Collecter des données pour l'analyse de la cause première du retour/plantage logiciel dans le pare-feu sécurisé

Table des matières

Introduction

Ce document décrit les étapes à suivre pour collecter des données en cas de retraçage logiciel.

Conditions préalables

Exigences

Connaissances de base sur les produits.

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.

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

Fond

Le logiciel FTD ou ASA peut effectuer un retraçage et généralement un rechargement pour différentes raisons, notamment :

- Défauts logiciels, y compris les défauts du système d'exploitation et des composants tiers.
- Exceptions matérielles, telles que des erreurs de mémoire de bas niveau ou de CPU.
- Dans certains cas, en raison d'un manque de ressources système, telles que la mémoire.
- Déclenché manuellement par l'utilisateur à des fins de diagnostic sous la supervision du TAC :

```
<#root>

>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower>

enable


Password:
firepower#

crashinfo force ?


page-faultc  Crash by causing a page fault exception
process     Crash the specified process
watchdog    Crash by causing a watchdog timeout
```

Dans le cas d'un traceback également connu sous le nom de crash, en fonction du processus, généralement un crashinfo, core ou minidump fichiers sont générés :

- crashinfo contient un minimum de données de diagnostic de la mémoire de processus.
- Le fichier core est un vidage complet de la mémoire du processus au moment du retour arrière.
- Le fichier minidump est spécifique à Snort3 et contient des données de diagnostic de la mémoire de processus.

Dans le logiciel Secure Firewall, le processus qui a fait l'objet d'un suivi peut se trouver dans l'un des composants suivants :

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

Outre les fichiers Core et Crashinfo, l'analyse de la cause première (RCA) d'un suivi nécessite des informations supplémentaires, telles que les fichiers de dépannage et show-tech, les messages Syslog, etc.

Le centre d'assistance technique et Cisco traitent les problèmes de coeur et de panne lors de l'analyse des fichiers dans le cadre d'une demande de service (dossier).

Collecte de données

Procédez comme suit pour collecter les données nécessaires à l'analyse de la récurrence du retour arrière. En raison du risque de perte de données provoqué par les rotations de fichiers, veuillez fournir les données demandées dès que possible.

1. Clarifiez ces éléments :

1 bis. Matériel exact.

1 ter. La version logicielle,

1 quater. Type de logiciel de pare-feu sécurisé (ASA ou FTD).

1 quinquies. Mode de déploiement (mode natif ou multi-instance).

Référez-vous à Vérifier les versions du logiciel Firepower et Vérifier la configuration de Firepower, Instance, Availability, Scalability pour les étapes de vérification détaillées.

2. Préciser s'il y a eu des changements environnementaux récents, tels que :

2a. Ajout de trafic.

2 ter. Modifications majeures de la configuration, y compris les commandes.

Assurez-vous d'inclure les horodatages et le fuseau horaire aussi précisément que possible.

3. Si le retour arrière s’est produit après des modifications de configuration à l’aide de commandes spécifiques, collectez les sorties de session de terminal. Si l'autorisation de commande est configurée sur l'ASA, collectez les rapports d'autorisation de commande à partir du serveur distant, tel que Identity Services Engine (ISE).

4. Dans les étapes suivantes, assurez-vous de vérifier les fichiers crashinfo, core ou minidump avec les horodatages les plus récents et prenez note du chemin d'accès complet à chaque fichier. Les chemins d'accès complets sont nécessaires pour la collecte des fichiers, comme indiqué dans Comment collecter les fichiers Crashinfo, Coredump et Minidump à partir de Secure Firewall ? de l'Aide.

ASA

4.1. Vérifiez la présence d'un fichier crashinfo. Pour afficher les dernières informations de panne, exécutez la commande show crashinfo. Les fichiers crashinfo se trouvent dans le résultat de la commande dir.

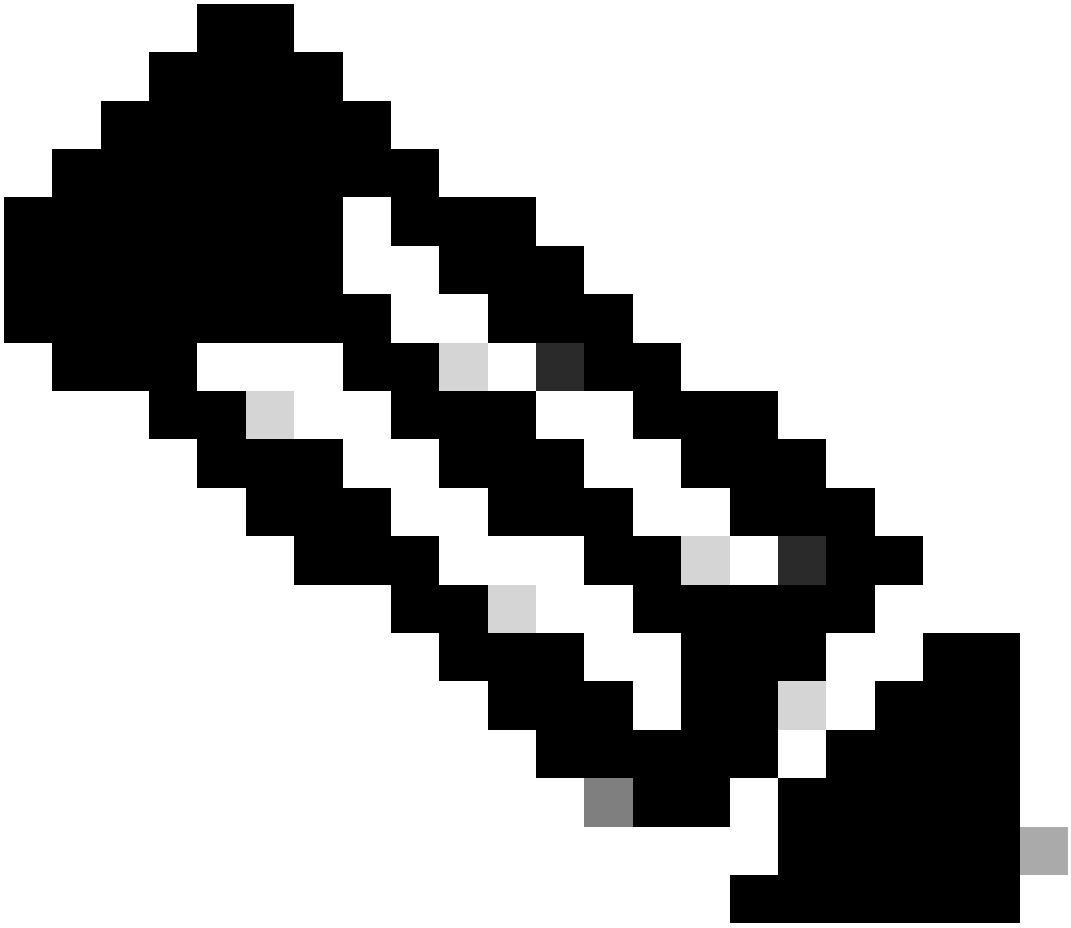
<#root>

```
asa#
dir

Directory of disk0:/
…
1610891723  -rw-  413363       20:51:22 Aug 13 2025
crashinfo_lina.14664.20250813.205102
```

4.2. Vérifiez la présence des fichiers de base ASA à l'aide de la commande dir coredumpfsys :

<#root>

```
asa#
dir coredumpfsys

Directory of disk0:/coredumpfsys/
24577  -rw-  419619286    12:43:07 Aug 04 2025
core.lina.11.10335.1754311379.gz

11     drwx  16384        00:15:57 Jan 01 2010  lost+found
```



Remarque : Sur l'ASA virtuel, la fonction coredump par défaut est désactivée :

<#root>

```
ciscoasa#
```

show coredump

filesystem 'disk0:' has no coredump filesystem

Pour activer la fonctionnalité coredump, référez-vous à la section coredump enable dans le Guide de référence des commandes de la gamme Cisco Secure Firewall ASA, Commandes A-H.

