Raccolta dei dati per l'analisi della causa principale del software traceback/crash in Secure Firewall

Sommario

Introduzione

In questo documento viene descritta la procedura per raccogliere dati in caso di traceback del software.

Prerequisiti

Requisiti

Conoscenze base dei prodotti.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Firewall 1200, 3100, 4200

- Firepower 1000, 4100, 9300
- Cisco Secure eXtensible Operating System (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
- Adaptive Security Appliance (ASA) 9.2.2.9

Introduzione

Il software FTD o ASA può tracciare e ricaricare la memoria solitamente per diversi motivi, ad esempio:

- Difetti del software, inclusi i difetti del sistema operativo e dei componenti di terze parti.
- Eccezioni hardware, ad esempio errori di memoria o CPU di basso livello.
- In alcuni casi, a causa di risorse di sistema insufficienti, ad esempio la memoria.
- Attivato manualmente dall'utente a scopo diagnostico sotto supervisione 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
```

Nel caso di un traceback noto anche come crash, a seconda del processo, in genere vengono generati un file crashinfo, core o minidump:

- crashinfo contiene i dati diagnostici minimi dalla memoria del processo.
- core file è un dump completo della memoria di processo al momento del traceback.
- Il file di minidump è specifico di Snort3 e contiene i dati di diagnostica della memoria del processo.

Nel software Secure Firewall, il processo che disponeva di un traceback può essere incluso in uno dei seguenti componenti:

- Chassis Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100 e 4200.
- Moduli di sicurezza Firepower 4100, 9300.

Oltre ai file core e crashinfo, l'analisi della causa principale (RCA) di un traceback richiede informazioni aggiuntive, come la risoluzione dei problemi e i file show-tech, i messaggi syslog e così via.

L'analisi dei file core e crashfinfo viene gestita da TAC e Cisco come parte di una richiesta di servizio (caso).

Raccolta dati

Procedere come segue per raccogliere i dati necessari per l'RCA del traceback. A causa del rischio di perdita di dati causato dalla rotazione dei file, fornire i dati richiesti il prima possibile.

1. Chiarire quanto segue:

1 bis. Hardware esatto.

1 ter. Versione del software.

1 quater. Tipo di software firewall sicuro (ASA o FTD).

1 quinquies. Modalità di distribuzione (modalità nativa o a più istanze).

Per ulteriori informazioni, fare riferimento a Verifica delle versioni del software Firepower e Verifica della configurazione di Firepower, istanza, disponibilità e scalabilità.

2. Chiarire se vi sono stati cambiamenti ambientali recenti, quali:

2 bis. Aggiunta di traffico.

2 ter. Modifiche di configurazione principali, inclusi i comandi.

Assicurarsi di includere i timestamp e il fuso orario nel modo più preciso possibile.

3. Se il traceback si è verificato dopo le modifiche della configurazione utilizzando comandi specifici, raccogliere gli output della sessione terminale. Se l'autorizzazione dei comandi è configurata sull'appliance ASA, raccogliere i report di autorizzazione dei comandi dal server remoto, ad esempio Identity Services Engine (ISE).

4. Nei passi successivi, assicurati di verificare i file crashinfo, core o minidump con i timestamp più recenti e prendi nota del percorso completo di ciascun file. I percorsi completi sono necessari per la raccolta dei file, come mostrato nella sezione How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall? (Come raccogliere file Crashinfo, Coredump e Minidump da Secure Firewall) sezione.

ASA

4.1. Verificare la presenza di un file crashinfo. Per visualizzare le informazioni più recenti su

crashinfo, eseguire il comando show crashinfo. I file crashinfo sono disponibili nell'output del comando dir.

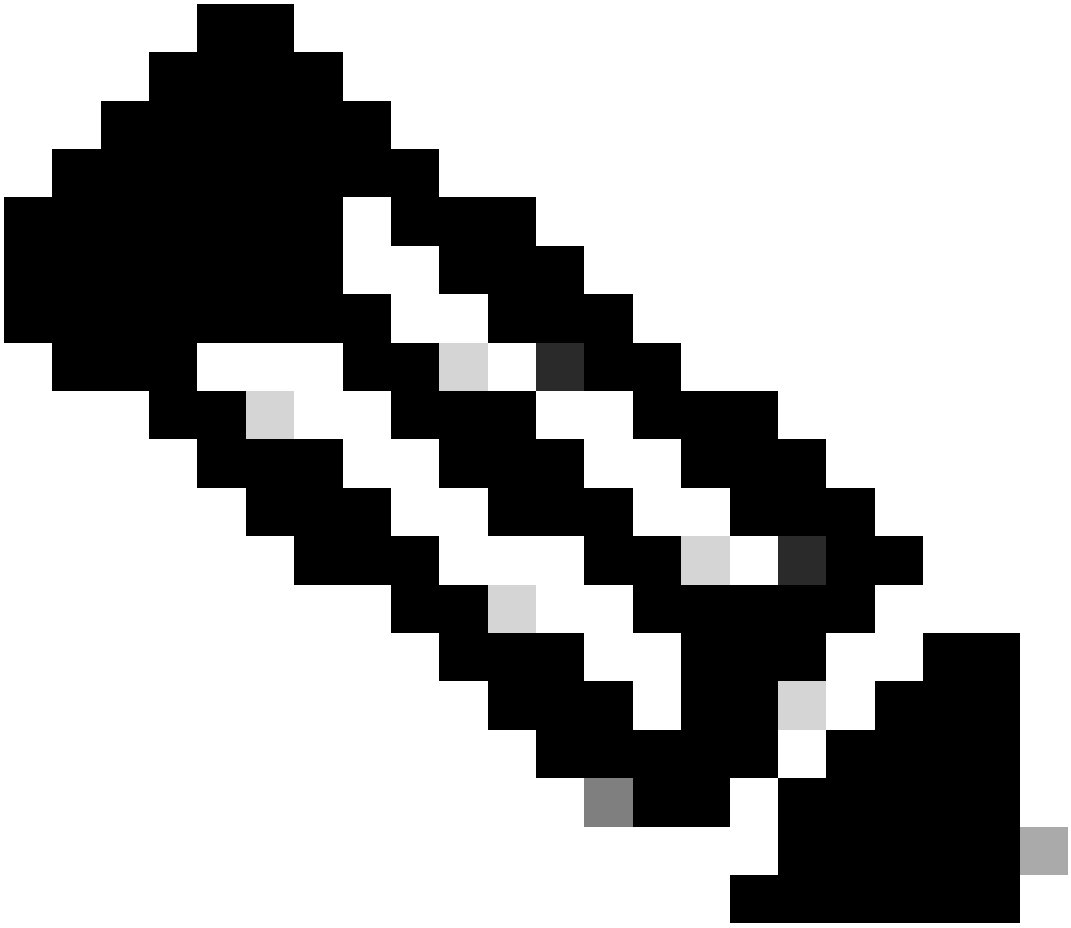
<#root>

