Dépannage du pare-feu sécurisé et du redémarrage Firepower inattendus

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Abréviations
- Informations générales
- Workflow de dépannage
- Étapes de dépannage
  - Firepower 1000, 2100, Secure Firewall 1200, 3100 et 4200 exécutant FTD en mode natif ou ASA
  - Pare-feu sécurisé 3100, 4200 exécutant FTD en mode conteneur
  - Firepower 4100/9300
  - Plates-formes virtuelles exécutant FTD
  - Module de sécurité Firepower 4100/9300 exécutant FTD en mode natif ou exécutant ASA
  - Module de sécurité Firepower 4100/9300 exécutant FTD en mode conteneur
- Analyser la disponibilité
- Analyser les fichiers de messages FTD
- Analyser les fichiers de messages du module de sécurité ou du châssis
- Analyser les fichiers ssp-pm.log
- Analyser les fichiers ssp-shutdown.log
- Analyse des raisons de réinitialisation du châssis
- Analyser les erreurs ou les exceptions matérielles
- Analyser les fichiers journaux des autres plates-formes
- Analyser les fichiers SEL/OBFL
- Analyser les journaux de console ASA/FTD
- Analyse des problèmes de tension et d'alimentation
- Références

Introduction

Ce document décrit les étapes de dépannage pour les rechargements inattendus des pare-feu Secure Firewall/Firepower.

Conditions préalables

Exigences

Connaissances de base sur les produits.

Composants utilisés

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

- Pare-feu sécurisé 1200, 3100, 4200
- Firepower 1000, 4100, 9300
- Système d'exploitation extensible sécurisé Cisco (FXOS) 2.16(0.136)
- Cisco Secure Firewall Threat Defense (FTD) 7.6.1.291
- Cisco Secure Firewall Management Center (FMC) 7.6.1.291
- Appareil de sécurité adaptatif (ASA) 9.22.2.9

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.

Abréviations

Abréviations	Explication
FXOS	Système d'exploitation extensible Firepower : Système d'exploitation sous-jacent qui s'exécute sur les plates-formes Firepower 1000, 2100, 3100, 4100, 4200 et 9300.
Application	Toute application s'exécutant sur la plate-forme FXOS (ASA ou Secure Firewall Threat Defense).
SSP	Plate-forme de services de sécurité : Ce terme fait référence aux plates-formes matérielles de sécurité Cisco qui exécutent FXOS.

OBFL	Journalisation des défaillances embarquées : Le fichier journal qui stocke les données relatives aux pannes ; par exemple, erreurs de mémoire, erreurs de bus, interruptions. Le fichier réside dans le CIMC.
CMC	Contrôleur de gestion du châssis.
CIMC	Contrôleur de gestion intégré Cisco.
SEL	Journal des événements système (SEL) : Le journal des événements système réside sur le CIMC du module de sécurité dans la mémoire NVRAM.
PSU	Unité d'alimentation.
PDU	Unité de distribution d'alimentation.
PECI	Platform Environment Control Interface Bus : Il s'agit du bus entre le contrôleur de gestion de carte (BMC) et le processeur et le concentrateur de contrôleur de plate-forme (PCH). PECI est utilisé pour collecter des données à partir du processeur, du module DIMM, etc.
BMC	Contrôleur de gestion du conseil.
NPU	Unité de processeur réseau.
FPGA	Réseau De Portes Programmable Par L'Utilisateur.
SAM	La gestion FXOS est un ensemble de processus qui fournit une fonctionnalité de gestion du châssis et est également appelée collectivement SAM (Server Array Manager).
ECC	La mémoire à code correcteur d'erreurs est un type de mémoire informatique qui peut détecter et corriger les erreurs dans les données lorsqu'elles sont stockées ou récupérées.
PCIe	PCI Express, Peripheral Component Interconnect Express.
PBTN (bouton d'alimentation) :	PBTN représente un bouton d'alimentation physique.

Informations générales

Dans ce document, « reboot », « reload » et « restart » sont utilisés de façon interchangeable. Du point de vue de l'utilisateur, un redémarrage inattendu peut être défini en gros comme n'importe quel redémarrage, à l'exception des cas bien connus, documentés ou attendus :

1. Redémarrer en raison de l'installation ou des mises à niveau logicielles.
2. Redémarrage en raison d'actions déclenchées par l'utilisateur, telles qu'un redémarrage à partir de l'interface de ligne de commande (CLI), de l'interface utilisateur graphique (UI) ou des actions de mise hors tension/sous tension manuelle.

Selon le déclencheur, un redémarrage peut être gracieux ou disgracieux :

1. Un redémarrage en douceur désigne généralement le redémarrage d'un système, d'un périphérique ou d'un service qui permet à tous les processus actuels de se terminer correctement et à tous les fichiers ou données d'être enregistrés avant le redémarrage. Cela permet d'éviter la perte ou la corruption des données. Exemples de redémarrage en douceur :
    - Redémarrer en raison de l'installation ou des mises à niveau logicielles.
    - Redémarre en raison d'actions déclenchées par l'utilisateur, comme un redémarrage à partir de l'interface de ligne de commande ou de l'interface utilisateur graphique.
    - Dans certains cas, le traçage logiciel.

---

2. Un redémarrage disgracieux est l'opposé d'un redémarrage en douceur, quand le système redémarre disgracieusement, c'est-à-dire sans fin gracieuse des processus. Des redémarrages malhonnêtes peuvent entraîner une perte ou une corruption des données. Voici des exemples de déclencheurs :
    - Mettez hors tension et sous tension accidentellement en débranchant tous les câbles d'alimentation ou en appuyant sur le bouton d'alimentation.
    - Pénuries d'alimentation, problèmes dans les unités d'alimentation du châssis.
    - Différents problèmes matériels, FPGA, environnementaux, etc., qui entraînent un ou plusieurs redémarrages brusques.

Causes courantes des redémarrages :

- Actions des utilisateurs à partir de la CLI ou de l'interface utilisateur de gestion.
- Mises à niveau ou rétrogradations logicielles.
- Traceback logiciel.
- Déclenche par les processus critiques du système d'exploitation/système pour des raisons

autres que le retraçage dans le logiciel.
- Problèmes matériels tels que SSD endommagé, erreurs de mémoire, exceptions dans le processeur, FPGA interne, etc.
- Problèmes environnementaux, tels que la perte d'énergie, la surchauffe, etc.
- Défauts logiciels ou autres problèmes dans les composants tiers.
- Utilisation élevée de l'espace disque.

Dans les plates-formes basées sur des châssis, il est important de tenir compte de l'étendue du redémarrage, en particulier de ce qui a été exactement redémarré :

- Application ASA/FTD.
- Le module de sécurité (Firepower 4100/9300).
- Le châssis.

Le comportement par défaut inclut :

