

# Dépannage des problèmes de haute disponibilité de Firepower Threat Defense

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Options de conception](#)

[Terminologie HA](#)

[États HA](#)

[Diagramme de flux d'état haute disponibilité](#)

[Vérification UI](#)

[Centre de gestion Firepower Géré FTD HA](#)

[FTD HA géré par FDM](#)

[ASA HA gérée par ASDM](#)

[Gestionnaire de châssis Firepower pour 4100/9300 exécutant FTD/ASA HA](#)

[Vérifier CLI](#)

[Dépannage](#)

[Scénarios](#)

[Échec de APP-SYNC](#)

[Le noeud de veille ne parvient pas à joindre HA avec « CD App Sync error is App Config Apply Failed »](#)

[Échec de la connexion du noeud de veille à HA avec « Échec de la progression de l'état HA en raison du délai d'attente APP SYNC »](#)

[Le noeud de secours ne parvient pas à joindre la haute disponibilité avec l'erreur « CD App Sync is Failed to apply SSP config on standby »](#)

[Échec du contrôle d'intégrité](#)

[Panne de Snort Down ou de disque](#)

[Le moteur de détection \(instance SNORT\) est arrêté](#)

[Le Périphérique Présente Une Utilisation Élevée Du Disque](#)

[Défaillance de la carte de service](#)

[Défaillance de pulsation MIO](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les procédures de fonctionnement, de vérification et de dépannage de la haute disponibilité (HA) sur Firepower Threat Defense (FTD).

# Conditions préalables

## Exigences

Cisco recommande de connaître les sujets suivants :

- Plates-formes FTD et ASA
- Captures de paquets sur les appareils FTD

Il est vivement recommandé de lire le guide de configuration de Firepower [Configure FTD High Availability on Firepower Appliances](#) pour mieux comprendre les concepts décrits dans ce document.

## Composants utilisés

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

- Périphérique FTD Cisco
- Cisco Firepower Management Center (FMC)

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

Les informations et les exemples sont basés sur le FTD, mais la plupart des concepts sont également pleinement applicables à l'appliance de sécurité adaptative (ASA).

Un FTD prend en charge deux modes de gestion principaux :

- Offbox via FMC, également appelé gestion à distance
- On-box via Firepower Device Manager (FDM), également appelé gestion locale