```
asa#
dir

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

4.2. Verificare la presenza di file core ASA usando il 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: Sull'appliance ASA virtuale, la funzione coredump è disabilitata per impostazione predefinita:

<#root>

ciscoasa#

show coredump

filesystem 'disk0:' has no coredump filesystem

Per abilitare la funzione coredump, consultare la sezione coredump enable nella guida di riferimento dei comandi di Cisco Secure Firewall serie ASA, comandi A-H.

FTD

4.1. Verificare la presenza di un file crashinfo FTD. Per visualizzare le informazioni più recenti su crashinfo, eseguire il comando show crashinfo. I file crashinfo sono disponibili nell'output del comando dir.

```
<#root>

ftd#

dir


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

crashinfo_lina.14664.20250813.205102
```

Su FTD, i file crashinfo si trovano nella directory /mnt/disk0/expert mode:

```
<#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
```

Nel file di risoluzione dei problemi FTD, i file crashinfo si trovano in 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. Verificare la presenza di file di base FTD. Su FTD, i file core sono accessibili nelle directory expert mode /ngfw/var/data/cores/ e /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
```

Nel file di risoluzione dei problemi FTD i nomi dei file principali si trovano nel file command-outputs/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
```

Dump coredump specifico di FTD Snort3

Questa sezione è applicabile solo all'FTD su cui è in esecuzione il motore Snort3.

4.1. Verificare la presenza di Snort3 engine crashinfo file snort3-crashinfo.* si trovano nella directory /ngfw/var/log/crashinfo/expert mode.

<#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
```

Nel file di risoluzione dei problemi FTD, gli stessi file si trovano in dir-archives/var-log/crashinfo/.

4.2. Verificare la presenza di file Snort3 minidump minidump_* in /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
```

Nel file di risoluzione dei problemi FTD i file di minidump sono in 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
```

Moduli di sicurezza Firepower 4100 e 9300

Questa sezione è applicabile solo ai moduli Firepower 4100 e 9300.

4.1. Verificare la presenza di crashinfo e dei file di 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. Sugli chassis Firepower 1000, 2100 e Secure Firewall 1200, 3100 e 4200, verificare la presenza di file di base utilizzando i comandi dir workspace:/core e dir workspace:/cores_fxos nella shell local-mgmt.

Se è installata l'applicazione ASA, connettersi alla shell FXOS utilizzando il 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
```

I file principali sono menzionati anche in /opt/cisco/platform/logs/prune_cores.log nel file di risoluzione dei problemi dello chassis:

```
<#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. Sugli chassis Firepower 4100 e 9300, verificare la presenza di file core utilizzando i comandi dir workspace:/core nella shell local-mgmt:

```
<#root>

firewall(local-mgmt)#

dir workspace:/cores


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

I nomi dei file principali si trovano all'interno del file di risoluzione dei problemi dello chassis, negli

output del comando show cores nel file *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, dove * è la parte del nome del file di risoluzione dei problemi, ad esempio, 20250311123356_FW_BC1_all.tar.

5. Verificare se i file crashinfo, coredump e minidump sono rilevanti per l'incidente.

- Confrontare i timestamp del file con il timestamp dell'incidente o.
- Convertire il timestamp dell'epoca dal nome del file alla data utilizzando il comando data di Linux.

Per i file core e minidump, i timestamp epoch possono essere convertiti in data e ora usando la data su qualsiasi 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.