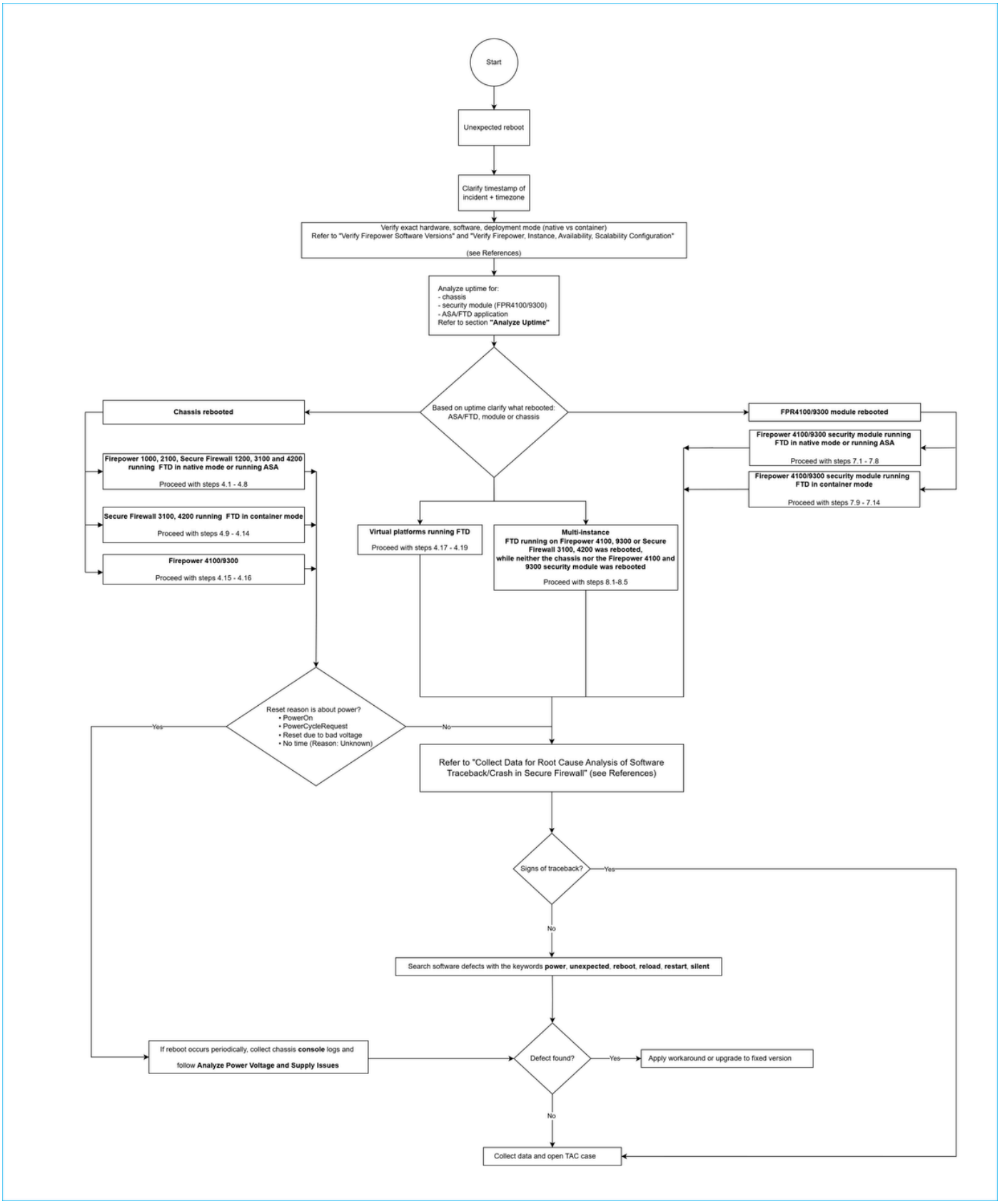
- Si un redémarrage sur FTD s'exécutant en mode natif, ASA sur Firepower 1000/2100 ou Secure Firewall 3100/4200 est déclenché ; le châssis redémarre également.
- Si un redémarrage sur FTD s'exécute en mode natif, ASA sur Firepower 4100/9300 ou si des modules de sécurité sont déclenchés, le module de sécurité redémarre également. Le châssis n'est pas affecté.
- Si un redémarrage en mode FTD multi-instance sur les modules de sécurité Firepower 4100/9300 est déclenché, seule cette instance redémarre et le module de sécurité et le châssis ne sont pas affectés.
- Si un redémarrage en mode FTD multi-instance sur Secure Firewall 3100 et 4200 est déclenché, seule cette instance redémarre et le châssis n'est pas affecté.
- Un redémarrage sur le module de sécurité Firepower 4100/9300 redémarre également, toutes les applications s'exécutant sur les modules concernés indépendamment du mode multiinstance natif.
- Un redémarrage sur le châssis redémarre également tous les modules de sécurité et toutes les applications.

L'arrêt de certains processus critiques, qu'ils soient gracieux ou non, peut entraîner des redémarrages. Exemple :

- Si le processus du plan de données, également connu sous le nom de lina se termine en raison de traceback, le pare-feu redémarre. La seule exception est la version logicielle avec la fonctionnalité « Data plane quick reload » introduite dans ASA 9.20(x) et FTD 7.4.1 pour des plates-formes spécifiques.
- Si le gestionnaire de processus pm se termine, le pare-feu redémarre.

Workflow de dépannage

Examinez le workflow de dépannage qui fait référence aux étapes de dépannage :



Étapes de dépannage

1. Prenez note de l'horodatage de l'événement aussi précisément que possible, en vous assurant de tenir compte du fuseau horaire.
2. Vérifiez le matériel exact, sécurisez le type de logiciel de pare-feu (ASA ou FTD), la version du logiciel et le mode de déploiement (mode natif ou multi-instance). Référez-vous à Vérifier les versions du logiciel Firepower, Vérifier Firepower, Instance, Disponibilité, Évolutivité Configuration pour les étapes de vérification détaillées.

3. Reportez-vous à la section Analyser la disponibilité pour corréler la disponibilité de l'application ASA/FTD, du module de sécurité (Firepower 4100/9300 uniquement) et du châssis. L'objectif est de clarifier l'étendue du redémarrage, l'application, le module de sécurité ou le châssis.
4. Si le châssis a été redémarré, procédez comme suit :

Firepower 1000, 2100, Secure Firewall 1200, 3100 et 4200 exécutant FTD en mode natif ou ASA

4.1. Consultez la section Analyser les fichiers de messages FTD (FTD uniquement).

4.2. Consultez la section Analyser les fichiers ssp-pm.log.

4.3. Consultez la section Analyze ssp-shutdown.log Files.

4.4. Consultez la section Analyser les journaux de la console ASA/FTD.

4.5. Suivez les étapes de la section Collecte de données pour l'analyse de la cause première du retour/plantage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

4.6. Consultez la section Analyser les motifs de réinitialisation du châssis.

4.7. Consultez la section Analyser les erreurs matérielles ou les exceptions.

4.8. Consultez la section Analyser les fichiers journaux de la plate-forme.

Pare-feu sécurisé 3100, 4200 exécutant FTD en mode conteneur

4.9. Consultez la section Analyser les fichiers ssp-pm.log.

4.10. Vérifiez la section Analyze ssp-shutdown.log Files.

4.11. Suivez les étapes de la section Collecte de données pour l'analyse des causes premières du retour/blocage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

4.12. Consultez la section Analyser les motifs de réinitialisation du châssis.

4.13. Consultez la section Analyser les erreurs matérielles ou les exceptions.

4.14. Consultez la section Analyser les fichiers journaux de la plate-forme.

Firepower 4100/9300

4.15. Consultez la section Analyser les motifs de réinitialisation du châssis.

4.16. Suivez les étapes de la section Collecte de données pour l'analyse des causes premières du retour/blocage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

Plates-formes virtuelles exécutant FTD

4.17. Consultez la section Analyser les fichiers de messages FTD.

4.18. Consultez la section Analyser les journaux de la console ASA/FTD.

4.19. Suivez les étapes de la section Collecte de données pour l'analyse des causes premières du retour/blocage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

---

5. Si des raisons de réinitialisation telles que celles-ci sont trouvées dans la section Analyser les raisons de réinitialisation du châssis, alors référez-vous à Analyser la tension d'alimentation et les problèmes d'alimentation :

- Mise sous tension
- DemandeCycleAlimentation
- Réinitialisation en raison d'une tension incorrecte
- Pas de temps (raison : Inconnu)

---

6. Si le redémarrage du châssis est récurrent, collectez les journaux de la console.

7. Procédez comme suit pour Firepower 4100/9300 si le module de sécurité a été redémarré :

Module de sécurité Firepower 4100/9300 exécutant FTD en mode natif ou exécutant ASA

7.1. Consultez la section Analyser les fichiers de messages FTD (FTD uniquement).

7.2. Consultez la section Analyser les fichiers ssp-pm.log.

7.3. Consultez la section Analyze ssp-shutdown.log Files.

7.4. Consultez la section Analyser les journaux de la console ASA/FTD.

7.5. Suivez les étapes de la section Collecte de données pour l'analyse des causes premières du retour/plantage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

7.6. Consultez la section Analyser les erreurs matérielles ou les exceptions.

7.7. Consultez la section Analyser les fichiers SEL/OBFL.

7.8. Consultez la section Analyser les fichiers journaux de la plate-forme.

Module de sécurité Firepower 4100/9300 exécutant FTD en mode conteneur

7.9. Consultez la section Analyser les fichiers ssp-pm.log.

7.10. Consultez la section Analyze ssp-shutdown.log Files.

7.11. Suivez les étapes de la section Collecte de données pour l'analyse des causes premières du retour/plantage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

7.12. Consultez la section Analyser les erreurs matérielles ou les exceptions.

7.13. Consultez la section Analyser les fichiers SEL/OBFL.

7.14. Consultez la section Analyser les fichiers journaux de la plate-forme.

---

8. Procédez comme suit si un FTD multi-instance exécuté sur Firepower 4100, 9300 ou Secure Firewall 3100, 4200 a été redémarré, mais que ni le châssis ni le module de sécurité Firepower 4100 et 9300 n'ont été redémarrés :