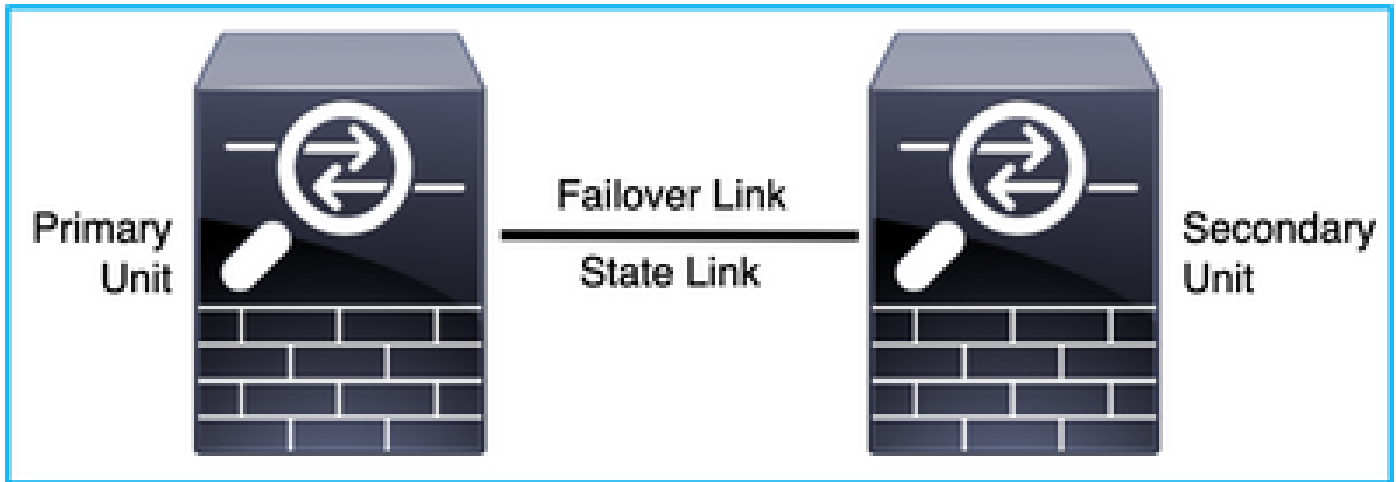
---

 Remarque : le FTD géré via FDM peut être ajouté dans la haute disponibilité à partir du code de version Firepower v6.3.0.

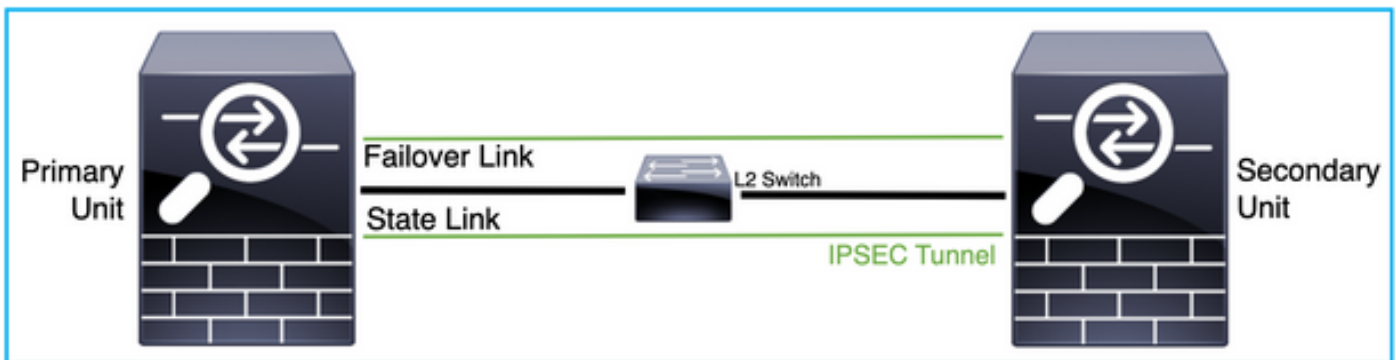
---

## Options de conception

Du point de vue de la conception du FTD, il peut être directement connecté, comme le montre cette image :



Il peut également être connecté via un commutateur de couche 2 (L2), comme illustré dans cette image :



## Terminologie HA

Actif	L'ASA actif reçoit tous les flux de trafic et filtre tout le trafic réseau. Les modifications de configuration sont effectuées sur l'ASA actif.
Liaison haute disponibilité	<p>Les deux unités d'une paire de basculement communiquent constamment via une liaison de basculement afin de déterminer l'état de fonctionnement de chaque unité et de synchroniser les modifications de configuration. Les informations partagées sur le lien sont les suivantes :</p> <ul style="list-style-type: none"> <li>• L'état de l'unité (active ou en veille)</li> <li>• Messages Hello (keep-alive)</li> <li>• État de la liaison réseau</li> <li>• échange d'adresses MAC</li> <li>• Réplication et synchronisation de la configuration</li> </ul>
Principal	Il s'agit de l'unité généralement configurée en premier lorsque vous créez une haute disponibilité. L'importance de ceci est que si les deux périphériques d'une ASA HA devaient être mis en place au même

