Dépannage d'un pare-feu Cisco Secure Firewall qui ne répond pas

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Dépannage
  - Étape 1 : Inspection visuelle (panneau avant)
  - Étape 2 : Inspection visuelle (panneau arrière)
  - Étape 3 : Contrôles du ventilateur
  - Étape 4 : Contrôles d'environnement physique
  - Étape 5 : Contrôles des ports de console et de gestion
  - Étape 6 : Test de connectivité IP de gestion
  - Étape 7 : Vérifications des périphériques adjacents
  - Étape 8 : Vérifications des périphériques HA/cluster
  - Étape 9 : Collecter les journaux de console
  - Étape 10 : Effectuer un redémarrage à froid
  - Étape 11 : Collecter des graphiques Health Monitor à partir de FMC
  - Étape 12: Vérifier les problèmes de disque
  - Étape 13 : Analyse du journal
  - Étape 14 : Captures
  - Étape 15 : Informations supplémentaires à fournir au TAC Cisco
- Problèmes courants
  - Erreur : Expiration de la communication avec DME
  - Erreur disque : manquant ou inutilisable
  - Avis sur le champ : FN72077 - FPR9300 et FPR4100
  - Utilisation des disques 100 %
  - Le CSF 3100 ne s'active pas après une panne de courant
  - Appareils de sécurité Cisco Firepower 2100 : Certaines Unités Peuvent Présenter Des Défaillances De Mémoire
- Références

Introduction

Ce document décrit les étapes recommandées pour dépanner un pare-feu Cisco Secure Firewall Threat Defense (FTD) qui ne répond pas sur les plates-formes matérielles 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx et 93xx.

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Notions de base sur Cisco Secure FTD (installation/configuration).

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Système d'exploitation extensible Cisco Firepower (FXOS)

Composants utilisés

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 certains cas, un périphérique Cisco FTD peut ne plus répondre. Les symptômes typiques sont :

- Aucun accès SSH.
- Aucun accès console.
- L'accès à la console fonctionne, mais pas les identifiants de connexion.
- Le trafic de transit ne traverse pas le périphérique.
- Les interfaces sont désactivées (données ou gestion).
- Les voyants sont éteints ou orange (clignotants ou fixes).
- Le module sécurisé (4100, 9300) ne répond plus.

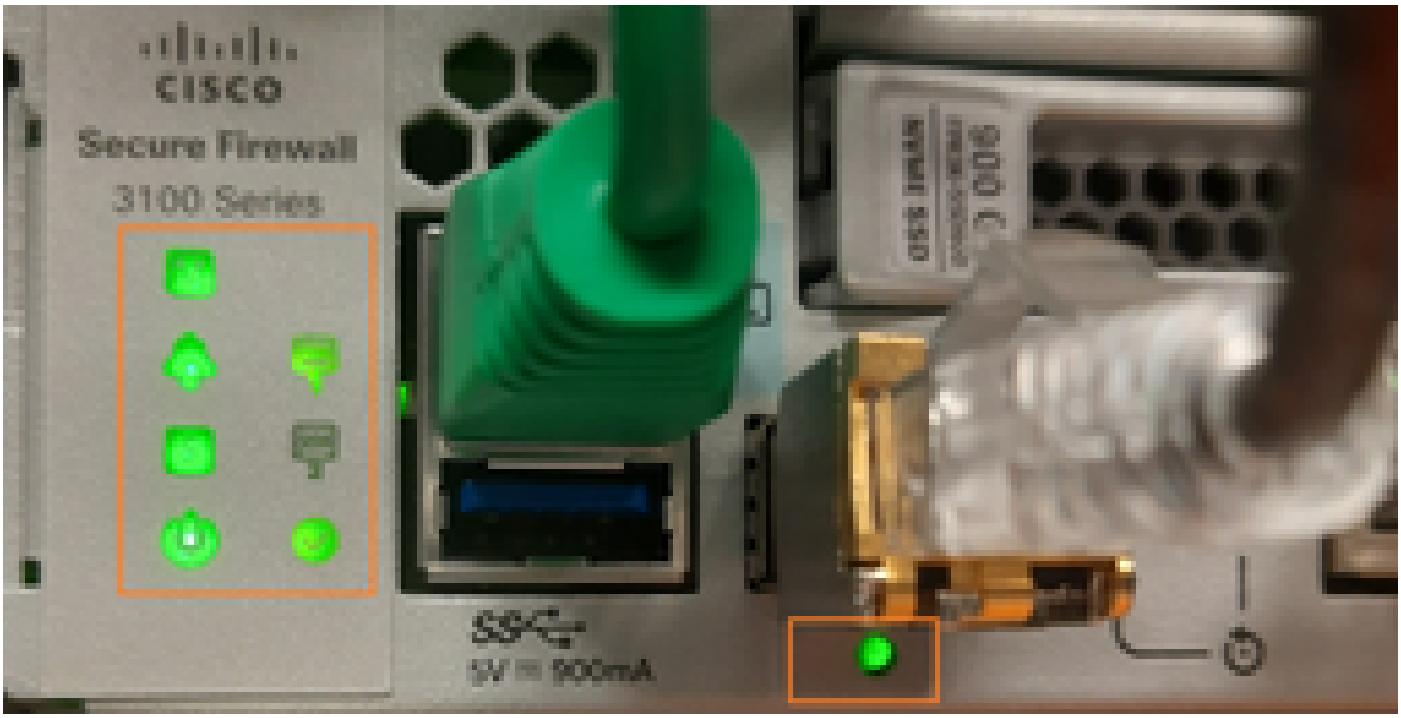
Notez que, selon la situation, certains d'entre eux ne seront pas présents. Par exemple, vous pouvez avoir un trafic de transit en transit, mais seul l'accès de gestion ne fonctionne pas.

