Sammeln von Daten zur Ursachenanalyse von Software-Traceback/Absturz in einer sicheren Firewall

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Sammeln von Daten bei einem Software-Traceback beschrieben.

Voraussetzungen

Anforderungen

Grundlegendes Produktwissen.

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Sichere 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) 9.22.2.9

Hintergrund

FTD- oder ASA-Software kann zurückverfolgt werden und wird in der Regel aus verschiedenen Gründen neu geladen, z. B.:

- Software-Fehler, einschließlich der Fehler im Betriebssystem und Komponenten von Drittanbietern.
- Hardwareausnahmen, z. B. Fehler beim Arbeitsspeicher oder bei der CPU.
- In einigen Fällen aufgrund fehlender Systemressourcen, z. B. Arbeitsspeicher.
- Manuelle Auslösung durch den Benutzer zu Diagnosezwecken unter TAC-Aufsicht:

```
<#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
```

Bei einem Traceback, der je nach Prozess auch als Crash bezeichnet wird, werden in der Regel Crashfo-, Core- oder Minidump-Dateien generiert:

- crashinfo enthält minimale Diagnosedaten aus dem Prozessspeicher.
- core file ist ein vollständiges Dump des Prozessspeichers zum Zeitpunkt des Tracebacks.
- minidump-Datei ist spezifisch für Snort3 und enthält Diagnosedaten aus dem Prozessspeicher.

In der Secure Firewall-Software kann der Prozess, für den ein Traceback durchgeführt wurde, in

einer der folgenden Komponenten liegen:

- FirePOWER 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200-Chassis
- Sicherheitsmodule FirePOWER 4100 und 9300

Abgesehen von Core- und Crashfo-Dateien erfordert die Ursachenanalyse (RCA) eines Tracebacks zusätzliche Informationen, wie z. B. Fehlerbehebung und Show-Tech-Dateien, Syslog-Meldungen usw.

Die Core- und Crashfinfo-Dateianalyse wird von TAC und Cisco im Rahmen einer Serviceanfrage (Case) durchgeführt.

Datensammlung

Fahren Sie mit diesen Schritten fort, um die erforderlichen Daten für die RCA des Tracebacks zu sammeln. Aufgrund des Risikos von Datenverlusten aufgrund von Dateirotierungen, geben Sie die angeforderten Daten bitte so schnell wie möglich an.

1. Folgende Punkte sollten geklärt werden:

1a) Exakte Hardware.

1b) Software-Version.

1c) Typ der sicheren Firewall-Software (ASA oder FTD).

1d) Bereitstellungsmodus (nativer oder Multi-Instanzmodus).

Detaillierte Verifizierungsschritte finden Sie unter Verifizieren der Firepower-Softwareversionen und Verifizieren der Firepower, Instanz, Verfügbarkeit und Skalierbarkeitskonfiguration.

2. Klärung, ob es in letzter Zeit Umweltveränderungen gab, wie z. B.:

(2a) Hinzufügen von Datenverkehr.

2b) Wichtige Konfigurationsänderungen, einschließlich Befehle.

Achten Sie darauf, die Zeitstempel und die Zeitzone möglichst genau einzuschließen.

3. Wenn die Rückverfolgung nach Konfigurationsänderungen mithilfe bestimmter Befehle erfolgt ist, erfassen Sie Terminalsitzungsausgaben. Wenn die Befehlsautorisierung auf der ASA konfiguriert ist, sammeln Sie Berichte zur Befehlsautorisierung vom Remote-Server, z. B. von der Identity Services Engine (ISE).

4. In den nächsten Schritten stellen Sie sicher, dass die crashinfo-, core- oder minidump-Dateien mit den aktuellsten Zeitstempeln und nehmen Sie eine Notiz des vollständigen Pfads zu jeder Datei. Die vollständigen Pfade werden für die Sammlung der Dateien benötigt, wie im How to Collect Crashinfo, Coredump and Minidump Files from Secure Firewall (Wie sammle ich Crashinfo-, Coredump- und Minidump-Dateien von einer sicheren Firewall? Abschnitt.