	moment, le principal assume le rôle actif.
Secondaire	Il s'agit de l'unité généralement configurée en deuxième position lorsque vous créez une haute disponibilité. L'importance de ceci est que, si les deux périphériques d'une ASA HA devaient être mis en place au même moment, le secondaire assumerait le rôle de veille.
En veille	L'ASA de secours ne gère aucun trafic actif, il synchronise les connexions et la configuration à partir du périphérique actif, et assume le rôle actif en cas de basculement.
Lien d'état	L'unité active utilise la liaison d'état pour transmettre les informations d'état de connexion au périphérique en veille. Par conséquent, l'unité en veille peut maintenir certains types de connexions et ne vous affecte pas. Ces informations aident l'unité en veille à maintenir les connexions existantes en cas de basculement. Remarque : lorsque vous utilisez la même liaison pour le basculement et le basculement avec état, vous conservez les interfaces au mieux. Cependant, vous devez envisager une interface dédiée pour la liaison d'état et la liaison de basculement, si vous disposez d'une configuration étendue et d'un réseau à trafic élevé. Nous recommandons que la bande passante du lien de basculement dynamique corresponde à la bande passante la plus large des interfaces de données sur le périphérique.

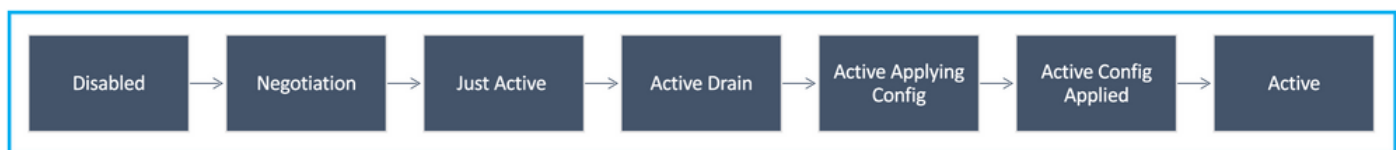
## États HA

Actif	Le périphérique gère actuellement le trafic actif sur le réseau et toutes les modifications de configuration qui doivent être effectuées doivent être effectuées sur ce périphérique.
Synchronisation des applications	Le périphérique dans cet état synchronise la configuration à partir du périphérique actif.
Synchronisation en bloc	Le périphérique dans cet état synchronise la configuration à partir du périphérique actif.
Désactivé	Le basculement sur l'unité a été désactivé (commande : no failover).

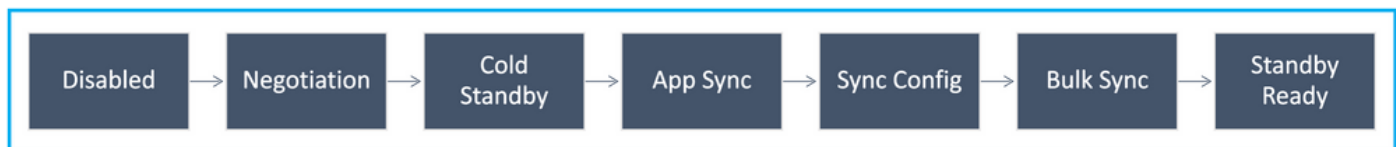
Négociation	Le périphérique vérifie la disponibilité du périphérique actif et joue le rôle actif s'il s'avère que le périphérique actif n'est pas prêt pour la mise en veille.
Veille prête	Le périphérique ne gère actuellement pas le trafic mais prend le rôle actif si le périphérique actif présente des problèmes de contrôle d'intégrité.
Configuration de synchronisation	La configuration est répliquée du périphérique actif vers le périphérique en veille.
Veille à froid	Le périphérique devient actif lors du basculement, mais ne réplique pas les événements de connexion.

## Diagramme de flux d'état haute disponibilité

Principal (sans homologue connecté) :



Secondaire (avec un homologue connecté actif) :



## Vérification UI

### Centre de gestion Firepower Géré FTD HA

L'état FTD HA peut être vérifié à partir de l'interface utilisateur FMC lorsque vous naviguez vers Device > Device Management, comme illustré dans cette image :

Firepower Management Center  
Devices / Device Management

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy Search Settings admin

View By: Group

Deployment History

All (2) Error (0) Warning (0) Offline (0) Normal (2) Deployment Pending (0) Upgrade (0) Snort 3 (2)

Search Device Add

Collapse All

Name	Model	Version	Chassis	Licenses	Access Control Policy
Ungrouped (1)					
FTD-HA High Availability					
<span style="color: green;">●</span> <b>FTD01(Primary, Active)</b> Snort 3 10.197.224.69 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base
<span style="color: green;">●</span> <b>FTD02(Secondary, Standby)</b> Snort 3 10.197.224.89 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base