FTD

4.1. Vérifiez la présence d'un fichier FTD crashinfo. Pour afficher les informations de panne les plus récentes, exécutez la commande show crashinfo. Les fichiers crashinfo se trouvent dans le résultat de la commande dir.

```
<#root>

ftd#

dir


Directory of disk0:/
…
1610891723  -rw-  413363       20:51:22 Aug 13 2025

crashinfo_lina.14664.20250813.205102
```

Sur FTD, les fichiers crashinfo se trouvent dans le répertoire expert mode /mnt/disk0/ :

```
<#root>

>

expert


admin@firepower:~$

ls -l /mnt/disk0/


total 496472
..
-rw-r--r-- 1 root root    460812 Aug 13 10:31

crashinfo_lina.13050.20250813.103059
```

Dans le fichier de dépannage FTD, les fichiers crashinfo se trouvent dans dir-archives/var-log/mnt-disk0/:

```
<#root>

$

ls -l


/dir-archives/mnt-disk0


total 9456
```

```
-rw-r--r-- 1 root root  453024 Aug  8 23:51
crashinfo_lina.13949.20250808.235100
```

4.2. Vérifier la présence de fichiers de base FTD. Sur FTD, les fichiers de coeur sont accessibles en mode expert /ngfw/var/data/cores/ et /ngfw/var/common/ répertoires :

```
<#root>
admin@ftd:~$
ls -l /ngfw/var/data/cores/

total 1255512
-rw-r--r-- 1 root root 602208441 Jul 24 09:28
core.lina.11.14993.1753342057.gz

-rw-r--r-- 1 root root 682148808 Jul 24 09:38
core.lina.11.80997.1753342659.gz
```

Dans le fichier de dépannage FTD, les noms des fichiers principaux sont dans le fichier command-output/for\ CORE\ in\ \`ls\ *:

```
<#root>
 command-outputs $
cat for\ CORE\ in\ \`ls\ *

/var/data/cores/core.lina.11.38967.1732272744.gz: gzip compressed data, was "core.lina.11.38967.1732272
```

FTD Snort3-specific coredump

Cette section s'applique uniquement au FTD exécutant le moteur Snort3.

4.1. Vérifier la présence des fichiers crashinfo du moteur Snort3 snort3-crashinfo.* sont dans le répertoire /ngfw/var/log/crashinfo/ du mode expert.

```
<#root>
admin@ftd$
ls -l /ngfw/var/log/crashinfo
```

```
total 8
-rw-r--r-- 1 root root 1104 Aug 22 19:10
 snort3-crashinfo.1755889806.134825

-rw-r--r-- 1 root root 1104 Aug 22 19:15
snort3-crashinfo.1755890128.201213
```

Dans le fichier de dépannage FTD, les mêmes fichiers sont dans dir-archives/var-log/crashinfo/.

4.2. Vérifier la présence des fichiers de minidump Snort3 minidump_* dans /ngfw/var/data/cores/ :

```
<#root>
admin@firepower:~$
ls -l /ngfw/var/data/cores/

total 936580
-rw------- 1 root root    977760 Aug 22 19:10
minidump_1755889805_firepower_snort3_17455.dmp
```

Dans le fichier de dépannage FTD, les fichiers de minidump sont dans file-contents/ngfw/var/data/cores/ :

```
<#root>
$
ls -l file-contents/ngfw/var/data/cores/

total 1904
-rw------- 1 root root 977760 Aug 22 19:10
minidump_1755889805_firepower_snort3_17455.dmp
```

Modules de sécurité Firepower 4100 et 9300

Cette section s'applique uniquement aux modules Firepower 4100 et 9300.

4.1. Vérifier la présence de crashinfo et des fichiers de base :

```
<#root>
```

```
firepower #
```

connect module 1 console

```
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:
```

Crashinfo_and_Core_Files

```
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 14:43:07 | 419619286  | core.lina.11.10335.1754311379.gz
2025-08-13 12:45:11 | 419798152  | core.lina.11.10466.1755081904.gz
2025-08-14 13:35:02 | 419449591  | core.lina.11.46717.1755171295.gz
2025-08-18 12:48:26 | 419624883  | core.lina.6.10412.1755514099.gz
([b] to go back)
…
```

FXOS

4.1. Sur les châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100 et 4200, vérifiez la présence des fichiers de base à l'aide des commandes dir workspace:/cores et dir workspace:/cores_fxos dans l'interpréteur de commandes local-mgmt.

Si l'application ASA est installée, alors connectez-vous au shell FXOS en utilisant la commande connect fxos admin :

<#root>

```
firepower-1120#
```

connect local-mgmt

```
Warning: network service is not available when entering 'connect local-mgmt'
```

```
firepower-1120(local-mgmt)#
dir workspace:/cores

1 119710270 Jul 25 11:41:12 2025
core.lina.6.19811.1753443666.gz

2     16384 Jul 22 21:13:57 2025 lost+found/
3      4096 Jul 22 21:16:07 2025 sysdebug/

Usage for workspace://
159926181888 bytes total
5545205760 bytes used
154380976128 bytes free

firepower-1120(local-mgmt)#
dir workspace:/cores_fxos

1 9037 Jul 25 10:52:17 2025 kp_init.log
```

Les fichiers principaux sont également mentionnés dans les fichiers /opt/cisco/platform/logs/prune_cores.log du fichier de dépannage du châssis :

```
<#root>
$
less opt/cisco/platform/logs/prune_cores.log

Fri Jul 25 11:41:31 UTC 2025 -  Avoiding compress/move for for ./core.lina.6.19811.1753443666: UptimeIn
Fri Jul 25 11:42:32 UTC 2025 -  Number of pre-compressed core file : 0
Fri Jul 25 11:42:32 UTC 2025 -
Uncompressed file ./core.lina.6.19811.1753443666: uptimeInSec: 3141; SafeIntval:45; Timestamp Diff: 80;
```

4.2. Sur les châssis Firepower 4100 et 9300, vérifiez la présence des fichiers de base à l'aide des commandes dir workspace:/cores dans l'interpréteur de commandes local-mgmt :

```
<#root>
firewall(local-mgmt)#
dir workspace:/cores

Usage for workspace://
4160421888 bytes total
461549568 bytes used
3484127232 bytes free
```

Les noms des fichiers principaux se trouvent dans le fichier de dépannage du châssis, dans les sorties de la commande show cores dans le fichier *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, où * est la partie du nom du fichier de dépannage, par exemple, 20250311123356_ FW_BC1_all.tar.

