

Dépannage des rechargements inattendus ASA ou FTD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Éléments communs à vérifier sur toutes les plates-formes et tous les périphériques logiques](#)

[Vérifiez que le périphérique \(logique ou châssis\) a redémarré ou est bloqué](#)

[Recherchez Crashinfo dans le cas d'une panne de logiciel ASA/ina \(sur FTD\)](#)

[Éléments à vérifier sur les plates-formes ASA](#)

[Toutes les plates-formes ASA exécutant une image ASA](#)

[Plates-formes ASA prenant en charge l'image FTD](#)

[Éléments à vérifier sur les plates-formes Firepower](#)

[FXOS FP9300/FP4100](#)

[Sur FP9300/FP4100 exécutant FTD](#)

[Sur FP9300/FP4100 exécutant ASA](#)

[Sur FP2100 FXOS/ASA/FTD](#)

[Sur FP1000 FXOS/ASA/FTD](#)

[Télécharger les fichiers principaux](#)

[Autres éléments à vérifier \(spécifiques aux plates-formes Firepower 4100 et 9300\)](#)

[Afficher les fichiers principaux dans le module](#)

[Bogues connus liés à la panne du système](#)

Introduction

Ce document décrit comment dépanner des scénarios où un périphérique Firepower Threat Defense (FTD) ou Adaptive Security Appliance (ASA) se recharge sans raison évidente.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comprendre les bases des plates-formes matérielles Firepower et ASA
- Comprendre les périphériques logiques sur les plates-formes Firepower

Composants utilisés

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

- ASA 5500-X avec logiciel ASA version 9. x
- ASA 5500-X avec logiciel FTD versions 6.2.3 et ultérieures
- Gammes Firepower 1000, 1100, 2100, 4100 et 9300 avec logiciel ASA version 9. x
- Firepower 1000, 1100, 2100, 4100 et 9300 avec le logiciel FTD version 6.2.3 et ultérieure

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

Dans ce document, le périphérique fait référence aux pare-feu ASA ou Firepower de nouvelle génération (NGFW), rebaptisés pare-feu sécurisés Cisco, qui exécutent une image ASA ou FTD en tant que périphérique logique.

Les pare-feu sécurisés Cisco incluent différentes versions matérielles et logicielles. La gamme ASA comprend les pare-feu de la gamme 5500-X et la gamme Firepower comprend les périphériques des gammes FPR 1000, 2100, 4100 et 9300. Ce document discute de l'approche de départ afin d'identifier le niveau que le périphérique ou le logiciel a planté sur toutes les plates-formes mentionnées et si le crash était réel ou non. Il répertorie également tous les artefacts à collecter, où les trouver et comment les utiliser afin de trouver la cause première du crash.

Éléments communs à vérifier sur toutes les plates-formes et tous les périphériques logiques

Vérifiez que le périphérique (logique ou châssis) a redémarré ou est bloqué

Pour ASA, utilisez la commande du mode de configuration afin de vérifier la disponibilité du périphérique : `# show version | in Up`

Sur le matériel Firepower, utilisez ces commandes afin de vérifier la disponibilité du périphérique et du châssis (niveau FXOS) :

```
FP4100-3# connect fxos
```

```
FP4100-3(fxos)# show system uptime
```

```
System start time: Thu Oct 31 22:50:09 2019
```

```
System uptime: 391 days, 19 hours, 30 minutes, 45 seconds
```

```
Kernel uptime: 391 days, 19 hours, 34 minutes, 34 seconds
```

Active supervisor uptime: 391 days, 19 hours, 30 minutes, 45 seconds

 Remarque : si vous constatez que le périphérique est activé au moment du problème, cela confirme le redémarrage du périphérique.

Vérifiez et confirmez si des problèmes d'alimentation peuvent entraîner des redémarrages soudains du périphérique.

Si le temps de fonctionnement n'est pas lié à l'horodatage du temps d'arrêt sur le réseau (ou du basculement ou de l'unité quittant le cluster), cela signifie que le problème ne s'est pas produit en raison du rechargement du périphérique et que le diagnostic doit naviguer dans une direction complètement différente.

