# Recopilación de datos para el análisis de la causa raíz del rastreo/desperfecto del software en un firewall seguro

## Contenido



## Introducción

Este documento describe los pasos para recopilar datos en caso de una trazabilidad de software.

## Prerequisites

### Requirements

Conocimiento básico del producto.

### Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Firewall seguro 1200, 3100 y 4200
- Firepower 1000, 4100 Y 9300

- Sistema operativo extensible seguro (FXOS) 2.16(0.136) de Cisco
- Cisco Secure Firewall Threat Defence (FTD) 7.6.1.291
- Cisco Secure Firewall Management Center (FMC) 7.6.1.291
- Adaptive Security Appliance (ASA) 9.2.2.9

# Background

El software FTD o ASA puede rastrearse y, normalmente, recargarse debido a diferentes motivos, como:

- Defectos de software, incluidos los defectos del sistema operativo y de los componentes de terceros.
- Excepciones de hardware, como memoria de bajo nivel o errores de CPU.
- En algunos casos, debido a la falta de recursos del sistema, como memoria.
- Activado manualmente por el usuario con fines de diagnóstico bajo supervisión del 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
```

En el caso de un rastreo también conocido como crash, dependiendo del proceso, generalmente se generan los archivos crashinfo, core o minidump:

- crashinfo contiene datos de diagnóstico mínimos de la memoria del proceso.
- el archivo de núcleo es un volcado completo de la memoria del proceso en el momento del seguimiento.
- El archivo minidump es específico de Snort3 y contiene datos de diagnóstico de la memoria del proceso.

En el software de Secure Firewall, el proceso que tenía una trazabilidad puede estar en

cualquiera de estos componentes:

- Chasis Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200.
- Módulos de seguridad Firepower 4100 y 9300.

Aparte de los archivos core y crashinfo, el análisis de causa raíz (RCA) de un seguimiento requiere información adicional, como la solución de problemas y los archivos show-tech, los mensajes syslog, etc.

TAC y Cisco gestionan el análisis de archivos de núcleo y crashfinfo como parte de una solicitud de servicio (caso).

## Recolección de datos

Siga estos pasos para recopilar los datos necesarios para el RCA de la devolución de seguimiento. Debido al riesgo de pérdida de datos causada por rotaciones de archivos, proporcione los datos solicitados lo antes posible.

1. Aclare estos elementos:

1 bis. Hardware exacto.

1 ter. Versión del software.

1 quáter. Tipo de software de firewall seguro (ASA o FTD).

1d. Modo de implementación (modo nativo o de varias instancias).

Consulte Verificación de las Versiones del Software Firepower y Verificación de la Configuración de Firepower, Instancia, Disponibilidad y Escalabilidad para obtener los pasos de verificación detallados.

2. Aclarar si se han producido cambios ambientales recientes, como:

2a. Adición de tráfico.

2 ter. Cambios de configuración importantes, incluidos los comandos.

Asegúrese de incluir las marcas de tiempo y la zona horaria con la mayor precisión posible.

3. Si el seguimiento ocurrió después de los cambios de configuración usando comandos específicos, recopile los resultados de la sesión de terminal. Si se configura la autorización de comandos en ASA, recopile informes de autorización de comandos del servidor remoto, como Identity Services Engine (ISE).

4. En los siguientes pasos asegúrese de verificar los archivos crashinfo, core o minidump con las marcas de tiempo más recientes y tome nota de la ruta completa a cada archivo. Las rutas completas son necesarias para la recolección de los archivos como se muestra en Cómo recopilar archivos Crashinfo, Coredump y Minidump de Secure Firewall? sección.

ASA

4.1. Verifique la presencia de un archivo crashinfo. Para ver la información crashinfo más reciente, ejecute el comando show crashinfo. Los archivos crashinfo se pueden encontrar en la salida del comando dir.

<#root>

asa#

**dir**

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

**crashinfo_lina.14664.20250813.205102**

4.2. Verifique la presencia de los archivos de núcleo ASA mediante el comando dir coredumpfsys:

<#root>

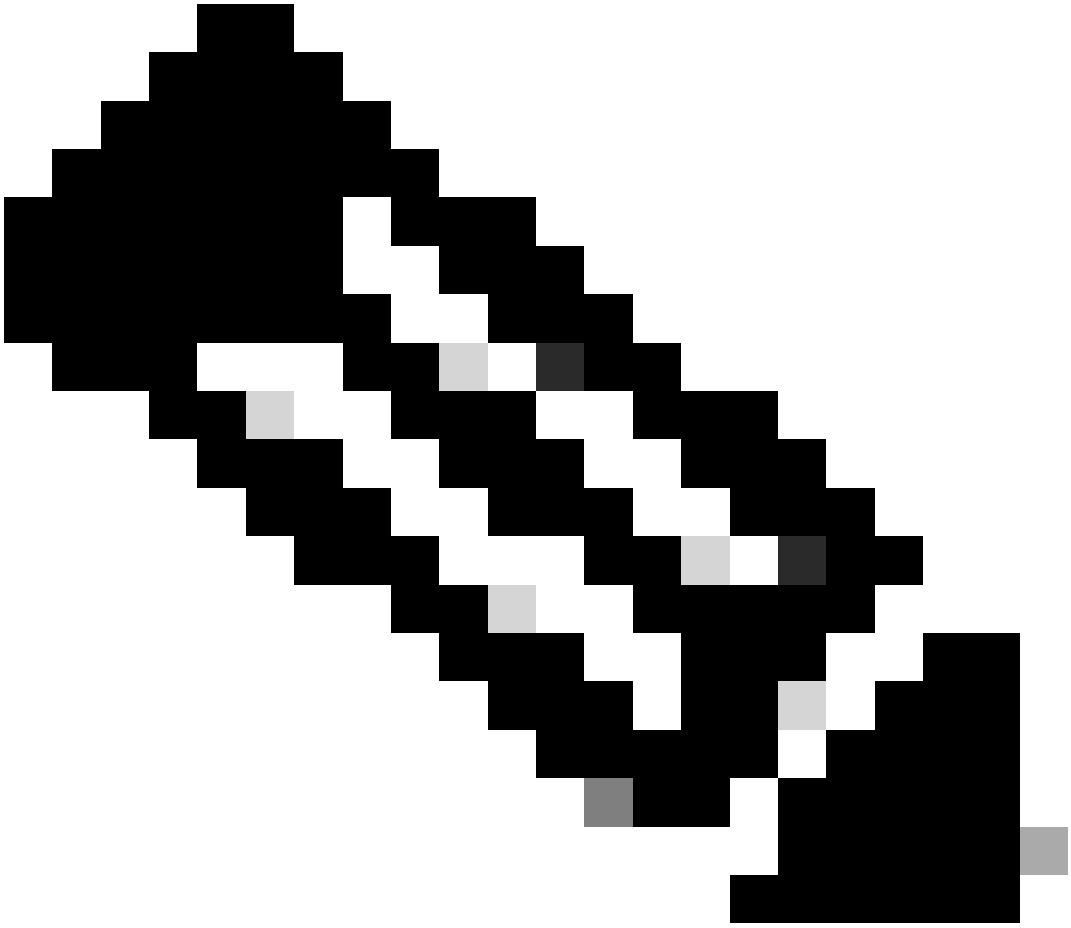
asa#

**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



Nota: En el ASA virtual, la función coredump está desactivada de forma predeterminada:

<#root>

ciscoasa#

**show coredump**

**filesystem 'disk0:' has no coredump filesystem**

Para habilitar la función coredump, consulte la sección coredump enable en la Referencia de Comandos de la Serie ASA de Cisco Secure Firewall, Comandos A-H.

FTD

4.1. Verifique la presencia de un archivo crashinfo de FTD. Para ver la información crashinfo más reciente, ejecute el comando show crashinfo. Los archivos crashinfo se pueden encontrar en la salida del comando dir.