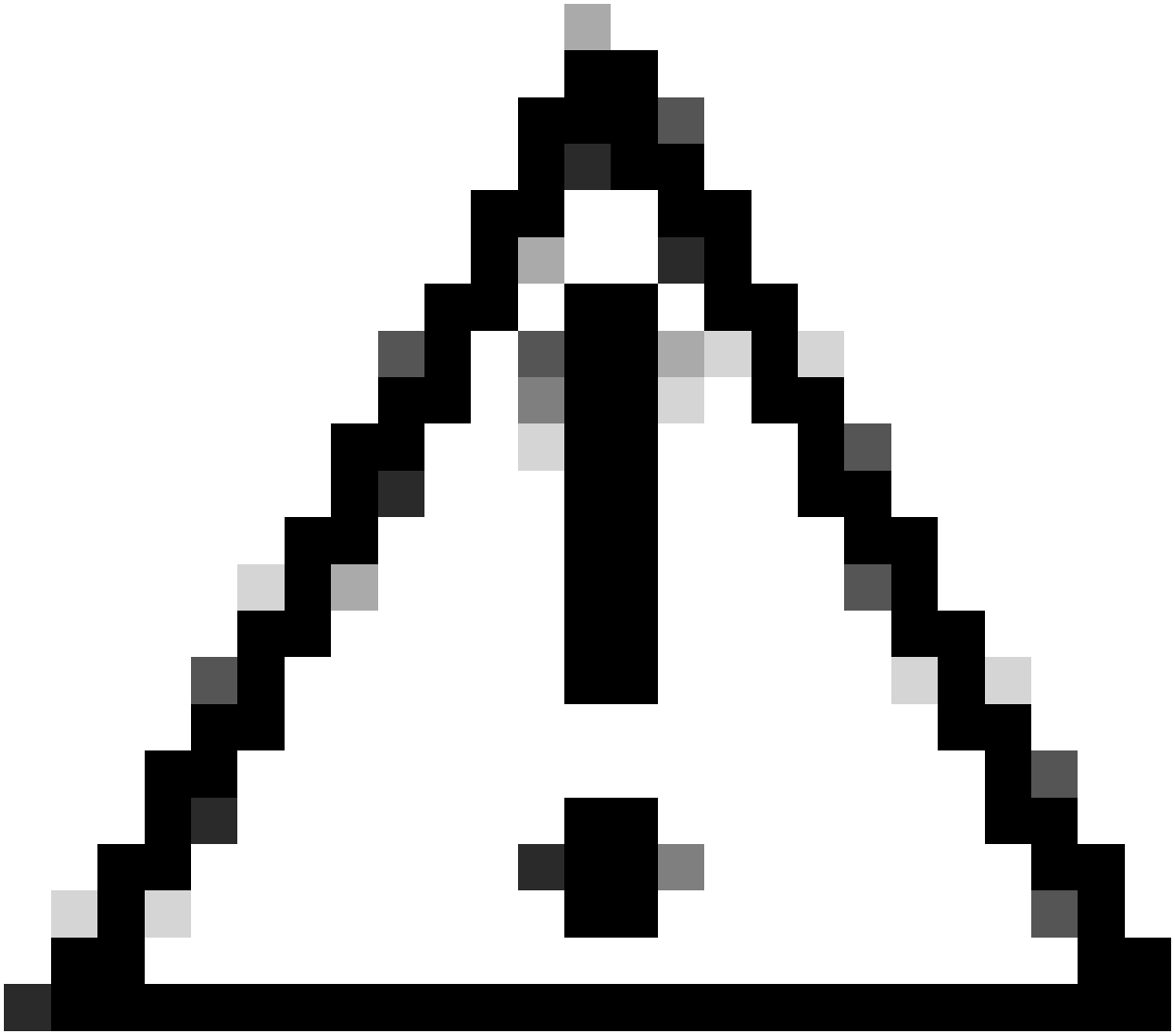
gz

linux $

date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025

6. Fare riferimento alla sezione How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall? per scaricare i file crashinfo, minidump e core dai punti 4-5.



Attenzione: Non rinominare i file core, crashinfo o minidump.

7. Procedere con i passaggi in Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower per raccogliere i file show-tech e risolvere i problemi:

7 bis. File ASA show-tech.

7 ter. File di risoluzione dei problemi FTD.