Dépannage

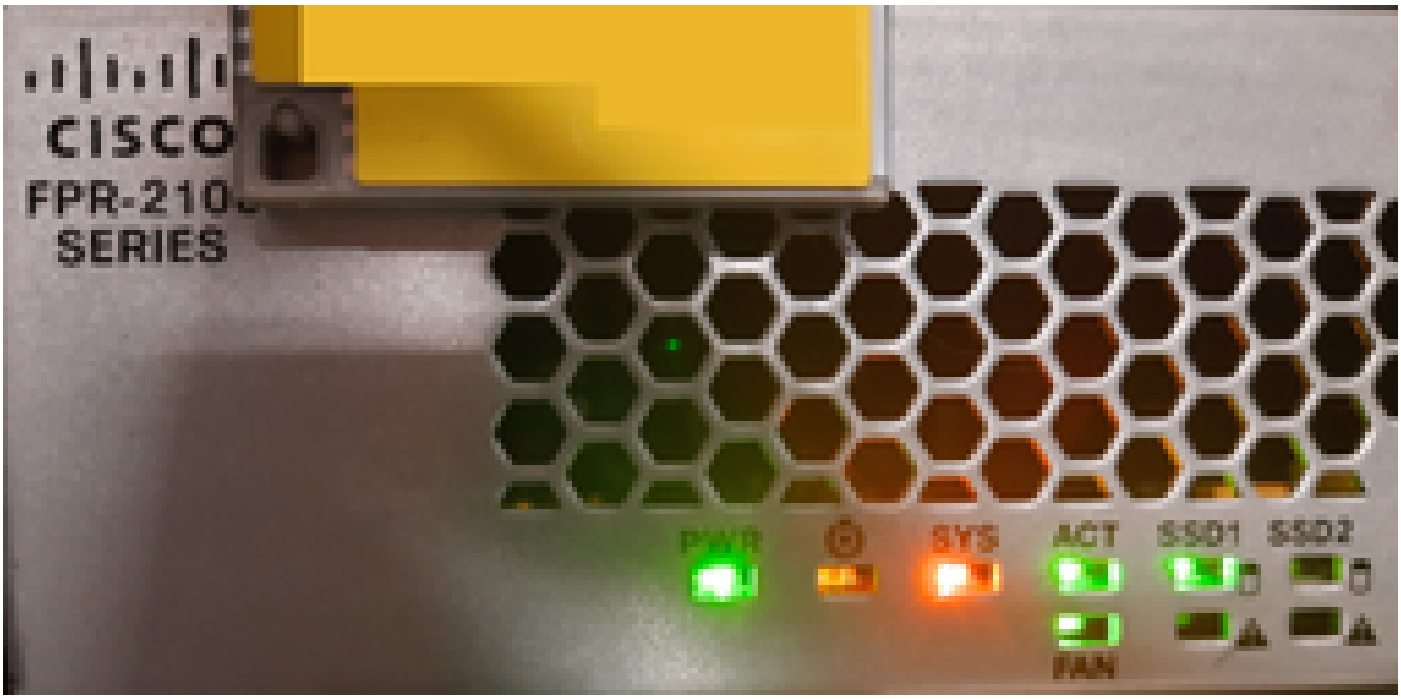
Cette section décrit les étapes et les actions recommandées à effectuer. Vous pouvez fournir ces informations au TAC Cisco pour une analyse plus approfondie.