5. Vérifiez si les fichiers crashinfo, coredump et minidump sont pertinents pour l'incident.

- Comparez les horodatages des fichiers à l'horodatage de l'incident, ou..
- Convertissez l'horodatage de l'époque du nom de fichier à la date à l'aide de la commande date Linux.

Pour les fichiers core et minidump, les horodatages d'époque peuvent être convertis en date time en utilisant la date sur n'importe quel hôte Linux :

<#root>

admin@ftd:~$

ls -l /ngfw/var/data/cores/

total 1255512
-rw-r--r-- 1 root root 602208441 Jul 24 09:28 core.lina.11.14993

.1753342057.

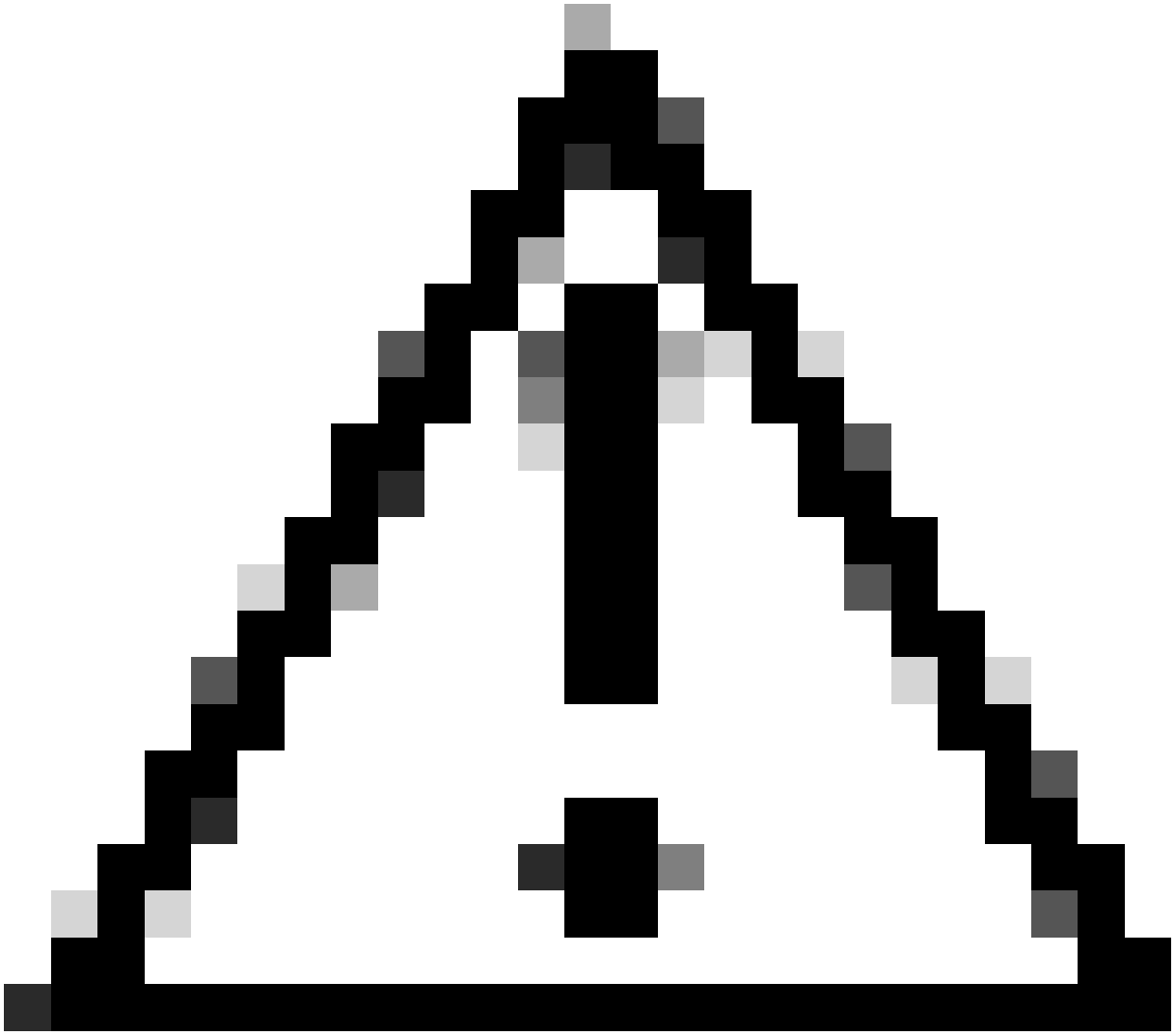
gz

linux $

date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025

6. Reportez-vous à la section Comment collecter les fichiers Crashinfo, Coredump et Minidump à partir de Secure Firewall ? pour télécharger les fichiers crashinfo, Minidump et Core des étapes 4-5.



Mise en garde : Ne renommez pas les fichiers Core, Crashinfo ou Minidump.

7. Suivez les étapes des procédures de génération de fichiers de dépannage Firepower pour collecter des fichiers show-tech et dépanner :

7 bis. Fichier show-tech ASA.

7 ter. Fichier de dépannage FTD.

7 quater. Fichier show-tech des modules de sécurité Firepower 4100 et 9300.