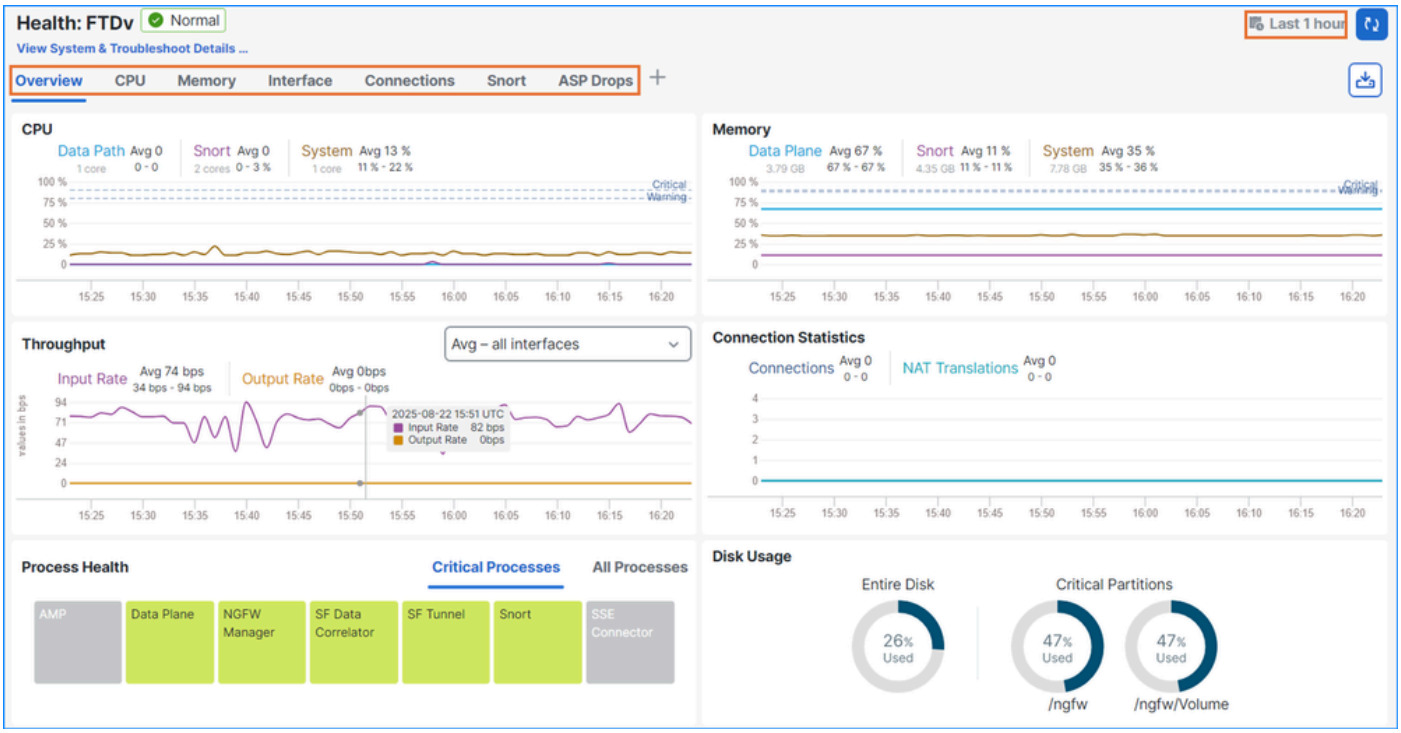
7 quater. Firepower 4100 e 9300 modulo di sicurezza show-tech file.

7 quinquies. File show-tech dello chassis Firepower 4100 e 9300.

7 sexies. Firepower 1000, 2100 e file show-tech Secure Firewall 1200, 3100 e 4200. I file di risoluzione dei problemi dello chassis per Secure Firewall 3100, 4200 in modalità contenitore possono essere scaricati dal FMC > Dispositivi > [chassis] > 3 punti > opzione Risoluzione dei problemi dei file.

8. Nel caso di FTD, raccogliere gli screenshot delle schede di monitoraggio dello stato su FMC che coprono almeno 30 minuti prima del traceback. Assicurarsi di includere gli screenshot di tutte le schede evidenziate. In caso di traceback ricorrente, raccogliere gli screenshot che coprono alcuni incidenti.

Inoltre, in caso di elevata disponibilità e clustering, raccogliere gli screenshot per tutte le unità interessate:



9. Raccogliere messaggi syslog del motore Lina raw (non analizzati) dai server syslog relativi ad almeno 30 minuti prima del traceback. Il formato raw è essenziale per l'elaborazione interna da parte di TAC e strumenti di ingegneria.

In caso di traceback ricorrente, raccogliere i messaggi non elaborati che coprono alcuni incidenti. Inoltre, in caso di elevata disponibilità e clustering, raccogliere i syslog non elaborati da tutte le unità interessate.

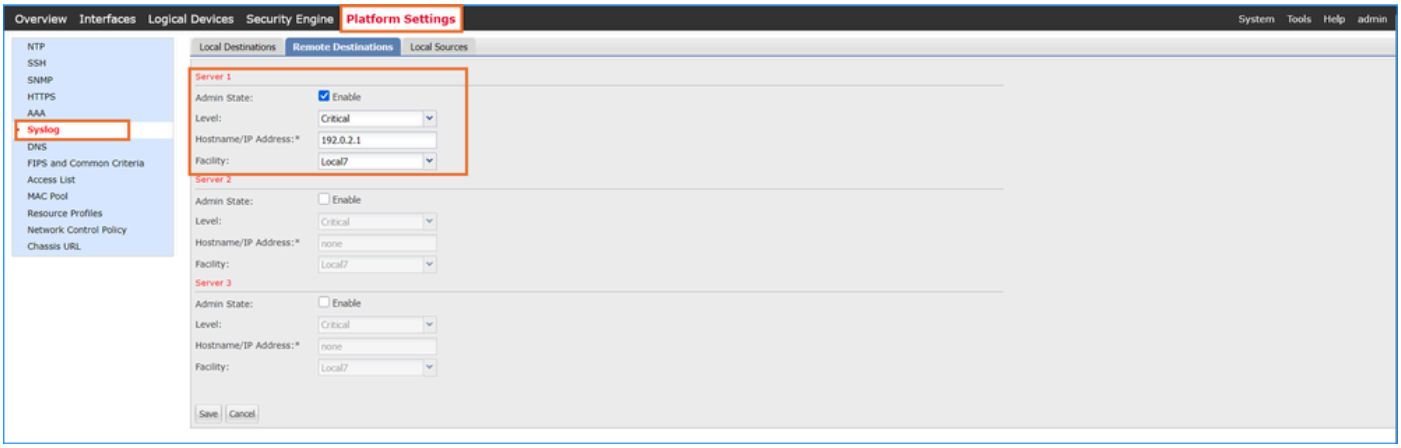
Verifica sulla CLI ASA/FTD:

```
<#root>

ftd#

show run logging


logging enable
logging trap informational
logging host inside

192.0.2.1

<-- syslog server address
```

10. Nel caso di Firepower 4100 e 9300, raccogliere messaggi FXOS non analizzati dai server syslog almeno 10 minuti prima del traceback. Il formato raw è essenziale per l'elaborazione interna da parte di TAC e strumenti di ingegneria.