Étape 1 : Inspection visuelle (panneau avant)

Prenez une vidéo ou une photo des voyants du panneau avant. Voici quelques exemples où tous les voyants sont clairement visibles :



Sur la photo suivante, le voyant SYS indique un problème de périphérique :



Vous pouvez consulter le guide matériel de votre modèle de périphérique pour obtenir des informations supplémentaires sur le voyant, par exemple :

Maquette	Infos LED
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overvie
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/overv
1210CE, 1210CP, 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-121
1230, 1240, 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/o
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/m
4110, 4120, 4140,	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/o

4150	
4112, 4115, 4125, 4145	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.h
4200	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200-install/m
9300	https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300/b

Étape 2 : Inspection visuelle (panneau arrière)

Prenez une vidéo ou une photo des voyants situés sur le panneau arrière, par exemple :

Si aucun voyant d'alimentation ne s'allume :

- Essayez de réinstaller les modules d'alimentation (le cas échéant).
- Si possible, essayez de remplacer l'alimentation.

Étape 3 : Contrôles du ventilateur

Vérifiez si les ventilateurs situés à l'arrière de l'appliance sont en cours d'exécution.

Étape 4 : Contrôles d'environnement physique

Vérifiez si le périphérique émet un bruit ou une odeur.

Étape 5 : Contrôles des ports de console et de gestion

Assurez-vous que les ports de console et de gestion sont correctement connectés. Si le problème se situe uniquement sur le port de gestion, essayez de changer le SFP (le cas échéant) et le câble réseau.

Étape 6 : Test de connectivité IP de gestion

Essayez d’envoyer une requête ping (ICMP) à l’adresse IP de gestion du périphérique.

Étape 7 : Vérifications des périphériques adjacents

Vérifiez l'état des ports des périphériques adjacents, par exemple :

<#root>

```
switch#
```

show interface description | i FW-4215-1

```
Gi7/1                          up             up       FW-4215-1 ETH1/1
Gi7/2                          up             up       FW-4215-1 ETH1/2
Gi7/3                          up             up       FW-4215-1 MGMT
```

Étape 8 : Vérifications des périphériques HA/cluster

En cas de haute disponibilité (HA) ou de configuration de cluster, collectez un bundle de dépannage auprès des périphériques homologues.

Étape 9 : Collecter les journaux de console

Connectez un ordinateur portable au port de console et copiez les messages affichés. Essayez d'appuyer sur les touches haut/bas du clavier ou sur PageUp pour afficher tous les messages à l'écran.

