

# Entender mensagens de status de failover para FTD

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Mensagens de Status de Failover](#)

[Caso de uso - Enlace inativo sem failover](#)

[Caso de uso - Falha de integridade da interface](#)

[Caso de uso - Uso de alto disco](#)

[Caso de uso - Lina Traceback](#)

[Caso de uso - Instância de Snort inativa](#)

[Caso de uso - falha de hardware ou energia](#)

[Caso de uso - Falha de MIO-Heartbeat \(dispositivos de hardware\)](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como compreender as mensagens de status de Failover no Secure Firewall Threat Defense (FTD).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de Alta Disponibilidade (HA) para Cisco Secure FTD
- Utilização básica do Cisco Firewall Management Center (FMC)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Visão Geral do Monitoramento de Integridade de Failover:

O dispositivo FTD monitora cada unidade quanto à integridade geral e à integridade da interface. O FTD executa testes para determinar o estado de cada unidade com base no Monitoramento de Integridade da Unidade e Monitoramento da Interface. Quando um teste para determinar o estado de cada unidade no par HA falha, os eventos de failover são acionados.

## Mensagens de Status de Failover

### Caso de uso - Enlace inativo sem failover

Quando o monitoramento de interface não está habilitado no HA do FTD e em caso de falha de link de dados, um evento de failover não é acionado, pois os testes do monitor de integridade das interfaces não são executados.

Esta imagem descreve os alertas de uma falha de link de dados, mas nenhum alerta de failover é disparado.

The screenshot shows the Cisco Secure FTD management console interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, a notification bell with a red dot, a settings gear, a help icon, 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 inativo

Para verificar o estado e o status dos enlaces de dados, use este comando:

- `show failover` Exibe as informações sobre o status de failover de cada unidade e interface.

```

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)

```

Quando o estado da interface é 'Waiting', significa que a interface está ativa, mas ainda não recebeu um pacote hello da interface correspondente na unidade peer.

Por outro lado, o estado 'Sem link (não monitorado)' significa que o link físico para a interface está inativo, mas não é monitorado pelo processo de failover.

Para evitar uma interrupção, é altamente recomendável ativar o Monitor de integridade da interface em todas as interfaces sensíveis com seus endereços IP em espera correspondentes.

Para habilitar o monitoramento de interface, navegue até [Device > Device Management > High Availability > Monitored Interfaces](#).

Esta imagem mostra a guia Interfaces Monitoradas:

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 monitoradas

Para verificar o status das interfaces monitoradas e dos endereços IP em standby, execute este comando:

- `show failover` Exibe as informações sobre o status de failover de cada unidade e interface.

```

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 de uso - Falha de integridade da interface

Quando uma unidade não recebe mensagens de hello em uma interface monitorada por 15 segundos e se o teste de interface falhar em uma unidade, mas funcionar na outra, a interface é considerada como tendo falhado.

Se o limite definido para o número de interfaces com falha for atingido e a unidade ativa tiver mais interfaces com falha do que a unidade em standby, ocorrerá um failover.

Para modificar o limite da interface, navegue até `Devices > Device Management > High Availability > Failover Trigger Criteria`.

Esta imagem descreve os alertas gerados em uma falha de interface:

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, settings, help, and the user 'admin'. Below the navigation, there are status indicators: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). A table lists devices with columns for Model, Version, Chassis, Licenses, and Access Control. Two Firepower 9300 units are shown. A notification panel on the right displays three alerts:

- Cluster/Failover Status - 10.82.141.169**: SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY\_FAILED (Interface check), SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY (Interface check), SECONDARY (FLM1946BCEX) 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**: SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY (Check peer event for reason), SECONDARY (FLM1946BCEX) FAILOVER\_STATE\_STANDBY (Check peer event for reason), PRIMARY (FLM19389LQR).

evento de failover com link inativo

Para verificar o motivo da falha, use estes comandos:

- `show failover state` - Este comando exibe o estado de failover de ambas as unidades e o último motivo reportado para o 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** - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo da alteração 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 de uso - Uso de alto disco

Caso o espaço em disco na unidade ativa esteja mais de 90% cheio, um evento de failover é acionado.

Esta imagem descreve os alertas gerados quando o disco está cheio:

The screenshot shows the Cisco Secure Firewall Management Center (FMC) interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, search, settings, and user '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 Firepower 9300 with FTD devices are listed. 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

Para verificar o motivo da falha, use estes comandos:

- `show failover history` - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo das alterações 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` Exibe as informações sobre o status de failover de cada unidade.

<#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` - Exibe as informações sobre todos os sistemas de arquivos montados, incluindo o tamanho total, o espaço usado, a porcentagem de uso e o ponto de montagem.

<#root>

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

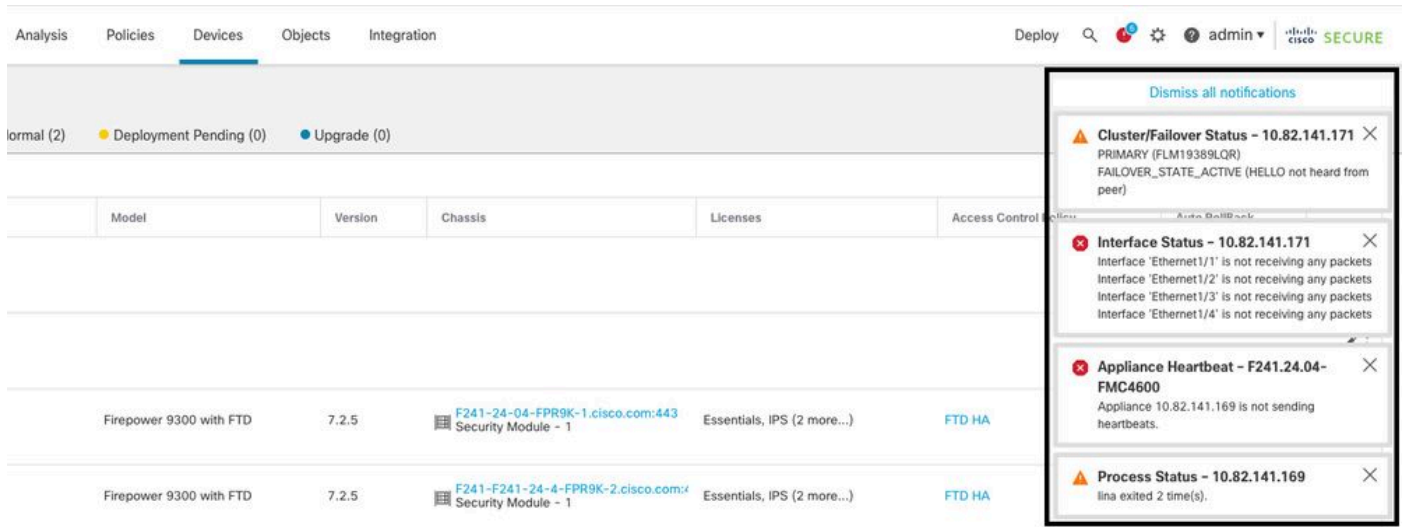
`df -h /ngfw`

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

# Caso de uso - Lina Traceback

No caso de um traceback de linha, um evento de failover pode ser disparado.

Esta imagem descreve os alertas gerados no caso do lina traceback:



failover com lina traceback

Para verificar o motivo da falha, use estes comandos:

- `show failover history` - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo da alteração 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)
```