8.1. Consultez la section Analyser les fichiers de messages FTD.

8.2. Consultez la section Analyser les fichiers ssp-pm.log.

8.3. Vérifiez la section Analyze ssp-shutdown.log Files.

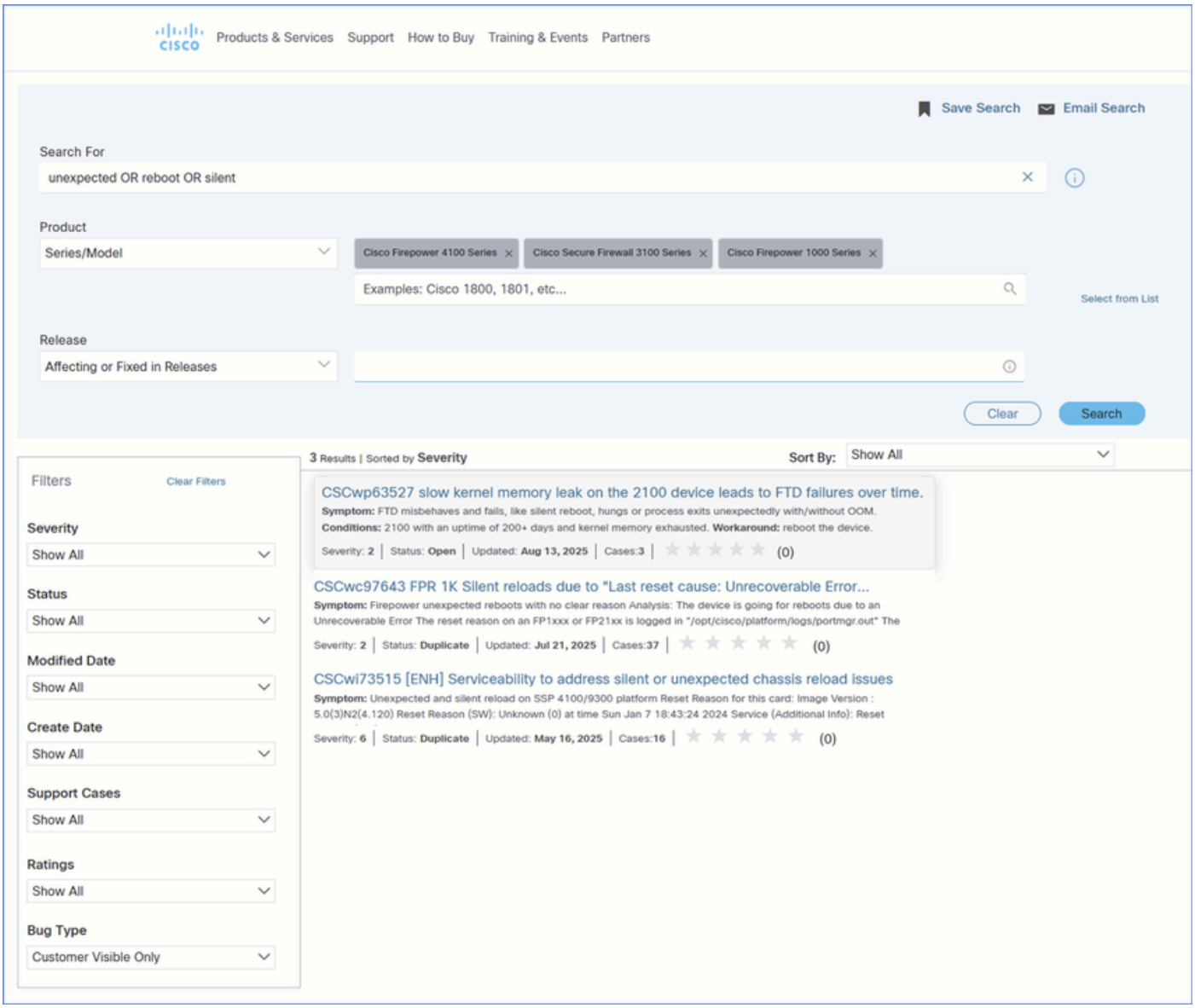
8.4. Consultez la section Analyser les journaux de la console ASA/FTD.

8.5. Suivez les étapes de la section Collecte de données pour l'analyse de la cause première du retour/plantage logiciel dans Secure Firewall afin de vérifier les symptômes du retour logiciel et pour la collecte de données.

---

9. S'il y a des signes de redémarrages en raison du retraçage du logiciel, ouvrez un dossier TAC et fournissez les données collectées.

10. Rechercher les défauts du logiciel avec les mots-clés inattendu, reboot, power, reload, restart, silent :



Si un défaut correspondant est détecté :

- Assurez-vous que] les symptômes et les conditions correspondent à ceux décrits dans le défaut.
- Appliquez un contournement, le cas échéant.
- Mettez à niveau vers la version fixe, le cas échéant.

---

11. Passez en revue la section Data Collection et ouvrez un dossier TAC.

Analyser la disponibilité

L'objectif de cette section est de vérifier la disponibilité de l'application ASA/FTD, du module de

sécurité (Firepower 4100/9300 uniquement) et du châssis.

1. Vérifiez le temps de disponibilité du moteur de pare-feu exécutant la commande show version sur ASA et la commande show version system sur FTD :

<#root>

```
>

show version system


---------------[ firewall-FTD ]---------------
Model                     : Cisco Firepower 4112 Threat Defense (76) Version 7.6.1 (Build 291)
UUID                      : e9460e12-674c-11f0-97e5-d5ad3617d287
LSP version               : lsp-rel-20241211-1948
VDB version               : 408
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.22(1)21
SSP Operating System Version 2.16(0.3007)

Compiled on Thu 29-May-25 01:38 GMT by fpbesprd
System image file is "disk0:/fxos-lfbff-k8.2.16.0.136.SPA"

Config file at boot was "startup-config"

firewall-FTD up 5 days 0 hours
```

Dans le fichier de dépannage FTD, vérifiez le fichier command-output/'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output' :

<#root>

```
/command-outputs$

less 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'


…
firewall-FTD up 5 days 0 hours
…
```

Pour ASA, vérifiez la disponibilité dans le fichier show-tech.

2. Pour les FTD fonctionnant en mode natif sur des plates-formes virtuelles, Firepower 1000,

2100, Secure Firewall 1200, 3100 et 4200 ; vérifiez la disponibilité du système d'exploitation (jours, heures et minutes) en mode expert. Dans ce cas, le temps de fonctionnement du châssis est à peu près le même que celui du système d'exploitation :

```
<#root>

>

expert


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

uptime


 06:30:40

 up 6 days,  8:01

,  1 user,  load average: 5.14, 5.45, 5.48
```

Dans le fichier de dépannage FTD, vérifiez le fichier dir-archives/var-log/top.log:

```
<#root>

dir-archives/var-log$

less top.log


================================================================================================

Tue Jul 22 04:02:11 UTC 2025

top - 04:02:11

up 6 days, 13:57

,  4 users,  load average: 2.23, 2.42, 2.59
Tasks: 167 total,   2 running, 165 sleeping,   0 stopped,   0 zombie
%Cpu(s): 26.6 us,  7.8 sy,  1.6 ni, 64.1 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   7629.8 total,   2438.4 free,   4559.6 used,    631.8 buff/cache
MiB Swap:   5369.2 total,   3713.7 free,   1655.5 used.   2849.9 avail Mem
```

---

3. Pour FTD en mode multi-instance sur Secure Firewall 3100 ou 4200 et ASA exécuté sur

Firepower 1000, 2100, Secure Firewall 1200, 3100 et 4200, aucune commande n'est disponible pour vérifier la disponibilité du châssis.

Vous pouvez vérifier la disponibilité des lames :

<#root>

>

connect fxos

…
firewall#

scope ssa

firewall /ssa #

show slot detail expand

Slot:
    Slot ID: 1
    …

Blade Uptime: up 16 hours, 2 min

Dans le fichier de dépannage du châssis, vérifiez la disponibilité dans le fichier opt/cisco/platform/logs/sysmgr/sam_logs/topout.log :

<#root>

opt/cisco/platform/logs/sysmgr/sam_logs/topout.log $

less topout.log

[Jul 23 13:15:22]
top - 13:15:22

up 16:02

```
,  1 user,  load average: 12.24, 11.85, 11.75
```

---

4. Dans le cas de Firepower 4100/9300, vérifiez la disponibilité du châssis et du module de sécurité dans l'interface de ligne de commande FXOS.

Temps de fonctionnement du châssis :

<#root>

```
firewall /ssa #

connect fxos


firewall(fxos)#

show system uptime


System start time:          Tue Jul 22 21:57:44 2025
System uptime:              6 days, 9 hours, 49 minutes, 50 seconds
Kernel uptime:              6 days, 9 hours, 45 minutes, 58 seconds
Active supervisor uptime:   6 days, 9 hours, 49 minutes, 50 seconds
```

Temps de disponibilité du module de sécurité :

<#root>

```
firewall#

scope ssa


firewall /ssa #

show slot detail expand


Slot:
    Slot ID: 1
    …
        Blade Uptime: up 5 days, 37 min
```

Dans le fichier de dépannage du châssis, exécutez les sorties de la commande show system uptime dans le fichier *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, et la commande show slot expand detail expand dans le fichier *_BC1_all/FPRM_A_TechSupport/sam_techsupportinfo où * est la partie du nom du fichier de dépannage, par exemple, 20250311123356_ FW_BC1_all.

Analyser les fichiers de messages FTD

Cette section couvre l'analyse du fichier de messages FTD qui contient des journaux liés à l'arrêt, au redémarrage et aux déclencheurs potentiels.

FTD exécuté sur toutes les plates-formes

Le fichier contient des journaux relatifs à l'arrêt, au redémarrage et à leurs déclencheurs potentiels sur le FTD exécuté sur :

- Plates-formes virtuelles, châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100 et 4200.
- Modules de sécurité Firepower 4100 et 9300.