Étape 10 : Effectuer un redémarrage à froid

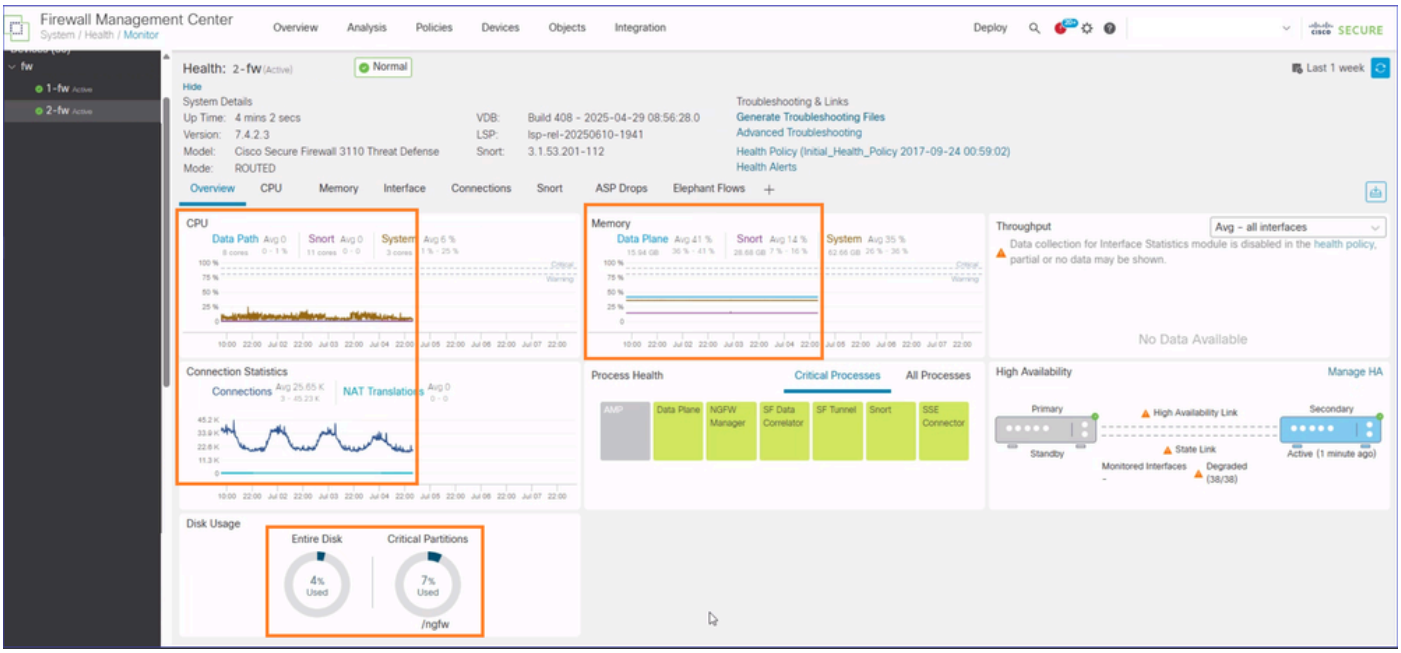
Avec un ordinateur portable connecté au port de console :

1. Débranchez tous les câbles d'alimentation et attendez quelques minutes avant de les rebrancher.
2. Dans le cas d'une configuration de basculement ou d'une configuration de cluster, afin de minimiser tout risque d'instabilité active/active ou de cluster, vous pouvez débrancher ou arrêter à partir du périphérique de commutateur adjacent toutes les interfaces de données de l'unité concernée, y compris les liaisons HA ou CCL.
3. Ensuite, rebranchez les câbles d'alimentation et mettez le périphérique sous tension.
4. Attendez environ 5 minutes.
5. Collectez le résultat de la console.

Notez que si le périphérique n'a pas été correctement arrêté et qu'il était opérationnel (les voyants du panneau avant étaient allumés), le redémarrage à froid peut entraîner une corruption de la base de données. Si le redémarrage à froid fait apparaître le périphérique, collectez une offre groupée de dépannage et contactez le centre d'assistance technique Cisco.

Étape 11 : Collecter des graphiques Health Monitor à partir de FMC

Si le périphérique est restauré et géré par un FMC, accédez à System > Health > Monitor, et sélectionnez le périphérique. Concentrez-vous sur les graphiques mis en surbrillance pour comprendre l'état du périphérique avant de ne plus répondre (par exemple, mémoire élevée, CPU élevé, utilisation élevée du disque, etc.).



Étape 12: Vérifier les problèmes de disque

Scénario hors fonctionnement (4100) :

<#root>

FW4100#

show server storage

```
Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD12345678
        HW Revision:
        PCI Addr: 00:31.2
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
           Vendor: Micron
           Model: 5300 MTFD
           Serial: MSA123456AB
           HW Rev:
           Operability: N/A
```

Presence: Missing <-----

```
            Size (MB): 200000
            Drive State: Online
            Power State: Active
            Link Speed: 6 Gbps
            Device Type: SSD

           Local Disk Config Definition:
              Mode: NO RAID
              Description:
              Protect Configuration: No
```

Exemple de sortie de 3100 où le disque est opérationnel :

<#root>

```
FW3105#

show server storage


Server 1/1:
    Disk Controller 1:
        Type: SOFTRAID
        Vendor: Cisco Systems Inc
        Model: FPR_SOFTRAID
        HW Revision:
        PCI Addr:
        Raid Support: raid1
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Optimal

        Local Disk 1:
            Presence: Equipped
            Model: SAMSUNG MZQL2960HCJR-00A07
            Serial: S64FNT0AB12345


Operability: Operable   <---


            Size (MB): 858306
            Device Type: SSD
            Firmware Version: GDC5A02Q

        Virtual Drive 1:
            Type: Raid
            Blocks: 878906048
            Operability: Degraded
            Presence: Equipped
            Size (MB): 858306
            Drive State: Degraded
```

Exemple de sortie de 4100 où le disque est opérationnel :