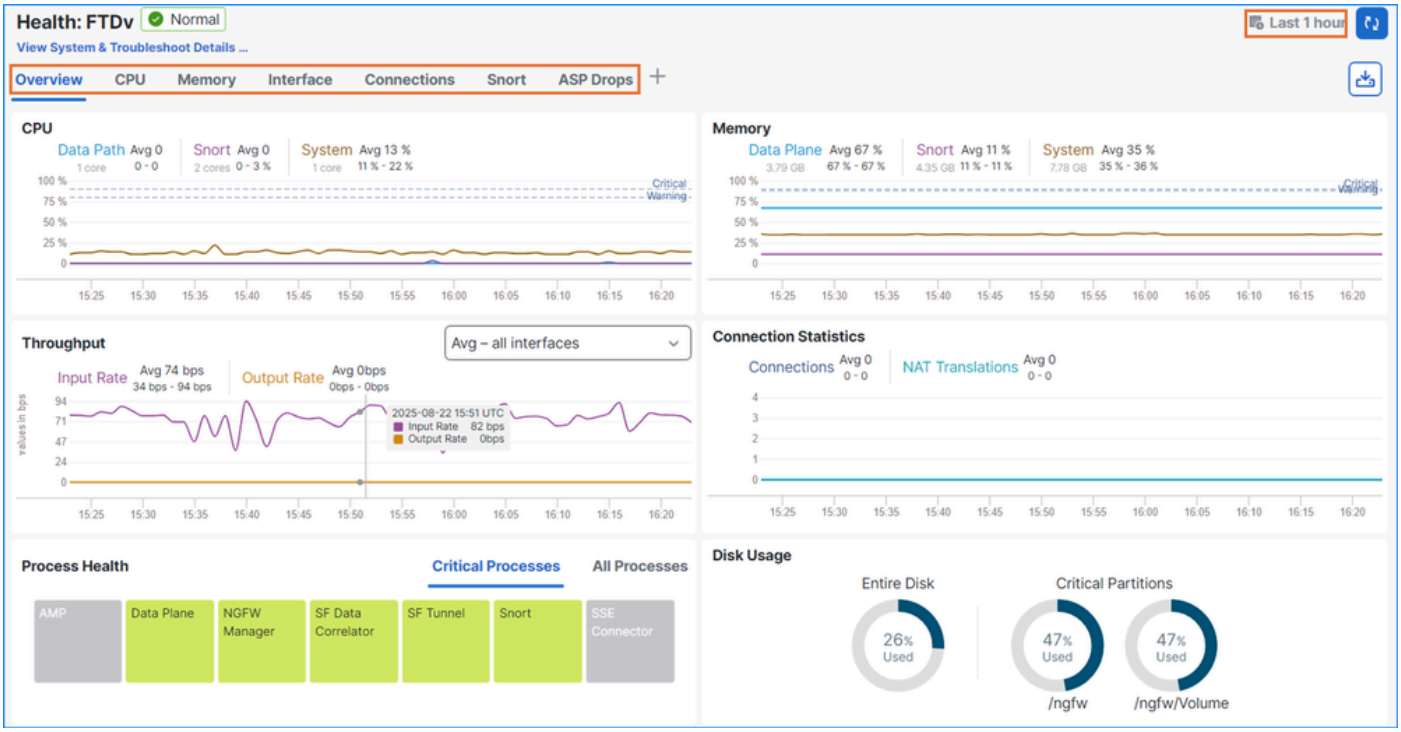
7 quinquies. Fichier show-tech des châssis Firepower 4100 et 9300.

7 sexies. Fichier show-tech des châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100 et 4200. Les fichiers de dépannage du châssis pour Secure Firewall 3100, 4200 en mode conteneur peuvent être téléchargés via l'option FMC > Devices > [chassis] > 3 dots > > Troubleshoot Files.

8. Dans le cas du FTD, collectez des captures d’écran des onglets de surveillance de l’état de

santé sur FMC pendant au moins 30 minutes avant le retour arrière. Veillez à inclure les captures d'écran de tous les onglets mis en surbrillance. Dans le cas d'un retour arrière récurrent, collectez des captures d'écran couvrant quelques incidents.

En outre, en cas de haute disponibilité et de mise en grappe, collectez des captures d'écran pour toutes les unités concernées :



9. Collectez les messages Syslog bruts (non analysés) du moteur Lina à partir des serveurs Syslog pendant au moins 30 minutes avant le retour arrière. Le format brut est essentiel au traitement interne par le TAC et les outils d'ingénierie.

En cas de retour arrière récurrent, collectez les messages bruts couvrant quelques incidents. En outre, en cas de haute disponibilité et de mise en grappe, collectez les syslogs bruts de toutes les unités concernées.

Vérification sur l'interface CLI ASA/FTD :

<#root>

```
ftd#
```

show run logging

```
logging enable
logging trap informational
logging host inside
```

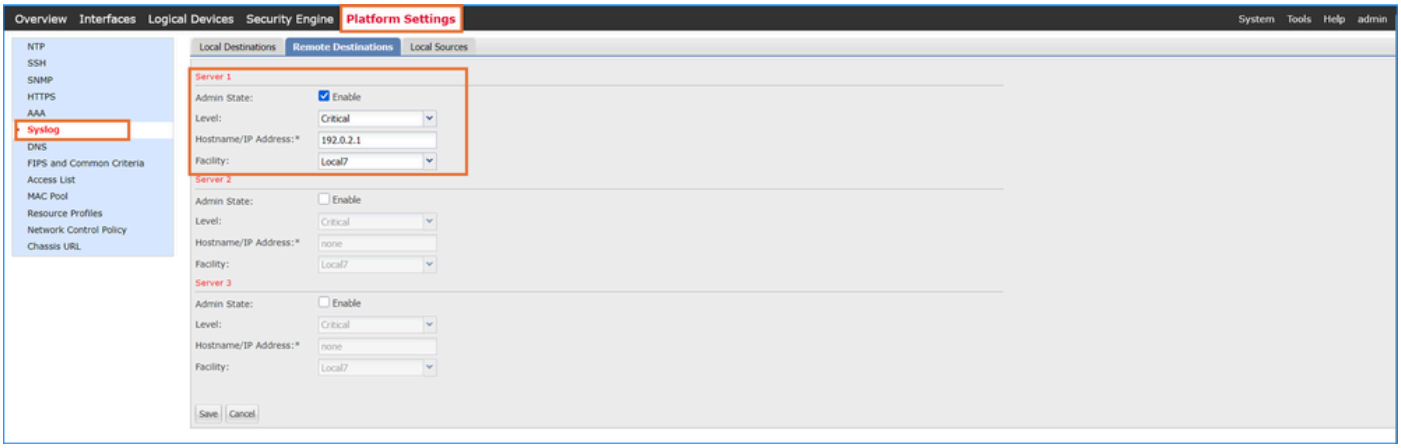
192.0.2.1

```
<-- syslog server address
```

10. Dans le cas de Firepower 4100 et 9300, collectez les messages FXOS bruts (non analysés) à partir des serveurs syslog au moins 10 minutes avant le retour arrière. Le format brut est essentiel au traitement interne par le TAC et les outils d'ingénierie.

En outre, en cas de haute disponibilité et de mise en grappe, collectez les syslogs bruts à partir de tous les châssis affectés.

Vérification sur l'interface utilisateur du gestionnaire de châssis Firepower (FCM) :



Vérification sur l'interface de ligne de commande FXOS :

<#root>

```
firepower #
```

scope monitoring

```
firepower /monitoring #
```

show syslog

```
console
    state: Disabled
    level: Critical

monitor
    state: Disabled
    level: Critical

file
    state: Enabled
    level: Critical
    name:  messages
    size:  4194304

remote destinations
    Name     Hostname             State    Level         Facility
    -------- -------------------- -------- ------------- --------
```

Server 1 192.0.2.1 Enabled Critical Local7

```
<-- syslog server address
```

```
    Server 2 none                Disabled Critical      Local7
    Server 3 none                Disabled Critical      Local7

sources
    faults: Enabled
    audits: Disabled
    events: Disabled
```

11. Collectez le CPU, la mémoire et les données d'interface ASA ou FTD, y compris les déroutements, à partir des serveurs SNMP configurés. Veillez à inclure les données couvrant au moins 30 minutes avant le retour arrière.

En cas de retour arrière récurrent, collectez les messages bruts couvrant quelques incidents. En outre, en cas de haute disponibilité et de mise en grappe, collectez les messages bruts de tous les châssis affectés.