```
<#root>

ftd#

dir


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

crashinfo_lina.14664.20250813.205102
```

En FTD, los archivos crashinfo se pueden encontrar en el directorio 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
```

En el archivo de solución de problemas de FTD, los archivos crashinfo están en 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. Verificar la presencia de ficheros de núcleo FTD. En FTD, los archivos de núcleo son accesibles en los directorios expert mode /ngfw/var/data/cores/ y /ngfw/var/common/:

<#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
```

En el archivo de resolución de problemas de FTD, los nombres de los archivos principales se encuentran en el archivo 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

Esta sección sólo es aplicable al FTD con el motor Snort3.

4.1. Verifique la presencia de los archivos crashinfo del motor Snort3 snort3-crashinfo.* se encuentran en el directorio /ngfw/var/log/crashinfo/ del modo experto.

<#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
```

En el archivo de solución de problemas de FTD, los mismos archivos están en dir-archives/var-log/crashinfo/.

4.2. Verifique la presencia de los archivos minidump de Snort3 minidump_* en /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
```

En el archivo de resolución de problemas de FTD, los archivos de minivolcado se encuentran en 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
```

Módulos de seguridad Firepower 4100 y 9300

Esta sección solo se aplica a los módulos Firepower 4100 y 9300.

4.1. Verificar la presencia de crashinfo y archivos de núcleo:

<#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. En los chasis Firepower 1000, 2100 y Secure Firewall 1200, 3100, 4200, Verifique la presencia de los archivos de núcleo mediante los comandos dir workspace:/cores y dir workspace:/cores_fxos en el shell local-mgmt.

Si la aplicación ASA está instalada, conéctese al shell FXOS usando el comando 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
```

Los archivos de núcleo también se mencionan en los archivos /opt/cisco/platform/logs/prune_cores.log en el archivo de solución de problemas del chasis:

```
<#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. En los chasis Firepower 4100 y 9300, verifique la presencia de los archivos de núcleo mediante los comandos dir workspace:/cores en el shell local-mgmt:

```
<#root>

firewall(local-mgmt)#

dir workspace:/cores


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

Los nombres de archivo de núcleo se pueden encontrar dentro del archivo de solución de problemas del chasis, en las salidas del comando show cores en el archivo *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, donde * es la parte del nombre del archivo de solución de problemas, por ejemplo, 20250311123356_ FW_BC1_all.tar.

5. Verifique si los archivos crashinfo, coredump y minidump son relevantes para el incidente.

- Compare las marcas de tiempo del archivo con la marca de tiempo del incidente o..
- Convierta la marca de tiempo epoch del nombre de archivo a la fecha usando el comando Linux date.

Para los archivos de núcleo y minivolcado, las marcas de tiempo de época se pueden convertir en fecha y hora usando la fecha en cualquier host 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.**

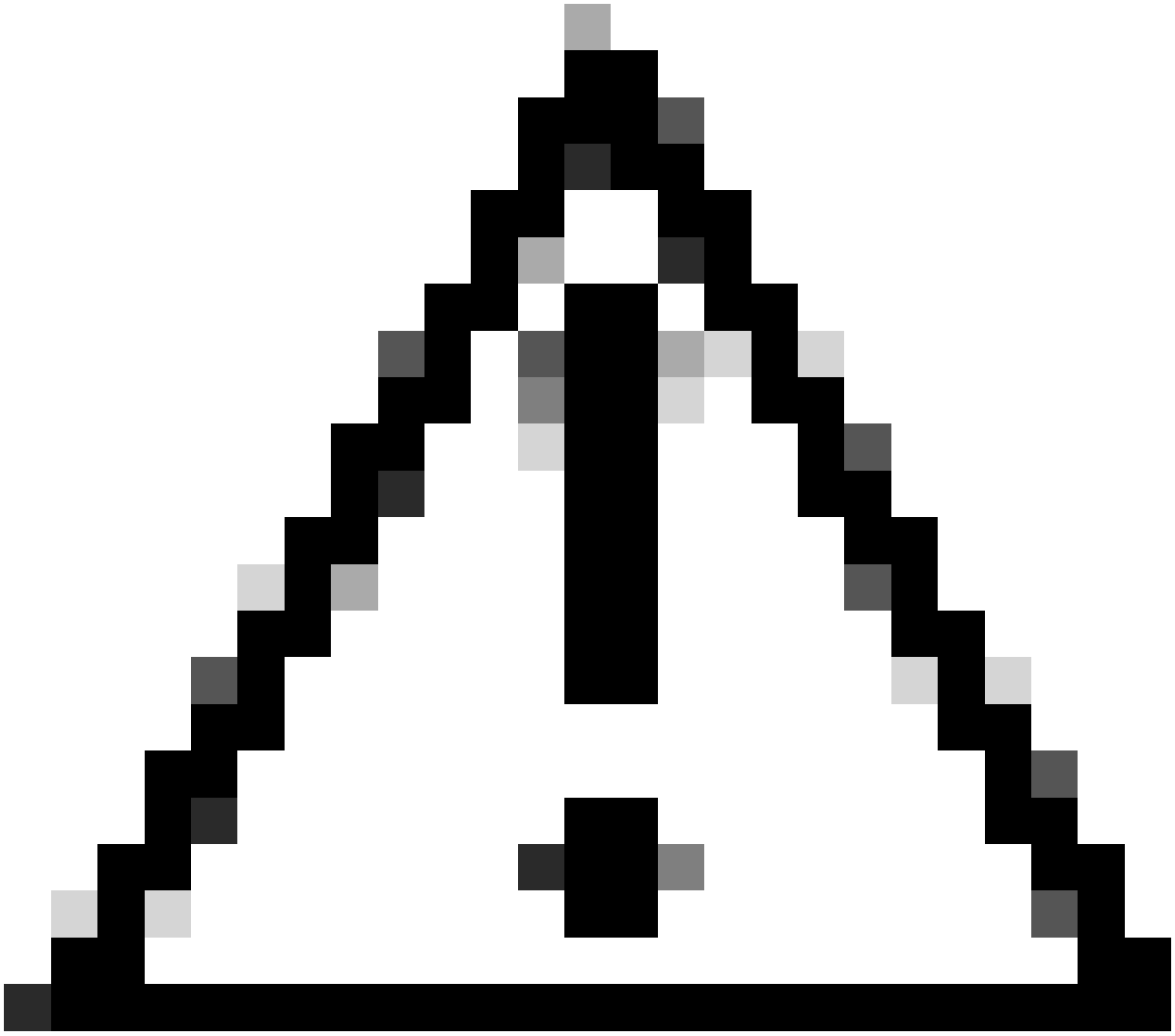
gz

linux $

**date -d @1753342057**

Thu Jul 24 07:27:37 UTC 2025

6. Refiérase a la sección Cómo Recolectar los Archivos Crashinfo, Coredump y Minidump de Secure Firewall? para descargar los archivos crashinfo, minidump y core de los pasos 4-5.



Precaución: No cambie el nombre de los archivos core, crashinfo o minidump.

---

7. Continúe con los pasos en Troubleshooting de los Procedimientos de Generación de Archivos de Firepower para recopilar los archivos show-tech y troubleshooting:

7 bis. Archivo show-tech de ASA.

7 ter. Archivo de solución de problemas de FTD.

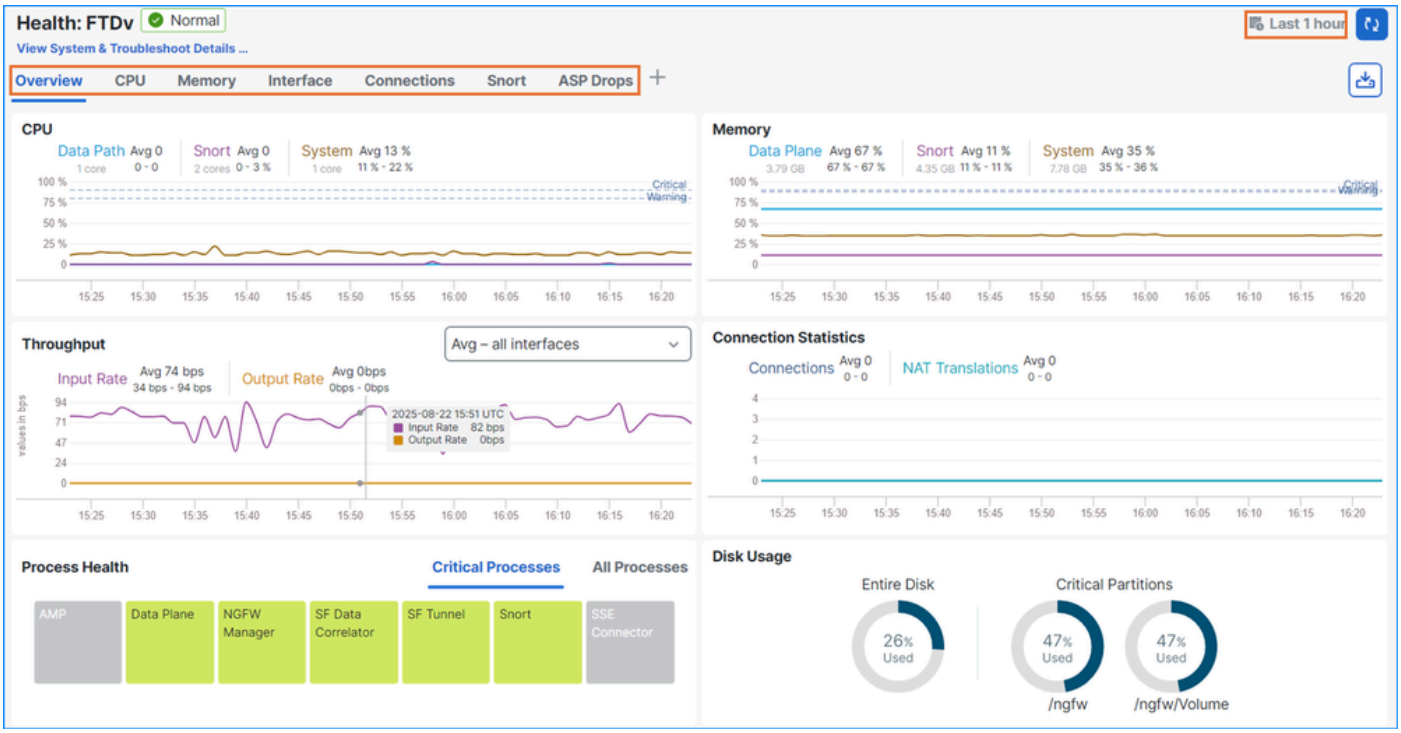
7 quater. Archivo show-tech del módulo de seguridad Firepower 4100 y 9300.

7 quinquies. Archivo show-tech de los chasis Firepower 4100 y 9300.

7 sexies. Archivo show-tech de firepower 1000, 2100 y firewall seguro 1200, 3100, 4200. Los archivos de resolución de problemas del chasis para Secure Firewall 3100, 4200 en modo contenedor se pueden descargar a través de la opción FMC > Devices > [chassis] > 3 dots > Troubleshoot Files.

8. En el caso del FTD, recopile capturas de pantalla de las pestañas de supervisión de la salud del FMC que cubran al menos 30 minutos antes del seguimiento. Asegúrese de incluir las capturas de pantalla de todas las pestañas resaltadas. En caso de seguimiento periódico, recopile capturas de pantalla que cubran algunos incidentes.

Además, en el caso de alta disponibilidad y agrupamiento, recopile capturas de pantalla de todas las unidades afectadas:




9. Recopile los mensajes raw (unparsed) syslog del motor de línea de los servidores syslog que cubran al menos 30 minutos antes del seguimiento. El formato sin procesar es esencial para el procesamiento interno por parte del TAC y las herramientas de ingeniería.

En caso de seguimiento recurrente, recopile los mensajes sin procesar que cubran algunos incidentes. Además, en caso de alta disponibilidad y agrupamiento, recopile los registros del sistema sin procesar de todas las unidades afectadas.

Verificación en ASA/FTD CLI:

<#root>

