

Comprendere i messaggi di stato di failover per FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Messaggi di stato di failover](#)

[Caso di utilizzo - Collegamento dati non attivo senza failover](#)

[Caso di utilizzo - Errore di integrità dell'interfaccia](#)

[Caso di utilizzo - Utilizzo elevato del disco](#)

[Caso di utilizzo - Lina Traceback](#)

[Use Case - Snort istanza verso il basso](#)

[Caso di utilizzo - Errore hardware o di alimentazione](#)

[Caso di utilizzo - Errore MIO-Heartbeat \(dispositivi hardware\)](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come comprendere i messaggi di stato di failover in Secure Firewall Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di High Availability (HA) per Cisco Secure FTD
- Usabilità di base di Cisco Firewall Management Center (FMC)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Panoramica sul monitoraggio dello stato di failover:

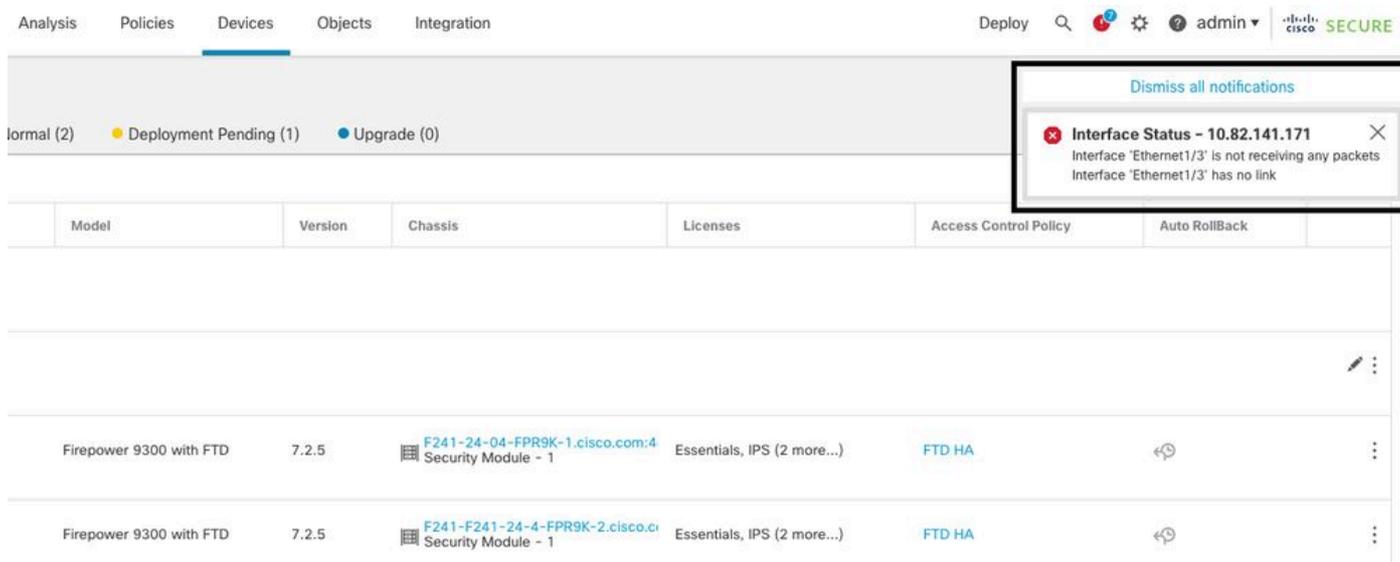
Il dispositivo FTD controlla ogni unità per lo stato complessivo e per lo stato dell'interfaccia. L'FTD esegue dei test per determinare lo stato di ciascuna unità in base al monitoraggio dello stato delle unità e al monitoraggio dell'interfaccia. Quando un test per determinare lo stato di ciascuna unità nella coppia HA ha esito negativo, vengono attivati gli eventi di failover.

Messaggi di stato di failover

Caso di utilizzo - Collegamento dati non attivo senza failover

Quando il monitoraggio dell'interfaccia non è abilitato sull'FTD HA e in caso di errore del collegamento dati, non viene attivato un evento di failover in quanto i test del monitoraggio dello stato per le interfacce non vengono eseguiti.