Le fichier est accessible dans :

- FTD CLISH en mode expert : /ngfw/var/log/messages
- Fichier de dépannage FTD : dir-archives/var-log/messages

Pour trouver le déclencheur des arrêts ou redémarrages, vérifiez les messages contenant Defense dans le fichier de messages dans les fichiers de dépannage FTD. Vérifiez tous les fichiers de messages, y compris messages.1, messages.2, etc. Ces messages indiquent clairement un arrêt progressif :

- Arrêt de Cisco Secure Firewall...ou arrêt de Cisco Firepower...
- ...Threat Defense est en cours d'arrêt

<#root>

```
root@CSF1220-2:/ngfw/var/log#
```

grep -a Defense /ngfw/var/log/messages

```
messages:Jul 22 21:07:10 firepower-1220 SF-IMS[36894]: [36894] S11audit-startup-shutdown:start [INFO] C
messages:Jul 22 21:12:37 firepower-1220 SF-IMS[62594]: [62594] sensor:CLI Start [INFO] Starting Cisco S
messages:Jul 22 21:13:03 firepower-1220 SF-IMS[65410]: [65410] S99sensor:CLI Start [INFO] Starting Cisc
```

```
messages:Jul 23 12:56:43 CSF1220-2 SF-IMS[61878]: [61878] K01sensor:CLI Stop [INFO] Stopping Cisco Secur
```

```
messages:Jul 23 12:57:03 CSF1220-2 SF-IMS[62749]: [62749] K69audit-startup-shutdown:stop [INFO] Cisco Se
```

```
messages:Jul 23 13:00:21 CSF1220-2 SF-IMS[10866]: [10866] S11audit-startup-shutdown:start [INFO] Cisco S
```

```
messages:Jul 23 13:00:36 CSF1220-2 SF-IMS[13443]: [13443] S99sensor:CLI Start [INFO] Starting Cisco Secu
```

<#root>

```
root@1140-2:/ngfw/var/log#
```

```
grep -a Defense /ngfw/var/log/messages
```

```
messages:Jul 22 09:20:42 FPR1140-2 SF-IMS[6012]: [6012] S11audit-startup-shutdown:start [INFO] Cisco Fi
messages:Jul 22 09:21:35 FPR1140-2 SF-IMS[9050]: [9050] S99sensor:CLI Start [INFO] Starting Cisco Firep
```

```
messages:Jul 22 11:32:37 FPR1140-2 SF-IMS[15129]: [15129] K01sensor:CLI Stop [INFO] Stopping Cisco Firep
```

```
messages:Jul 22 11:32:55 FPR1140-2 SF-IMS[15940]: [15940] K69audit-startup-shutdown:stop [INFO] Cisco Fi
```

```
messages:Jul 22 11:36:38 FPR1140-2 SF-IMS[5980]: [5980] S11audit-startup-shutdown:start [INFO] Cisco Fir
```

```
messages:Jul 22 11:36:53 FPR1140-2 SF-IMS[7594]: [7594] S99sensor:CLI Start [INFO] Starting Cisco Firepo
```

Analyser les fichiers de messages du module de sécurité ou du

châssis

Cette section traite de l'analyse du module de sécurité ou du fichier de messages du châssis qui contient les journaux associés au noyau du système d'exploitation.

Le fichier contient des journaux relatifs à l'arrêt, au redémarrage et à leurs déclencheurs potentiels sur le FTD exécuté sur :

- Châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200.
- Modules de sécurité Firepower 4100 et 9300.

Le fichier est accessible dans :

- FTD basé sur le matériel s'exécutant en mode natif : /opt/cisco/platform/log/messages.
- Dépannez le fichier de FTD basé sur le matériel qui s'exécute en mode natif : dir-archives/opt-cisco-platform-logs/messages.
- Fichier de dépannage des châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100 et 4200 : /opt/cisco/platform/log/messages.
- Fichier show-tech du module de sécurité Firepower 4100/9300 : /opt/cisco/platform/log/messages.

Voici les points clés des journaux de ce fichier :

- Vérifiez tous les fichiers de messages, y compris messages.1, messages.2, etc.
- Lorsque le noyau du système d'exploitation démarre, les journaux du noyau sont écrits dans ce fichier. Sur les plates-formes matérielles et les modules de sécurité, les journaux sont initialement écrits dans le fuseau horaire UTC jusqu'à ce que le fuseau horaire personnalisé soit appliqué pendant le démarrage.

Pour cette raison, différents journaux dans le même fichier peuvent avoir des horodatages différents avec des fuseaux horaires différents.

Considérez cet exemple d'un module de sécurité Firepower 4100 avec le fuseau horaire UTC+2 :

<#root>

2025-08-18T14:54:16+02:00 Firepower-module1/2 root: FXOS shutdown log started: pid = 52994 cmdline = /bi

```
2025-08-18T14:54:16+02:00 Firepower-module1/2 root: FXOS shutdown log completed: pid = 52994
```

```
2025-08-18T14:54:17+02:00 Firepower-module1/2 syslog-ng[1230]: syslog-ng shutting down; version='3.36.1'
```

```
2025-08-18T12:57:11+00:00 intel-x86-64/1 syslog-ng[1237]: syslog-ng starting up; version='3.36.1' <--- s
```

```
2025-08-18T12:57:11+00:00 intel-x86-64/1 kernel: [    0.000000] Linux version 5.10.200-yocto-standard (
2025-08-18T12:57:11+00:00 intel-x86-64/1 kernel: [    0.000000] Command line: rw console=ttyS0,38400 lo
…
2025-08-18T12:58:34+00:00 intel-x86-64/1 csp-console: Adi not started yet, trying to bring up
2025-08-18T12:58:34+00:00 intel-x86-64/1 ssp_tz[12159]: INFO: Lina is started
2025-08-18T12:58:34+00:00 intel-x86-64/1 SMA: INFO ExecProcessorMain [140588852127296]: finished proces
2025-08-18T12:58:34+00:00 intel-x86-64/1 ssp_tz[12167]: INFO: notify TZ to ASA LINA <---- Time zone cha
2025-08-18T14:58:35+02:00 intel-x86-64/1 ssp_tz[12192]: INFO: successfully notified TZ to ASA LINA, wai
2025-08-18T14:58:36+02:00 intel-x86-64/1 csp-console: Adi not started yet, trying to bring up
2025-08-18T14:58:39+02:00 intel-x86-64/1 csp-console[1237]: Last message 'Adi not started yet,' repeate
```

Analyser les fichiers ssp-pm.log

Cette section couvre l'analyse des fichiers /opt/cisco/platform/logs/ssp-pm.log qui contiennent des journaux liés à l'arrêt ou au redémarrage de l'application ASA/FTD.

Le fichier contient des journaux d'arrêt ou de redémarrage pour les applications ASA/FTD exécutées sur :

- Châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200.
- Modules de sécurité Firepower 4100 et 9300 (pas le châssis).

Le fichier est uniquement accessible dans :

- FTD mode natif (non multi-instance) CLISH en mode expert : opt/cisco/platform/logs/ssp-pm.log.
- Fichier de dépannage du mode natif FTD : dir-archives/opt-cisco-platform-logs/ssp-pm.log.
- Fichier de dépannage du châssis sur Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200 : /opt/cisco/platform/logs/ssp-pm.log.

Pour identifier les arrêts ou redémarrages en douceur, recherchez des lignes comme SHUTDOWN WARNING correspondant à l'horodatage de redémarrage/arrêt. Assurez-vous de vérifier tous les fichiers ssp-pm.log, y compris ssp-pm.log.1, ssp-pm.log.2, et ainsi de suite. Ces messages indiquent clairement un arrêt progressif :

<#root>

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Beginning System Shutdown request for CSP Ap

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-GetShutdownMaxForceQuitTimer: acquiring max

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Upgrade process ready for reboot

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-GetShutdownMaxForceQuitTimer: No force_quit_

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Continue System Shutdown request for CSP App

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: corre

cisco-asa.9.22.2.9__asa_001_JMX2324G1DJ947ECO1.conf

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: corre

...cspCfg_cisco-asa.9.22.2.9__asa_001_JMX2324G1DJ947ECO1.xml.allocated_cpu_core

…
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: stop
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: Stop

Analyser les fichiers ssp-shutdown.log

Cette section traite de l'analyse des fichiers /opt/cisco/platform/logs/ssp-shutdown.log, qui contiennent des journaux générés lorsque le châssis/module de sécurité s'arrête ou redémarre.

Le fichier contient des journaux d'arrêt ou de redémarrage pour :

- Châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200.
- Modules de sécurité Firepower 4100 et 9300 (pas le châssis).

Le fichier est accessible uniquement dans :

- FTD mode natif (non multi-instance) CLISH en mode expert : opt/cisco/platform/logs/ssp-shutdown.log.
- Fichier de dépannage du mode natif FTD : dir-archives/opt-cisco-platform-logs/ssp-shutdown.log.
- fichier de dépannage du châssis de Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200 : /opt/cisco/platform/logs/ssp-shutdown.log.
- Fichier de dépannage du module de sécurité Firepower 4100/9300 : opt/cisco/platform/logs/ssp-shutdown.log.