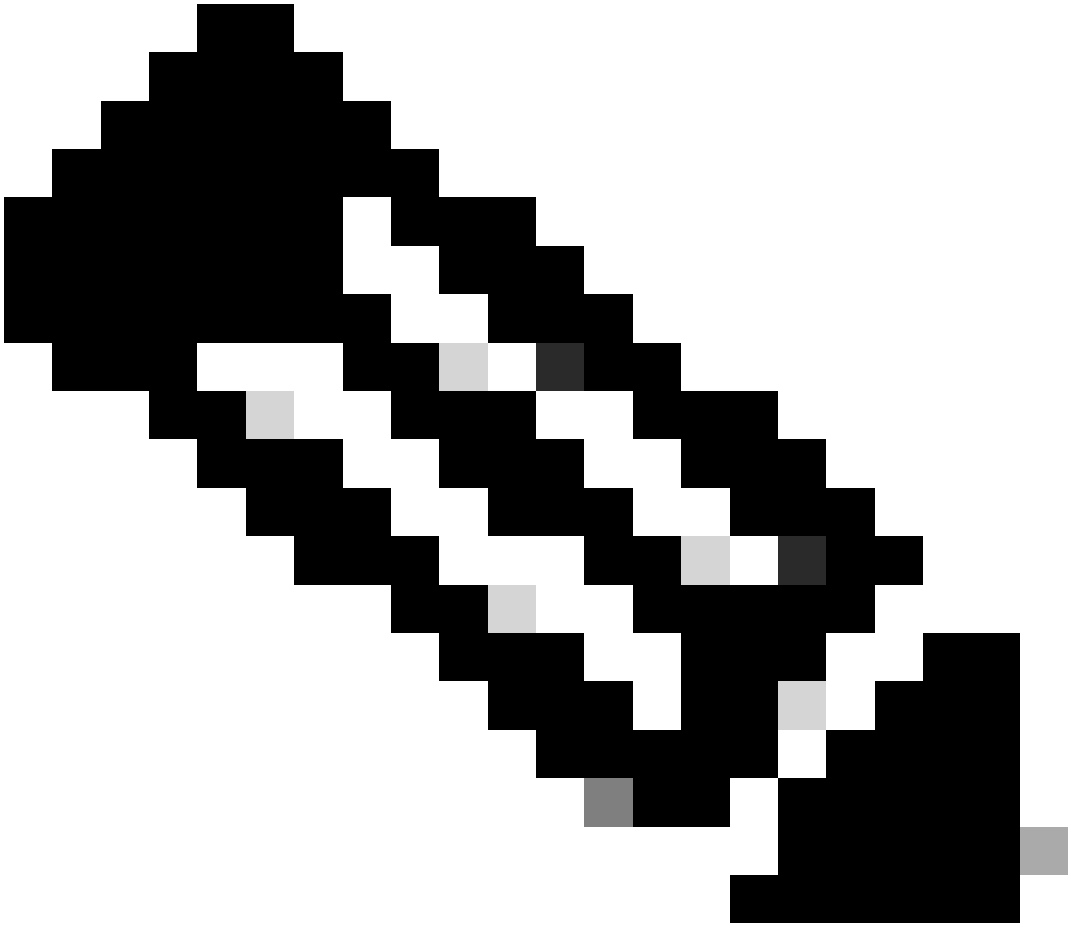
ASA

4.1. Überprüfen Sie, ob eine Crashinfo-Datei vorhanden ist. Führen Sie den Befehl show crashinfo aus, um das neueste Crashinfo anzuzeigen. Die crashinfo-Dateien finden Sie in der Ausgabe des Befehls dir.

```
<#root>

asa#

dir


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

crashinfo_lina.14664.20250813.205102
```

4.2. Überprüfen Sie mithilfe des Befehls dir coredumpfsys, ob ASA-Core-Dateien vorhanden sind:

```
<#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
```



Anmerkung: Auf virtueller ASA ist die Coredump-Funktion standardmäßig deaktiviert:

<#root>

```
ciscoasa#
show coredump


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

Informationen zum Aktivieren der Coredump-Funktion finden Sie im Abschnitt Coredump-Aktivierung in der Befehlsreferenz für die Cisco Secure Firewall ASA-Serie, A-H-Befehle.

FTD

4.1. Überprüfen Sie, ob eine FTD-Crashinfo-Datei vorhanden ist. Führen Sie den Befehl show crashinfo aus, um den neuesten Crashinfo anzuzeigen. Die crashinfo-Dateien finden Sie in der Ausgabe des Befehls dir.