```
ftd#
```

**show run logging**

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

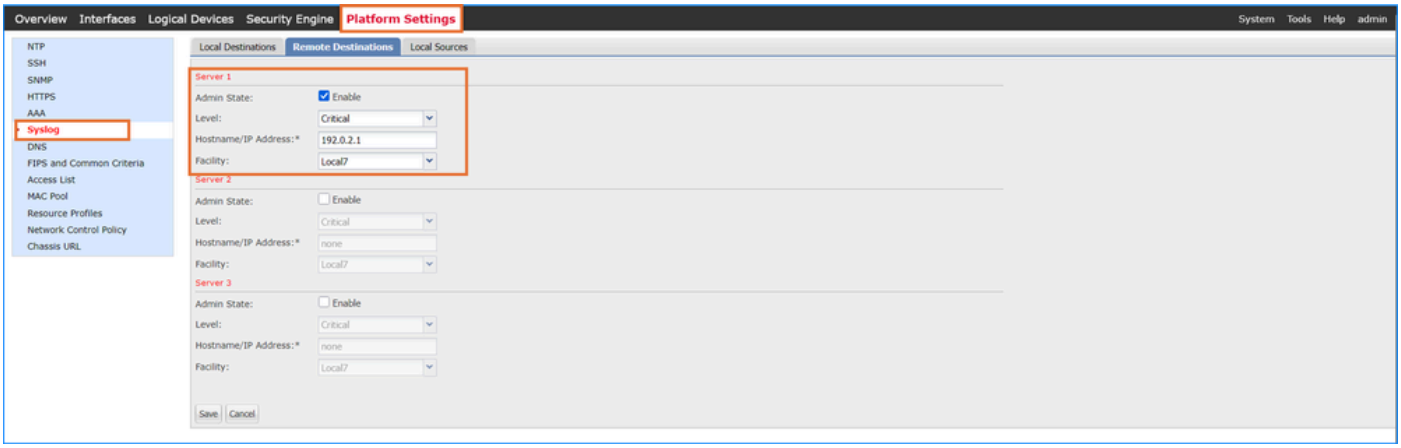
**192.0.2.1**

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

10. En el caso de Firepower 4100 y 9300, recopile los mensajes FXOS sin procesar (sin analizar) de los servidores syslog al menos 10 minutos antes del seguimiento. El formato sin procesar es esencial para el procesamiento interno por parte del TAC y las herramientas de ingeniería.

Además, en el caso de alta disponibilidad y clustering, recopile los registros del sistema sin procesar de todos los chasis afectados.

Verificación en la interfaz de usuario (IU) de Firepower Chassis Manager (FCM):




Verificación en la CLI de 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. Recopile datos de interfaz, memoria y CPU de ASA o FTD, incluidas las capturas de los servidores SNMP configurados. Asegúrese de incluir datos que cubran al menos 30 minutos antes del seguimiento.

En caso de seguimiento recurrente, recopile los mensajes sin procesar que cubran algunos incidentes. Además, en el caso de alta disponibilidad y clustering, recopile mensajes sin procesar de todos los chasis afectados.

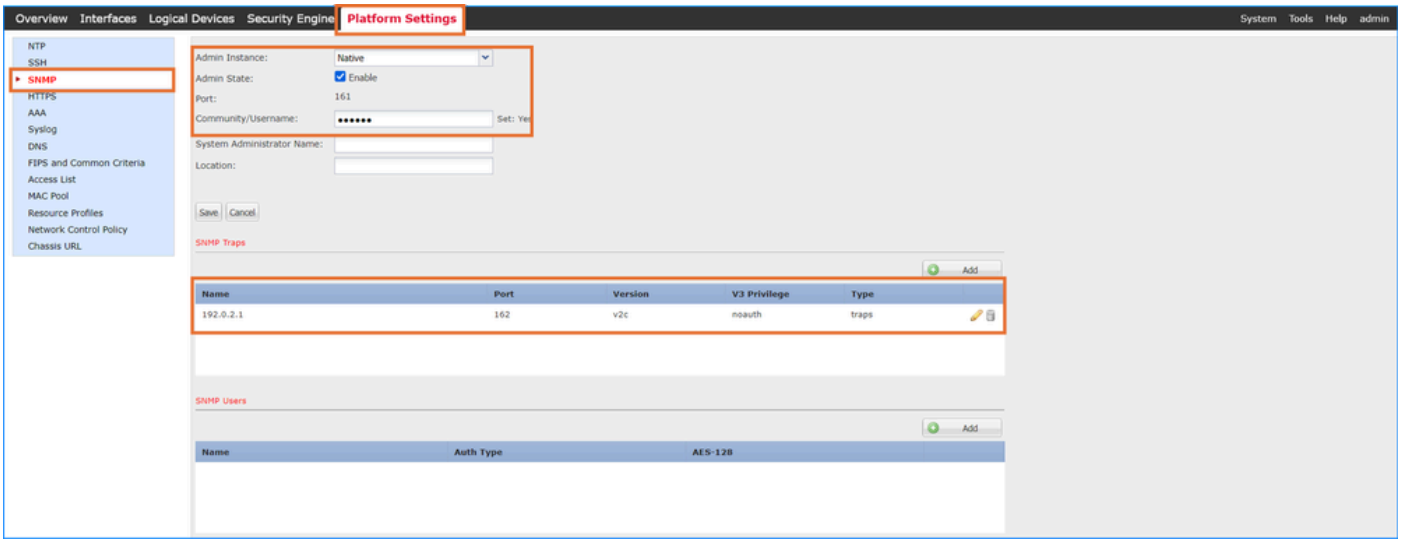
Verificación en ASA/FTD CLI:

```
<#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. En el caso de Firepower 4100 y 9300, recopile la CPU, la memoria y los datos de la interfaz, incluidas las trampas, de los servidores SNMP configurados. Asegúrese de incluir datos que cubran al menos 30 minutos antes del seguimiento.

En caso de seguimiento recurrente, recopile los mensajes sin procesar que cubran algunos incidentes. Además, en el caso de alta disponibilidad y clustering, recopile mensajes sin procesar de todos los chasis afectados.

Verificación en la IU de FCM:




Verificación en la CLI de 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. Recopile el perfil de tráfico de los recopiladores de Netflow. Asegúrese de incluir datos que cubran al menos 30 minutos antes del seguimiento.

En caso de seguimiento recurrente, recopile datos que cubran algunos incidentes.  Además, en el caso de alta disponibilidad y agrupación en clústeres, recopile datos de todos los chasis afectados.

Verificación en ASA/FTD CLI:

<#root>

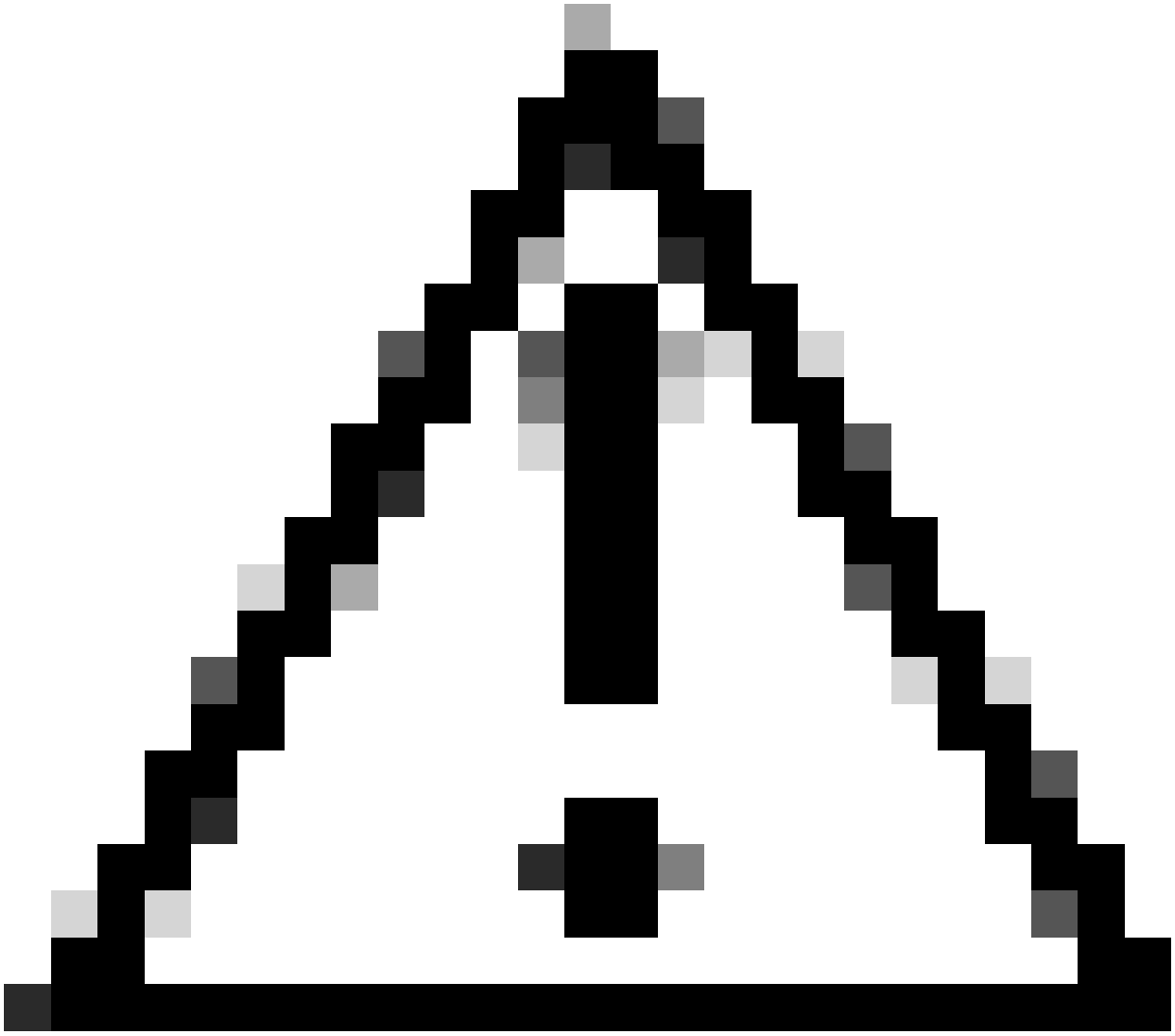
```
ftd#
show run flow-export


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. En el caso de seguimiento recurrente, recopile el resultado de las sesiones de la consola.

15. Abra un caso TAC y proporcione todos los datos.

# ¿Cómo se recopilan los archivos Crashinfo, Coredump y Minidump de Secure Firewall?

Continúe con estos pasos crashinfo, coredump y minidump Files from Secure Firewall:



Precaución: Advertencia: No cambie el nombre de los archivos core, crashinfo o minidump.

## ASA

Cargue archivos desde la CLI de ASA al servidor remoto:

<#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

### Opción 1: Recopilación de archivos mediante la CLI de Lina

1. Si se puede acceder al servidor remoto desde el motor de línea, copie los archivos a /mnt/disk0 y cargue los archivos desde la CLI de línea:

```
<#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. Cuando se descarguen los archivos del servidor remoto, asegúrese de eliminar los archivos copiados de /mnt/disk0/ en FTD:

<#root>

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

**cd /mnt/disk0/**

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

**sudo rm core.lina.11.13050.1755081050.gz**

Opción 2: Recopilar archivos mediante la CLI en modo experto

Con los clientes TFTP, SFTP o SCTP de Linux, cargue los archivos desde el modo experto al servidor remoto:

<#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
```

Opción 3: Recopilar archivos mediante la CLI de gestión local de FXOS

En el modo nativo FTD que se ejecuta en el chasis Firepower 1000, 2100 y Secure Firewall 1200, 3100, 4200, los archivos de núcleo y minivolcado se pueden recopilar desde la CLI de gestión local de FXOS:

<#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
```