## FTD HA géré par FDM

Page Aperçu de FDM principal :



Page Secondary FDM Overview :



## ASA HA gérée par ASDM

Page d'accueil d'ASDM vers ASA principal :

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.62

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

### Device Information

General License Virtual Resources

Host Name: **ciscoasa**  
 ASA Version: **9.12(3)12**  
 ASDM Version: **7.12(2)14**  
 Firewall Mode: **Routed**  
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 36m 28s**  
 Device Type: **ASAv**  
 Number of vCPUs: **8**  
 Total Memory: **8192 MB**

### Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
backup	109.106.53.100/24	up	up	3
inside	10.106.60.55/24	up	up	1
management	10.106.47.62/24	up	up	5
outside	10.106.48.65/24	up	up	1

Select an interface to view input and output Kbps

### Failover Status

This Host: **PRIMARY (Active)**      Other Host: **SECONDARY (Standby Ready)**      [Details](#)

### Traffic Status

Connections Per Second Usage

UDP: 0    TCP: 0    Total: 0

backup

'backup' Interface Traffic Usage (Kbps)

Input Kbps: 3    Output Kbps: 0

Latest ASDM Syslog Messages

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

[Enable Logging](#)

Device configuration loaded successfully.

Active admin 15 25/11/21 2:40:45 AM UTC

Page d'accueil ASDM vers ASA secondaire :

Cisco ASDM 7.12(2)14 for ASA - 10.106.47.64

Home Configuration Monitoring Save Refresh Back Forward Help Type topic Go

Device Dashboard

### Device Information

General License Virtual Resources

Host Name: **ciscoasa**  
 ASA Version: **9.12(3)12**  
 ASDM Version: **7.12(2)14**  
 Firewall Mode: **Routed**  
 Total Flash: **8192 MB**

Device Uptime: **30d 20h 39m 10s**  
 Device Type: **ASAv**  
 Number of vCPUs: **8**  
 Total Memory: **8192 MB**

### Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
backup	no ip address	up	up	2
inside	no ip address	up	up	1
management	10.106.47.64/24	up	up	89
outside	no ip address	up	up	1

Select an interface to view input and output Kbps

### Failover Status

This Host: **SECONDARY (Standby Ready)**      Other Host: **PRIMARY (Active)**      [Details](#)

### Traffic Status

Connections Per Second Usage

UDP: 0    TCP: 2    Total: 2

backup

'backup' Interface Traffic Usage (Kbps)

Input Kbps: 2    Output Kbps: 0

Latest ASDM Syslog Messages

ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

[Enable Logging](#)

Device configuration loaded successfully.

Standby admin 15 25/11/21 2:43:25 AM UTC

Gestionnaire de châssis Firepower pour 4100/9300 exécutant FTD/ASA HA

Page Primary FCM Logical Device :

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
ASA	9.12.4.18		10.197.216.7	10.197.216.1	Ethernet1/7	Online
Interface Name		Type		Attributes		
Ethernet1/1		data		Cluster Operational Status : not-applicable		
Ethernet1/2		data		HA-LINK-INTF : Ethernet3/7		
Ethernet1/3		data		HA-LAN-INTF : Ethernet3/7		
Ethernet1/4		data		HA-ROLE : active		
Ethernet1/5		data				
Ethernet1/6		data				
Ethernet1/8		data				
Ethernet3/7		data				
Ethernet3/8		data				

Page Secondary FCM Logical Device :

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Logical Device List (1 Instance) 0% (0 of 70) Cores Available Refresh Add

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
ASA	9.12.4.18		10.197.216.8	10.197.216.1	Ethernet1/7	Online
Interface Name		Type		Attributes		
Ethernet1/1		data		Cluster Operational Status : not-applicable		
Ethernet1/2		data		HA-LINK-INTF : Ethernet3/7		
Ethernet1/3		data		HA-LAN-INTF : Ethernet3/7		
Ethernet1/4		data		HA-ROLE : standby		
Ethernet1/5		data				
Ethernet1/6		data				
Ethernet1/8		data				
Ethernet3/7		data				
Ethernet3/8		data				