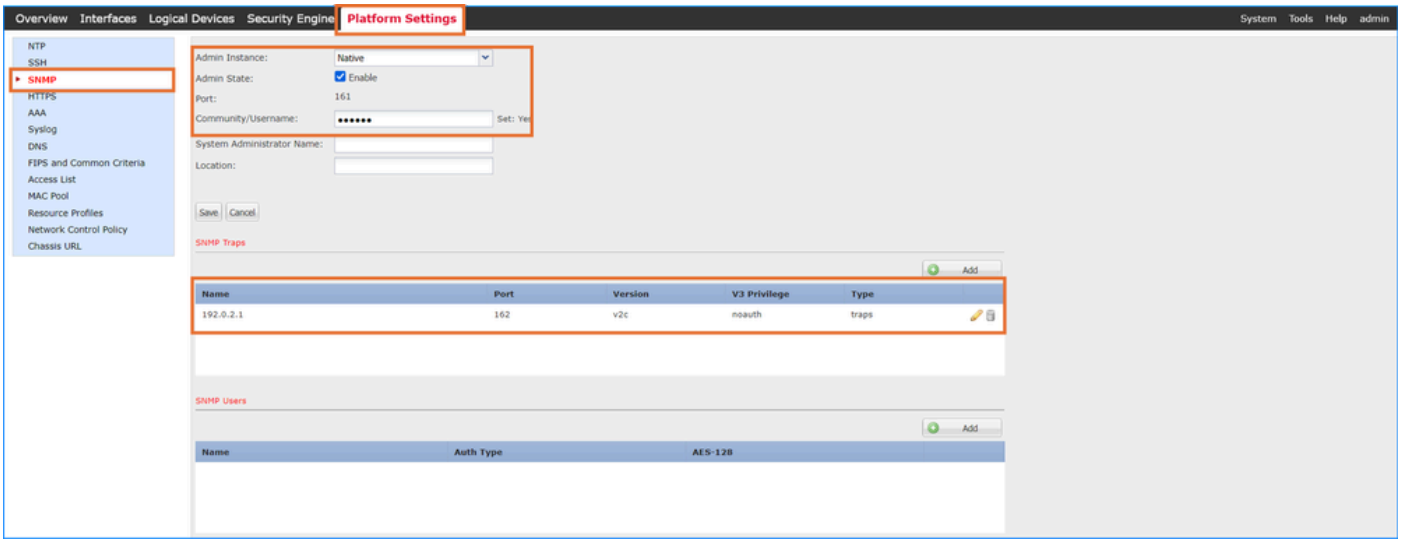
Vérification sur l'interface CLI ASA/FTD :

```
<#root>

ftd#

show run snmp-server


snmp-server host inside 192.0.2.1 community ***** version 2c

<-- SNMP server addresses

snmp-server host inside 192.0.2.2 community ***** version 2c


no snmp-server location
no snmp-server contact
```

12. Dans le cas de Firepower 4100 et 9300, collectez le CPU, la mémoire, les données d'interface, y compris les déroutements à partir des serveurs SNMP configurés. Veillez à inclure les données couvrant au moins 30 minutes avant le retour arrière.

En cas de retour arrière récurrent, collectez les messages bruts couvrant quelques incidents. En outre, en cas de haute disponibilité et de mise en grappe, collectez les messages bruts de tous les châssis affectés.

Vérification sur l'interface utilisateur FCM :



Vérification sur l'interface de ligne de commande FXOS :

<#root>

```
firepower #
```

scope monitoring

```
firepower /monitoring #
```

show configuration

```
 …
     enable snmp


     enter snmp-trap 192.0.2.1
<-- SNMP server address
 !        set community
          set notificationtype traps
          set port 162
          set v3privilege noauth
          set version v2c
```

13. Collectez le profil de trafic des collecteurs Netflow. Veillez à inclure les données couvrant au moins 30 minutes avant le retour arrière.

En cas de retraçage récurrent, collectez des données couvrant quelques incidents. En outre, en cas de haute disponibilité et de mise en grappe, collectez les données de tous les châssis concernés.

Vérification sur l'interface CLI ASA/FTD :

<#root>

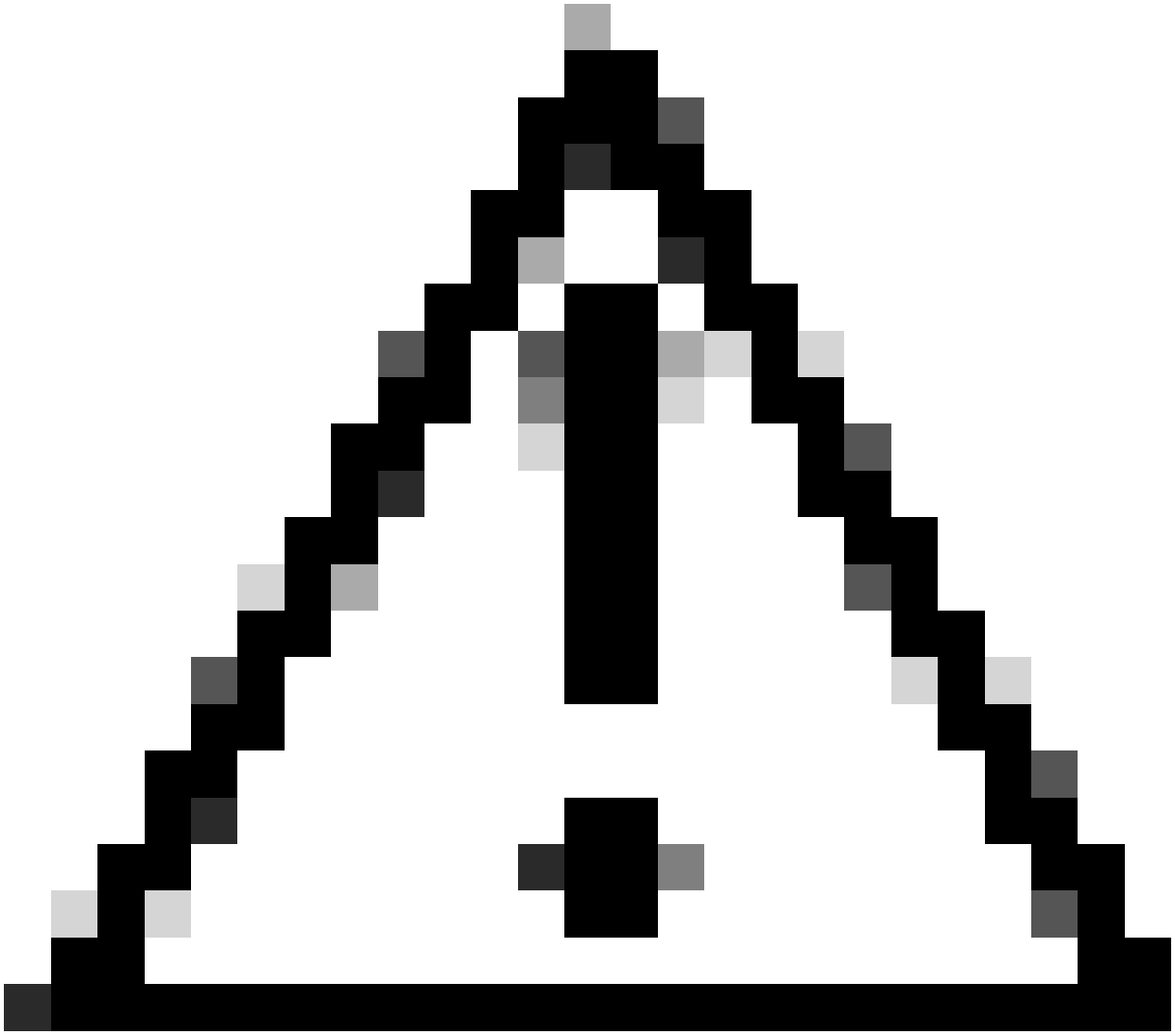
```
ftd#
show run flow-export


flow-export destination inside 192.0.2.1 1255
<-- Netflow collector address
flow-export delay flow-create 1


ftd#
show run policy-map global_policy


!
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP


class netflow


  flow-export event-type all destination 192.0.2.1
<-- Netflow collector address
  class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

14. Dans le cas d’un retour arrière récurrent, collectez le résultat des sessions de console.

15. Ouvrez un dossier TAC et fournissez toutes les données.

Comment collecter les fichiers Crashinfo, Coredump et Minidump à partir de Secure Firewall ?

Procédez comme suit crashinfo, coredump et minidump Fichiers de Secure Firewall :



Mise en garde : Avertissement : Ne renommez pas les fichiers Core, Crashinfo ou Minidump.

ASA

Téléchargez des fichiers depuis l'interface de ligne de commande ASA vers le serveur distant :

<#root>

ASA#

copy flash:/crashinfo_lina.14664.20250813.205102 ?