Reportez-vous à la section Dépannage des procédures de génération de fichiers Firepower sur la façon de générer le FTD, le châssis et le module de sécurité pour dépanner les fichiers.

Pour trouver le déclencheur des arrêts ou redémarrages en douceur, procédez comme suit :

1. Vérifiez que les lignes comme arrêt FXOS commencé correspondent à l'horodatage de redémarrage/arrêt. Assurez-vous de vérifier tous les fichiers ssp-shutdown.log, y compris ssp-shutdown.log.1, ssp-shutdown.log.2, et ainsi de suite.

```
#### Wed Jul 23 12:56:42 UTC 2025: FXOS shutdown started: pid = 61677 cmdline = /bin/sh/sbin/fxos_log_s
```

---

2. Recherchez dans l'arborescence des processus les lignes qui contiennent fxos_log_shutdown ou shutdown ou reboot.sh.

Exemple 1 : La demande de redémarrage provient d'un homologue avec l'UUID 068f09e6-3825-11ee-a72c-e78d34d303cc et l'adresse IP 192.0.2.100, qui est le FMC :

```
<#root>

root     61074  4593  2 12:56 ?        00:00:00          |   \_ /usr/bin/perl /ngfw/usr/local/sf/bin/ex

192.0.2.100 068f09e6-3825-11ee-a72c-e78d34d303cc

 SF::System::
Privileged::RebootSystem
root     61097 61074  0 12:56 ?        00:00:00          |       \_ /bin/sh /ngfw/usr/local/sf/bin/rebo
root     61670 61097  0 12:56 ?        00:00:00          |

\_ /bin/sh /sbin/shutdown -r now


root     61671 61670  0 12:56 ?        00:00:00          |               \_ /bin/sh /sbin/exec_fxos_log
root     61676 61671  0 12:56 ?        00:00:00          |                   \_ /usr/bin/timeout 15 /sb
root     61677 61676  0 12:56 ?        00:00:00          |                       \_ /bin/sh /sbin/fxos_
root     61685 61677  0 12:56 ?        00:00:00          |                           \_ /bin/ps -ef –fo

>

show managers


Type                      : Manager

Host                      : 192.0.2.100


Display name              : 192.0.2.100
Version                   : 7.6.1 (Build 291)

Identifier                : 068f09e6-3825-11ee-a72c-e78d34d303cc


Registration              : Completed
Management type           : Configuration and analytics
```

Exemple 2 : Redémarrage en raison d'une mise à niveau logicielle :

```
<#root>

root      2432     1  0 03:59 ?        00:00:00 /bin/bash /isan/bin/kp_reboot.sh Reboot requested for So
```

```
root      2694  2432  0 03:59 ?        00:00:00  \_ /bin/sh /isan/bin/sam_reboot.sh Reboot requested for

root      3774  2694  0 04:00 ?        00:00:00      \_ /usr/bin/sudo /sbin/shutdown -r now Reboot reque

root      3777  3774  0 04:00 ?        00:00:00          \_ /bin/sh /sbin/shutdown -r now Reboot request

root      3778  3777  0 04:00 ?        00:00:00              \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root      3783  3778  0 04:00 ?        00:00:00                  \_ /usr/bin/timeout 15 /sbin/fxos_log_
root      3784  3783  0 04:00 ?        00:00:00                      \_ /bin/sh /sbin/fxos_log_shutdown
root      3790  3784  0 04:00 ?        00:00:00                          \_ /bin/ps -ef –forest
```

Exemple 3 : Un redémarrage a été demandé par l'utilisateur admin en exécutant la commande CLISH reboot :

<#root>

```
root     22189     1  0 Jul23 ?        00:00:01 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root     20963 22189  0 06:55 ?        00:00:00  \_ sshd: admin [priv]
admin    20970 20963  0 06:55 ?        00:00:00  |   \_ sshd: admin@pts/0
admin    20975 20970  0 06:55 pts/0    00:00:00  |       \_ /isan/bin/ucssh --ucs-mgmt -p admin -c conn
admin    21077 20975  0 06:55 pts/0    00:00:00  |           \_ /ngfw/usr/bin/clish
admin    36022 21077  0 07:23 pts/0    00:00:00  |               \_ /ngfw/usr/bin/clish
admin    36023 21077  0 07:23 pts/0    00:00:00  |               \_ /bin/sh /tmp/klish.fifo.21077.1Hwyq
admin    36024 36023  8 07:23 pts/0    00:00:01  |

\_ /usr/bin/perl /usr/local/sf/bin/sfcli.pl reboot system

root     36083 36024  0 07:23 pts/0    00:00:00  |

\_ /usr/bin/sudo /ngfw/usr/local/sf/bin/reboot.sh

root     36088 36083  0 07:23 pts/0    00:00:00  |                           \_ /bin/sh /usr/local/sf/b
root     36433 36088  0 07:23 pts/0    00:00:00  |

\_ /bin/sh /sbin/shutdown -r now

root     36434 36433  0 07:23 pts/0    00:00:00  |                               \_ /bin/sh /sbin/e
root     36439 36434  0 07:23 pts/0    00:00:00  |                                   \_ /usr/bin/ti
root     36440 36439  0 07:23 pts/0    00:00:00  |                                       \_ /bin/sh
root     36448 36440  0 07:23 pts/0    00:00:00  |                                           \_ /bi
```

Exemple 4 : Un arrêt a été déclenché en cliquant sur le bouton d'alimentation. PBTN représente un bouton d'alimentation physique. Le fait d'appuyer sur le bouton d'alimentation d'une machine déclenche cet événement. Le script utilise cet événement pour lancer un processus d'arrêt, généralement parce qu'un utilisateur a l'intention de désactiver le pare-feu en toute sécurité :

<#root>

```
root      1310     1  0 00:14 ?        00:00:00 /usr/sbin/acpid -c /etc/acpi/events

root     50700  1310  0 00:32 ?        00:00:00  \_ /bin/sh /etc/acpi/acpi_handler.sh button/power PBTN


root     50701 50700  0 00:32 ?        00:00:00

\_ /bin/sh /sbin/shutdown -h now


root     50702 50701  0 00:32 ?        00:00:00          \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     50707 50702  0 00:32 ?        00:00:00              \_ /usr/bin/timeout 15 /sbin/fxos_log_shut
root     50708 50707  0 00:32 ?        00:00:00                  \_ /bin/sh /sbin/fxos_log_shutdown
root     50715 50708  0 00:32 ?        00:00:00                      \_ /bin/ps -ef -forest
```

Exemple 5 : Un redémarrage a été demandé par le processus interne npu_accel_mgr :

<#root>

```
root     12649  5280  0 13:59 ?        00:01:06  \_

npu_accel_mgr


root     19030 12649  0 18:22 ?        00:00:00  |

\_ /bin/sh /sbin/shutdown -r now


root     19031 19030  0 18:22 ?        00:00:00  |       \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     19036 19031  0 18:22 ?        00:00:00  |           \_ /usr/bin/ timeout 15 /sbin/fxos_log_shu
root     19037 19036  0 18:22 ?        00:00:00  |               \_ /bin/sh /sbin/fxos_log_shutdown
root     19043 19037  0 18:22 ?        00:00:00  |                   \_ /bin/ps -ef -forest
```

Exemple 6 : Un arrêt a été demandé par le processus poshd interne :

<#root>

```
root       643     1  0 13:00 ?        00:00:00
```

/usr/bin/poshd

```
root     13207   643  0 13:43 ?        00:00:00
```

_ /bin/sh /sbin/shutdown -h -P now

```
root     13208 13207  0 13:43 ?        00:00:00      \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     13213 13208  0 13:43 ?        00:00:00          \_ /usr/bin/timeout 15 /sbin/fxos_log_shutdown
root     13214 13213  0 13:43 ?        00:00:00              \_ /bin/sh /sbin/fxos_log_shutdown
root     13221 13214  0 13:43 ?        00:00:00                  \_ /bin/ps -ef -forest
```

poshd est responsable de l'arrêt progressif du périphérique en cas de problème d'alimentation (par le biais d'un bouton d'alimentation ou d'un facteur d'alimentation externe).