Recherchez Crashinfo dans le cas d'une panne de logiciel ASAlina (sur FTD)

Une panne système est une situation dans laquelle le système a détecté une erreur irrécupérable et a redémarré lui-même. Lorsqu'un pare-feu tombe en panne, il crée un fichier de format texte spécial appelé `crashinfo` fichier. Ce fichier fournit des informations de diagnostic et des journaux qui aident à déterminer la cause première d'une panne. Pour un ASA, le `crashinfo` est du texte brut stocké dans `Flash`: et contient le contenu du registre de mémoire avec une longue liste d'autres informations - version du logiciel, données collectées, etc.

Saisissez la commande `show crashinfo` dans l'interface de ligne de commande ASA en mode d'exécution privilégié. Vous pouvez consulter la sortie dans n'importe quel éditeur de texte ou même sur la console ASA elle-même.

```
show flash | in crash
```

Partagez ce résultat avec le centre d'assistance technique Cisco (TAC) dans une demande de service et ils peuvent le décoder à l'aide d'outils internes. Ce résultat fournit des informations utiles sur les processus et les threads, ce qui aide les développeurs à examiner et à corréliser la panne avec d'autres événements à l'intérieur du périphérique.

 Remarque : en général, lorsque vous collectez `show tech-support` sortie de l'ASA ou de Lina (sur FTD), `show crashinfo` est idéalement présent dans cette sortie. Cependant, le résultat est souvent différent ou incomplet par rapport à l'exécution directe de `show crashinfo erasecat4000_flash`: Par conséquent, il est recommandé de toujours saisir le `show crashinfo` directement sur l'interface CLI ASA ou Lina.

En plus des détails courants à vérifier, il y a plus d'informations et d'artefacts à collecter qui dépendent des différents niveaux de crash qui peuvent se produire. Sur les plates-formes ASA, il ne peut y avoir qu'un seul niveau de panne. Cependant, les plates-formes Firepower peuvent

présenter une panne au niveau du périphérique logique (FTD ou logiciel ASA) ou au niveau du châssis (FXOS).

Une fois que la disponibilité a confirmé que le périphérique est tombé en panne, un `coredump` est généré, ce qui est nécessaire pour un examen plus approfondi par le centre d'assistance technique Cisco. Les `coredump` peut être de différents types en fonction du composant du logiciel qui a planté. Les `coredump` les fichiers sont également enregistrés dans différents répertoires/parties du disque, en fonction du composant qui a planté.

Éléments à vérifier sur les plates-formes ASA

Les plates-formes ASA n'ont qu'un seul composant qui peut être ASA ou FTD.

Toutes les plates-formes ASA exécutant une image ASA

Les `corefiles` sont stockées sous `disk0` du lecteur flash interne en raison de la panne. Afin de vérifier la `corefiles`, saisissez la commande `dir disk0:/coredumpfsys` commande :

```
<#root>
```

```
ciscoasa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2021 sysdebug  
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core_lina.1227726922.258.11.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2021 lost+found
```

```
1 file(s) total size: 87580218 bytes  
16106127360 bytes total (15749222400 bytes free/97% free)
```

Saisissez la commande `show coredump filesystem` afin d'afficher tous les fichiers sur le `coredump` , qui indique également l'espace disque. Il est recommandé d'archiver le `coredump` lorsque cela est opportun, car il est possible qu'une `coredump` peut supprimer le précédent `coredump(s)` afin de s'adapter au coeur actuel.

```
<#root>
```

```
ciscoasa# show coredump filesystem
```

```
Coredump Filesystem Size is 100 MB
```

```
Filesystem type is FAT for disk0
```

```
Filesystem          1k-blocks      Used Available Use% Mounted on
/dev/loop0          102182         75240      26942    74% /mnt/disk0/coredumpfsys
```

Directory of disk0:/coredumpfsys/

```
246  -rwx  20205386   19:16:44 Nov 26 2021
```

```
core_lina.1227726922.258.11.gz
```

```
247  -rwx  36707919   19:21:56 Nov 26 2021
```

```
core_lina.1227727222.258.6.gz
```

```
248  -rwx  20130838   19:26:36 Nov 26 2021
```

```
core_lina.1227727518.258.11.gz
```