Inoltre, in caso di elevata disponibilità e clustering, raccogliere i syslog raw da tutti gli chassis interessati.

Verifica dell'interfaccia utente di Firepower Chassis Manager (FCM):



Verifica nella CLI di 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. Raccogliere CPU, memoria e dati di interfaccia ASA o FTD, incluse le trap, dai server SNMP configurati. Accertarsi di includere i dati relativi ad almeno 30 minuti prima del traceback.

In caso di traceback ricorrente, raccogliere i messaggi non elaborati che coprono alcuni incidenti. Inoltre, in caso di elevata disponibilità e clustering, raccogliere messaggi raw da tutti gli chassis interessati.

Verifica sulla CLI ASA/FTD:

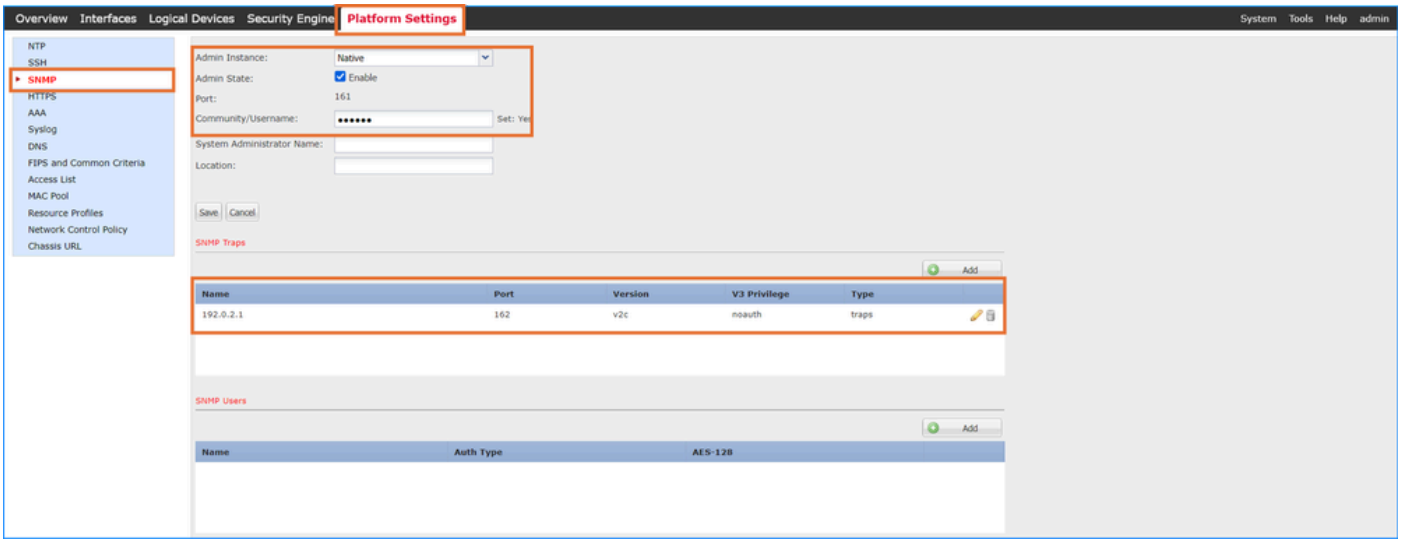
<#root>

```
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. Nel caso di Firepower 4100 e 9300, raccogliere CPU, memoria, dati di interfaccia, incluse le trap, dai server SNMP configurati. Accertarsi di includere i dati relativi ad almeno 30 minuti prima del traceback.

In caso di traceback ricorrente, raccogliere i messaggi non elaborati che coprono alcuni incidenti. Inoltre, in caso di elevata disponibilità e clustering, raccogliere messaggi raw da tutti gli chassis interessati.

Verifica nell'interfaccia utente di FCM:



Verifica nella CLI di 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. Raccogliere il profilo di traffico dagli agenti di raccolta Netflow. Accertarsi di includere i dati relativi ad almeno 30 minuti prima del traceback.

In caso di ricalco ricorrente, raccogliere i dati relativi a pochi incidenti. Inoltre, in caso di elevata disponibilità e clustering, raccogliere i dati da tutti gli chassis interessati.

Verifica sulla CLI ASA/FTD:

<#root>

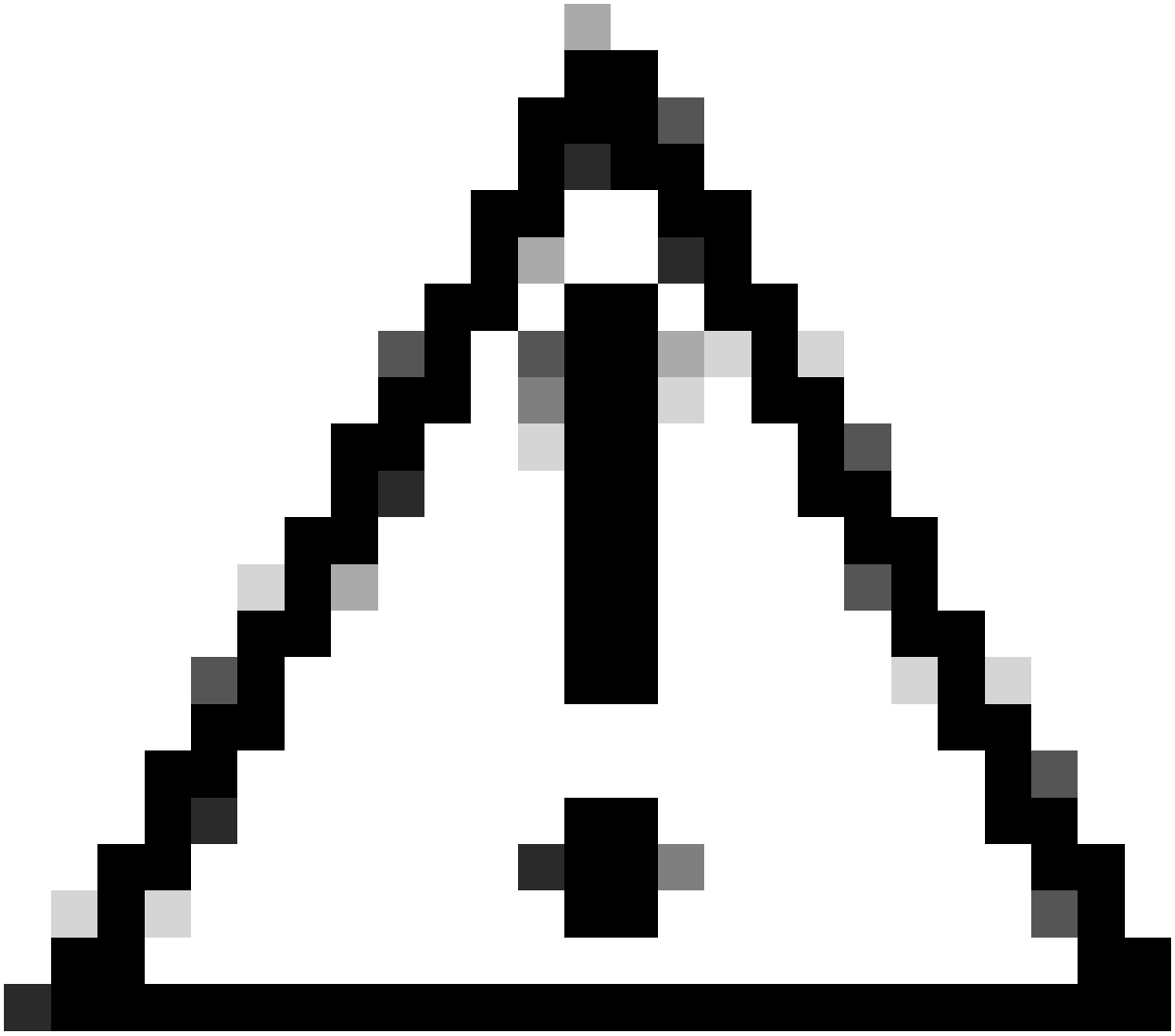
```
ftd#
show run flow-export