## Vérifier CLI

```
<#root>
```

```
>
```

```
show running-config failover
```

```
failover
```

```
failover lan unit secondary
```

```
failover lan interface failover-link GigabitEthernet0/2
```

```
failover replication http
```

```
failover link failover-link GigabitEthernet0/2
```

```
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

Les points importants à prendre en considération dans ce rapport sont les suivants :

basculement

failover lan unit secondary —> si l'unité est principale ou secondaire

failover lan interface failover-link GigabitEthernet0/2 —> failover link interface physique sur le périphérique

réplication de basculement http

failover link failover-link GigabitEthernet0/2



failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 —> adresses ip du lien de basculement du périphérique principal et du périphérique de secours.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
  This host: Secondary - Standby Ready
    Active time: 0 (sec)
    slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
    Interface outside (0.0.0.0): Normal (Not-Monitored)
    Interface inside (192.168.45.2): Normal (Not-Monitored)
    Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
  Other host: Primary - Active
    Active time: 707216 (sec)
    Interface outside (0.0.0.0): Normal (Not-Monitored)
    Interface inside (192.168.45.1): Normal (Not-Monitored)
    Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
    slot 1: snort rev (1.0) status (up)
    slot 2: diskstatus rev (1.0) status (up)
```

#### Stateful Failover Logical Update Statistics

```
Link : failover-link GigabitEthernet0/2 (up)
Stateful Obj      xmit      xerr      rcv      rerr
General           95752      0          115789    0
sys cmd           95752      0          95752     0
up time           0          0          0         0
RPC services      0          0          0         0
TCP conn          0          0          0         0
UDP conn          0          0          0         0
ARP tbl           0          0          20036    0
Xlate_Timeout     0          0          0         0
IPv6 ND tbl       0          0          0         0
VPN IKEv1 SA      0          0          0         0
VPN IKEv1 P2      0          0          0         0
VPN IKEv2 SA      0          0          0         0
VPN IKEv2 P2      0          0          0         0
VPN CTCP upd      0          0          0         0
VPN SDI upd       0          0          0         0
VPN DHCP upd      0          0          0         0
SIP Session       0          0          0         0
SIP Tx            0          0          0         0
```

SIP Pinhole	0	0	0	0
Route Session	0	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	1	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Rule DB B-Sync	0	0	0	0
Rule DB P-Sync	0	0	0	0
Rule DB Delete	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	5	504656
Xmit Q:	0	1	95752

Basculément activé : le basculément est activé ou désactivé.

Cet hôte : Secondaire - Prêt pour la veille. Le rôle de ce périphérique et les états des interfaces.

Autres hôtes : principal - actif. L'autre périphérique est à l'état Actif et communique avec le périphérique actuel.

<#root>

>

show failover history

```
=====
```

From State	To State	Reason
01:18:14 UTC Nov 25 2021 Not Detected	Negotiation	No Error
01:18:27 UTC Nov 25 2021 Negotiation	Just Active	No Active unit found
01:18:27 UTC Nov 25 2021 Just Active	Active Drain	No Active unit found
01:18:27 UTC Nov 25 2021 Active Drain	Active Applying Config	No Active unit found
01:18:27 UTC Nov 25 2021 Active Applying Config	Active Config Applied	No Active unit found
01:18:27 UTC Nov 25 2021 Active Config Applied	Active	No Active unit found

```
=====
```

Utilisez cette commande pour vérifier l'état historique des périphériques et les raisons de ces

changements d'état :

<#root>

>

show failover state

	State	Last Failure Reason	Date/Time
This host -	Secondary Standby Ready	None	
Other host -	Primary Active	None	

====Configuration State====

Sync Done - STANDBY

====Communication State====

Mac set

Vérifiez l'état actuel des périphériques et la raison du dernier basculement :