<#root>

```
FW4125#
```

show server storage

```
Server 1/1:
    RAID Controller 1:
        Type: SATA
        Vendor: Cisco Systems Inc
        Model: FPR4K-PT-01
        Serial: JAD1234567
        HW Revision:
        PCI Addr: 00:31.2
        Raid Support:
        OOB Interface Supported: No
        Rebuild Rate: N/A
        Controller Status: Unknown

        Local Disk 1:
            Vendor: TOSHIBA
            Model: KHK61RSE
            Serial: 11BS1234567AB
            HW Rev: 0
```

Operability: Operable

```
            Presence: Equipped
            Size (MB): 800000
            Drive State: Online
            Power State: Active
            Link Speed: 6 Gbps
            Device Type: SSD

        Local Disk Config Definition:
            Mode: No RAID
            Description:
            Protect Configuration: No
```

Étape 13 : Analyse du journal

Si le périphérique pare-feu récupère et que vous souhaitez analyser les journaux du serveur principal, générez un ensemble de dépannage et vérifiez les fichiers mentionnés dans le tableau. Notez que :

- Sur les plates-formes 1xxx, 12xx, 21xx (mode appliance), 31xx, 42xx, l'offre groupée de dépannage FTD contient également l'offre groupée de châssis (FPRM) de FXOS dans le chemin \dir-archives\var-common-platform_ts\. Vous devez extraire le contenu du bundle FPRM.
- Sur le 3100/4200 en mode Multi-Instance (MI), collectez le fichier TS du châssis à partir de l'interface utilisateur FMC ou de l'interface de ligne de commande du châssis (show tech-support fprm detail à partir de la portée de la commande local-mgmt), comme décrit dans

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400.

- Sur les plates-formes 41xx, 93xx, vous devez générer l'ensemble de châssis séparément de l'interface utilisateur du châssis ou de l'interface de ligne de commande FXOS, comme décrit dans https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400
- Pour les plates-formes de périphériques 4100 et 9300, vous devez collecter les ensembles de dépannage FXOS et FTD. Pour toutes les autres plates-formes, l'ensemble de dépannage FTD est suffisant puisqu'il contient également l'ensemble de dépannage FXOS.
- Pour ASA, le résultat de la commande 'show tech-support' après la récupération n'est pas très utile. Vous devez compter sur l'offre groupée de dépannage FXOS.
- Par rapport aux autres plates-formes, sur les modèles 41xx et 93xx, vous disposez de deux offres groupées de dépannage : châssis (BC1) et offre groupée de modules.
- L'offre groupée de châssis (BC1) sur 41xx, 93xx, contient entre autres les offres groupées FPRM et CIMC.
- L'ensemble de modules sur 41xx, 93xx contient principalement des journaux FXOS de la lame.
- Si vous avez installé un ASA, vous devez vous fier uniquement aux ensembles châssis, FPRM et module (le cas échéant) et à la sortie de commande « show tech-support » de l'ASA.
- Selon la plate-forme et l'incident, tous les fichiers ne seront pas présents.

Chemin d'accès du fichier dans l'offre groupée Dépannage	Descrip
Bundle FTD TS : /dir-archives/var-log/messages*	La chaî shutdov lors d'u progres La chaî starting au dém périphé
Bundle FTD TS : /dir-archives/var-log/ASAconsole.log Dans le cas d'un ASA sur 4100/9300, vous pouvez également trouver le fichier dans le bundle Module sous /opt/cisco/platform/logs/ASAconsole.log	Recher erreurs les pan
Bundle FTD TS : /dir-archives/var-log/dmesg.log	Recher erreurs les pan

Bundle FTD TS : /dir-archives/var/log/ngfwManager.log*	Recher erreurs les pan Ce fichi égalem informa événem HA/Clus
Bundle FTD TS : /command-outputs/LINA_troubleshoot/show_tech_output.txt	Le résu comma failover show cl peut fou informa supplér la séqu événem
Bundle FTD TS : /command-outputs/ Noms de fichiers : · pour CORE dans `ls opt-cisco-csp-cores _ grep core`_ do file -opt-cisco-csp-cores-_{CORE}_ done.output · pour CORE dans `ls var-common _ grep core`_ do file var-common-_{CORE}_ done.output · pour CORE dans `ls var-data-cores _ grep core`_ do file -var-data-cores-_{CORE}_ done.output	Recher fichiers potentie (trackba
Bundle FTD TS : /dir-archives/var/log/crashinfo/snort3-crashinfo.*	Recher fichiers Snort3.
Bundle FTD TS : /dir-archives/var/log/process_stderr.log*	Recher traces i exempl bogue CSCwh
Bundle FTD TS : /dir-archives/var/log/periodic_stats/	Le répe plusieu peuven