Si vous ne voyez pas de `coredump` dans `disk0`, il y a de fortes chances que le `coredump` n'est pas activé, ce qui signifie que la révision ne peut pas être effectuée pour cet événement. Afin d'activer `coredump` pour les occurrences futures, entrez cette commande :

```
ciscoasa(config)#coredump enable
```

WARNING: Enabling `coredump` on an ASA5505 platform will delay the reload of the system in the event of software forced reload. The exact time depends on the size of the `coredump` generated.

```
Proceed with coredump filesystem allocation of 60 MB
on 'disk0:' (Note this may take a while) ? [confirm]
```

```
Making coredump file system image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Coredump file system image created & mounted successfully
```

```
/dev/loop0 on /mnt/disk0/coredumpfsys type vfat
(rw, fmask=0022, dmask=0022, codepage=cp437, iocharset=iso8859-1)
```

Plates-formes ASA prenant en charge l'image FTD

Les plates-formes ASA 5506-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X et ASA 5555-X prennent en charge les images FTD et en font un pare-feu de nouvelle génération.

Sur toutes ces plates-formes ASA prises en charge qui exécutent l'image FTD, `corefiles` sont situés sous `/var/data/cores` OU `/ngfw/var/data/cores` via le mode expert. Elles sont également reflétées sous la `disk0:/coredumpfsys` de Lina flash.

```
<#root>
```

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

```
ls -l
```

```
total 59660
-rw-r--r-- 1 root root 4815651 Mar 14 17:07
core.SFDataCorrelato.2035.1552608478.gz

-rw-r--r-- 1 root root 56198339 Mar 14 16:47
core.lina.2113.1552607243.gz
```

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

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/

2498562 -rw- 56198339 23:47:26 Mar 14 2019
core.lina.2113.1552607243.gz

2498563 -rw- 4815651 00:07:58 Mar 15 2019
core.SFDataCorrelato.2035.1552608478.gz
```

```
2 file(s) total size: 61013990 bytes
42949672960 bytes total (39523602432 bytes free/92% free)
```

Éléments à vérifier sur les plates-formes Firepower

Les plates-formes Firepower sont livrées avec deux composants logiciels. Le premier est le FXOS, qui est le système d'exploitation du châssis, et le second est l'instance de l'application, également connue sous le nom de périphérique logique, qui peut être ASA ou FTD. Par conséquent, il est important d'identifier la pièce qui s'est écrasée afin de déterminer à quel emplacement télécharger le `corefiles`

Si l'instance de l'application tombe en panne sur Firepower 1000/2000/4100 et 9300, les informations de panne et `corefiles` sont toujours générées par défaut. Cependant, le core dump peut être désactivé dans certains cas.

Afin de vérifier si le core dump est activé sur 4100/9300, entrez ces commandes :

```
connect module 1 console
Firepower-module1>show platform coredumps
```

Activation ou désactivation des vidages principaux du module Firepower :

Activez les vidages de mémoire sur un module Firepower afin de faciliter le dépannage en cas de panne du système, ou pour l'envoyer au TAC Cisco si demandé.

```
Firepower# connect module 1 console
show coredump detail
```

La sortie de la commande affiche les informations d'état de vidage de mémoire actuelles et indique si la compression de vidage de mémoire est activée.

<#root>

```
Firepower-module1>
```

```
show coredump detail
```

```
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

Utilisez `config coredump` afin d'activer ou de désactiver les core dumps, et d'activer ou de désactiver la compression core dump pendant une panne.

- Saisissez la commande `config coredump enable` afin d'activer la création d'un core dump pendant une panne.
- Saisissez la commande `config coredump disable` afin de désactiver la création de core dump pendant une panne.
- Saisissez la commande `config coredump compress enable` afin d'activer la compression des core dumps.
- Saisissez la commande `config coredump compress disable` afin de désactiver la compression core dump.