Exemple 7 : Un redémarrage a été déclenché par les changements d'état du moteur de pare-feu Lina, tels que :

- En exécutant la commande reload dans l'interface de ligne de commande ASA ou l'interface de ligne de commande de diagnostic FTD
- Le traceback du moteur Lina (à l'exception des versions avec la fonctionnalité « Rechargement rapide du plan de données » introduite dans ASA 9.20(x) et FTD 7.4.1.)
- Synchronisation incomplète/partielle de l'unité active vers l'unité en veille

<#root>

```
root     56833 56198  0 00:48 ?        00:00:00  |   \_ /ngfw/usr/local/sf/bin/consoled /ngfw/var/run/li
```

```
root     57003 56833  0 00:48 ?        00:00:00  |
```

_ /bin/sh /sbin/shutdown -r now

```
root     59448 57003  0 00:48 ?        00:00:00  |           \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     59453 59448  0 00:48 ?        00:00:00  |               \_ /usr/bin/timeout 15 /sbin/fxos_log_
root     59454 59453  0 00:48 ?        00:00:00  |                   \_ /bin/sh /sbin/fxos_log_shutdown
root     59461 59454  0 00:48 ?        00:00:00  |                       \_ /bin/ps -ef -forest
```

Analyse des raisons de réinitialisation du châssis

Cette section traite de l'analyse des raisons de réinitialisation du châssis. Sur les châssis Firepower 4100/9300, la raison de réinitialisation est accessible uniquement dans :

- CLI FXOS :

<#root>

#

connect fxos

(fxos)#

show system reset-reason

- Dans le résultat de la commande show system reset-reason dans les fichiers de dépannage de châssis *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, où * est la partie du nom du fichier de dépannage, par exemple, 20250311123356_ FW_BC1_all

---

Sur Firepower 1000, 2100, Secure Firewall 1200, 3100, 4200, la raison de la réinitialisation est accessible uniquement dans :

- FTD mode natif (non multi-instance) CLISH en mode expert : opt/cisco/platform/logs/portmgr.out.
- Fichier de dépannage du mode natif FTD : dir-archives/opt-cisco-platform-logs/portmgr.out.
- fichier de dépannage du châssis sur Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200 : /opt/cisco/platform/logs/portmgr.out.

Reportez-vous à la section Dépannage des procédures de génération de fichiers Firepower sur la façon de générer les fichiers FTD, du châssis et du module de sécurité.

Pour connaître la raison de la réinitialisation des plates-formes matérielles autres que Firepower 4100/9300, procédez comme suit :

1. Dans /opt/cisco/platform/logs/portmgr.out, recherchez des lignes telles que, Last reset cause qui correspondent à l'horodatage de redémarrage/arrêt. Assurez-vous de vérifier tous les fichiers portmgr.out, y compris portmgr.out.1, portmgr.out.2, et ainsi de suite.

2. Reportez-vous à ce tableau pour obtenir des explications sur les raisons courantes de

réinitialisation :

Motif de réinitialisation	Explication
Mise sous tension	La dernière réinitialisation a été provoquée par un événement de mise sous tension (cycle d'alimentation CA).
LocalSoft	La dernière réinitialisation a été provoquée par une réinitialisation logicielle locale (réinitialisation logicielle à l'UC).
FanFail	La détection de l'absence ou de la défaillance du ventilateur du plateau de ventilation entraîne le redémarrage du système.
RP-Reset	Ce bit indique que le logiciel a demandé un cycle d'alimentation.
MiseÀNiveauBootRom	La dernière réinitialisation a été provoquée par une réinitialisation de la mémoire flash de mise à niveau d'image.
ÉchecMiseÀNiveauRomDémarrage	Échec du processus de mise à niveau.
Surveillance/PCH	La dernière réinitialisation a été provoquée par un délai d'expiration du temporisateur de surveillance dans la FPGA.
Manuel	La dernière réinitialisation a été provoquée par une réinitialisation manuelle par bouton-poussoir.
Désactiver	La dernière réinitialisation a été provoquée par une mise hors tension manuelle de l'interrupteur.
Erreur irrécupérable	Causé par le signal d'erreur catastrophique du processeur.
DemandeRéinitialisation	La dernière réinitialisation a été provoquée par l'activation du signal de réinitialisation par le processeur. Cela peut aussi être causé par une panique du noyau.

	Cette raison s'affiche également lorsqu'un redémarrage FTD est déclenché manuellement à partir de CLISH, Lina ou FMC.
DemandeCycleAlimentation	La dernière réinitialisation/mise hors tension a été provoquée par l'activation par le processeur de tous les signaux de veille.

Pour connaître la raison de la réinitialisation de Firepower 4100/9300, procédez comme suit :

1. Sur l'interface de ligne de commande de FXOS, exécutez la commande show system reset-reason dans l'interpréteur de commandes de FXOS.

<#root>

```
FPR4115-2 #

connect fxos


…
FPR4115-2(fxos)#

show system reset-reason


----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 612806449 usecs after Tue Jul 22 23:50:33 2025
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.141)

2) No time
    Reason: Unknown
    Service:
    Version: 5.0(3)N2(4.141)

3) No time
    Reason: Unknown
    Service:
    Version: 5.0(3)N2(4.141)

4) At 723697 usecs after Thu Oct  3 17:56:08 2024
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.120)
```

Le résultat de cette commande est également disponible dans le fichier de dépannage du châssis

*_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, où * fait partie du nom du fichier de dépannage. Par exemple, 20250311123356_ FW_BC1_all

<#root>

#

pwd

20250521112103_FPR9300_BC1_all/FPRM_A_TechSupport

#

less sam_techsupportinfo

Raisons les plus courantes :

Réinitialisation demandée par la commande CLI reload.
La dernière réinitialisation a été provoquée par le dépassement du délai de surveillance.
Réinitialisation demandée en raison d'une erreur système irrécupérable.
Réinitialisation demandée en raison d'une erreur irrécupérable du module.
Mise hors tension en raison d'un déclencheur de politique de capteur de température.
Réinitialisation en raison d'une tension incorrecte.
Réinitialisation demandée en raison d'une erreur système irrécupérable.

Réinitialisation causée par plusieurs erreurs de mémoire ASIC non corrigibles.
Réinitialisation en raison de la panique du noyau.
Réinitialisation déclenchée en raison de la stratégie de commutation HA.
Requête de redémarrage du noyau.
Réinitialiser pour une raison inconnue.

---

2. La raison Inconnu sans aucun temps à l'étape 1 indique généralement une coupure de courant brusque ou des problèmes d'unité d'alimentation (PSU). Il est recommandé de vérifier la présence de problèmes externes de perte d'alimentation ou de distribution de l'alimentation (PDU) dans les incidents.

---

3. En outre, exécutez le résultat de la commande show logging onboard internal reset-reason | no-more, commande. Le résultat de cette commande est également disponible dans le fichier de dépannage du châssis *_BC1_all/FPRM_A_TechSupport/sw_kernel_trace_log, où * est la partie du nom du fichier de dépannage. Par exemple, 20250311123356_FW_BC1_all :

<#root>

```
FPR4115-2 #

connect fxos


…
KSEC-FPR4115-2(fxos)#

show logging onboard internal reset-reason | no-more


----------------------------
OBFL Data for
    Module:  1
----------------------------
Reset Reason for this card:
        Image Version : 5.0(3)N2(4.141)

        Reset Reason (SW): Unknown (0) at time Fri Jul  4 23:57:21 2025
```

```
  Service (Additional Info):

Reset Reason (HW): FPGA  reset code: 0x0001


  FPGA Power-ON Reset at time Fri Jul  4 23:57:21 2025
```

Analyser les erreurs ou les exceptions matérielles

Cette section traite de l'analyse des fichiers contenant des erreurs ou des exceptions matérielles.

Modules de sécurité Firepower 1000, 2100, Secure Firewall 1200, 3100, 4200, Firepower 4100/9300

Les fichiers concernés sont les suivants :

- /opt/cisco/platform/logs/mce.log (Journaux des exceptions de vérification de l'ordinateur)
- /ngfw/var/log/dmesg.log (FTD uniquement)
- /opt/cisco/config/var/logs/dmesg.log
- /opt/cisco/platform/logs/messages

Ces fichiers peuvent contenir des erreurs matérielles ou des journaux d'exceptions pour :

- Châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200
- Modules de sécurité Firepower 4100 et 9300 (pas le châssis)

Les fichiers ne sont accessibles que dans :

- FTD mode natif (non multi-instance) CLISH en mode expert :
  - /opt/cisco/platform/logs/mce.log
  - /ngfw/var/log/dmesg.log (FTD uniquement)
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages

- Fichier de dépannage du mode natif FTD :
  - dir-archives/var-common-platform_ts/opt/cisco/platform/logs/mce.log
  - dir-archives/var-common-platform_ts/opt/cisco/platform/logs/messages
  - dir-archives/var-common-platform_ts/opt/cisco/config/var/logs/dmesg.log
  - dir-archives/var-log/dmesg.log
- Fichier de dépannage du châssis sur Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200 :
  - /opt/cisco/platform/logs/mce.log
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages
- Fichier show-tech du module de sécurité sur Firepower 4100/9300 :
  - /opt/cisco/platform/logs/mce.log
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages

Exemples d'erreurs liées au matériel :