No caso do lina traceback, use estes comandos para localizar os arquivos do 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
```

No caso do lina traceback, é altamente recomendável coletar os arquivos de solução de problemas, exportar os arquivos Core e entrar em contato com o TAC da Cisco.

## Caso de uso - Instância de Snort inativa

Caso mais de 50% das instâncias do Snort na unidade ativa estejam inativas, um failover é acionado.

Esta imagem descreve os alertas gerados quando o snort falha:

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. The main content area displays a table 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 panel is open on the right, showing two alerts:

- Cluster/Failover Status - 10.82.141.169**: 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-))
- Process Status - 10.82.141.169**: The Primary Detection Engine process terminated unexpectedly 1 time(s).

failover com snort traceback

Para para verificar o motivo da falha, use estes comandos:

- show failover history - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo da alteração 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` - Exibe as informações sobre o status de failover da unidade.

```
<#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#
```

No caso do snort traceback, use estes comandos para localizar os arquivos crashinfo ou 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

```

No caso do snort traceback, é altamente recomendável coletar os arquivos de solução de problemas, exportar os arquivos Core e entrar em contato com o TAC da Cisco.

## Caso de uso - falha de hardware ou energia

O dispositivo FTD determina a integridade da outra unidade monitorando o link de failover com mensagens de saudação. Quando uma unidade não recebe três mensagens hello consecutivas no link de failover e os testes falham nas interfaces monitoradas, um evento de failover pode ser disparado.

Esta imagem descreve os alertas gerados quando há uma falha de energia:

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, settings, help, and a user profile for 'admin'. Below the navigation, there is a status bar with indicators for Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). The main content area displays a table of devices. Two devices are visible, both identified as 'Firepower 9300 with FTD' running version '7.2.5'. The notification panel is open, showing two alerts:

- Interface Status - 10.82.141.171**: Interface 'Ethernet1/1' has no link, Interface 'Ethernet1/2' has no link.
- Cluster/Failover Status - 10.82.141.171**: CLUSTER\_STATE\_GENERAL\_FAILURE (Failover Stateful link down), CLUSTER\_STATE\_GENERAL\_FAILURE (Failover LAN link down), PRIMARY (FLM19389LQR), FAILOVER\_STATE\_ACTIVE (HELLO not heard from peer).

failover com falha de energia

Para para verificar o motivo da falha, use estes comandos:

- show failover history - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo da alteração 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 exibe o estado de failover de ambas as unidades e o último motivo reportado para o 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 de uso - Falha de MIO-Heartbeat (dispositivos de hardware)

A instância do aplicativo envia periodicamente heartbeats ao supervisor. Quando as respostas de heartbeat não são recebidas, um evento de failover pode ser acionado.

Para verificar o motivo da falha, use estes comandos:

- `show failover history` - Exibe o histórico de failover. O histórico de failover exibe as alterações de estado de failover anteriores e o motivo da alteração 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

Quando o MIO-heartbeat falhar, é altamente recomendável coletar os arquivos de solução de problemas, exibir registros técnicos do FXOS e entrar em contato com o TAC da Cisco.

Para o Firepower 4100/9300, colete o chassi show tech-support e o módulo show tech-support.

Para FPR1000/2100 e Secure Firewall 3100/4200, colete o formulário show tech-support.

## Informações Relacionadas

- [Alta disponibilidade para FTD](#)
- [Configurar a alta disponibilidade do FTD em dispositivos Firepower](#)
- [Solucionar problemas de procedimentos de geração de arquivos do Firepower](#)
- [Vídeo - Como gerar arquivos show Tech-Support no FXOS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.