Champ	Description
État de configuration	<p>Affiche l'état de la synchronisation de la configuration.</p> <p>États de configuration possibles pour l'unité en veille :</p> <ul style="list-style-type: none"><li>• Config Sync - STANDBY : défini pendant l'exécution de la configuration synchronisée.</li><li>• Synchronisation de configuration d'interface - VEILLE</li><li>• Sync Done - STANDBY : défini lorsque l'unité en veille a terminé une synchronisation de configuration à partir de l'unité active.</li></ul> <p>États de configuration possibles pour l'unité active :</p> <ul style="list-style-type: none"><li>• Config Sync : défini sur l'unité active lorsqu'elle effectue une synchronisation de configuration avec l'unité en veille.</li><li>• Configuration d'interface Synchronisation</li><li>• Synchronisation terminée : définit lorsque l'unité active a terminé une synchronisation de configuration réussie avec l'unité en veille.</li><li>• Ready for Config Sync : défini sur l'unité active lorsque l'unité en veille signale qu'elle est prête à recevoir une synchronisation de configuration.</li></ul>

Champ	Description
État de communication	<p>Affiche l'état de la synchronisation des adresses MAC.</p> <ul style="list-style-type: none"> <li>• Mac set : les adresses MAC ont été synchronisées entre l'unité homologue et cette unité.</li> <li>• Updated Mac : utilisé lorsqu'une adresse MAC est mise à jour et doit être synchronisée avec l'autre unité. Également utilisé au moment de la transition où l'unité met à jour les adresses MAC locales synchronisées à partir de l'unité homologue.</li> </ul>
Date/heure	Affiche la date et l'horodatage de l'échec.
Motif du dernier échec	<p>Affiche la raison du dernier échec signalé. Ces informations ne sont pas effacées, même si la condition d'échec est effacée. Ces informations ne sont modifiées que lorsqu'un basculement se produit.</p> <p>Raisons possibles des échecs :</p> <ul style="list-style-type: none"> <li>• Interface Failure : nombre d'interfaces qui ont échoué et qui ont satisfait aux critères de basculement et provoqué le basculement.</li> <li>• Comm Failure : la liaison de basculement a échoué ou l'homologue est hors service.</li> <li>• Panne Du Fond De Panier</li> </ul>
Province	Affiche l'état principal/secondaire et actif/veille de l'unité.
Cet hôte/Autres hôtes	Cet hôte indique les informations relatives au périphérique sur lequel la commande a été exécutée. Un autre hôte indique des informations pour l'autre périphérique de la paire de basculement.

<#root>

>

show failover descriptor

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

# Dépannage

## Déboguages

```
<#root>
```

```
>
```

```
debug fover ?
```

```
cable          Failover LAN status
cmd-exec       Failover EXEC command execution
fail           Failover internal exception
fmsg           Failover message
ifc            Network interface status trace
open           Failover device open
rx             Failover Message receive
rxdump         Failover recv message dump (serial console only)
rxip           IP network failover packet recv
snort          Failover NGFW mode snort processing
switch         Failover Switching status
sync           Failover config/command replication
tx             Failover Message xmit
txdump         Failover xmit message dump (serial console only)
txip           IP network failover packet xmit
verify         Failover message verify
```

## Captures:

Captures d'interface de basculement :

Vous pouvez vous référer à cette capture pour déterminer si les paquets Hello de basculement sont envoyés sur la liaison de basculement au rythme auquel ils sont envoyés.

```
<#root>
```

```
>
```

```
show capture
```

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
```

```
>
```

```
show capture capfail
```

```
15 packets captured
```

```
1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
```

```
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

Capture ARP sur le lien de basculement :

