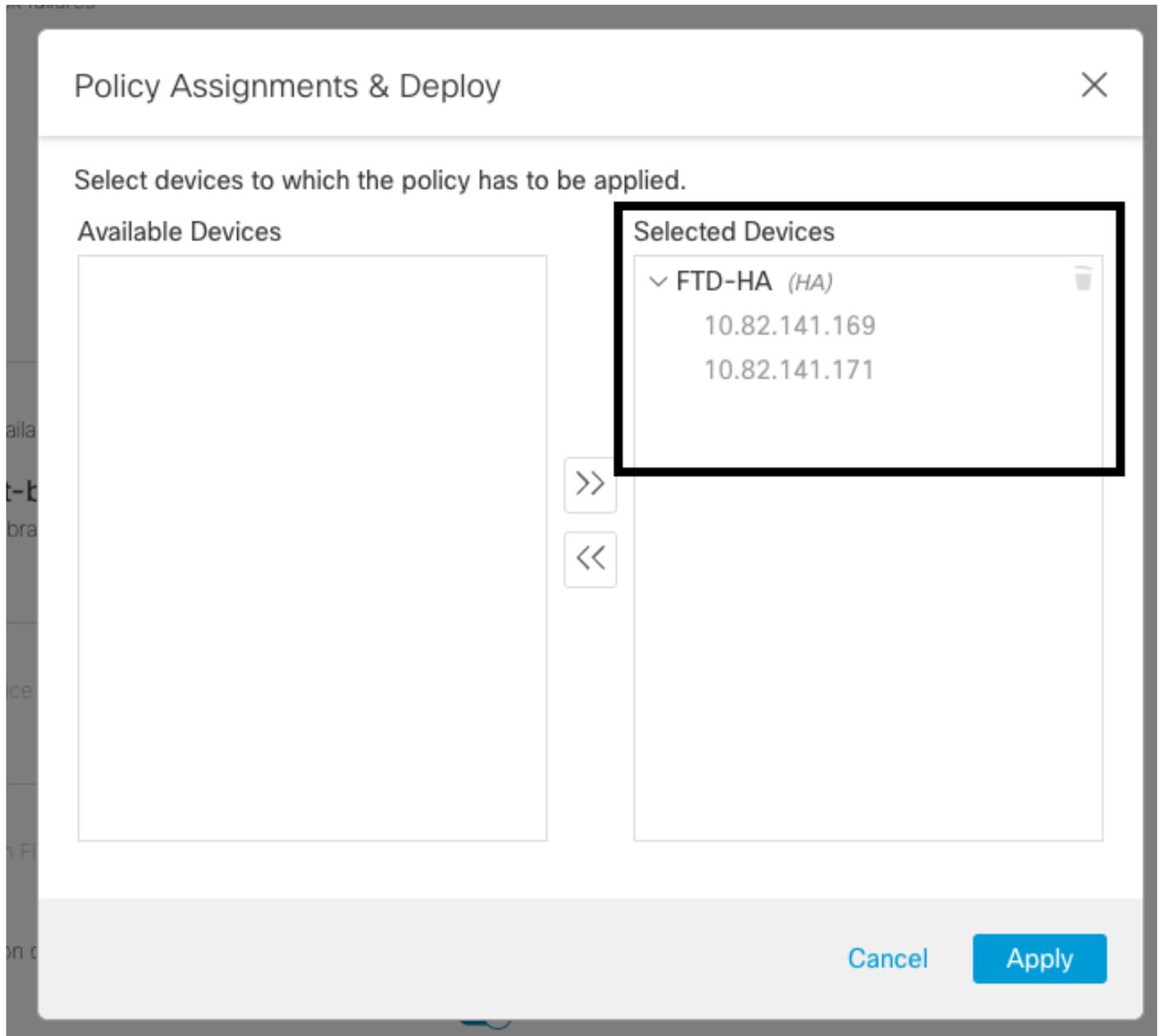
Configuración de estado de alta disponibilidad

### Paso 2. Asignación de políticas

Asegúrese de que la política de estado esté asignada a los pares HA que desea supervisar desde el FMC.

Para asignar la política, navegue hasta `System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy`.

Esta imagen muestra cómo asignar la política de estado al par HA:



asignación de HA

Una vez asignada y guardada la política, el CSP la aplica automáticamente al FTD.

### Paso 3. Alertas de eventos de failover

Según la configuración del HA, una vez que se activa un evento de failover, se muestran las alertas emergentes que describen el fallo de failover.