<#root>

```
opt/cisco/config/var/logs/ $

less dmesg.log


[Sun Apr 27 05:17:10 2025] mce: [Hardware Error]: Machine check events logged
[Sun Apr 27 05:17:10 2025] mce: [Hardware Error]: Machine check events logged

/opt/cisco/platform/logs $

less messages


Jul  9 17:39:38 fw2 kernel: [  628.949572] [Hardware Error]: Corrected error, no action required.
Jul  9 17:39:38 fw2 kernel: [  629.023798] [Hardware Error]: CPU:2 (19:1:1) MC18_STATUS[Over|CE|MiscV|A
Jul  9 17:39:38 fw2 kernel: [  629.152245] [Hardware Error]: Error Addr: 0x0000000068d06d40
Jul  9 17:39:38 fw2 kernel: [  629.152248] [Hardware Error]: PPIN: 0x02b0bc114ba60075
Jul  9 17:39:38 fw2 kernel: [  629.281830] [Hardware Error]: IPID: 0x0000009600550f00, Syndrome: 0x0004
Jul  9 17:39:38 fw2 kernel: [  629.374797] [Hardware Error]: Unified Memory Controller Ext. Error Code:
Jul  9 17:39:38 fw2 kernel: [  629.475078] [Hardware Error]: cache level: L3/GEN, tx: GEN, mem-tx: RD
Jul  9 17:44:40 fw2 kernel: [  930.967028] [Hardware Error]: Corrected error, no action required.
Jul  9 17:44:40 fw2 kernel: [  931.041247] [Hardware Error]: CPU:2 (19:1:1) MC18_STATUS[Over|CE|MiscV|A
Jul  9 17:44:40 fw2 kernel: [  931.169689] [Hardware Error]: Error Addr: 0x000000007191d0c0
Jul  9 17:44:40 fw2 kernel: [  931.237616] [Hardware Error]: PPIN: 0x02b0bc114ba60075
Jul  9 17:44:40 fw2 kernel: [  931.299275] [Hardware Error]: IPID: 0x0000009600550f00, Syndrome: 0x0000

/opt/cisco/platform/logs $

less mce.log
```

Hardware event. This is not a software error.

MCE 0
CPU 0 BANK 7 TSC 7b29f624ae62e
MISC 140129286 ADDR 3402b9a00
TIME 1745747035 Sun Apr 27 09:43:55 2025
MCG status:
MCi status:
Corrected error
MCi_MISC register valid
MCi_ADDR register valid
MCA: MEMORY CONTROLLER RD_CHANNEL0_ERR

Transaction: Memory read error

STATUS 8c00004000010090 MCGSTATUS 0
MCGCAP 1000c16 APICID 0 SOCKETID 0
PPIN afeebaf20487b95
MICROCODE 700000d
CPUID Vendor Intel Family 6 Model 86 Step 3

mcelog: failed to prefill DIMM database from DMI data

Erreurs catastrophiques (CATERR) sur les modules de sécurité Firepower 4100/9300

Une CARTER est une exception revendiquée par le processeur. Un CATERR peut indiquer une panne du processeur ou des problèmes de bas niveau qui rendent la lame inaccessible. Le superviseur du châssis redémarre le module de sécurité qui a fait l'expérience de CATERR. Les journaux CATERR sont situés dans le fichier de dépannage Firepower 4100/9300 dans CIMC<X>_TechSupport/obfl/ et CIMC<X>_TechSupport/var/log/sel, où <X> représente le numéro de module.

Exemple de fichier de dépannage de châssis *_BC1_all/CIMC<X>_TechSupport.tar.gz/CIMC<X>_TechSupport.tar/obfl/obfl-log, où * est la partie du nom du fichier de dépannage. Par exemple, 20250311123356_ FW_BC1_all et <X > est l'ID du module de sécurité :

<#root>

2022 Mar 25 22:33:13 CET:4.1(30b):selparser:1950: selparser.c:727: # BF 06 00 00 01 02 00 00 19 35 3E 6

Processor CATERR

_N #0x81 |

Predictive Failure asserted | Asserted

Le moteur de gestion des données (DME) actuel se connecte dans *_BC1_all/FPRM_A_TechSupport.tar.gz\FPRM_A_TechSupport.tar\var\sysmgr\sam_logs\svc_sam_dme.lo ou les journaux avant le redémarrage dans *_BC1_all/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar/opt/sam_logs.tgz/sam_logs.tar/sam_lo contiennent les lignes avec la lame de cycle d'alimentation X due à CATERR, où X est l'ID de la lame.

Dans le cas de CATERR, un vidage sur incident peut être généré. Le vidage sur incident se trouve dans *_BC1_all/CIMC<X>_TechSupport.tar.gz/CIMC<X>_TechSupport.tar/techsupport_pidxxxx/nv/etc/log/eng-repo/caterrlog.first.

Exemple de contenu :

```
CRASH DUMP START TIME = Mon Dec 19 00:42:40 2022
               SERVER: presidio
               GetCpuID: CPUID = 0x00050654
               PresidioCatErrHandler: CPU TYPE : Skylake
               handleCaterr_Purley: ---
               PECI BUS : LOCKED
               CPU Socket 1 : Populated
               CPU Socket 2 : Populated
               Stage1Dump: ---
               MC0: IFU - Instruction Fetch Unit and Instruction Cache
               CPU1 (0x30): ThreadID 0 : IA32_MC0_CTL (0x400) : 0x0000000000000fff
               CPU1 (0x30): ThreadID 0 : IA32_MC0_STATUS (0x401) : 0x0000000000000000
               CPU1 (0x30): ThreadID 0 : IA32_MC0_ADDR (0x402) : 0x0000000000000000
```

Analyser les fichiers journaux des autres plates-formes

Cette section traite de l'analyse des fichiers contenant les journaux de la plate-forme. Selon le matériel, certains de ces fichiers peuvent contenir des journaux liés à un redémarrage déclenché par des composants spécifiques.

Modules de sécurité Firepower 1000, 2100, Secure Firewall 1200, 3100, 4200, Firepower 4100/9300

Les fichiers contiennent les journaux du châssis pour :

- Châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200
- Modules de sécurité Firepower 4100 et 9300 (pas le châssis)

Les fichiers ne sont accessibles que dans :

- FTD mode natif (non multi-instance) CLISH en mode expert dans /opt/cisco/platform/logs/
- FTD mode natif dépannage du fichier dir-archives/var-common-platform_ts/opt/cisco/platform/logs/
- Fichier de dépannage du châssis sur Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200 in /opt/cisco/platform/logs/
- Fichier show-tech du module de sécurité sur Firepower 4100/9300 in /opt/cisco/platform/logs/

Pour rechercher des journaux potentiels liés à un redémarrage, recherchez les lignes contenant des mots clés tels que reboot, restart, power, shut, reload.



Remarque : Il s'agit d'une approche de type « best effort », car le résultat de la recherche peut renvoyer un grand nombre de lignes correspondantes (l'utilisateur doit analyser les lignes correspondantes).

Exemple 1 :

<#root>

```
admin@firewall:/opt/cisco/platform/logs$

grep -Ei "power|reboot|reload|restart|shut" *


...
npu_accel_fatal_err_stats.log:nic_top_inb_q_restart_drop_cnt = 0
npu_accel_fatal_err_stats.log:nic_top_norm_q_restart_drop_cnt = 0
npu_accel_fatal_err_stats.log:nic_top_inb_q_restart_drop_cnt = 0

npu_accel_mgr.log:2025 Oct 03 14:29:16 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev



npu_accel_mgr.log:2025 Oct 09 18:13:09 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev
```

npu_accel_mgr.log:2025 Oct 17 17:11:23 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 17 17:31:55 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 17 19:29:29 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

```
ntp.log:27 Sep 02:21:16 ntpd[1580]: 0.0.0.0 c016 06 restart
ntp.log:27 Sep 02:23:27 ntpd[10193]: 0.0.0.0 c016 06 restart
...
```

Dans ce cas, le redémarrage a été déclenché en raison de la défaillance de l'accélérateur NPU (Network Processing Unit) du pare-feu sécurisé 4200.

Analyser les fichiers SEL/OBFL

Cette section traite de l'analyse des fichiers avec les journaux des événements de sécurité (SEL) et les journaux des défaillances embarqués (OBFL) sur les modules de sécurité Firepower 4100/9300. Ces fichiers contiennent les événements matériels du module et les modifications de l'état de l'alimentation. Ils se trouvent dans le fichier de dépannage Firepower 4100/9300, dans CIMC<X>_TechSupport/obfl/ et CIMC<X>_TechSupport/var/log/sel, où <X> représente le numéro de module. Recherchez les lignes avec stop, shutdown, power off, reset, critical, qui ne respectent pas la casse.