```
  cluster:        Copy to cluster: file system
  disk0:          Copy to disk0: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
```

```
  scp:            Copy to scp: file system
  smb:            Copy to smb: file system
  startup-config  Copy to startup configuration
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
```

FTD

Option 1 : collecte des fichiers à l'aide de l'interface CLI de Lina

1. Si le serveur distant est accessible depuis le moteur Lina, copiez les fichiers vers /mnt/disk0 et téléchargez les fichiers depuis l'interface de ligne de commande Lina :

```
<#root>

>

expert


admin@firepower:~$

ls -l /ngfw/var/data/cores/


total 928152
-rw-r--r-- 1 root root 500163689 Aug 13 10:30

core.lina.11.13050.1755081050.gz


-rw-r--r-- 1 root root 449295230 Aug 13 20:51 core.lina.11.14664.1755118254.gz
drwx------ 2 root root     16384 Aug 10 20:59 lost+found
drwxr-xr-x 3 root root      4096 Aug 10 21:01 sysdebug

admin@firepower:~$

sudo cp /ngfw/var/data/cores/core.lina.11.13050.1755081050.gz /mnt/disk0/

admin@firepower:~$

 exit



>

system support diagnostic-cli


Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower>

enable


Password:
firepower#

dir
```

```
Directory of disk0:/
…
1610612928  -rw-  500163689    17:00:13 Aug 22 2025

core.lina.11.13050.1755081050.gz


firepower#

copy disk0:/core.lina.11.13050.1755081050.gz ?


  cache:    Copy to cache: file system
  cluster:  Copy to cluster: file system
  disk0:    Copy to disk0: file system
  disk1:    Copy to disk1: file system
  flash:    Copy to flash: file system
  ftp:      Copy to ftp: file system
  scp:      Copy to scp: file system
  smb:      Copy to smb: file system
  system:   Copy to system: file system
  tftp:     Copy to tftp: file system
```

2. Lorsque les fichiers du serveur distant sont téléchargés, assurez-vous de supprimer les fichiers copiés de /mnt/disk0/ sur FTD :

```
<#root>

admin@firepower:~$

cd /mnt/disk0/


admin@firepower:/mnt/disk0/:$

 sudo rm core.lina.11.13050.1755081050.gz
```

Option 2 - Collecter des fichiers à l'aide de l'ILC du mode expert

À l'aide des clients Linux TFTP, SFTP ou SCTP, téléchargez les fichiers du mode expert vers le serveur distant :

```
<#root>

>

expert


admin@firepower:~$

cd /ngfw/var/data/cores/
```

```
admin@firepower:/ngfw/var/data/cores$
sudo sctp core.lina.11.13050.1755081050.gz admin@192.0.2.1:/

admin@firepower:/ngfw/var/data/cores$
sudo tftp -l core.lina.11.13050.1755081050.gz -r core.lina.11.13050.1755081050.gz -p 192.0.2.1
```

Option 3 : collecte des fichiers à l'aide de l'interface de ligne de commande FXOS local-mgmt

Sur le FTD en mode natif exécuté sur les châssis Firepower 1000, 2100 et Secure Firewall 1200, 3100, 4200, les fichiers de base et de minidump peuvent être collectés à partir de l'interface de ligne de commande FXOS local-mgmt :

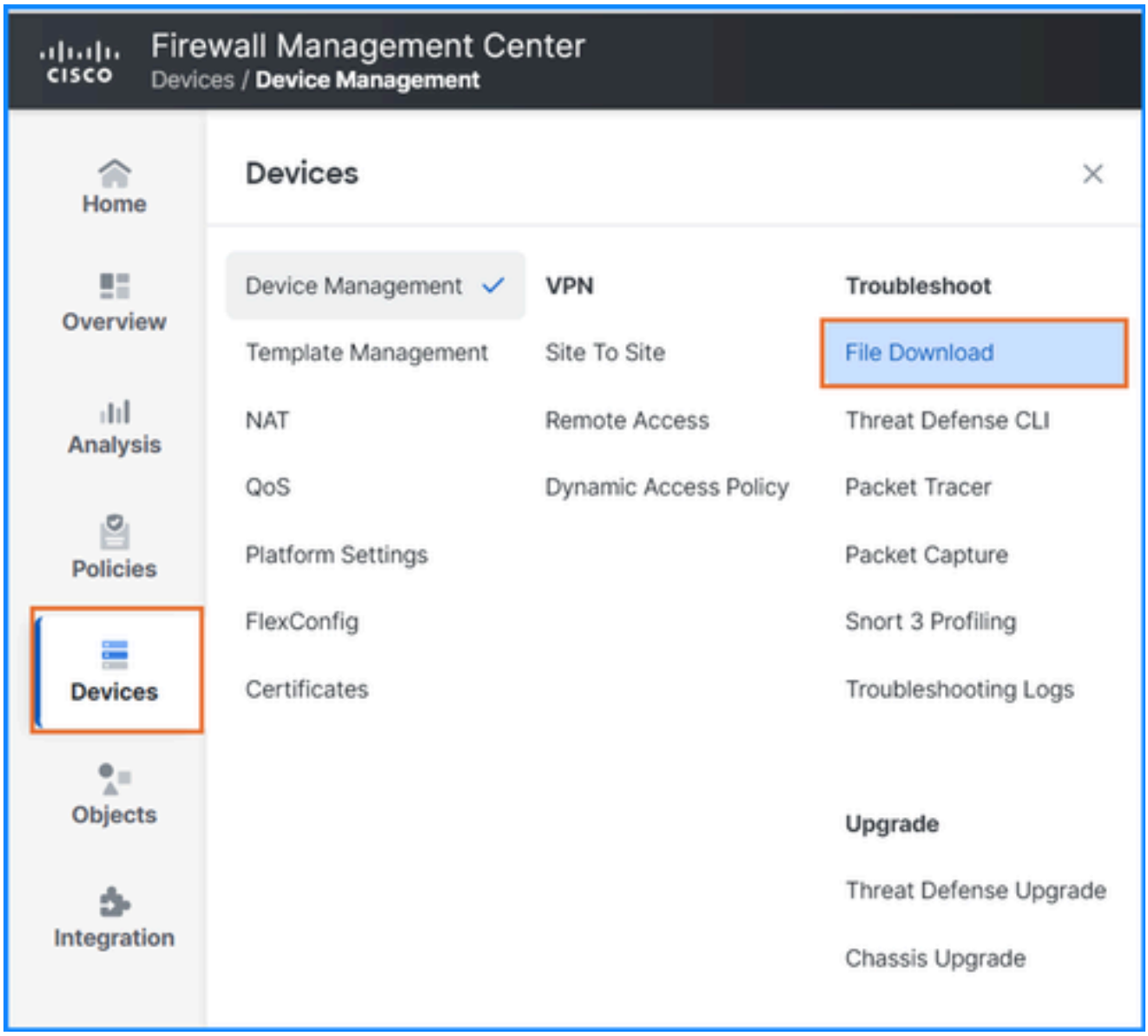
```
<#root>
firepower#
connect local-mgmt

