Gegevens verzamelen voor analyse van de hoofdoorzaak van softwaretraceback/crash in beveiligde firewall

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrond

gegevensverzameling

Hoe Crashinfo, Coredump en Minidump bestanden te verzamelen van Secure Firewall?

- ASA
- FTD
- Firepower 4100- en 9300-beveiligingsmodules
- Firepower 4100- en 9300-chassis

Referenties

Inleiding

In dit document worden de stappen beschreven voor het verzamelen van gegevens in het geval van een softwaretraceback.

Voorwaarden

Vereisten

Basisproductkennis.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Beveiligde firewall 1200, 3100, 4200
- Vuurkracht 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) 9.22.2.9

Achtergrond

FTD- of ASA-software kan traceren en meestal opnieuw laden om verschillende redenen, zoals:

- Softwarefouten, waaronder de defecten in het besturingssysteem en onderdelen van derden.
- Uitzonderingen op hardware, zoals geheugenfouten op laag niveau of CPU-fouten.
- In sommige gevallen vanwege een gebrek aan systeembronnen, zoals geheugen.
- Handmatig geactiveerd door de gebruiker voor diagnostische doeleinden onder TAC-toezicht:

```
<#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
```

In het geval van een traceback ook wel bekend als de crash, afhankelijk van het proces, meestal een crashinfo, core of minidump bestanden worden gegenereerd:

- CrashInfo bevat minimale diagnostische gegevens uit het procesgeheugen.
- Het kernbestand is een volledige dump van het procesgeheugen ten tijde van de traceback.
- minidump-bestand is specifiek voor Snort3 en bevat diagnostische gegevens uit het procesgeheugen.

In de Secure Firewall-software kan het proces dat een traceback heeft gehad in een van de volgende onderdelen worden uitgevoerd:

- Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200 chassis.

- Firepower 4100, 9300 beveiligingsmodules.

Afgezien van kern- en crashinfo-bestanden, vereist de root cause analysis (RCA) van een traceback aanvullende informatie, zoals het oplossen van problemen en show-tech-bestanden, syslog-berichten enzovoort.

Core- en crashfinfo-bestandsanalyse worden afgehandeld door TAC en Cisco als onderdeel van een serviceverzoek (case).

gegevensverzameling

Ga door met deze stappen om de benodigde gegevens te verzamelen voor de RCA van de traceback. Vanwege het risico van gegevensverlies als gevolg van rotatie van bestanden, verzoeken wij u de gevraagde gegevens zo snel mogelijk te verstrekken.

1. Deze objecten verduidelijken:

1 bis. Exacte hardware.

1 ter. Softwareversie.

1 quater. Type beveiligde firewallsoftware (ASA of FTD).

1d. Implementatiemodus (native of multi-instance modus).

Raadpleeg Versies van Firepower-software controleren en Firepower, instantie, beschikbaarheid, schaalbaarheid controleren voor gedetailleerde verificatiestappen.

2. Verduidelijken of er recente milieuveranderingen zijn opgetreden, zoals:

2 bis. Toevoeging van verkeer.

2 ter. Belangrijke configuratiewijzigingen, waaronder opdrachten.

Zorg ervoor dat u de tijdstempels en de tijdzone zo nauwkeurig mogelijk opneemt.

3. Als de traceback is opgetreden na configuratiewijzigingen met behulp van specifieke opdrachten, verzamelt u de uitvoer van de terminalsessie. Als opdrachtautorisatie is geconfigureerd op de ASA, verzamelt u opdrachtautorisatierapporten van de externe server, zoals de Identity Services Engine (ISE).

4. Controleer in de volgende stappen de crashinfo-, kern- of minidump-bestanden met de meest recente tijdstempels en noteer het volledige pad naar elk bestand. De volledige paden zijn nodig voor het verzamelen van de bestanden, zoals weergegeven in de sectie Hoe Crashinfo, Coredump en Minidump-bestanden van Secure Firewall te verzamelen?.

ASA

4.1. Controleer of er een crashinfo-bestand aanwezig is. Om de nieuwste crashinfo te bekijken, voert u de opdracht show crashinfo uit. De crashinfo bestanden zijn te vinden in de uitvoer van de

dir opdracht.

