

Comprendre les messages d'état de basculement pour FTD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Messages d'état de basculement](#)

[Cas d'utilisation - Liaison de données désactivée sans basculement](#)

[Exemple d'utilisation - Défaillance de l'interface](#)

[Cas d'utilisation - Utilisation élevée du disque](#)

[Cas d'utilisation - Lina Traceback](#)

[Cas d'utilisation - Arrêt de l'instance Snort](#)

[Cas d'utilisation - Panne matérielle ou d'alimentation](#)

[Exemple d'utilisation : défaillance MIO-Heartbeat \(périphériques matériels\)](#)

[Informations connexes](#)

Introduction

Ce document décrit comment comprendre les messages d'état de basculement sur Secure Firewall Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration haute disponibilité (HA) pour Cisco Secure FTD
- Facilité d'utilisation de base de Cisco Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Présentation de la surveillance du fonctionnement du basculement :

Le périphérique FTD surveille l'état général de chaque unité et l'état de l'interface. Le FTD effectue des tests afin de déterminer l'état de chaque unité en fonction de la surveillance de l'état de l'unité et de la surveillance de l'interface. Lorsqu'un test visant à déterminer l'état de chaque unité de la paire haute disponibilité échoue, des événements de basculement sont déclenchés.

Messages d'état de basculement

Cas d'utilisation - Liaison de données désactivée sans basculement

Lorsque la surveillance d'interface n'est pas activée sur la haute disponibilité FTD et en cas de défaillance d'une liaison de données, un événement de basculement n'est pas déclenché car les tests de surveillance de l'état des interfaces ne sont pas effectués.

Cette image décrit les alertes d'une défaillance de liaison de données, mais aucune alerte de basculement n'est déclenchée.

The screenshot shows the Cisco Secure Management Center 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. A notification box is overlaid on the right side of the table, titled 'Interface Status - 10.82.141.171'. The notification text reads: 'Interface 'Ethernet1/3' is not receiving any packets' and 'Interface 'Ethernet1/3' has no link'. The notification box also includes a 'Dismiss all notifications' link and a close button (X).

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	

alerte de liaison interrompue

Afin de vérifier l'état et l'état des liaisons de données, utilisez cette commande :

- `show failover` - Affiche les informations relatives à l'état de basculement de chaque unité et 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)

Lorsque l'état de l'interface est 'En attente', cela signifie que l'interface est active, mais qu'elle n'a pas encore reçu de paquet Hello de l'interface correspondante sur l'unité homologue.

D'autre part, l'état « No Link (Not-Monitored) » signifie que la liaison physique de l'interface est désactivée mais n'est pas surveillée par le processus de basculement.

Afin d'éviter une panne, il est fortement recommandé d'activer le Moniteur d'état de l'interface dans toutes les interfaces sensibles avec leurs adresses IP de secours correspondantes.

Afin d'activer la surveillance d'interface, accédez à [Device > Device Management > High Availability > Monitored Interfaces](#).

Cette image présente l'onglet Interfaces surveillées :

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 surveillées

Afin de vérifier l'état des interfaces surveillées et des adresses IP de secours, exécutez cette commande :

- `show failover` - Affiche les informations relatives à l'état de basculement de chaque unité et 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)

```

Exemple d'utilisation - Défaillance de l'interface

Lorsqu'une unité ne reçoit pas de messages Hello sur une interface surveillée pendant 15 secondes et si le test de l'interface échoue dans une unité mais fonctionne dans l'autre unité, l'interface est considérée comme ayant échoué.

Si le seuil que vous définissez pour le nombre d'interfaces défaillantes est atteint et que l'unité active a plus d'interfaces défaillantes que l'unité en veille, un basculement se produit.

Pour modifier le seuil de l'interface, accédez à [Devices > Device Management > High Availability > Failover Trigger Criteria](#).

Cette image décrit les alertes générées en cas de défaillance d'une interface :

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 are status indicators: Normal (2), Deployment Pending (0), Upgrade (0), and Snort 3 (2). A table below shows device details for two Firepower 9300 units. On the right side, a notification panel is open, displaying three alerts:

- Cluster/Failover Status - 10.82.141.169**: This alert contains five entries:
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY_FAILED (Interface check)
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Interface check)
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Interface check)
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_ACTIVE (Other unit wants me)
- Interface Status - 10.82.141.171**: This alert contains one entry:
 - Interface 'Ethernet1/4' has no link
- Cluster/Failover Status - 10.82.141.171**: This alert contains four entries:
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Check peer event for reason)
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Check peer event for reason)
 - SECONDARY (FLM1946BCEX) FAILOVER_STATE_STANDBY (Check peer event for reason)
 - PRIMARY (FLM19389LQR)

événement de basculement avec liaison désactivée

Afin de vérifier la raison de l'échec, utilisez ces commandes :

- `show failover state` - Cette commande affiche l'état de basculement des deux unités et la dernière raison signalée pour le basculement.

<#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` - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison du changement d'état.

<#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
```

Cas d'utilisation - Utilisation élevée du disque

Si l'espace disque de l'unité active est saturé à plus de 90 %, un événement de basculement est déclenché.