Vous pouvez effectuer cette capture pour voir si les homologues ont des entrées Mac dans la table ARP.

```
<#root>
```

```
>
```

```
show capture
```

```
capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
```

```
>
```

```
show capture caparp
```

```
22 packets captured
```

```
1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
```

```
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

## Scénarios

Si l'unité homologue ne parvient pas à rejoindre le groupe haute disponibilité ou échoue pendant que vous déployez les modifications à partir de l'unité active, connectez-vous à l'unité défaillante, accédez à la page Haute disponibilité et cliquez sur le lien Historique de basculement.

### Échec de APP-SYNC

Si le résultat de la commande `show failover history` indique un échec de synchronisation d'application, cela signifie qu'il y a eu un problème au moment de la phase de validation de haute disponibilité, au cours de laquelle le système vérifie que les unités peuvent fonctionner correctement en tant que groupe haute disponibilité.

Le message « All validation pass » (Toutes les validations passées) s'affiche lorsque l'état De est App Sync et que le noeud passe à l'état Prêt pour la veille.

Tout échec de validation fait passer l'homologue à l'état Désactivé (Échec). Résolvez les problèmes pour que les homologues fonctionnent à nouveau comme un groupe à haute disponibilité.

Notez que si vous corrigez une erreur de synchronisation d'application et apportez des modifications à l'unité active, vous devez les déployer, puis reprendre la haute disponibilité pour que le noeud homologue y adhère.

Les messages indiquent les échecs et expliquent comment résoudre les problèmes. Ces erreurs peuvent se produire lors de la jonction de noeuds et lors de chaque déploiement suivant.

Au moment de la jonction d'un noeud, le système effectue une vérification par rapport à la dernière configuration déployée sur l'unité active.

Le noeud de veille ne parvient pas à joindre HA avec « CD App Sync error is App Config Apply Failed »

Sur la ligne de commande FTD de secours, `/ngfw/var/log/action_queue.log` doit avoir la raison de l'échec de configuration.

Correction : une fois l'erreur de configuration identifiée et les modifications requises effectuées, la haute disponibilité peut être reprise.

Voir bogue Cisco [IDCSCvu15611](#).

<#root>

=====

From State	To State	Reason
15:10:16 CDT Sep 28 2021 Not Detected	Disabled	No Error
15:10:18 CDT Sep 28 2021 Disabled	Negotiation	Set by the config command
15:10:24 CDT Sep 28 2021 Negotiation	Cold Standby	Detected an Active mate
15:10:25 CDT Sep 28 2021 Cold Standby	App Sync	Detected an Active mate
15:10:55 CDT Sep 28 2021 App Sync	Disabled	

CD App Sync error is App Config Apply Failed

Échec de la connexion du noeud de veille à HA avec « Échec de la progression de l'état HA en raison du délai d'attente APP SYNC »

Sur la ligne de commande FTD Standby, /ngfw/var/log/ngfwmanager.log doit avoir la raison du délai d'attente app-sync.

À ce stade, les déploiements de stratégie échouent également car l'unité active pense que la synchronisation des applications est toujours en cours.

Le déploiement de la stratégie renvoie l'erreur : « étant donné que le processus newNode join/AppSync est en cours, les modifications de configuration ne sont pas autorisées et rejettent donc la demande de déploiement. Veuillez réessayer le déploiement ultérieurement. »

Correction : parfois, lorsque vous reprenez la haute disponibilité sur le noeud de secours, il peut résoudre le problème.

Voir ID de bogue Cisco [CSCvt48941](#)

Voir ID de bogue Cisco [CSCvx11636](#)

<#root>

From State	To State	Reason
19:07:01 EST MAY 31 2021 Not Detected	Disabled	No Error
19:07:04 EST MAY 31 2021 Disabled	Negotiation	Set by the config command
19:07:06 EST MAY 31 2021 Negotiation	Cold Standby	Detected an Active mate
19:07:07 EST MAY 31 2021 Cold Standby	App Sync	Detected an Active mate
21:11:18 EST Jun 30 2021 App Sync	Disabled	

HA state progression failed due to APP SYNC timeout



Le noeud de secours ne parvient pas à joindre la haute disponibilité avec l'erreur « CD App Sync is Failed to apply SSP config on standby »

Sur la ligne de commande Standby FTD, /ngfw/var/log/ngfwmanager.log doit avoir la raison exacte de l'échec.

Correction : parfois, lorsque vous reprenez la haute disponibilité sur le noeud Veille, il peut résoudre le problème.

Voir ID de bogue Cisco [CSCvy04965](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvy04965)

<#root>