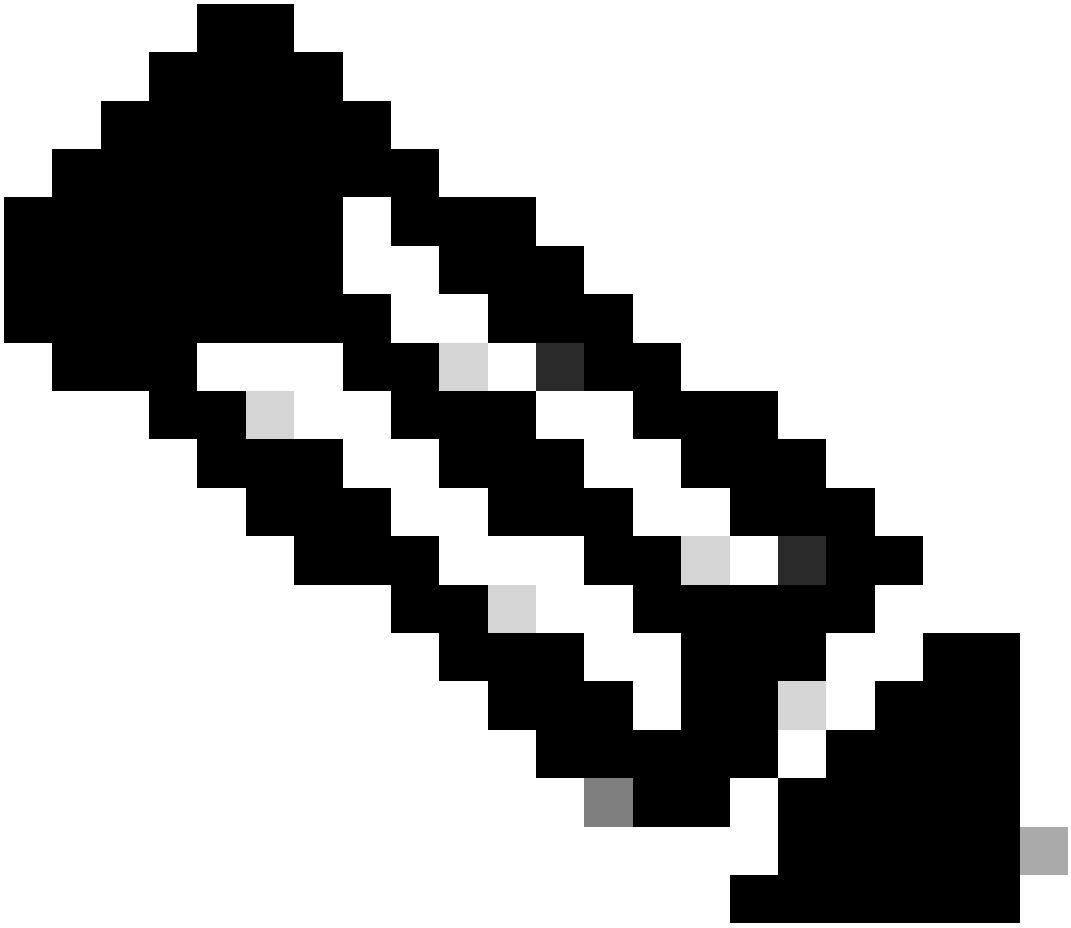
<#root>

```
asa#
dir

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

4.2. Controleer de aanwezigheid van ASA-kernbestanden met behulp van de opdracht 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
```



Opmerking: Bij virtueel ASA is de coredump-functie standaard uitgeschakeld:

<#root>

```
ciscoasa#
show coredump


filesystem 'disk0:' has no coredump filesystem
```

Als u de coredump-functie wilt inschakelen, raadpleegt u het gedeelte coredump inschakelen in de opdrachtverwijzing voor de Cisco Secure Firewall ASA Series, A-H-opdrachten.

FTD

4.1. Controleer of er een FTD-crashinfobestand aanwezig is. Om de nieuwste crashinfo te bekijken, voert u de opdracht show crashinfo uit. De crashinfo bestanden zijn te vinden in de uitvoer van de dir opdracht.

```
<#root>

ftd#

dir


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

crashinfo_lina.14664.20250813.205102
```

Op FTD zijn de crashinfo bestanden te vinden in de expert mode /mnt/disk0/ directory:

```
<#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
```

In het FTD-probleemoplossingsbestand bevinden de crashinfobestanden zich in dir-archieven/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. De aanwezigheid van FTD-kernbestanden verifiëren. Op FTD zijn de kernbestanden toegankelijk in de expert-modus /ngfw/var/data/cores/ en /ngfw/var/common/directory's:

<#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
```

In het FTD-probleemoplossingsbestand staan de kernbestandsnamen in het bestand 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
```

FTD Snort3-specifieke coredump

Dit gedeelte is alleen van toepassing op FTD met de Snort3-engine.

4.1. Controleer de aanwezigheid van Snort3 motor crashinfo bestanden snort3-crashinfo.* zijn in de expert mode /ngfw/var/log/crashinfo/ directory.

<#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
```

In het FTD-probleemoplossingsbestand bevinden dezelfde bestanden zich in dir-archieven/var-log/crashinfo/.

4.2. Controleer de aanwezigheid van Snort3-minidump-bestanden _* 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
```

In het FTD-probleemoplossingsbestand bevinden de minidump-bestanden zich in bestandsinhoud/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
```

Firepower 4100- en 9300-beveiligingsmodules

Deze sectie is alleen van toepassing op Firepower 4100- en 9300-modules.

4.1. Controleer de aanwezigheid van crashinfo en kernbestanden:

<#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. Controleer op het Firepower 1000-, 2100- en Secure Firewall 1200-, 3100- en 4200-chassis de aanwezigheid van kernbestanden met behulp van de dir-werkruimte:/cores en dir-werkruimte:/cores_fxos-opdrachten in de shell voor lokale beheer.

Als de ASA-toepassing is geïnstalleerd, maakt u verbinding met de FXOS-shell met de opdracht 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
```

De kernbestanden worden ook vermeld in / opt/cisco/platform/logs/prune_cores.log-bestanden in het probleemoplossingsbestand voor het 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. Controleer op het Firepower 4100- en 9300-chassis de aanwezigheid van kernbestanden met behulp van de opdrachten dir workspace:/cores in de local-mgmt-shell:

<#root>

```
firewall(local-mgmt)#

dir workspace:/cores


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

De kernbestandsnamen zijn te vinden in het bestand voor probleemoplossing van het chassis, in de uitgangen van de opdracht kernen weergeven in bestand *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, waarbij * het onderdeel is van de bestandsnaam voor probleemoplossing, bijvoorbeeld 20250311123356_ FW_BC1_all.tar.

5. Controleer of de crashinfo-, coredump- en minidump-bestanden relevant zijn voor het incident.

- Vergelijk de tijdstempels van het bestand met de tijdstempel van het incident, of..
- Converteer de tijdstempel van de bestandsnaam naar datum met de Linux-datum opdracht.

Voor kern- en minidump-bestanden kunnen de tijdstempels van het tijdperk worden geconverteerd naar datumtijd met behulp van de datum op elke Linux-host:

<#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.

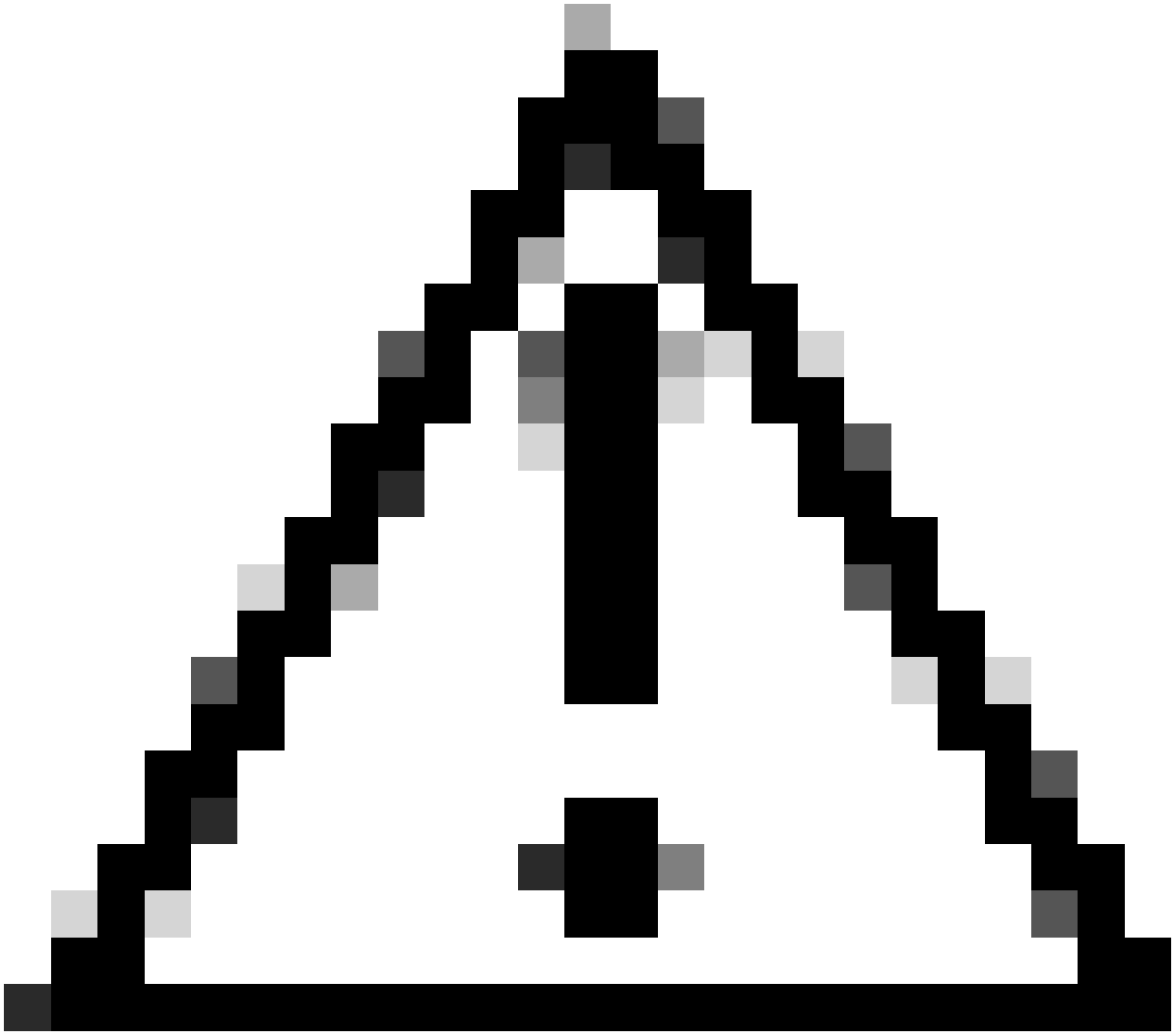
```
gz
```