Cette image décrit les alertes générées lorsque le disque est plein :

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ admin | SECURE

Normal (2) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (2)

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:44 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.co Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕

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 ✕

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 (4.8G Avail) of 191G

basculement avec utilisation du disque

Afin de vérifier la raison de l'échec, utilisez ces commandes :

- `show failover history` - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison de ces changements.

```
<#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` - Affiche les informations relatives à l'état de basculement de chaque unité.

```
<#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` - Affiche les informations sur tous les systèmes de fichiers montés, notamment la taille totale, l'espace utilisé, le pourcentage d'utilisation et le point de montage.

```
<#root>
```

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

```
df -h /ngfw
```

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

Cas d'utilisation - Lina Traceback

Dans le cas d'un retour arrière Lina, un événement de basculement peut être déclenché.

Cette image décrit les alertes générées dans le cas de lina traceback :

The screenshot shows the Cisco Secure Manager interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. Below the navigation bar, there are indicators for 'Normal (2)', 'Deployment Pending (0)', and 'Upgrade (0)'. A table lists two Firepower 9300 devices with FTD HA configuration. On the right, a notification panel displays four alerts:

- Cluster/Failover Status - 10.82.141.171**: PRIMARY (FLM19389LQR) FAILOVER_STATE_ACTIVE (HELLO not heard from peer)
- Interface Status - 10.82.141.171**: Interface 'Ethernet1/1' is not receiving any packets, Interface 'Ethernet1/2' is not receiving any packets, Interface 'Ethernet1/3' is not receiving any packets, Interface 'Ethernet1/4' is not receiving any packets
- Appliance Heartbeat - F241.24.04-FMC4600**: Appliance 10.82.141.169 is not sending heartbeats.
- Process Status - 10.82.141.169**: lina exited 2 time(s).

basculement avec lina traceback

Afin de vérifier la raison de l'échec, utilisez ces commandes :

- `show failover history` - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison du changement d'état.

```
<#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)

Dans le cas de lina traceback, utilisez ces commandes pour localiser les fichiers principaux :

```
<#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
```

Dans le cas de lina traceback, il est vivement recommandé de collecter les fichiers de dépannage, d'exporter les fichiers Core et de contacter le TAC Cisco.

Cas d'utilisation - Arrêt de l'instance Snort

Si plus de 50 % des instances Snort de l'unité active sont hors service, un basculement est déclenché.

Cette image décrit les alertes générées en cas d'échec de la commande snort :

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 🔔 admin | **SECURE**

Normal (0) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (2)

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:44 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.co Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

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).

basculement avec snort traceback

Afin de Pour vérifier la raison de l'échec, utilisez ces commandes :

- show failover history - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison du changement d'état.

<#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 - Affiche les informations relatives à l'état de basculement de l'unité.

<#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#
```

Dans le cas de snort traceback, utilisez ces commandes pour localiser les fichiers 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
```

Dans le cas de snort traceback, il est vivement recommandé de collecter les fichiers de dépannage, d'exporter les fichiers Core et de contacter le TAC Cisco.

Cas d'utilisation - Panne matérielle ou d'alimentation

Le périphérique FTD détermine l'état de l'autre unité en surveillant la liaison de basculement à l'aide de messages Hello. Lorsqu'une unité ne reçoit pas trois messages Hello consécutifs sur la liaison de basculement et que les tests échouent sur les interfaces surveillées, un événement de basculement peut être déclenché.

Cette image décrit les alertes générées en cas de panne de courant :

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | cisco SECURE

Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

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

Dismiss all notifications

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)

basculement avec panne d'alimentation

Afin de Pour vérifier la raison de l'échec, utilisez ces commandes :

- `show failover history` - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison du changement d'état.

<#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` - Cette commande affiche l'état de basculement des deux unités et la dernière raison signalée pour le basculement.

```
<#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

Exemple d'utilisation : défaillance MIO-Heartbeat (périphériques matériels)

L'instance d'application envoie régulièrement des pulsations au superviseur. Lorsque les réponses de pulsation ne sont pas reçues, un événement de basculement peut être déclenché.

Afin de Pour vérifier la raison de l'échec, utilisez ces commandes :

- `show failover history` - Affiche l'historique de basculement. L'historique de basculement affiche les changements d'état de basculement passés et la raison du changement d'état.

```
<#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
```

En cas d'échec de la fonction MIO-heartbeat, il est vivement recommandé de collecter les fichiers de dépannage, d'afficher les journaux techniques de FXOS et de contacter le centre d'assistance technique Cisco.

Pour Firepower 4100/9300, collectez le châssis `show tech-support` et le module `show tech-support`.

Pour FPR1000/2100 et Secure Firewall 3100/4200, collectez le formulaire show tech-support.

Informations connexes

- [Haute disponibilité pour FTD](#)
- [Configurer la haute disponibilité FTD sur les appareils Firepower](#)
- [Dépannage des procédures de génération de fichiers Firepower](#)
- [Vidéo - Comment générer des fichiers Show Tech-Support sur FXOS](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.