Exemple 1 :

<#root>

```
2023 Sep 21 13:53:13:4.1(30b):cipmi:1088: [[xxxCVxxx]]:oem_command.c:457:IPMI Request Message --> Chan:
```

2023 Sep 21 13:53:13:4.1(30b):selparser:1203: [[xxxCVxxx]]:selparser.c:727: # A9 04 00 00 01 02 00 00 49

```
2023 Sep 21 13:53:14:4.1(30b):cipmi:1088: peci.c:278:Error: Failed to read local PCI config after 3 ret
2023 Sep 21 13:53:15:4.1(30b):kernel:-:<5>[platform_reset_cb_handler]:75:Platform Reset ISR -> ResetSta
2023 Sep 21 13:53:15:4.1(30b):cipmi:1088: ocmds_intel_me.c:251:Intel ME Operating State:[MO without UMA
2023 Sep 21 13:53:15:4.1(30b):cipmi:1088: ocmds_intel_me.c:261:Intel ME is initializing.
```

Exemple 2 : Arrêt au niveau du système d'exploitation :

<#root>

```
2025 Jul 30 23:31:02 UTC:4.1(30b):cipmi:1052: [[xxxCVxxx]]:oem_command.c:457:IPMI Request Message --> C
2025 Jul 30 23:31:02 UTC:4.1(30b):selparser:1169: [[xxxCVxxx]]:selparser.c:727: # 48 03 00 00 01 02 00
2025 Jul 30 23:31:04 UTC:4.1(30b):kernel:-:<5>[platform_reset_cb_handler]:75:Platform Reset ISR -> Rese
2025 Jul 30 23:31:05 UTC:4.1(30b):kernel:-:<4>[peci_ioctl]:293:non-responsive controller, resetting pec
2025 Jul 30 23:31:05 UTC:4.1(30b):cipmi:1052: ocmds_intel_me.c:251:Intel ME Operating State:[M0 without
2025 Jul 30 23:31:05 UTC:4.1(30b):cipmi:1052: ocmds_intel_me.c:261:Intel ME is initializing.

2025 Jul 30 23:31:05 UTC:4.1(30b):information_logger:589: uptime.c:1219:Host Transition Ocurred. Event C
```

Exemple 3 : Le contrôleur de gestion de la carte mère a été réinitialisé en raison de la surveillance :

<#root>

```
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:487:BMC Watchdog resetted BMC.
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:489:BMC Watchdog System Bus Debug Status F
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:523:BMC Watchdog resetted BMC due to OOM.
```

Analyser les journaux de console ASA/FTD

Cette section couvre l'analyse des fichiers ASAConsole.log qui contiennent des journaux du moteur Lina et qui peuvent être vérifiés pour les signes de retraçage ou de redémarrages du logiciel. Le fichier contient des journaux d'arrêt ou de redémarrage pour ASA/FTD exécutés sur des plates-formes virtuelles, les modules de sécurité Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200, et Firepower 4100 et 9300 (pas le châssis).

Le fichier est uniquement accessible dans :

- FTD CLISH en mode expert : /ngfw/var/log/ASAConsole.log
- Fichier de dépannage FTD : dir-archives/opt-cisco-platform-logs/ASAConsole.log.
- Fichier de dépannage du module de sécurité sur Firepower 4100/9300 : /opt/platform/logs/ASAConsole.log
- Les châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100 et 4200 affichent le fichier technique : /opt/platform/logs/ASAConsole.log

---

Symptômes du retour arrière et de la génération de fichiers principaux :

<#root>

```
root@KSEC-CSF1210-6:/ngfw/var/log#

less ASAconsole.log


2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:35 !! !! First Crash in tid: 14834 signo: 11
2025-08-09 01:06:35
2025-08-09 01:06:35 Writing live core file to flash. Please do not reload.
2025-08-09 01:06:35
2025-08-09 01:06:35 Coredump starting....
2025-08-09 01:06:35 Corehelper: /opt/cisco/csp/cores/core.lina.11.14550.1754701595
2025-08-09 01:06:35 Waiting for Corehelper to finish....
2025-08-09 01:06:35 Livecore: generating coredump of 14550
2025-08-09 01:06:35 [New LWP 14795]
2025-08-09 01:06:35 [New LWP 14796]
2025-08-09 01:06:35 [New LWP 14834]
2025-08-09 01:06:35 [New LWP 14835]
2025-08-09 01:06:35 [New LWP 14836]
2025-08-09 01:06:35 [New LWP 14869]
2025-08-09 01:06:35 [New LWP 14934]
2025-08-09 01:06:35 [New LWP 14939]
2025-08-09 01:06:35 [New LWP 14940]
2025-08-09 01:06:35 [New LWP 14941]
2025-08-09 01:06:35 [New LWP 14942]
2025-08-09 01:06:35 [New LWP 14943]
2025-08-09 01:06:35 [New LWP 14945]
2025-08-09 01:06:35 [New LWP 14947]
2025-08-09 01:06:35 [New LWP 14948]
```

Symptômes d'un démarrage du moteur Lina (remarquez l'écart dans les horodatages du journal) :

<#root>

```
root@KSEC-CSF1210-6:/ngfw/var/log#

less ASAconsole.log


2024-11-13 22:43:09 INFO: SW-DRBG health test passed.
2024-11-13 22:43:09 M_MMAP_THRESHOLD 65536, M_MMAP_MAX 82155
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 User enable_1 logged in to firepower
2024-11-13 22:43:10 Logins over the last 1 days: 1.
```

```
2024-11-13 22:43:10 Failed logins since the last login: 0.
2024-11-13 22:43:10 Type help or '?' for a list of available commands.

2024-11-13 22:43:10 ^Mfirepower>



2025-04-04 09:11:46 System Cores 8 Nodes 1 Max Cores 24



2025-04-04 09:11:46 Number of Cores 3
2025-04-04 09:11:46 IO Memory Nodes: 1
2025-04-04 09:11:46 IO Memory Per Node: 1073741824 bytes num_pages = 262144 page_size = 4096
2025-04-04 09:11:46
2025-04-04 09:11:46 Global Reserve Memory Per Node: 2147483648 bytes Nodes=1
2025-04-04 09:11:46
2025-04-04 09:11:46 LCMB: got DMA 1073741824 bytes on numa-id=0, phys=0x00000001c0000000, virt=0x000040
2025-04-04 09:11:46 LCMB: HEAP-CACHE POOL got 2147483648 bytes on numa-id=0, virt=0x0000400080000000
2025-04-04 09:11:46
2025-04-04 09:11:46 total_reserved_mem = 1073741824
2025-04-04 09:11:46
2025-04-04 09:11:46 total_heapcache_mem = 2147483648
2025-04-04 09:11:46 total mem 5384115842 system 16318316544 kernel 21847377 image 85732792
2025-04-04 09:11:46 new 5384115842 old 1159474616 reserve 3221225472 priv new 2184737747 priv old 0
2025-04-04 09:11:46 Processor memory:   5384115842
2025-04-04 09:11:46 POST started...
2025-04-04 09:11:46 POST finished, result is 0 (hint: 1 means it failed)
2025-04-04 09:11:46
2025-04-04 09:11:46 Cisco Adaptive Security Appliance Software Version 9.22(1)1
```

Analyse des problèmes de tension et d'alimentation

Poursuivez avec cette section si dans le cadre de la section Analyser les raisons de réinitialisation du châssis des raisons de réinitialisation comme celles-ci sont trouvées :

- Mise sous tension
- DemandeCycleAlimentation
- Réinitialisation en raison d'une tension incorrecte
- Raison inconnue :

```
No time
    Reason: Unknown
    Service:
    Version:
```

Ces raisons peuvent indiquer des problèmes potentiels avec un ou plusieurs des éléments

suivants :

- Pénuries d'alimentation électrique
- Problèmes avec les unités d'alimentation (PSU)
- Problèmes avec les câbles d'alimentation
- Problèmes avec les unités de distribution de l'alimentation (PDU) dans le rack
- Problèmes d'alimentation

Procédez comme suit :

1. Pour réduire la portée du problème, répondez aux questions suivantes :

- La perte d'alimentation était-elle un problème ponctuel ou récurrent ?
- Le pare-feu comporte-t-il des blocs d'alimentation redondants ?
- Les blocs d'alimentation sont-ils connectés à différentes sources d'alimentation et/ou unités d'alimentation ?
- D'autres périphériques sont-ils connectés à la même source d'alimentation et/ou à la même unité d'alimentation ?
- D'autres périphériques connectés à la même source d'alimentation et/ou au même bloc d'alimentation ont-ils également subi une perte d'alimentation ?

---

2. Si, d'après les questions de la première étape, seul le pare-feu est affecté, assurez-vous que :

- Les câbles d'alimentation sont fermement connectés à la source d'alimentation et au châssis.
- Les câbles d'alimentation ne sont pas endommagés et essayez de les remplacer afin d'éviter tout problème potentiel.

---

3. Si le châssis continue à redémarrer de manière inattendue, collectez le résultat de ces commandes dans FXOS plusieurs fois :

<#root>

scope chassis 1

show psu detail expand

```
scope psu 1

show stats history psu-stats detail expand

show stats psu-stats detail expand

exit

scope psu 2

show stats history psu-stats detail expand

show stats psu-stats detail expand
```

---

4. Collectez le fichier de dépannage du châssis.

Références

1. Vérifier les versions du logiciel Firepower
2. Vérification de la puissance de feu, des instances, de la disponibilité et de l'évolutivité
3. Collecter des données pour l'analyse de la cause première du retour/plantage logiciel dans le pare-feu sécurisé
4. Dépannage des procédures de génération de fichiers Firepower

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.