```
linux $
```

date -d @1753342057

```
Thu Jul 24 07:27:37 UTC 2025
```

6. Raadpleeg de sectie Hoe Crashinfo-, Coredump- en Minidump-bestanden van Secure Firewall te verzamelen? om de crashinfo-, minidump- en kernbestanden van stap 4-5 te downloaden.



Let op: geef de naam van de kern-, crashinfo- of minidump-bestanden geen nieuwe waarde.

---

7. Ga verder met stappen in Problemen oplossen met Firepower File Generation Procedures om showtech-bestanden te verzamelen en problemen op te lossen:

7 bis. ASA show-tech bestand.

7 ter. FTD-probleemoplossingsbestand.

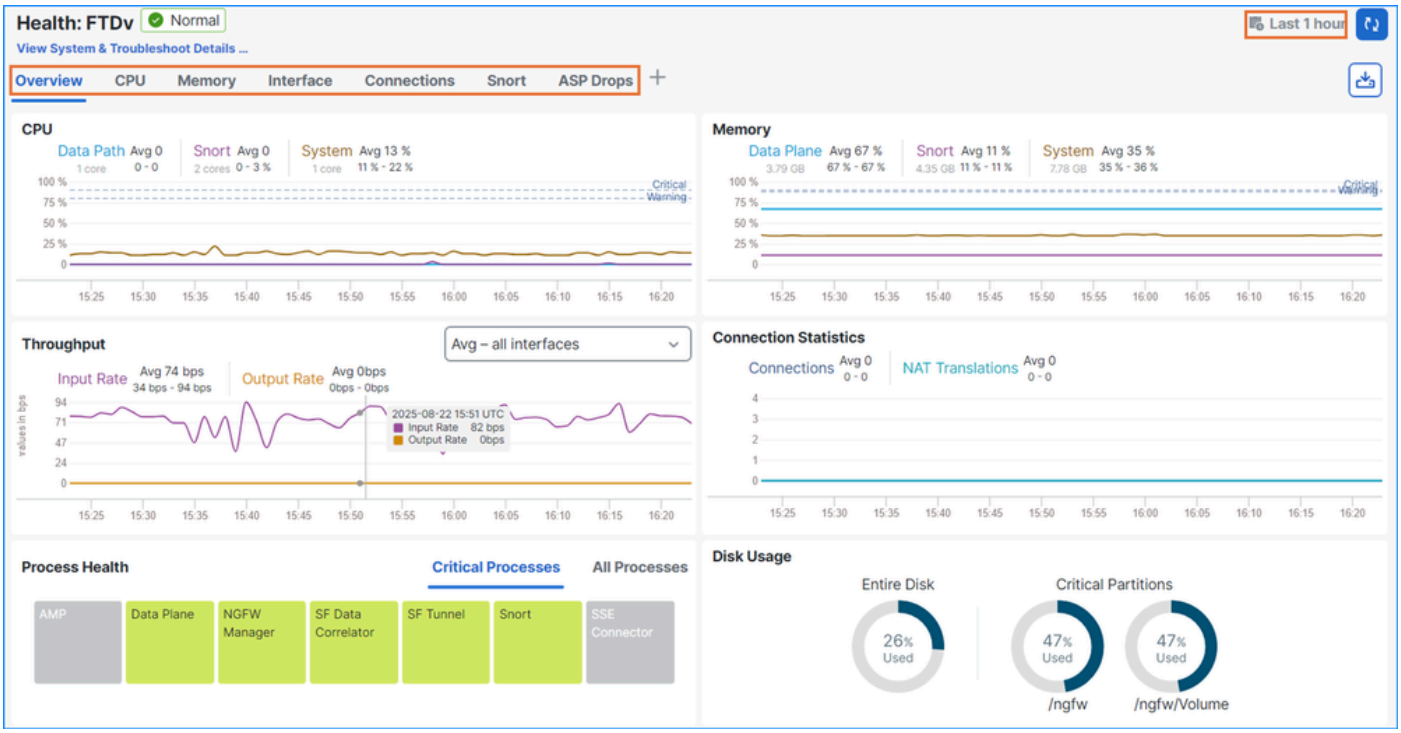
7 quater. Firepower 4100- en 9300-beveiligingsmodule tonen technisch bestand.

7d. Firepower 4100- en 9300-chassis tonen technisch bestand.

7 sexies. Firepower 1000, 2100 en Secure Firewall 1200, 3100, 4200 chassis tonen technisch bestand. Chassisproblemen oplossen Bestanden voor Secure Firewall 3100, 4200 in containermodus kunnen worden gedownload via de optie FMC > Apparaten > [chassis] > 3 punten > Bestanden oplossen.

8. Verzamel in het geval van FTD screenshots van de tabbladen voor gezondheidsmonitoring van het VCC die ten minste 30 minuten vóór de traceback bestrijken. Zorg ervoor dat u de schermafbeeldingen van alle gemarkeerde tabbladen opneemt. In het geval van terugkerende traceback, verzamelen screenshots die een paar incidenten.

Bovendien, in het geval van hoge beschikbaarheid en clustering, verzamel screenshots voor alle getroffen eenheden:



9. Verzamel onbewerkte (ongeparseerde) syslog-berichten van de Lina-engine van syslog-servers die ten minste 30 minuten voor de traceback bestrijken. Het ruwe formaat is essentieel voor de interne verwerking door TAC en technische hulpmiddelen.

In het geval van terugkerende traceback, verzamelen de ruwe berichten die een paar incidenten. Bovendien, in het geval van hoge beschikbaarheid en clustering, verzamel ruwe syslogs van alle getroffen eenheden.

Verificatie op de ASA/FTD CLI:

<#root>