firepower(local-mgmt)#
dir workspace:/cores

1 500163689 Aug 13 10:30:59 2025
core.lina.11.13050.1755081050.gz

firepower(local-mgmt)#
copy workspace:/core.lina.11.13050.1755081050.gz

?

  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI
```

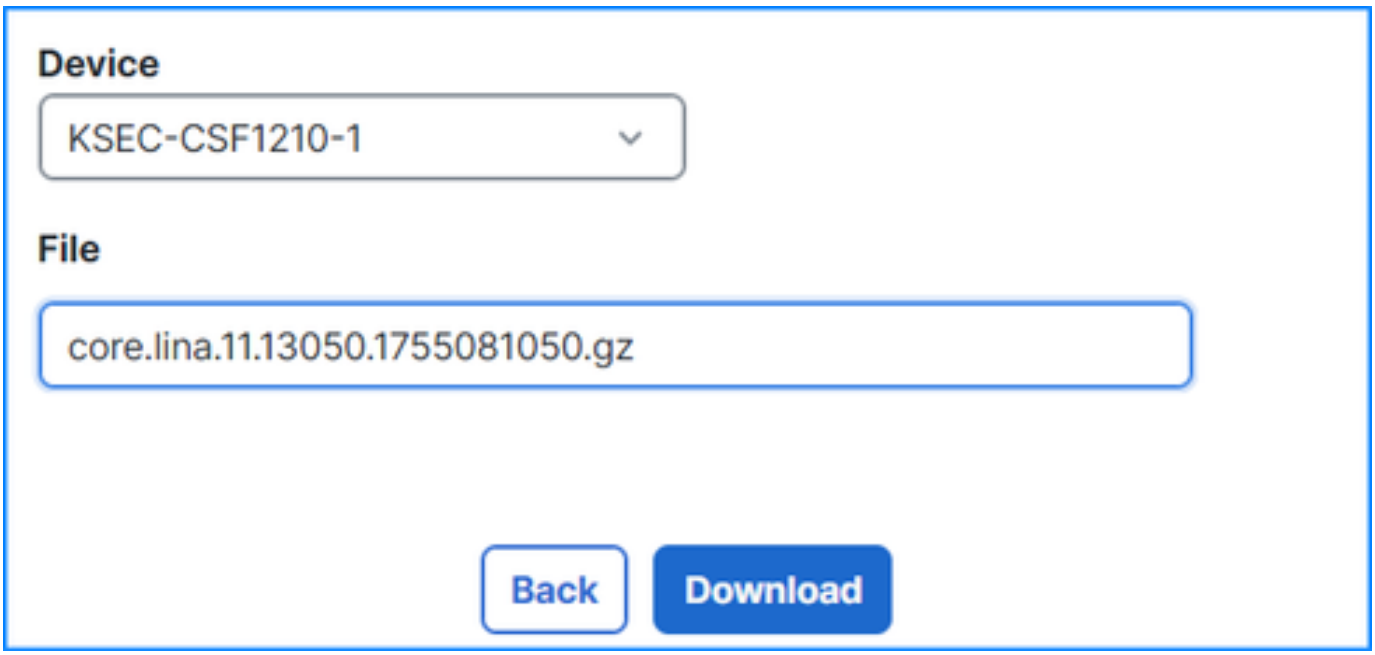
Option 4 : collecte des fichiers à l'aide de l'interface utilisateur FMC

Copiez les fichiers dans /ngfw/var/common :

```
<#root>

>

expert


admin@firepower:~$

ls -l /ngfw/var/data/cores/


total 928152
-rw-r--r-- 1 root root 500163689 Aug 13 10:30

core.lina.11.13050.1755081050.gz


-rw-r--r-- 1 root root 449295230 Aug 13 20:51 core.lina.11.14664.1755118254.gz
drwx------ 2 root root     16384 Aug 10 20:59 lost+found
drwxr-xr-x 3 root root      4096 Aug 10 21:01 sysdebug

admin@firepower:~$

sudo cp /ngfw/var/data/cores/core.lina.11.13050.1755081050.gz /ngfw/var/common/

admin@firepower:~$

ls -l /ngfw/var/common/

total 928152
1610612928  -rw-  500163689    17:00:13 Aug 22 2025

core.lina.11.13050.1755081050.gz
```

2. Téléchargez le fichier à partir de l'interface utilisateur FMC en utilisant l'option Devices > File Download :





3. Lorsque les fichiers du serveur distant sont téléchargés, assurez-vous de supprimer les fichiers

copiés de /ngfw/var/common/ sur FTD :

<#root>

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

cd

/ngfw/var/common/

```
admin@firepower:/mnt/disk0/:$
```

sudo rm core.lina.11.13050.1755081050.gz

Modules de sécurité Firepower 4100 et 9300

1. Connectez-vous au module et collectez les fichiers core et crashinfo dans le fichier show-tech du module :

<#root>

```
firepower #
```

connect module 1 console

```
Firepower-module1>
```

support diagnostic

```
======= Diagnostic =======
1. Create default diagnostic archive
2. Manually create diagnostic archive
3. Exit