Cet exemple montre comment activer le core dump :

<#root>

```
Firepower-module1>
```

```
config coredump enable
```

```
CoreDump enabled successfully.
```

```
ASA coredump enabled, do 'config coredump disableAsa' to disable
```

```
Firepower-module1>config coredump compress enable
```

```
WARNING: Enabling compression delays system reboot for several minutes after a system failure. Are you
```

```
y
```

```
Firepower-module1>
```

 Remarque : les fichiers de vidage du coeur consomment de l'espace disque. Si l'espace est faible et que la compression n'est pas activée, un fichier de vidage du coeur n'est pas enregistré même si les vidages du coeur sont activés.

Les fichiers de panne et les fichiers de mémoire doivent être téléchargés pour une analyse complète, car il est possible que le fichier de panne ne contienne pas toutes les données.

FXOS FP9300/FP4100

Sur FP9300/FP4100, le FXOS `corefiles` sont situés sous le `local-mgmt cores` répertoire.

```
firepower-4110# connect local-mgmt
firepower-4110(local-mgmt)# dir cores

1 9337521 Apr 30 11:28:15 2016 1462040896_0x101_snm_log.5289.tar.gz
1 1067736 Oct 09 10:38:49 2017 1507570679_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 798663 Oct 10 18:05:54 2017 1507683913_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 348160 Feb 11 23:53:25 2019 core.21845

Usage for workspace://
3999125504 bytes total
64200704 bytes used
3730071552 bytes free
firepower-4110(local-mgmt)#
```

Afin de copier le fichier principal de FXOS sur votre ordinateur local, entrez cette commande :

```
firepower-4110(local-mgmt)# copy workspace:/cores:/<file>.tar.gz scp://username@x.x.x.x
```

Sur FP9300/FP4100 exécutant FTD

Sur FP9300/FP4100 exécutant FTD, `corefiles` sont situés sous `/var/data/cores` ou `/ngfw/var/data/cores` via le mode expert. Elles sont également reflétées sous la `disk0:/coredumpfsys` de Lina flash.

```
root@firepower:/var/data/cores# ls -l
total 59660
-rw-r--r-- 1 root root 4815651 Mar 14 17:07 core.SFDataCorrelato.2035.1552608478.gz
-rw-r--r-- 1 root root 56198339 Mar 14 16:47 core.lina.2113.1552607243.gz
root@firepower:/var/data/cores#
```

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
2498562 -rw- 56198339 23:47:26 Mar 14 2019 core.lina.2113.1552607243.gz
2498563 -rw- 4815651 00:07:58 Mar 15 2019 core.SFDataCorrelato.2035.1552608478.gz
```

2 file(s) total size: 61013990 bytes
42949672960 bytes total (39523602432 bytes free/92% free)

Sur FP9300/FP4100 exécutant ASA

Sur FP9300/FP4100 exécutant ASA, `corefiles` sont situés sous le `disk0:/coredumpfsys` répertoire.

```
<#root>
```

```
asa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
11 drwx 16384 17:34:50 Sep 10 2018 lost+found  
12 -rw- 317600388 16:43:40 Mar 14 2019
```

```
core.lina.6320.1552607012.gz
```

1 file(s) total size: 317600388 bytes
21476089856 bytes total (21255872512 bytes free/98% free)

Sur FP2100 FXOS/ASA/FTD

Sur FP2100 FXOS/ASA/FTD, `corefiles` sont situés sous le `local-mgmt cores` que vous utilisiez ASA ou FTD. Sur FTD, ils sont également mis en miroir sous `/ngfw/var/data/cores` (ou `/var/data/cores`) et `/ngfw/var/common/` via le mode expert. Cependant, notez que les plates-formes FP2100 n'ont pas le `disk0 :/coredumpfsys` répertoire.



Remarque : l'ID de bogue Cisco [CSCvh01912](#) a été envoyé afin de rendre FP2100 compatible avec la plate-forme FP9300/4100. Tant que cette question n'est pas résolue, utilisez l'emplacement décrit afin de trouver le `corefiles`.

Emplacement des fichiers principaux Firepower lorsque le FTD est dans Firepower 2100, 1000, appliance ASA et appliance ISA 3000 :

Pour toutes ces plates-formes, utilisez cette procédure afin de localiser les fichiers de base liés à tous les processus Firepower.

Sous `/ngfw/var/common/`:

1. Connectez-vous à l'interface de ligne de commande du matériel via SSH ou la console.

2. Passez en mode expert :

```
> expert
admin@firepower:~$
```

3. Devenez un utilisateur root.