```
ftd#
```

show run logging

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

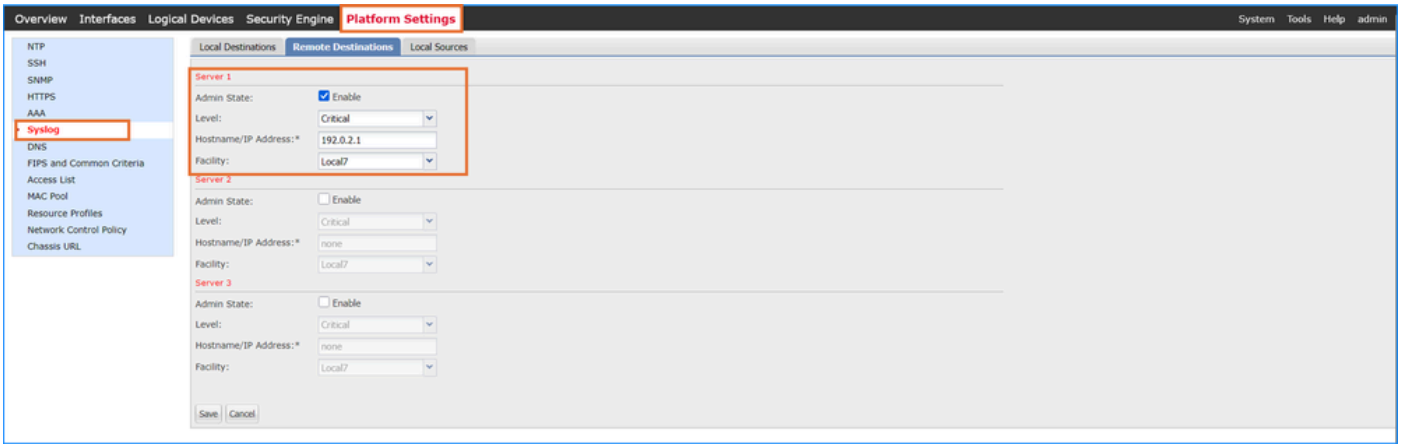
192.0.2.1

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

10. In het geval van Firepower 4100 en 9300, verzamel onbewerkte (ongeparseerde) FXOS-berichten van syslog-servers ten minste 10 minuten vóór de traceback. Het ruwe formaat is essentieel voor de interne verwerking door TAC en technische hulpmiddelen.

In het geval van hoge beschikbaarheid en clustering kunt u bovendien ruwe syslogs van alle getroffen chassis verzamelen.

Verificatie via de gebruikersinterface van Firepower Chassis Manager (FCM):



Verificatie op de FXOS CLI:

<#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. Verzamel ASA- of FTD-CPU-, geheugen- en interfacegegevens, inclusief traps, van de geconfigureerde SNMP-servers. Zorg ervoor dat u gegevens opneemt die ten minste 30 minuten voor de traceback bestrijken.

In het geval van terugkerende traceback, verzamelen de ruwe berichten die een paar incidenten. In het geval van hoge beschikbaarheid en clustering, verzamelt u bovendien onbewerkte berichten van alle getroffen chassis.

Verificatie op de ASA/FTD CLI:

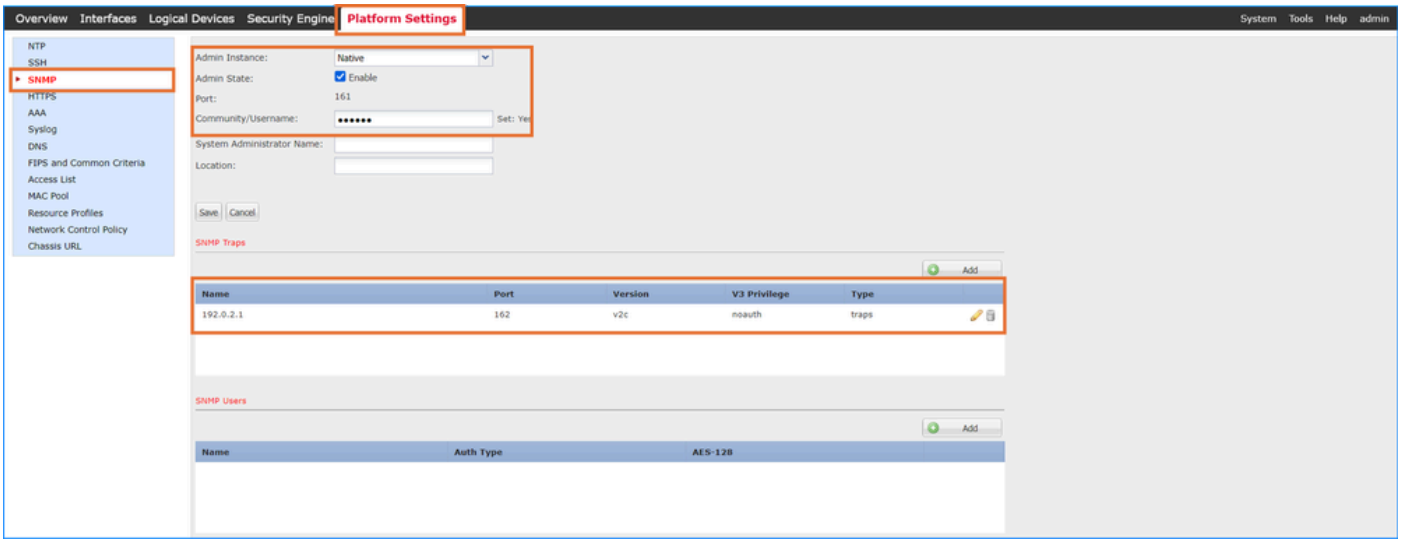
<#root>

```
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. Verzamel in het geval van Firepower 4100 en 9300 CPU-, geheugen- en interfacegegevens, inclusief traps, van de geconfigureerde SNMP-servers. Zorg ervoor dat u gegevens opneemt die ten minste 30 minuten voor de traceback bestrijken.

In het geval van terugkerende traceback, verzamelen de ruwe berichten die een paar incidenten. In het geval van hoge beschikbaarheid en clustering, verzamelt u bovendien onbewerkte berichten van alle getroffen chassis.

Verificatie op de FCM UI:



Verificatie op de FXOS CLI:

<#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. Verzamel het verkeersprofiel van de Netflow-collectors. Zorg ervoor dat u gegevens opneemt die ten minste 30 minuten voor de traceback bestrijken.

In het geval van terugkerende traceback, verzamel gegevens over een paar incidenten. In het geval van hoge beschikbaarheid en clustering verzamelen we bovendien gegevens van alle betrokken chassis.

Verificatie op de ASA/FTD CLI:

<#root>

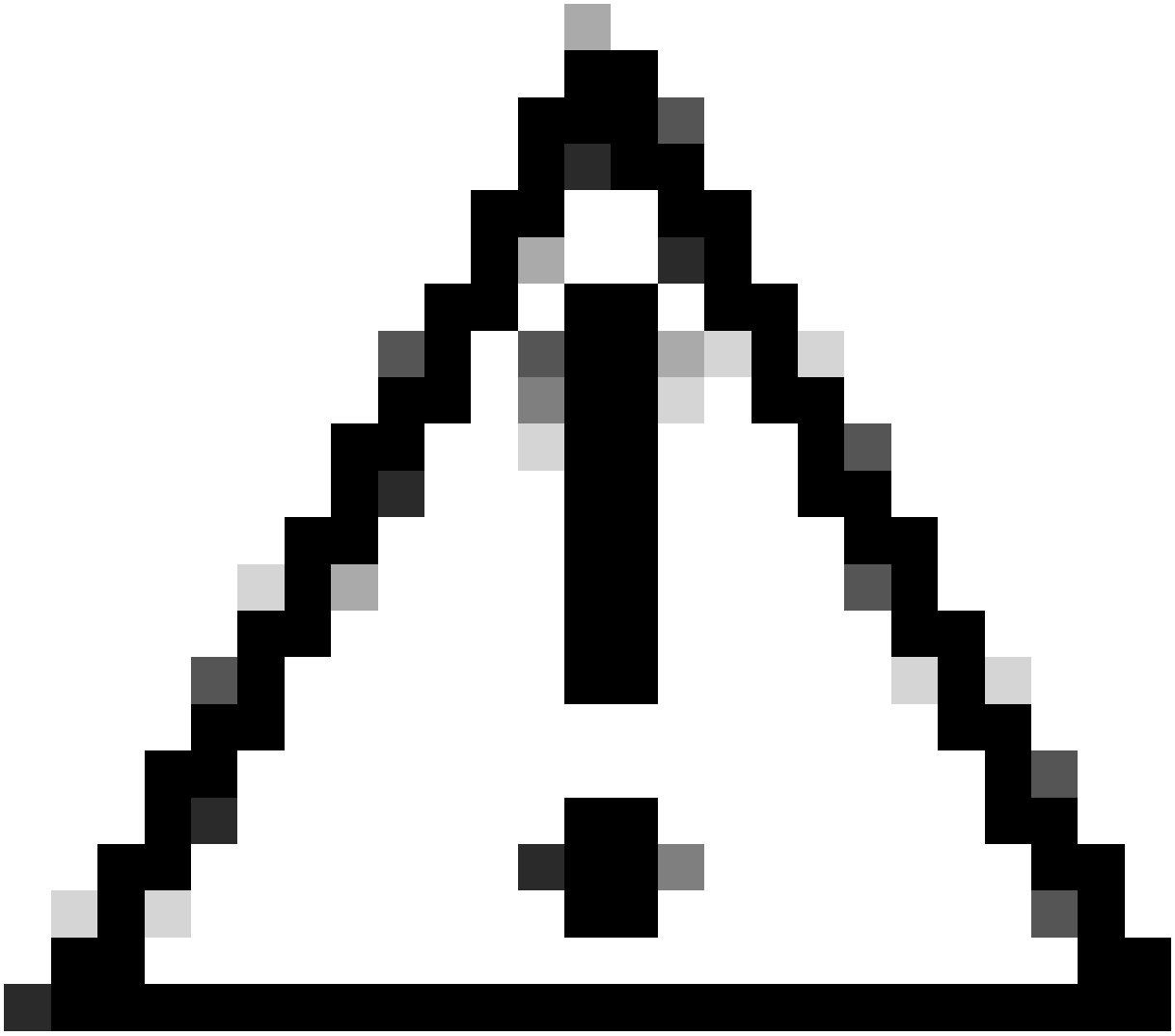
```
ftd#
show run flow-export


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. Verzamel in het geval van terugkerende traceback de uitvoer van de consolesessies.

15. Open een TAC-zaak en verstrek alle gegevens.

Hoe Crashinfo, Coredump en Minidump bestanden te verzamelen van Secure Firewall?

Ga verder met deze stappen crashinfo, coredump en minidump Bestanden van Secure Firewall:



Let op: Waarschuwing: de naam van de kern-, crashinfo- of minidump-bestanden mag niet worden gewijzigd.

ASA

Upload bestanden van de ASA CLI naar de externe server:

<#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

Optie 1 – Bestanden verzamelen met behulp van de Lina CLI

1. Als de externe server bereikbaar is vanuit de Lina-engine, kopieert u bestanden naar /mnt/disk0 en uploadt u bestanden vanuit de Lina CLI:

```
<#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. Wanneer de bestanden van de externe server worden gedownload, moet u ervoor zorgen dat de gekopieerde bestanden van /mnt/disk0/ op FTD worden verwijderd:

<#root>

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

cd /mnt/disk0/

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

sudo rm core.lina.11.13050.1755081050.gz

Optie 2 – Bestanden verzamelen met behulp van de Expert-modus CLI

Met behulp van Linux TFTP-, SFTP- of SCTP-clients kunt u de bestanden vanuit de expertmodus uploaden naar de externe server:

<#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
```

Optie 3 – Bestanden verzamelen met de CLI voor lokaal beheer van FXOS

In de standaard FTD-modus die wordt uitgevoerd op het Firepower 1000-, 2100- en Secure Firewall 1200-, 3100- en 4200-chassis, kunnen de kern- en minidump-bestanden worden verzameld via de CLI voor lokale beheer van 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
```