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. In caso di traceback ricorrente, raccogliere l'output delle sessioni console.

15. Aprire una richiesta TAC e fornire tutti i dati.

Come raccogliere i file Crashinfo, Coredump e Minidump da Secure Firewall?

Procedere come segue: crashinfo, coredump e minidump Files from Secure Firewall:



Attenzione: Avviso: Non rinominare i file core, crashinfo o minidump.

ASA

Caricare i file dalla CLI di ASA sul server 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

Opzione 1 - Raccolta dei file tramite la CLI di Lina

1. Se il server remoto è raggiungibile dal motore Lina, copiare i file in /mnt/disk0 e caricare i file dalla CLI di 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. Quando i file dal server remoto vengono scaricati, assicurarsi di eliminare i file copiati da /mnt/disk0/ su FTD:

<#root>

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

cd /mnt/disk0/

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

sudo rm core.lina.11.13050.1755081050.gz

Opzione 2 - Raccolta dei file tramite la CLI in modalità Expert

Utilizzando i client Linux TFTP, SFTP o SCTP, caricare i file dalla modalità Expert al server 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
```

Opzione 3 - Raccolta dei file tramite la CLI di gestione locale di FXOS

Su FTD in modalità nativa in esecuzione su chassis Firepower 1000, 2100 e Secure Firewall 1200, 3100 e 4200, i file core e minidump possono essere raccolti dalla CLI di gestione locale di 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
```