```
<#root>
```

```
admin@firepower:~$
```

```
sudo su
```

```
Password:
```

```
root@firepower:/home/admin#
```

4. Accédez à la page `/ngfw/var/common/` , où se trouvent les fichiers de base.

```
root@firepower:/home/admin# cd /ngfw/var/common/
```

5. Recherchez le fichier dans le dossier.

```
root@firepower:/ngfw/var/common# ls -l | grep -i core
total 21616
-rw-r--r-- 1 root root 22130788 Nov  6  2020 process.core.tar.gz
```

FTD sur FP2100 : sous `/ngfw/var/data/cores:`

```
> expert
admin@firepower:~$ sudo su
[cut]
root@firepower:/home/admin# ls -l /ngfw/var/data/cores
total 133740
-rw-r--r-- 1 root root 4761622 Jun  4 05:13 core.SFDataCorrelato.28634.1622783636.gz
-rw-r--r-- 1 root root 132014190 Jun  4 05:17 core.lina.11.1378.1622783800.gz
drwx----- 2 root root 16384 Nov  5 2019 lost+found
drwxr-xr-x 3 root root 4096 Nov  5 2019 sysdebug
```

```
> connect fxos
```

```
[cut]
```

```
firepower# connect local-mgmt
```

```
firepower(local-mgmt)# dir cores
```

```
1 4761622 Jun 04 05:13:56 2021 core.SFDataCorrelato.28634.1622783636.gz
1 132014190 Jun 04 05:17:25 2021 core.lina.11.1378.1622783800.gz
2 16384 Nov 05 22:35:15 2019 lost+found/
3 4096 Nov 05 22:36:05 2019 sysdebug/
```

```
Usage for workspace://
85963259904 bytes total
15324155904 bytes used
70639104000 bytes free
firepower(local-mgmt)#
```

ASA sur FP2100 :

```
firepower-2110(local-mgmt)# dir cores
```

```
1 167408075 Jul 04 00:43:25 2018 core.lina.6.2025.1530657764.gz
2 16384 Mar 28 16:17:56 2018 lost+found/
3 4096 Mar 28 16:18:43 2018 sysdebug/
```

 Remarque : le FXOS corefiles sont stockées dans le même répertoire de coeurs à partir de la connexion local-mgmt.

Sur FP1000 FXOS/ASA/FTD

Sur FP1000 FXOS/ASA/FTD, ce processus est similaire à celui du FP2100. En outre, la `disk0:/coredumpfsys` est disponible du côté de Lina.

FTD sur FP1000 :

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
FP1010> ena
```

```
Password:
```

```
FP1010# dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
13 -rw- 86493184 19:59:39 Jun 03 2021 core.lina.18707.1622750370.gz
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
14 -rw- 4770749 20:19:24 Jun 03 2021 core.SFDataCorrelato.7098.1622751564.gz
12 -rw- 197689 23:01:08 May 19 2021 core.top.6163.1621465268.gz
16 -rw- 4752067 20:28:03 Jun 03 2021 core.SFDataCorrelato.28195.1622752083.gz
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
15 -rw- 5048839 20:20:32 Jun 03 2021 core.SFDataCorrelato.18952.1622751632.gz
```

```
5 file(s) total size: 101262528 bytes
123418959872 bytes total (110302621696 bytes free/89% free)
```

```
> connect fxos
[cut]
```

```
FP1010# connect local-mgmt
FP1010(local-mgmt)# dir cores
```

```
1 5048839 Jun 03 20:20:32 2021 core.SFDataCorrelato.18952.1622751632.gz
1 4752067 Jun 03 20:28:03 2021 core.SFDataCorrelato.28195.1622752083.gz
1 4770749 Jun 03 20:19:24 2021 core.SFDataCorrelato.7098.1622751564.gz
1 86493184 Jun 03 19:59:39 2021 core.lina.18707.1622750370.gz
1 197689 May 19 23:01:08 2021 core.top.6163.1621465268.gz
2 16384 Aug 30 23:13:37 2019 lost+found/
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://
159926181888 bytes total
17475063808 bytes used
142451118080 bytes free
```

```
> expert
```

```
admin@FP1010:~$ sudo su
```

```
Password:
```

```
root@FP1010:/home/admin# ls -l /var/data/cores
```

```
total 99048
```

```
-rw-r--r-- 1 root root 5048839 Jun 3 20:20 core.SFDataCorrelato.18952.1622751632.gz
-rw-r--r-- 1 root root 4752067 Jun 3 20:28 core.SFDataCorrelato.28195.1622752083.gz
-rw-r--r-- 1 root root 4770749 Jun 3 20:19 core.SFDataCorrelato.7098.1622751564.gz
-rw-r--r-- 1 root root 86493184 Jun 3 19:59 core.lina.18707.1622750370.gz
-rw-r--r-- 1 root root 197689 May 19 23:01 core.top.6163.1621465268.gz
drwx----- 2 root root 16384 Aug 30 2019 lost+found
drwxr-xr-x 3 root root 4096 Aug 30 2019 sysdebug
```