In questa immagine vengono descritti gli avvisi relativi a un errore del collegamento dati ma non viene attivato alcun avviso di 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, help, and user '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: 'Interface Status - 10.82.141.171', 'Interface 'Ethernet1/3' is not receiving any packets', and '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	

avviso collegamento non attivo

Per verificare lo stato e lo stato dei collegamenti dati, utilizzare questo comando:

- show failover - Visualizza le informazioni sullo stato di failover di ciascuna unità e interfaccia.

```

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 lo stato dell'interfaccia è 'In attesa', significa che l'interfaccia è attiva, ma non ha ancora ricevuto un pacchetto hello dall'interfaccia corrispondente sull'unità peer.

D'altra parte, lo stato 'Nessun collegamento (non monitorato)' indica che il collegamento fisico per l'interfaccia è inattivo ma non viene monitorato dal processo di failover.

Per evitare interruzioni, si consiglia di abilitare l'Health Monitor dell'interfaccia in tutte le interfacce sensibili con gli indirizzi IP di standby corrispondenti.

Per abilitare il monitoraggio dell'interfaccia, passare a `Device > Device Management > High Availability > Monitored Interfaces`.

Nell'immagine è illustrata la scheda Interfacce monitorate:

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				●

interfacce monitorate

Per verificare lo stato delle interfacce monitorate e gli indirizzi IP in standby, eseguire questo comando:

- `show failover` - Visualizza le informazioni sullo stato di failover di ciascuna unità e interfaccia.

```

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 di utilizzo - Errore di integrità dell'interfaccia

Quando un apparecchio non riceve messaggi di saluto su un'interfaccia monitorata per 15 secondi e se il test dell'interfaccia non riesce su un apparecchio ma funziona sull'altro, l'interfaccia è considerata guasta.

Se viene raggiunta la soglia definita per il numero di interfacce con errori e l'unità attiva presenta un numero di interfacce con errori maggiore rispetto all'unità di standby, si verifica un failover.

Per modificare la soglia dell'interfaccia, passare a [Devices > Device Management > High Availability > Failover Trigger Criteria](#).

In questa immagine vengono descritti gli avvisi generati in caso di errore dell'interfaccia:

The screenshot shows the Cisco Secure GUI 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 with status indicators: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). The main content area displays a table of devices. The table has columns for Model, Version, Chassis, Licenses, and Access Control. Two rows are visible, both for Firepower 9300 with FTD, version 7.2.5, with Security Module - 1. The first row has license F241-24-04-FPR9K-1.cisco.com:4 and Essentials, IPS (2 more...). The second row has license F241-F241-24-4-FPR9K-2.cisco.c and Essentials, IPS (2 more...). On the right side, a notification panel is open, showing 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 di failover con collegamento non attivo

Per verificare la causa dell'errore, utilizzare i seguenti comandi:

- `show failover state` - Questo comando visualizza lo stato di failover di entrambe le unità e l'ultimo motivo segnalato per il 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** - Visualizza la cronologia di failover. Nella cronologia del failover vengono visualizzate le modifiche dello stato del failover precedenti e il motivo della modifica dello stato.

<#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 di utilizzo - Utilizzo elevato del disco

Se lo spazio su disco dell'unità attiva è pieno per oltre il 90%, viene attivato un evento di failover.

Questa immagine descrive gli allarmi generati quando il disco è pieno:

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, settings, and user 'admin'. Below the navigation, there is a summary bar with status indicators: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). A table below lists devices with columns for Model, Version, Chassis, Licenses, and Access Control. Two Firepower 9300 with FTD devices are listed. On the right side, a notification panel is open, displaying three alerts: two 'Cluster/Failover Status' alerts (one with a yellow triangle, one with a red triangle) and one 'Disk Usage' alert (with a red X). The 'Disk Usage' alert indicates that the /ngfw partition is using 98% of its 191G space, with 4.8G available.

Per verificare la causa dell'errore, utilizzare i seguenti comandi:

- `show failover history` - Visualizza la cronologia di failover. Nella cronologia di failover vengono visualizzate le modifiche dello stato di failover precedenti e il motivo delle modifiche.

<#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` - Visualizza le informazioni sullo stato di failover di ciascuna unità.

<#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` - Visualizza le informazioni su tutti i file system installati, tra cui le dimensioni totali, lo spazio utilizzato, la percentuale di utilizzo e il punto di accesso.