Esta imagen muestra las alertas de failover generadas:

The screenshot shows the Cisco Firepower Management Center interface. At the top, there are navigation tabs for 'Devices', 'Objects', and 'Integration'. The main content area displays a table of devices with columns for 'Name', 'Version', 'Chassis', 'Licenses', and 'Access Control Policy'. Two devices are listed, both with version 7.2.5 and chassis 'F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1'. A notification panel on the right side is open, showing three alerts:

- 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

Alertas de conmutación por fallas

También puede navegar hasta [Notifications > Health](#) para visualizar las alertas de estado de failover.

Esta imagen muestra las alertas de failover bajo las notificaciones:

The screenshot shows the 'Health' section of the Cisco Firepower Management Center interface. The 'Health' section displays a summary of 20+ total notifications, including 15 warnings, 7 critical, and 0 errors. A table lists specific alerts:

- Smart License Monitor**: Smart Agent is not registered with Smart Licensing Cloud
- URL Filtering Monitor**: URL Filtering registration failure
- 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
- 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

Notificaciones de HA

## Paso 4. Eventos históricos de failover

El FMC proporciona una forma de visualizar los eventos de conmutación por fallo que se han producido en el pasado. Para filtrar los eventos, navegue hasta [System > Health > Events > Edit Search](#) y especifique el Nombre del Módulo como Estado de Clúster/Failover. Además, el filtro se puede aplicar en función del estado.

Esta imagen muestra cómo filtrar eventos de failover:



Module Name X	Test Name X	Time X	Description X	Value X	Units X	Status X	Device X
Cluster/Failover Status	Cluster/Failover Status	2023-09-28 11:41:52	PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAIL...  PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-)).	0		🚨	10.82.141.171

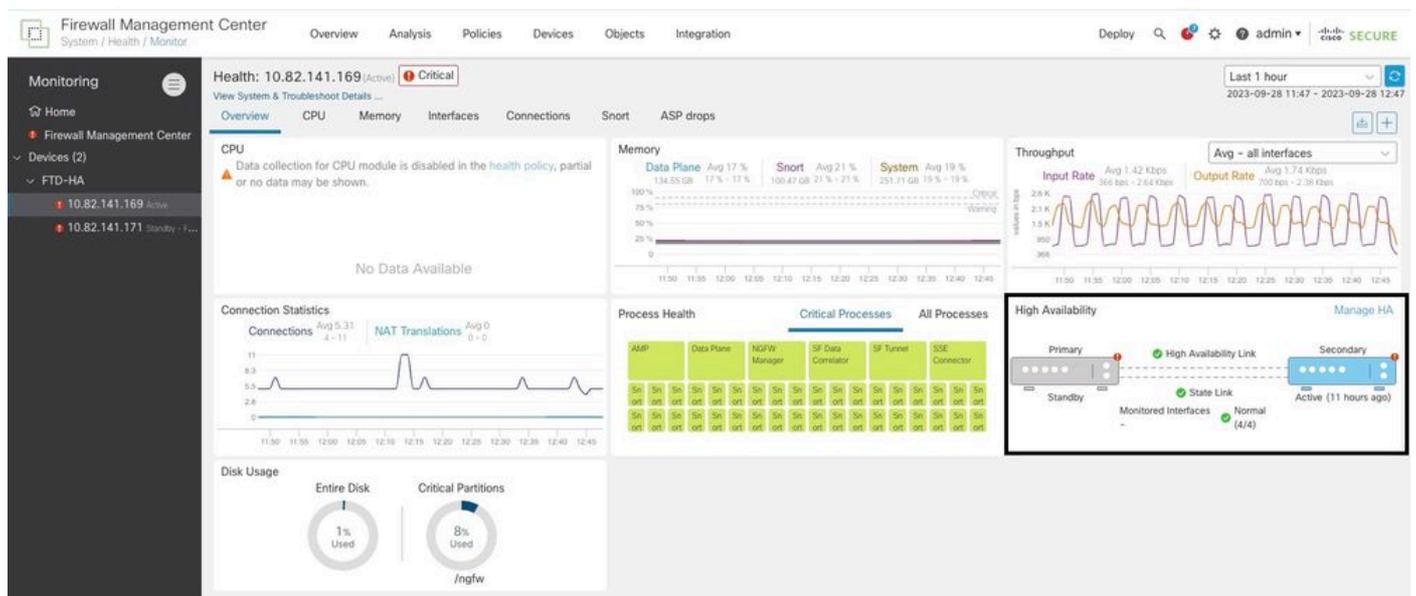
detalles de failover

## Paso 5. Panel de alta disponibilidad

Otra forma de supervisar la conmutación por error se puede encontrar en System > Health Monitor > Select Active or Standby Unit.

El monitor de HA proporciona información sobre el estado del HA y el enlace de estado, las interfaces supervisadas, el ROL y el estado de las alertas en cada unidad.

Esta imagen muestra el monitor HA:



Gráficos de estado

Para visualizar las alertas, navegue hasta System > Health Monitor > Select Active or Standby Unit > Select the Alerts.