	informa l'heure
Offre groupée FPRM : présentation_support_technique	Vérifiez show fa
Offre groupée FPRM : /opt/cisco/platform/logs/kern.log	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/messages*	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/mce.log Le même fichier existe également dans l'ensemble de modules (41xx, 93xx).	Il s'agit (Machir Excepti Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/portmgr.out	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/ssp-pm.log Le même fichier existe également dans l'ensemble de modules (41xx, 93xx).	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/sma.log Le même fichier existe également dans l'ensemble de modules (41xx, 93xx).	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/heimdall.log	Recher erreurs les pan

Offre groupée FPRM : /opt/cisco/platform/logs/ssp-shutdown.log Le même fichier existe également dans l'ensemble de modules (41xx, 93xx).	Il contie ps, top lignes c quand l ou l'arr Disponi 1000/2
Offre groupée FPRM : /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	Recher erreurs les pan
Offre groupée FPRM : /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	Recher erreurs les pan
Offre groupée CIMC (41xx, 93xx) : /obfl/obfl-log*	Recher erreurs les pan
Offre groupée CIMC (41xx, 93xx) : /CIMC1_TechSupport.tar.gz/CIMC1_TechSupport.tar/tmp/techsupport_pid*/CIMC1_TechSupport-nvram.tar.gz/CIMC1_TechSupport-nvram.tar/nv/etc/log/eng-repo/messages*	Recher erreurs les pan Spécial CATER
Offre groupée de modules (41xx, 93xx) : /tmp/mount_media.log/mount_media.log	Recher erreurs les pan

Étape 14 : Captures

Si une interface spécifique ne répond plus, prenez des captures sur le pare-feu et le périphérique adjacent. Vous pouvez consulter ce document pour plus de détails :

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Assurez-vous également que les tables ARP et CAM des périphériques adjacents sont correctement remplies.

Étape 15 : Informations supplémentaires à fournir au TAC Cisco

En plus des éléments mentionnés ci-dessus, il est fortement recommandé de fournir également ces informations :

15 bis. Si le périphérique récupéré collecte un ensemble de dépannage (consultez l'étape 13 pour plus de détails).

15 ter. Si le périphérique ne répond toujours pas, fournissez les informations suivantes :

- Informations matérielles (modèle).
- Informations logicielles.
- Informations sur le logiciel FMC (le cas échéant).
- Déploiement (autonome/haute disponibilité/cluster).

15 quater. Heure approximative (date/heure) à laquelle le périphérique est devenu insensible.

15 quinquies. Temps de fonctionnement approximatif du périphérique avant qu'il ne réponde plus.

15 sexies. S'agit-il d'une nouvelle configuration ou d'une configuration existante ?

15 septies. Quelle a été la dernière action effectuée avant que le périphérique ne cesse de répondre ?

15 octies. Syslog du plan de données du pare-feu (LINA) à partir du moment où le périphérique n'a pas répondu (essayez d'obtenir les journaux environ 5 minutes avant l'incident). Il est recommandé de configurer syslog au niveau 6 (Informationnel), comme pratique recommandée.

15 nonies. Si vous avez configuré un serveur syslog sur le châssis (FXOS sur 4100/9300), fournissez les journaux (en commençant environ 5 minutes avant l'incident).

15 decies. Syslog des périphériques adjacents à partir du moment de l'incident.

15 undecies. Diagramme de topologie montrant les connexions physiques entre le périphérique pare-feu et les périphériques adjacents.

Problèmes courants

Erreur : Expiration de la communication avec DME

Si vous vous connectez à la console et voyez :

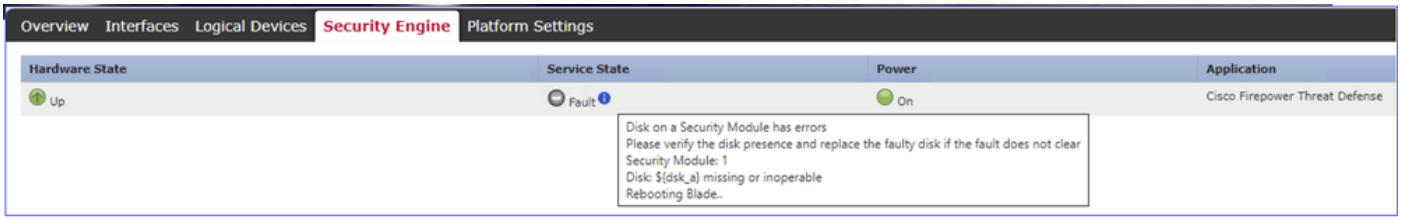
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

La plupart du temps, cela indique un problème logiciel.