<#root>

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

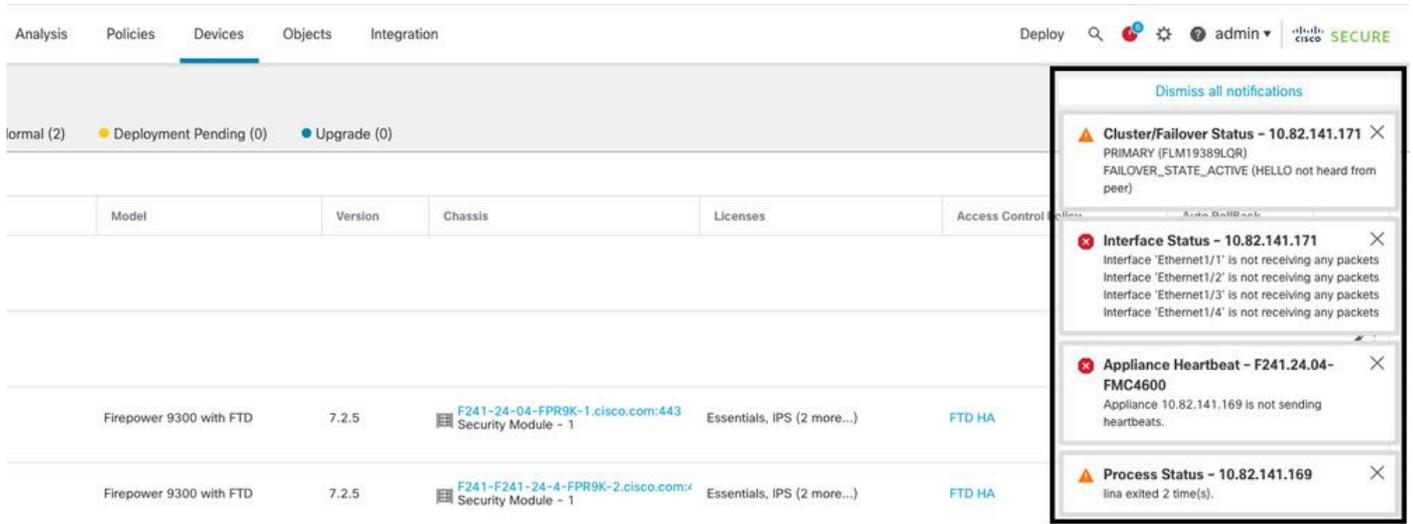
`df -h /ngfw`

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

Caso di utilizzo - Lina Traceback

Nel caso di un traceback basato su lina, può essere attivato un evento di failover.

In questa immagine vengono descritti gli avvisi generati in caso di traceback Lina:



failover con traceback lina

Per verificare la causa dell'errore, utilizzare i seguenti comandi:

- `show failover history` - Visualizza la cronologia di failover. La cronologia del failover visualizza le modifiche dello stato del failover precedenti e il motivo della modifica dello stato.

```
<#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)
```

Nel caso del traceback Lina, utilizzare questi comandi per individuare i file principali:

```
<#root>
```

```
root@firepower:/opt/cisco/csp/applications#
```

```
cd /var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 29016
```

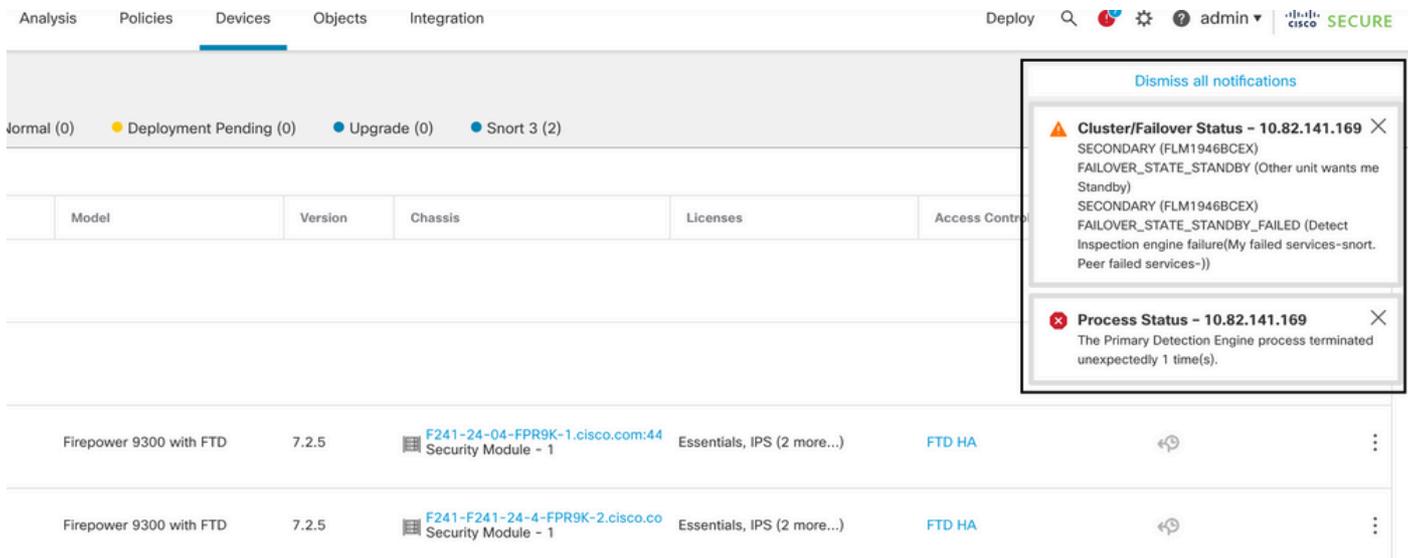
```
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

Nel caso di lina traceback, si consiglia di raccogliere i file di risoluzione dei problemi, esportare i file di base e contattare Cisco TAC.

Use Case - Snort istanza verso il basso

Se più del 50% delle istanze Snort sull'unità attiva sono inattive, viene attivato un failover.

In questa immagine vengono descritti gli avvisi generati quando l'operazione di snort non riesce:



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 error messages:

- 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 con snort traceback

Per verificare la causa dell'errore, utilizzare i seguenti comandi:

- `show failover history` - Visualizza la cronologia di failover. La cronologia del failover visualizza le modifiche dello stato del failover precedenti e il motivo della modifica dello stato.