Firewall Management Center  
System / Health / Monitor

Overview Analysis Policies Devices Ob

**Monitoring**

- Home
- Firewall Management Center
- Devices (2)
  - FTD-HA
    - 10.82.141.169 Active
    - 10.82.141.171 Standby - F...

**Health: 10.82.141.171** (Standby - Failed) **Critical**

View System & Troubleshoot Det

Overview CPU

**CPU**

Data collection for CPU or no data may be show

**FTD-HA (HA-Standby - Failed)**

10.82.141.171 - Critical

Alerts: 2 | 0 | 17

Top 5 Alerts

- Disk Usage
- Interface Status
- Firewall Threat Defense HA (Split-brain check)
- Snort Identity Memory Usage
- Configuration Resource Utilization

[View all alerts](#)

No Data Available

Alertas

Para obtener más detalles de las alertas, seleccione [View all alerts > see more.](#)

Esta imagen muestra el estado del disco que causó el failover:

**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**

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**

All appliances are sending heartbeats correctly.

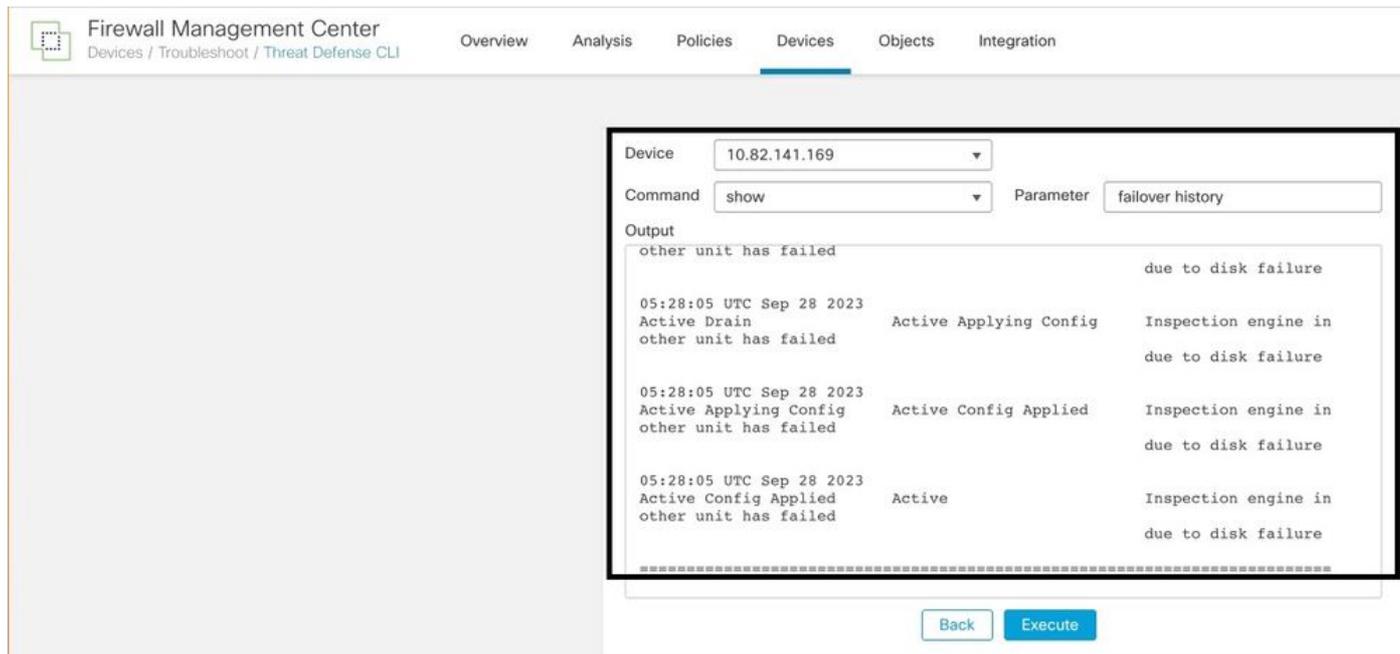
**Automatic Application Runas Status**

Sep 28, 2023 12:47 PM

## Paso 6. CLI de Threat Defence

Por último, para recopilar información adicional sobre FMC, puede navegar hasta `Devices > Troubleshoot > Threat Defense CLI`. Configure los parámetros como Device y el comando a ejecutar y haga clic en `Execute`.

Esta imagen muestra un ejemplo del comando `show failover history` que se puede ejecutar en el FMC donde se puede identificar la falla de failover.



## Información Relacionada

- [Alta disponibilidad para FTD](#)
- [Configuración de alta disponibilidad de FTD en dispositivos Firepower](#)
- [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).