Action recommandée : Contactez le centre d'assistance technique Cisco TAC

Erreur disque : manquant ou inutilisable

Cette sortie provient d'une appliance matérielle 4100/9300 où une défaillance liée au disque est générée :

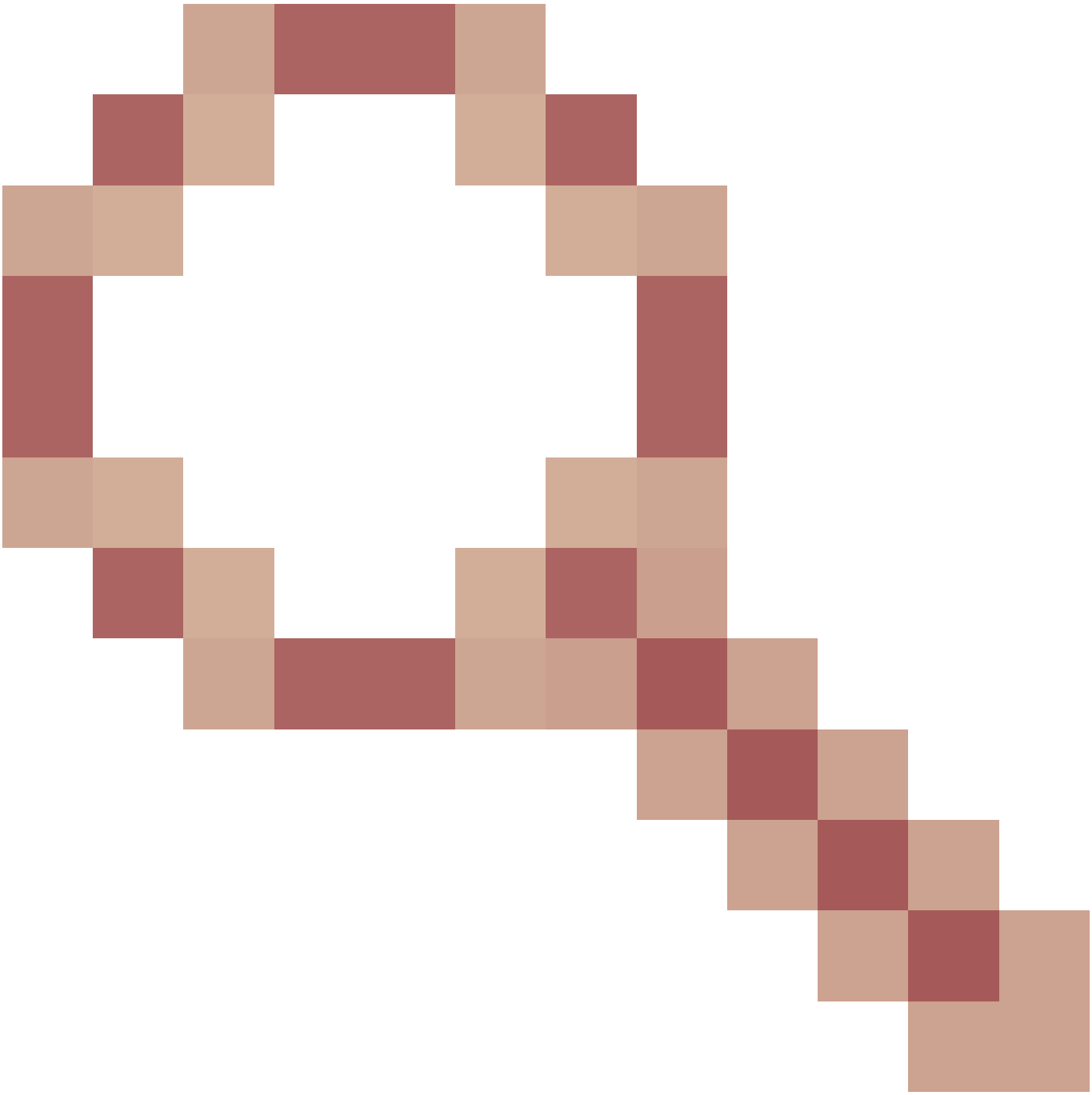


Action recommandée : Réinstallez le disque SSD. Si cela ne vous aide pas, collectez le bundle de dépannage de châssis et contactez le TAC Cisco.