Opzione 4 - Raccolta dei file tramite l'interfaccia utente di FMC

Copiare i file in /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/

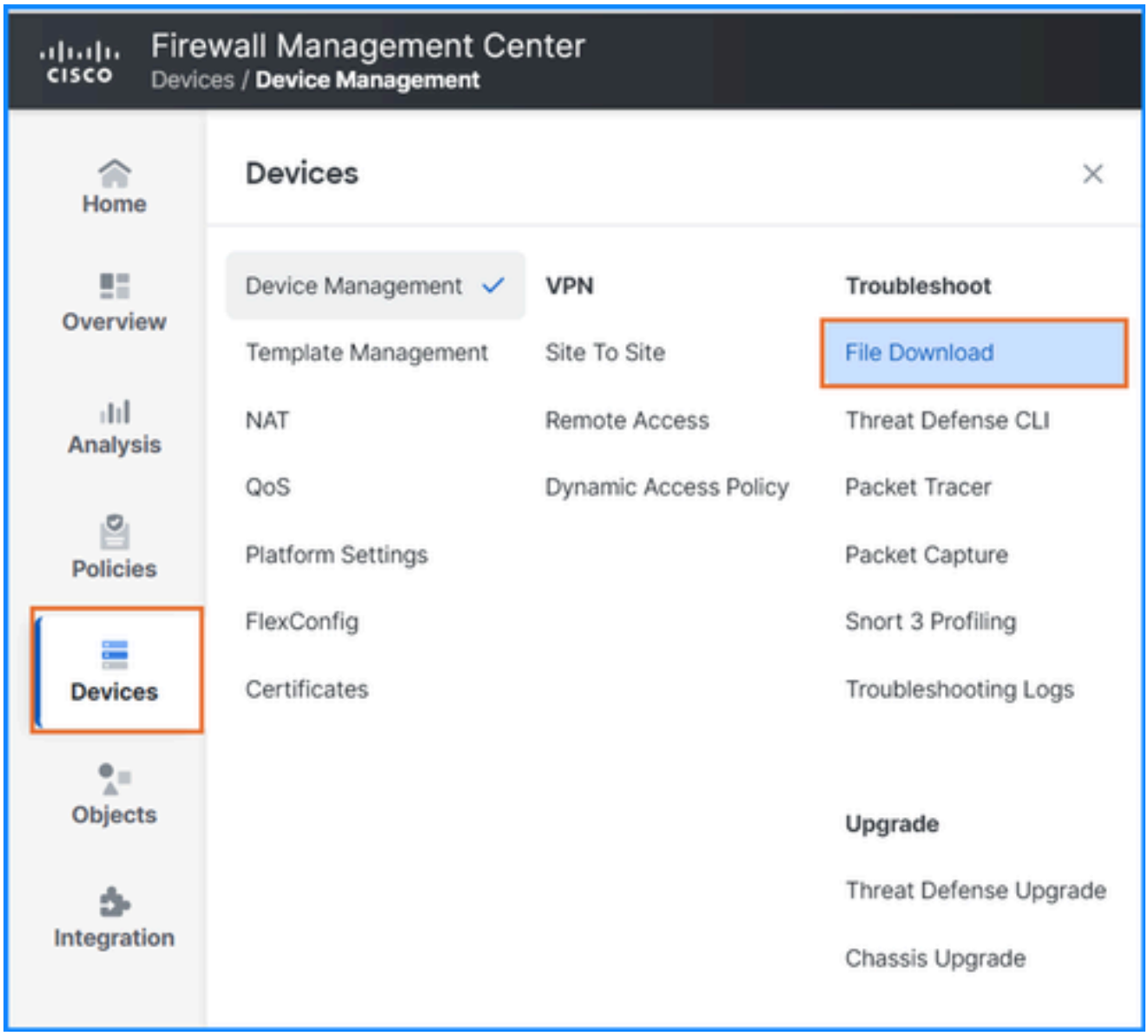
admin@firepower:~$

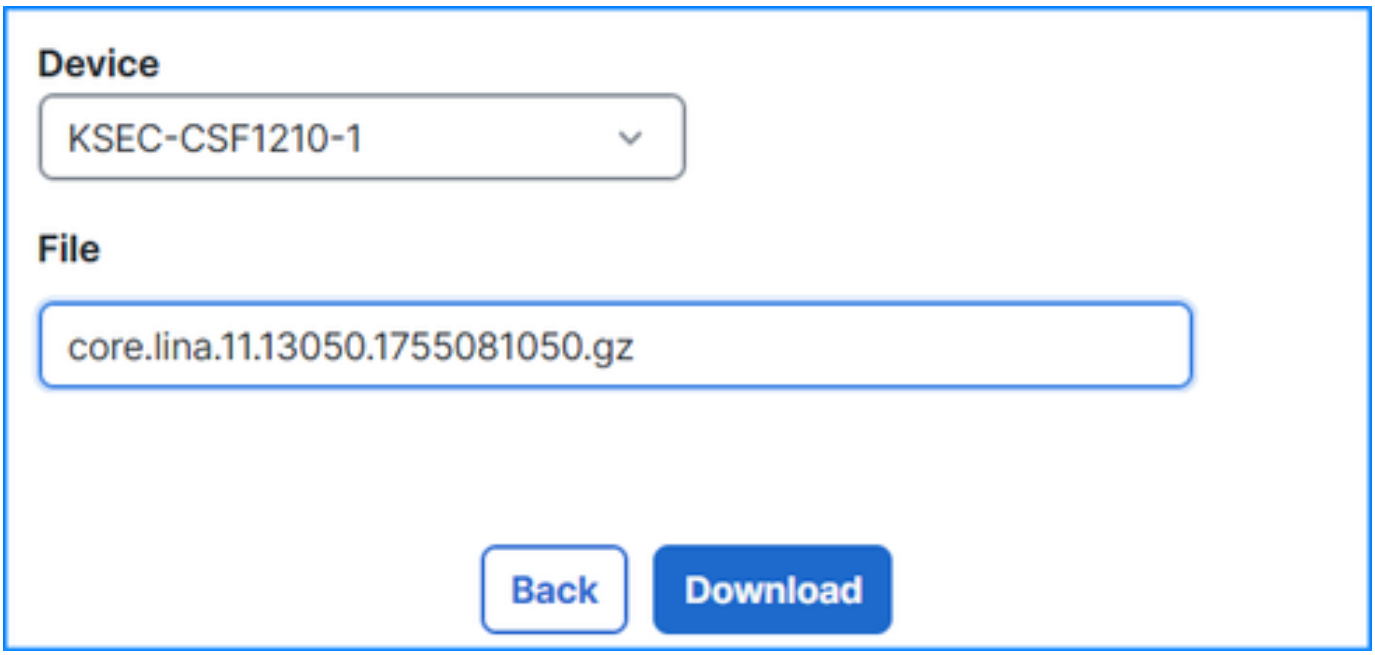
ls -l /ngfw/var/common/

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

core.lina.11.13050.1755081050.gz

2. Scaricare il file dall'interfaccia utente di FMC utilizzando l'opzione Dispositivi > Download file:





3. Quando i file dal server remoto vengono scaricati, assicurarsi di eliminare i file copiati da

/ngfw/var/common/ su FTD:

<#root>

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

cd

/ngfw/var/common/

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

sudo rm core.lina.11.13050.1755081050.gz

Moduli di sicurezza Firepower 4100 e 9300

1. Collegarsi al modulo e raccogliere i file core e crashinfo come parte del modulo show-tech file:

<#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

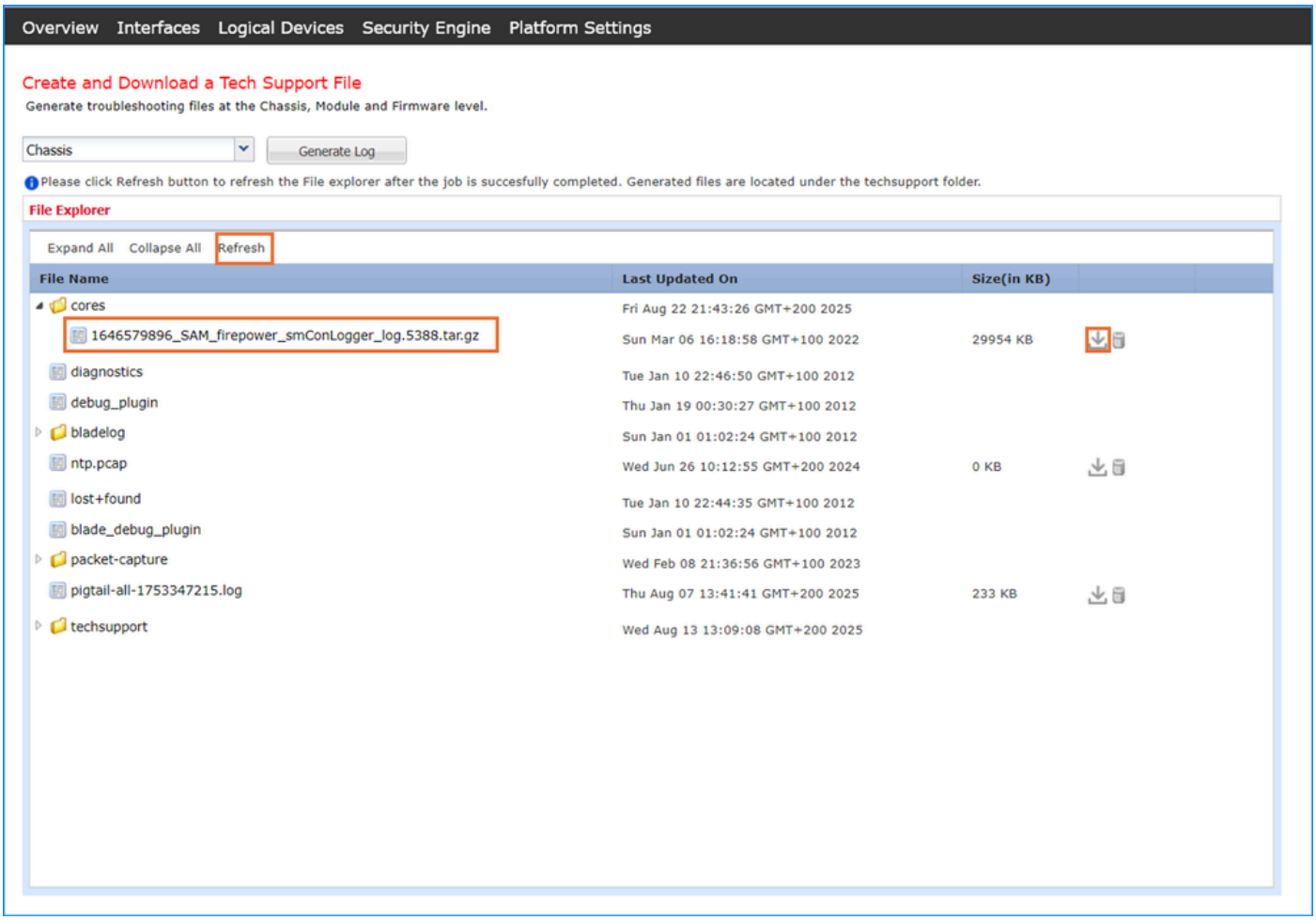
Chassis Firepower 4100 e 9300

1. Raccogliere i file di base utilizzando la CLI di gestione locale di 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. In alternativa, raccogliere i file dall'interfaccia utente di FCM tramite Strumenti > Log per la risoluzione dei problemi. Fare clic su Refresh (Aggiorna) per aggiornare la visualizzazione della directory dei file e l'icona di download accanto al file principale:



Riferimenti

- Verifica delle versioni del software Firepower
- Verifica della configurazione di Firepower, istanza, disponibilità e scalabilità
- Risoluzione dei problemi relativi alle procedure di generazione dei file di Firepower
- Guida di riferimento ai comandi ASA

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).