Optie 4 – Bestanden verzamelen met de FMC-gebruikersinterface

Bestanden kopiëren naar /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/

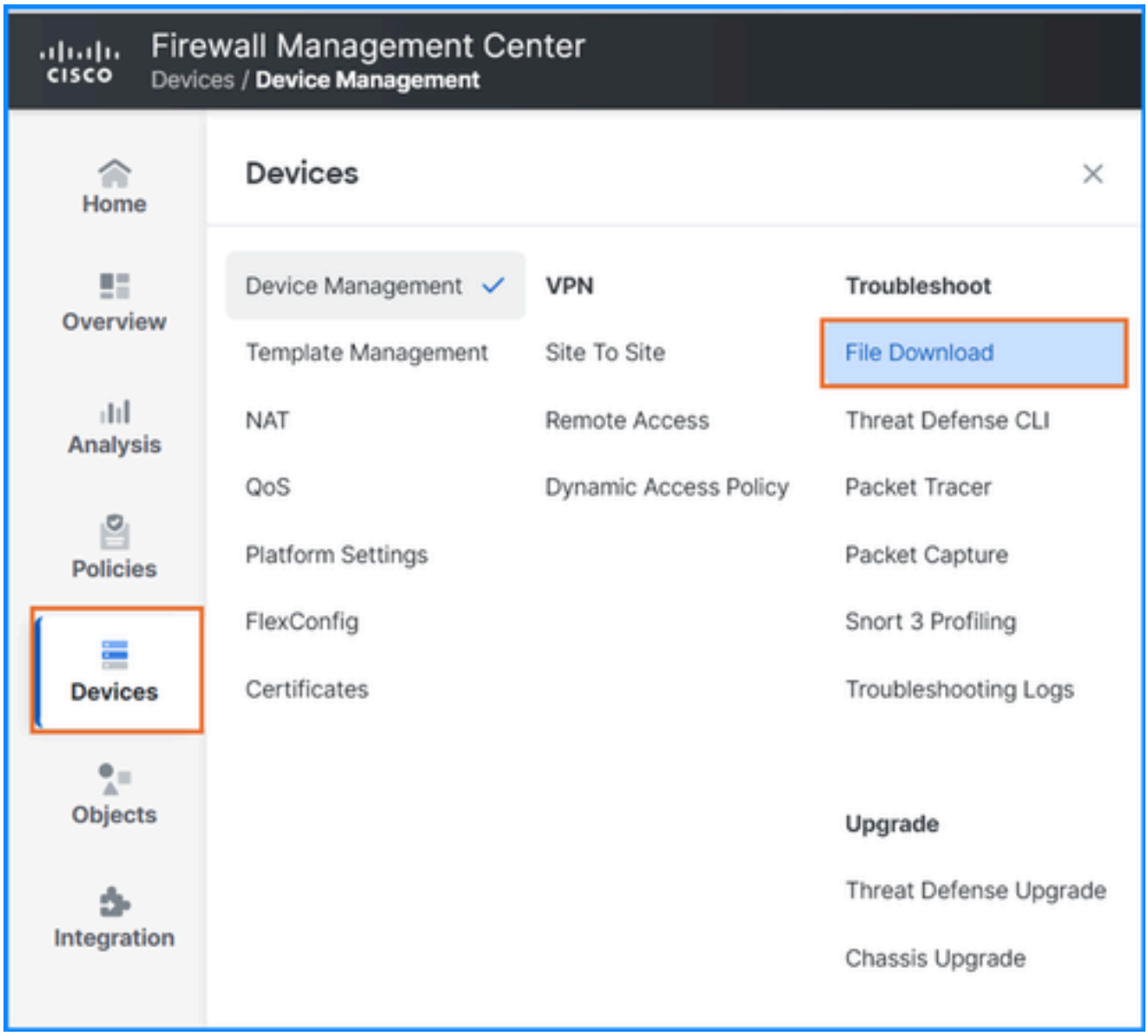
admin@firepower:~$

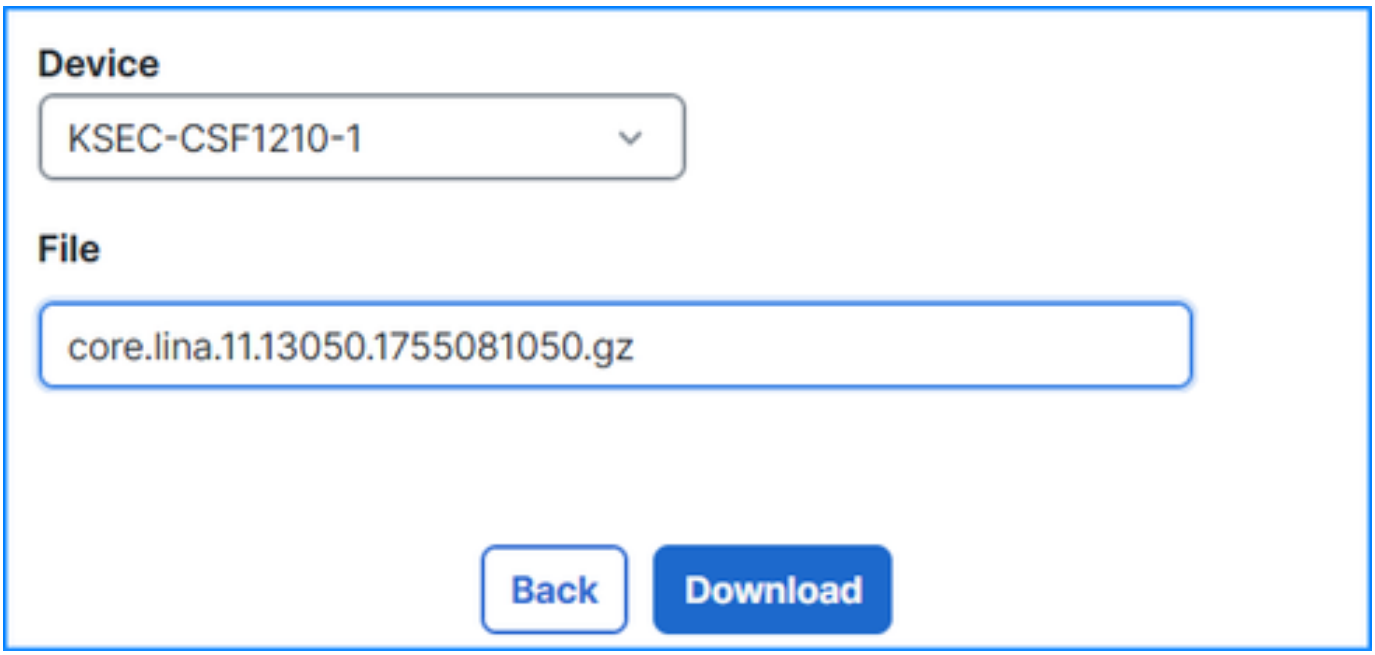
ls -l /ngfw/var/common/

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

core.lina.11.13050.1755081050.gz

2. Download het bestand van de FMC UI met de optie Apparaten > Bestand downloaden:





3. Wanneer de bestanden van de externe server worden gedownload, moet u ervoor zorgen dat

de gekopieerde bestanden worden verwijderd uit /ngfw/var/common/ op FTD:

<#root>

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

cd

/ngfw/var/common/

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

sudo rm core.lina.11.13050.1755081050.gz

Firepower 4100- en 9300-beveiligingsmodules

1. Maak verbinding met de module en verzamel de kern- en crashinfo-bestanden als onderdeel van het show-tech-bestand van de 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

Firepower 4100- en 9300-chassis

1. Verzamel kernbestanden met de CLI voor lokaal beheer van FXOS:

<#root>

```
firepower#
```

connect local-mgmt

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

dir workspace:/cores

```
1 30673335 Mar 06 16:18:58 2022
```

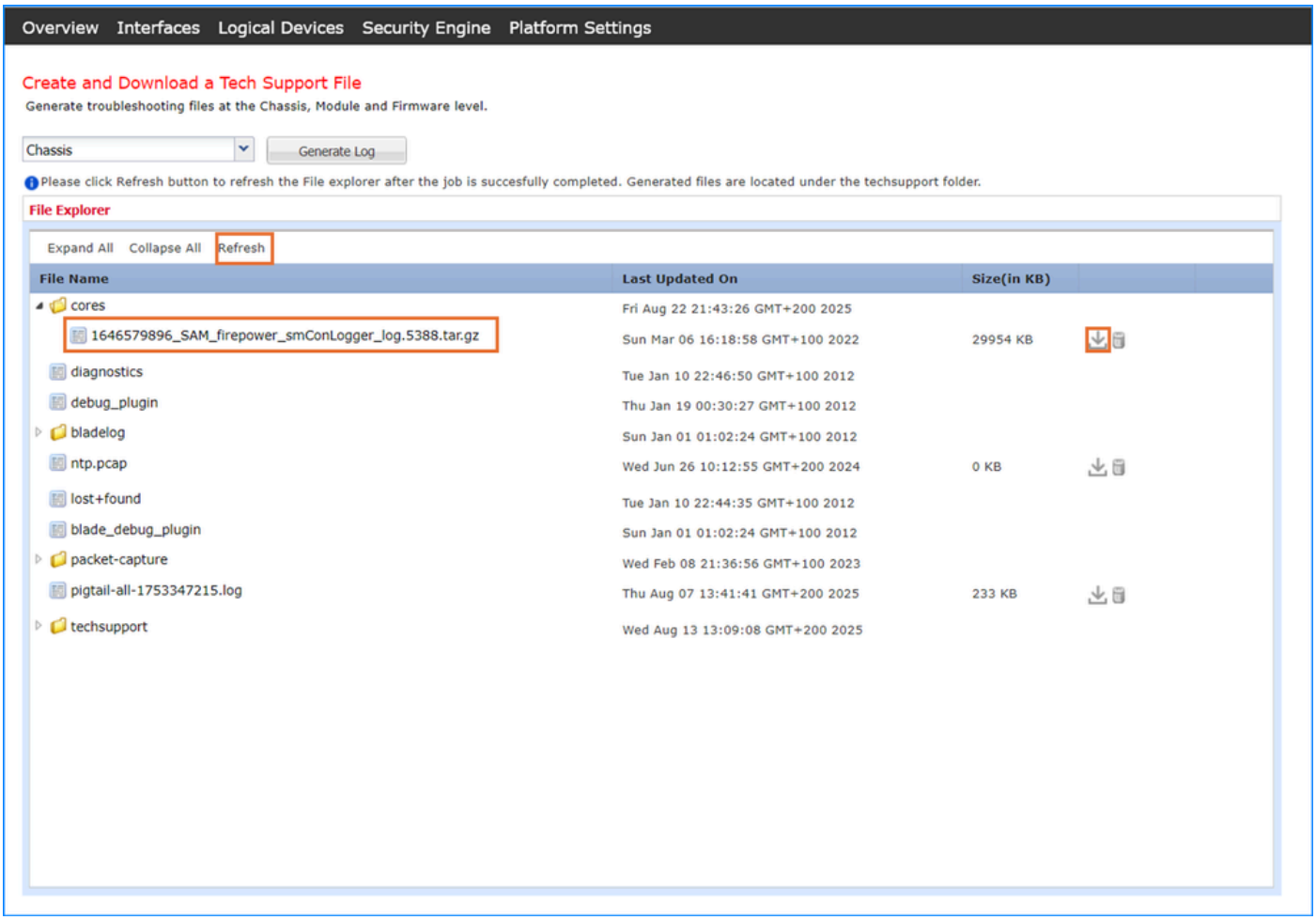
1646579896_SAM_firepower-1_smConLogger_log.5388.tar.gz

```
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. U kunt ook bestanden van de FCM UI verzamelen via Tools > Logboeken voor probleemoplossing. Klik op Vernieuwen om de bestandsmapweergave en het downloadpictogram naast het kernbestand bij te werken:



Referenties

- Versies van Firepower-software controleren
- Controleer Firepower, instantie, beschikbaarheid, schaalbaarheid en configuratie
- Problemen oplossen bij procedures voor het genereren van Firepower-bestanden
- ASA-opdrachtverwijzing

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.