ASA sur FP1000 :

```
<#root>
```

```
ciscoasa# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core.lina.27515.1622782155.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
```

```
1 file(s) total size: 87580218 bytes
16106127360 bytes total (15749222400 bytes free/97% free)
```

```
ciscoasa#
```

```
connect fxos
```

```
[cut]
```

```
FP1010#
```

```
connect local-mgmt
```

```
FP1010(local-mgmt)#
```

```
dir cores
```

```
1 87580218 Jun 04 04:49:23 2021
```

```
core.lina.27515.1622782155.gz
```

```
2 16384 Aug 30 23:13:37 2019 lost+found/
```

```
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://  
159926181888 bytes total  
5209071616 bytes used  
154717110272 bytes free
```

 Remarque : FXOS corefiles sont stockées dans le même répertoire de coeurs à partir de la connexion local-mgmt.

Télécharger les fichiers principaux

Il y a un `copy` commandement sous `connect local-mgmt` et Lina/ASA CLI. Pour le mode expert FTD, utilisez la commande `scp erasecat4000_flash:`.

Autres éléments à vérifier (spécifiques aux plates-formes Firepower 4100 et 9300)

Vérifiez le résultat de la commande `show pmon state` commandement sous `local-mgmt` sur FXOS. Cet exemple montre la sortie souhaitée lorsqu'aucun des processus ne s'est arrêté. Cette sortie capture non seulement les pannes au niveau du périphérique, mais aussi les pannes du module d'interface/DME, etc.

```
<#root>
```

```
fp1120-v-1(local-mgmt)#
```

```
show pmon state
```

SERVICE NAME	STATE	RETRY(MAX)	EXITCODE	SIGNAL	CORE
-----	----	-----	-----	-----	----
svc_sam_dme	running	0(4)	0	0	no
svc_sam_dcosAG	running	0(4)	0	0	no
svc_sam_portAG	running	0(4)	0	0	no
svc_sam_statsAG	running	0(4)	0	0	no

httpd.sh	running	0(4)	0	0	no
svc_sam_sessionmgrAG	running	0(4)	0	0	no
sam_core_mon	running	0(4)	0	0	no
svc_sam_svcmonAG	running	0(4)	0	0	no
svc_sam_serviceOrchAG	running	0(4)	0	0	no
svc_sam_appAG	running	0(4)	0	0	no
svc_sam_envAG	running	0(4)	0	0	no

Si vous ne trouvez aucun fichier core dans les répertoires FTD/ASA associés, les fichiers core peuvent être présents dans la CLI de démarrage sur 4100/9300.

Afficher les fichiers principaux dans le module

Entrez cette commande afin de vous connecter à la console du module :

```
<#root>
```

```
/ssa # connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

```
support filelist
```

```
=====
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
Crashinfo_and_Core_Files
Boot_Files
ApplicationLogs
Transient_Core_Files
Type a sub-dir name to list its contents, or [x]

to Exit: Transient_Core_Files
```

```
-----files-----
[No files]
([b] to go back)
Type a sub-dir name to list its contents: b
```