```
<#root>

ftd#

dir


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

crashinfo_lina.14664.20250813.205102
```

Auf FTD befinden sich die Crashfo-Dateien im Verzeichnis 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
```

In der FTD-Fehlerbehebungsdatei befinden sich die crashinfo-Dateien 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. Überprüfen Sie, ob FTD-Kerndateien vorhanden sind. Auf FTD sind die Core-Dateien im Expert-Modus/ngfw/var/data/cores/ und/ngfw/var/common/Verzeichnisse zugänglich:

<#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 der FTD-Problembehebungsdatei befinden sich die Namen der Kerndateien in den Befehlsausgaben/für\ 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-spezifisches Core Dump

Dieser Abschnitt gilt nur für FTD mit der Snort3-Engine.

4.1. Überprüfen Sie, ob die Crashfo-Dateien der Snort3-Engine snort3-crashinfo.* sich im Verzeichnis expert mode/ngfw/var/log/crashinfo/ befinden.

<#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 der FTD-Fehlerbehebungsdatei befinden sich dieselben Dateien in dir-archives/var-log/crashinfo/.

4.2. Überprüfen Sie, ob die Snort3-Minidump-Dateien minidump_* in /ngfw/var/data/cores/ vorhanden sind:

<#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 der FTD-Fehlerbehebungsdatei befinden sich die Minidump-Dateien in file-content/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 und 9300 Sicherheitsmodule

Dieser Abschnitt gilt nur für Firepower 4100- und 9300-Module.

4.1. Überprüfen Sie, ob Crashfo- und Core-Dateien vorhanden sind:

<#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. Überprüfen Sie auf den Chassis Firepower 1000, 2100 und Secure Firewall 1200, 3100, 4200 mithilfe der Befehle dir workspace:/cores und dir workspace:/cores_fxos in der local-mgmt-Shell das Vorhandensein von Kerndateien.

Wenn die ASA-Anwendung installiert ist, stellen Sie mit dem Befehl connect fxos admin eine Verbindung zur FXOS-Shell her:

<#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
```

Die Core-Dateien werden auch in /opt/cisco/platform/logs/prune_cores.log-Dateien in der Chassis-Fehlerbehebungsdatei erwähnt:

```
<#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. Überprüfen Sie auf Firepower 4100- und 9300-Chassis mithilfe der Befehle dir workspace:/cores in der local-mgmt-Shell, ob Core-Dateien vorhanden sind:

```
<#root>

firewall(local-mgmt)#

dir workspace:/cores


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

Die Namen der Core-Dateien finden Sie in der Fehlerbehebungsdatei des Chassis, in den Ausgaben des Befehls show cores in der Datei *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, wobei * der Teil des Namens der Fehlerbehebungsdatei ist, z. B. 20250311123356_FW_BC1_all.tar.

5. Überprüfen Sie, ob die Crashfo-, Coredump- und Minidump-Dateien für den Vorfall relevant sind.

- Vergleichen Sie die Datei-Zeitstempel mit dem Zeitstempel des Vorfalls, oder..
- Konvertieren Sie den Zeitstempel der Epoche aus dem Dateinamen in das Datum, indem Sie den Linux-Befehl date verwenden.

Für Core- und Minidump-Dateien können die Epoch-Zeitstempel mit dem Datum auf jedem Linux-Host in Datums-Zeit umgewandelt werden:

<#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.

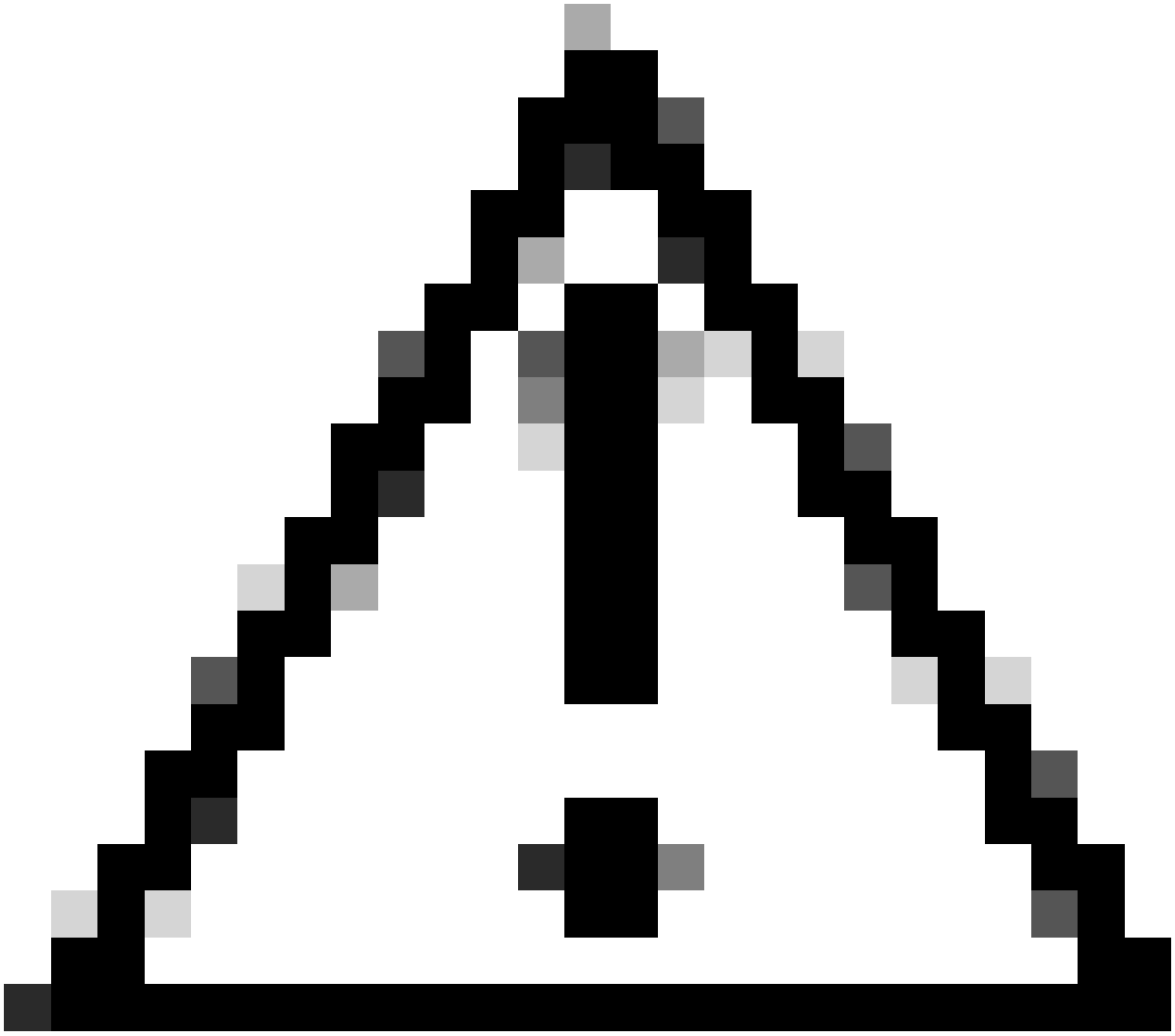
gz

linux $

date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025