```
=====
From State          To State          Reason
=====
04:15:15 UTC Apr 17 2021
Not Detected        Disabled          No Error
04:15:24 UTC Apr 17 2021
Disabled           Negotiation      Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation        Cold Standby     Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby       App Sync         Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync           Disabled
CD App Sync error is Failed to apply SSP config on standby
=====
```

## Échec du contrôle d'intégrité

« HELLO not heard from mate » signifie que le partenaire est hors ligne ou que le lien de basculement ne communique pas les messages HELLO keepalive.

Essayez de vous connecter à l'autre périphérique, si SSH ne fonctionne pas, obtenez l'accès à la console et vérifiez si le périphérique est opérationnel ou hors ligne.

S'il est opérationnel, identifiez la cause de la panne avec la commande show failover state.

S'il n'est pas opérationnel, essayez un redémarrage en douceur et vérifiez si vous voyez des journaux de démarrage sur la console, sinon, le périphérique peut être considéré comme défectueux.

<#root>

```
=====
From State          To State          Reason
=====
```

```

=====
04:53:36 UTC Feb 6 2021
Failed                               Standby Ready

Interface check

02:12:46 UTC Jul 11 2021
Standby Ready                         Just Active                     HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied                 Active                           HELLO not heard from mate
=====

```

## Panne de Snort Down ou de disque

Si le FTD donne cette erreur, "Detect Inspection engine failure due to disk failure", il y a 2 possibilités.

Le moteur de détection (instance SNORT) est arrêté

Cela peut être validé avec la commande du côté Linux, `pmtool status | grep -i de`,

Correction : si l'une des instances est désactivée, recherchez `/ngfw/var/log/messages` et identifiez la cause.

## Le Périphérique Présente Une Utilisation Élevée Du Disque

Cela peut être validé avec la commande côté Linux, `df -Th`.

Correction : identifiez le répertoire qui consomme la plus grande partie du disque et contactez le TAC pour supprimer les fichiers indésirables.

<#root>

```

=====
From State          To State          Reason
=====
Active Config Applied Active          No Active unit found
16:07:18 UTC Dec 5 2020
Active              Standby Ready    Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready       Failed
Detect Inspection engine failure due to disk failure

16:07:29 UTC Dec 5 2020
Failed              Standby Ready    My Inspection engine is as good as peer due to di
=====

```

## Défaillance de la carte de service

De tels problèmes sont généralement signalés en raison d'une défaillance du module Firepower sur les périphériques ASA 5500-X. Veuillez vérifier la santé du module via show module sfr details.

Correction : collectez le Syslog ASA au moment de la panne, et ceux-ci peuvent contenir des détails comme le contrôle ou la panne du plan de données.

Cela peut être dû à diverses raisons dans le module SFR. Il est recommandé d'ouvrir le centre d'assistance technique pour trouver la cause première de ce problème sur l'IPS.

<#root>

```
=====
From State          To State          Reason
=====
21:48:19 CDT Aug 1 2021
Active             Standby Ready     Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready     Just Active
Service card in other unit has failed

21:48:19 CDT Aug 1 2021
Active Config Applied Active             Service card in other unit has failed
=====
```

## Défaillance de pulsation MIO

Firepower Threat Defense/ASA signale une panne due à une « panne de pulsation de la lame MIO » sur les routeurs FPR1K, 2K, 4K et 9K.

Voir ID de bogue Cisco [CSCvy14484](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvy14484)

Voir ID de bogue Cisco [CSCvh26447](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvh26447)

<#root>

```
=====
From State          To State          Reason
=====
20:14:45 EDT Apr 14 2021
Active Config Applied Active             No Active unit found
20:15:18 EDT Apr 14 2021
Active             Failed
MIO-blade heartbeat failure

20:15:19 EDT Apr 14 2021
Failed             Negotiation       MIO-blade heartbeat recovered
=====
```

## Informations connexes

- <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html>
- [https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id\\_72185](https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185)
- [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.