```
<#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` - Visualizza le informazioni sullo stato di failover dell'unità.

```
<#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#
```

In caso di snort traceback, utilizzare questi comandi per individuare i file 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
```

In caso di snort traceback, si consiglia di raccogliere i file di risoluzione dei problemi, esportare i file di base e contattare Cisco TAC.

Caso di utilizzo - Errore hardware o di alimentazione

Il dispositivo FTD determina lo stato dell'altra unità monitorando il collegamento di failover con i messaggi di saluto. Quando un'unità non riceve tre messaggi hello consecutivi sul collegamento di failover e i test hanno esito negativo sulle interfacce monitorate, è possibile attivare un evento di failover.

In questa immagine vengono descritti gli avvisi generati in caso di interruzione dell'alimentazione:

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active, showing a list of devices. A notification window is open, displaying the following details:

- Dismiss all notifications** (button)
- Interface Status - 10.82.141.171** (red X icon)
 - Interface 'Ethernet1/1' has no link
 - Interface 'Ethernet1/2' has no link
- Cluster/Failover Status - 10.82.141.171** (yellow triangle icon)
 - 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)

The background table shows the following columns: Model, Version, Chassis, Licenses, and Access Control. Two devices are listed:

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.cor	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisc	Essentials, IPS (2 more...)	FTD HA

failover con interruzione dell'alimentazione

Per per verificare la causa dell'errore, utilizzare i seguenti comandi:

- show failover history - Visualizza la cronologia di failover. La cronologia del failover visualizza le modifiche dello stato del failover precedenti e il motivo della modifica dello stato.

```
<#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` - Questo comando visualizza lo stato di failover di entrambe le unità e l'ultimo motivo segnalato per il 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 di utilizzo - Errore MIO-Heartbeat (dispositivi hardware)

L'istanza dell'applicazione invia periodicamente heartbeat al supervisore. Quando le risposte heartbeat non vengono ricevute, è possibile attivare un evento di failover.

Per verificare la causa dell'errore, utilizzare i seguenti comandi:

- `show failover history` - Visualizza la cronologia di failover. La cronologia del failover visualizza le modifiche dello stato del failover precedenti e il motivo della modifica dello stato.

```
<#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 MIO-heartbeat non funziona, si consiglia di raccogliere i file di risoluzione dei problemi, visualizzare i log tecnici da FXOS e contattare Cisco TAC.

Per Firepower 4100/9300, raccogliere lo chassis show tech-support e il modulo show tech-support.

Per i modelli FPR1000/2100 e Secure Firewall 3100/4200, è possibile raccogliere il modulo show tech-support.

Informazioni correlate

- [Alta disponibilità per FTD](#)
- [Configurazione della funzionalità FTD High Availability nei dispositivi Firepower](#)
- [Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower](#)
- [Video - Come generare i file di supporto tecnico su FXOS](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).