Please enter your choice:
```

2

```
=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

1

```
=== Add files to package | Manual Diagnostic ===
1. Platform Logs
```

```
2. Config Platform Logs
3. Crash Info files & Core dumps
4. Applications Logs
5. ASA Logs
b. Back to main menu

Please enter your choice:
```

3

```
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286  |
```

core.lina.11.13050.1755081050.gz

```
([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:
```

s

```
Type the partial name of the file to add ([*] for all, [<] to cancel)
>
```

core.lina.11.13050.1755081050.gz

```
core.lina.11.13050.1755081050.gz
Are you sure you want to add these files? (y/n)
```

y

```
=== Package Contents ===
[Added] core.lina.11.13050.1755081050.gz
========================
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286  | core.lina.11.13050.1755081050.gz

([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:
```

b

```
=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

2

```
=== Package Contents ===
core.lina.11.13050.1755081050.gz
```

```
========================

=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

3

```
Creating Manual archive
Added file: core.lina.11.13050.1755081050.gz
```

Created archive file Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-module1>
```

support fileupload

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

1

```
-----------files------------
2025-08-04 13:17:50.723396 | 419624960  |
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
([s] to select files or [x] to Exit):
```

s

```
Type the partial name of the file to add, [<] to cancel
>
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-Module1_08_04_2025_13_17_50.tar
Are you sure you want to add these files? (y/n)
```

y

```
=== Package Contents ===
[Added] Firepower-Module1_08_04_2025_13_17_50.tar
=========================

Type the partial name of the file to add, [<] to cancel
>
```

<

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:
```

2

```
1 : Firepower-Module1_08_04_2025_13_17_50.tar

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

3

Transfer of Firepower-Module1_08_04_2025_13_17_50.tar started.

```
Firepower-module1>
Firepower-module1>
Firepower-module1> ß
```

Shift + ~

```
telnet> quit
Connection closed.

firepower /ssa #
```

connect local-mgmt

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

dir workspace:/bladelog/blade-1/

```
1 152828400 Aug 04 13:26:35 2025
```

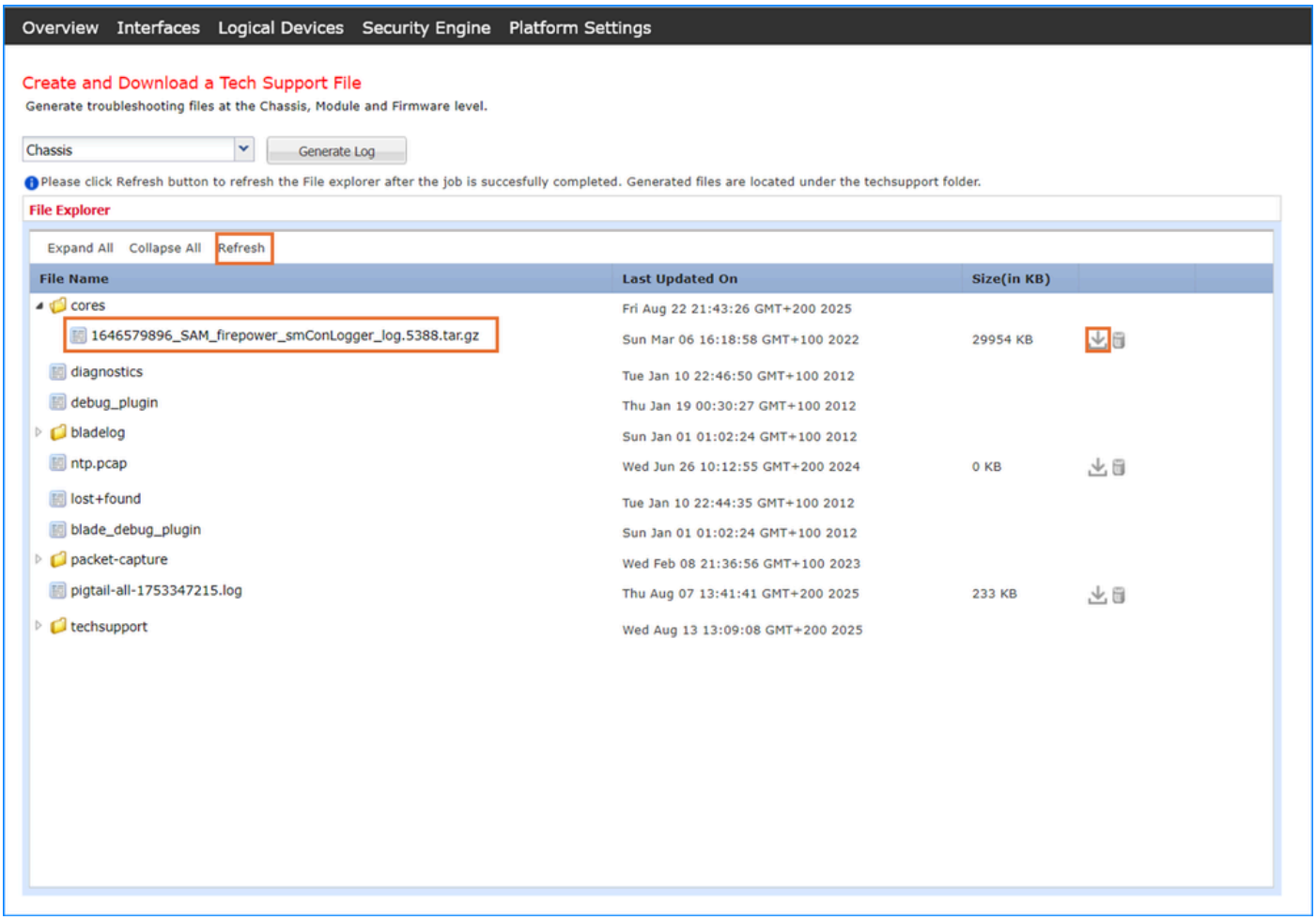
Firepower-Module1_08_04_2025_13_17_50.tar

Châssis Firepower 4100 et 9300

1. Collectez les fichiers principaux à l'aide de l'interface de ligne de commande FXOS local-mgmt :

```
<#root>

firepower#

connect local-mgmt


firepower(local-mgmt)#

dir workspace:/cores


1 30673335 Mar 06 16:18:58 2022

1646579896_SAM_firepower-1_smConLogger_log.5388.tar.gz


firepower(local-mgmt)#

copy workspace:/cores/1646579896_SAM_firepower-1_smConLogger_log.5388.tar.gz ?


  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
  sftp:       Dest File URI
  tftp:       Dest File URI
  usbdrive:   Dest File URI
  volatile:   Dest File URI
  workspace:  Dest File URI
```

2. Vous pouvez également collecter des fichiers à partir de l'interface utilisateur de FCM via Outils > Journaux de dépannage. Cliquez sur Refresh pour mettre à jour la vue du répertoire de fichiers et l'icône de téléchargement en regard du fichier principal :



Références

- Vérifier les versions du logiciel Firepower
- Vérification de la puissance de feu, des instances, de la disponibilité et de l'évolutivité
- Dépannage des procédures de génération de fichiers Firepower
- Référence des commandes ASA

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.