Avis sur le champ : FN72077 - FPR9300 et FPR4100

- Les appareils de sécurité des gammes FPR9300 et FPR4100 ne transmettent plus le trafic réseau.
- Les utilisateurs disposant d'informations d'identification valides ne peuvent pas se connecter à la console de gestion.
- CLI affiche le message d'erreur : "Erreur logicielle : Exception lors de l'exécution : [Erreur : Expiration de la communication avec DME]

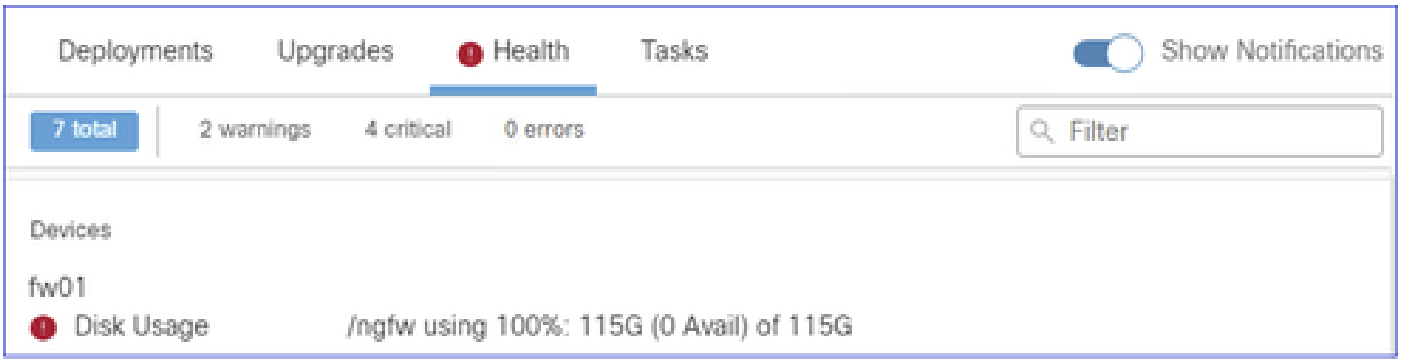
Action recommandée : Un cycle d'alimentation du châssis 4100/9300 est requis afin de récupérer temporairement de ce problème. Vérifiez l'ID de bogue Cisco CSCvx99172 pour plus de détails et une version qui a un correctif.



(Avis sur le champ : FN72077 - Appareils de sécurité des gammes FPR9300 et FPR4100 - Certains appareils peuvent ne pas transmettre le trafic après 3,2 ans de disponibilité).

Utilisation des disques 100 %

Un espace disque insuffisant sur le pare-feu peut empêcher le périphérique de répondre. Si le périphérique est géré par FMC, vous pouvez obtenir des alertes d'intégrité comme ceci :



Action recommandée : Si vous avez FMC et FTD en cours d'exécution sur le logiciel 7.7.0 et supérieur, essayez d'effacer de l'espace disque en utilisant la procédure décrite à l'adresse https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space

Si cela n'est pas possible ou ne vous aide pas, contactez le TAC Cisco.

Le CSF 3100 ne s'active pas après une panne de courant

Action recommandée : Effectuez une mise à niveau vers une version logicielle comportant un correctif pour :

ID de bogue Cisco CSCwm14729
La gamme CSF 3100 ne redémarre pas après une panne de courant, nécessitant un cycle d'alimentation manuel.

Appareils de sécurité Cisco Firepower 2100 : Certaines Unités Peuvent Présenter

Des Défaillances De Mémoire

- Défaillances DIMM dans les 5 ans de service en raison de problèmes de processus des composants
- FN associé : https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html
- ID de bogue Cisco associé CSCwb74948

Action recommandée : Remplacement des composants DIMM ou du dispositif de sécurité

Références

- https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html
- https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#
- https://www.cisco.com/c/en/us/support/docs/field-notices/720/fn72077.html
- https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/216245-collection-of-core-files-from-a-firepowe.html#anc6
- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

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.