Opción 4: Recopilar archivos mediante la interfaz de usuario de FMC

Copiar archivos a /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/**

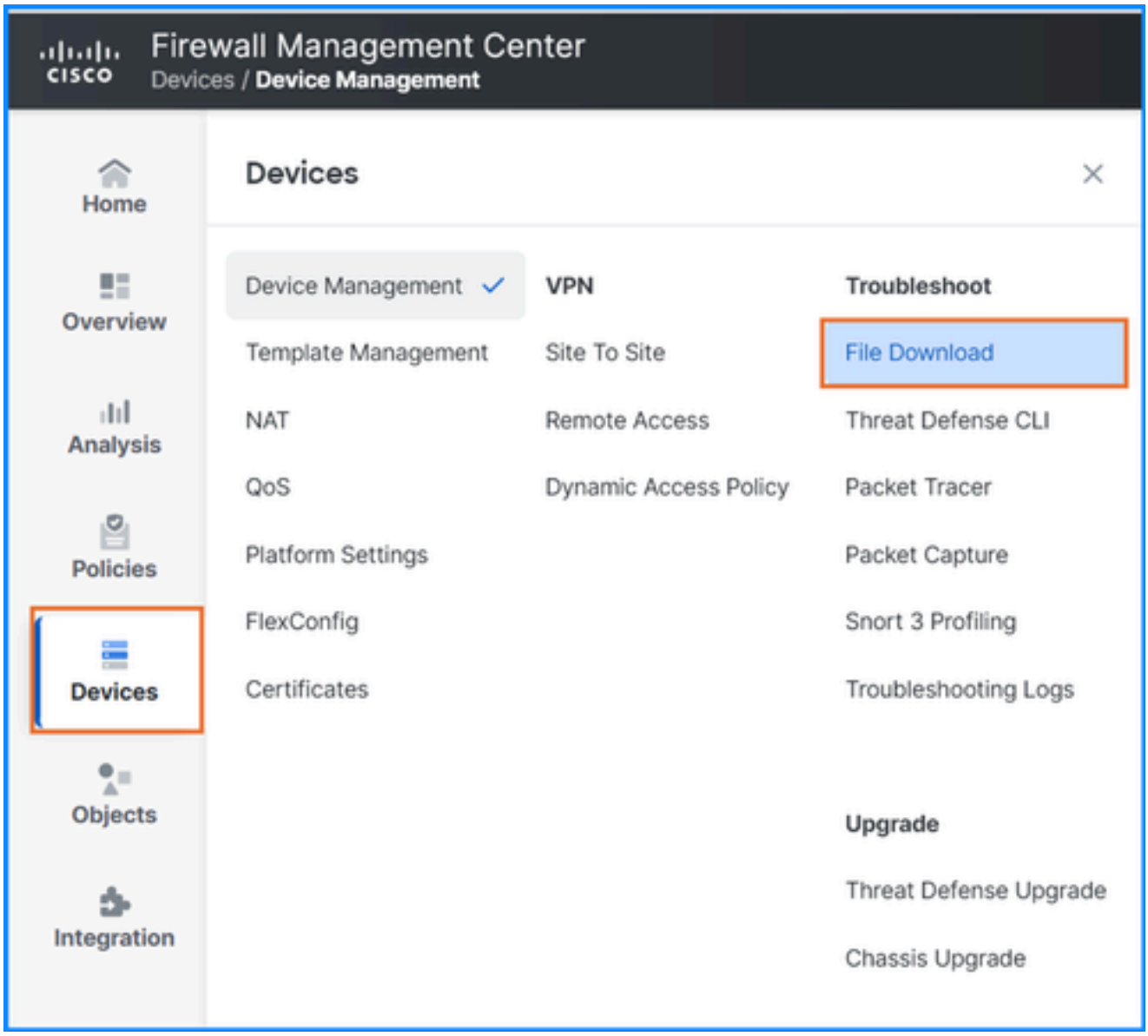
admin@firepower:~$

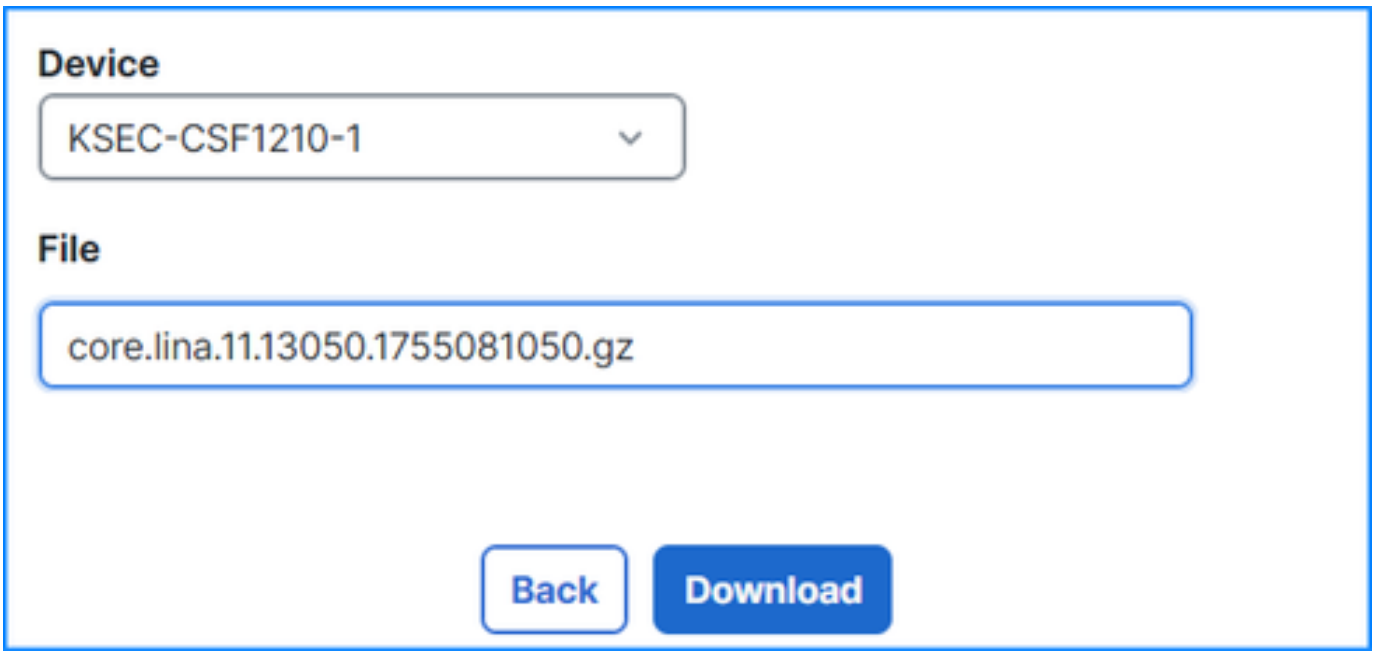
**ls -l /ngfw/var/common/**

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

**core.lina.11.13050.1755081050.gz**

2. Descargue el archivo desde la interfaz de usuario de FMC mediante la opción Devices > File Download:




3. Cuando se descarguen los archivos del servidor remoto, asegúrese de eliminar los archivos

copiados de /ngfw/var/common/ en FTD:

<#root>

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

**cd**

**/ngfw/var/common/**

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

**sudo rm core.lina.11.13050.1755081050.gz**

## Módulos de seguridad Firepower 4100 y 9300

1. Conéctese al módulo y recopile los archivos core y crashinfo como parte del archivo show-tech del módulo:

<#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**

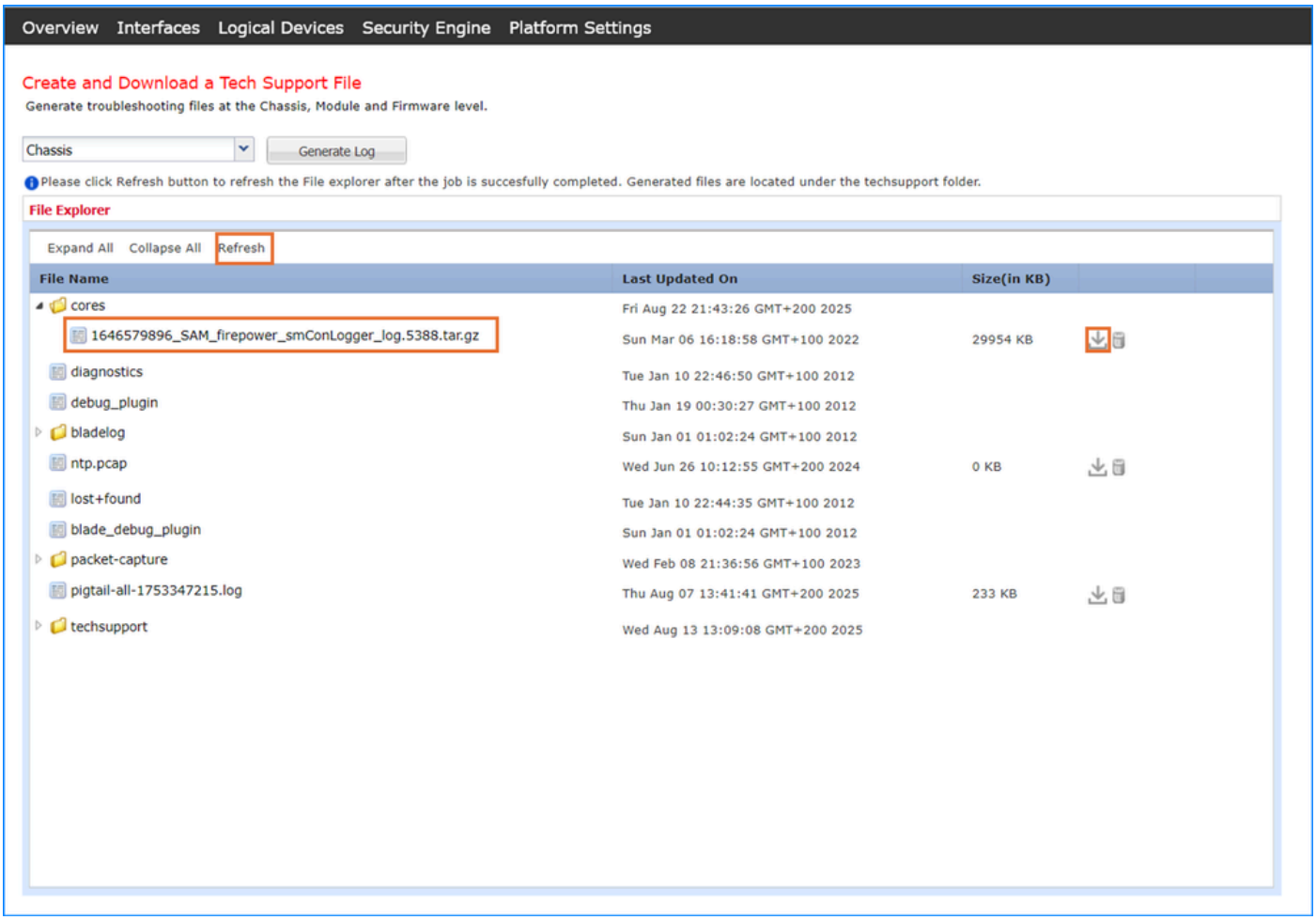
## Chasis Firepower 4100 y 9300

1. Recopile los archivos principales mediante la CLI de gestión local de FXOS:

<#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. Alternativamente, recopile archivos de la interfaz de usuario de FCM a través de Herramientas > Registros de solución de problemas. Haga clic en Refresh para actualizar la vista del directorio de archivos y el icono de descarga junto al archivo principal:




# Referencias

- Verificar versiones del software Firepower
- Verificar configuración de Firepower, instancia, disponibilidad y escalabilidad
- Solucionar problemas de procedimientos de generación de archivos Firepower
- Referencia de Comandos de ASA

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).