```
=====
Directory: /
Downloads_Directory
CSP_Downloaded_Files
Archive_Files
Crashinfo_and_Core_Files
Boot_Files
ApplicationLogs
Transient_Core_Files
Type a sub-dir name to list its contents, or [x] to Exit:
```

Crashinfo_and_Core_Files

-----sub-dirs-----

lost+found

-----files-----

```
2017-03-20 20:45:06 | 40639151 | core.lina.48857.1490042695.gz
2017-03-20 20:48:47 | 40638054 | core.lina.18113.1490042915.gz
2017-03-20 20:52:28 | 40638186 | core.lina.18112.1490043137.gz
2017-03-20 20:56:10 | 40638466 | core.lina.18123.1490043359.gz
2017-03-20 20:59:53 | 40638345 | core.lina.18262.1490043582.gz
2017-03-20 21:03:35 | 40638120 | core.lina.18476.1490043803.gz
2017-03-20 21:07:22 | 40638335 | core.lina.18529.1490044031.gz ([b] to go back)
```

Type a sub-dir name to list its contents: b =====

Directory: /

Downloads_Directory

CSP_Downloaded_Files

Archive_Files

Crashinfo_and_Core_Files

Boot_Files

ApplicationLogs

Transient_Core_Files Type a sub-dir name to list its contents, or [x] to Exit: x

Firepower-module1>

S'il n'y a pas de fichiers de base à bootCLI, vous pouvez vérifier les journaux au niveau FXOS :

connect fxos

```
1-(fxos)# show logging onboard obfl-logs
2-(fxos)# show logging onboard stack-trace
3-(fxos)# show logging onboard kernel-trace
4-(fxos)# show logging onboard exception-log
5-(fxos)# show logging onboard internal kernel
6-(fxos)# show logging onboard internal platform
7-(fxos)#show logging onboard internal kernel | no-more
8-(fxos)#show logging onboard internal kernel-big | no-more
9-(fxos)#show logging onboard internal platform | no-more
10-(fxos)#show logging onboard internal reset-reason | no-more
```

If logging at fxos level is enabled, you can check the logs on fxos.

It contains the syslog buffer and OBFL logs stored in NVRAM

Connect fxos

show logging log -----This is a non-persistent syslog buffer

show logging onboard obfl-logs -----Non-volatile storage for history of boot up and reset occurrences.

show logging nvram -----Non-volatile storage for critical logs.Important for historical is

On FXOS CLI, at the top-level scope use following command.

show fault detail or show fault

If you want to view faults for a specific object, scope to that object and then enter the show fault co

You can check for audit-logs which is a persistent store of user operations.

This moreover stores the sequence of user operations done.

firepower# scope security

firepower# /security # show audit-logs

Parfois, le périphérique tombe en panne silencieusement et ne génère aucun fichier de panne ou de mémoire centrale. Dans ce cas, vous pouvez rechercher les journaux :

```
At FTD instance or device level:  
#####
```

```
# Navigate to the /ngfw/var/log or /var/log and open the messages log file. Check all the logs generated.  
You can search for following messages (in /ngfw/var/log or /var/log) to confirm if device rebooted with
```

```
firepower shutdown[2313]: shutting down for system reboot  
Stopping Cisco Firepower 2130 Threat Defense  
pm:process [INFO] Begin Process Shutdown
```

```
# Check for syslogs messages (specific to device up and down )generated when the device rebooted.  
You can check for syslogs messages generated 15-30 min before and after the device reboot to know if
```

Bogues connus liés à la panne du système

Reportez-vous à ces pages pour obtenir des informations supplémentaires sur la panne du système :

- ID de bogue Cisco [CSCvu84127](#) - FTD crash silencieux sans générer de fichier core ou crash
- ID de bogue Cisco [CSCwa35845](#) - ASA 5516 rechargé en générant des fichiers principaux
- ID de bogue Cisco [CSCvw99444](#) - FTD planté avec `crashinfo/corefile`
- ID de bogue Cisco [CSCv86926](#) - FTD bloqué lors de la génération `crashfile`
- ID de bogue Cisco [CSCvp16482](#) - ASA est tombé en panne en générant un fichier principal
- ID de bogue Cisco [CSCvm53545](#) - ASA peut effectuer un retraçage et un rechargement sans générer de `crashinfo` fichier

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.