6. Lesen Sie den Abschnitt Wie sammle ich Crashinfo-, Coredump- und Minidump-Dateien von der sicheren Firewall?, um die crashinfo-, minidump- und core-Dateien aus den Schritten 4-5 herunterzuladen.



Vorsicht: Benennen Sie keine Core-, Crashfo- oder Minidump-Dateien um.

---

7. Fahren Sie mit den Schritten in Fehlerbehebung für FirePOWER-Dateigenerierungsverfahren fort, um Dateien zu sammeln, die Show-Tech-Fehler aufweisen, und beheben Sie diese:

7a) ASA Show-Tech-Datei

7b) FTD-Fehlerbehebungsdatei

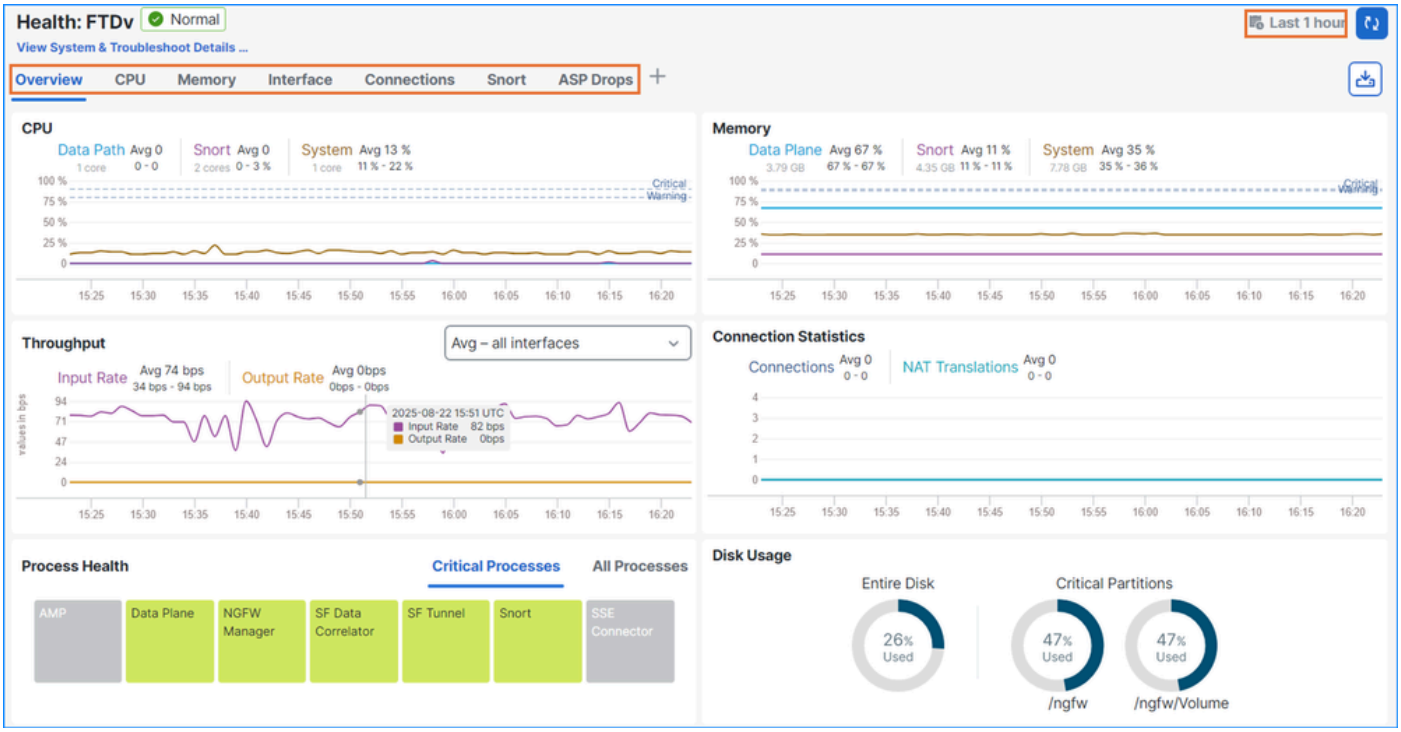
7c) Firepower 4100 und 9300 Sicherheitsmodul show-tech file.

7d) Show-Tech-Datei für Chassis für Firepower 4100 und 9300

7e. Show-Tech-Datei für Firepower 1000, 2100 und Secure Firewall 1200, 3100, 4200 Chassis. Dateien für die Chassis-Fehlerbehebung für Secure Firewall 3100, 4200 im Containermodus können über FMC > Devices > [Chassis] > 3 Dots > Troubleshoot Files Option heruntergeladen werden.

8. Im Fall von FTD sollten Sie Screenshots der Registerkarten für die Statusüberwachung auf dem FMC sammeln, die mindestens 30 Minuten vor der Rückverfolgung abdecken. Stellen Sie sicher, dass alle hervorgehobenen Registerkarten Screenshots enthalten sind. Im Fall einer wiederkehrenden Rückverfolgung sollten Sie Screenshots für einige Vorfälle sammeln.

Bei hoher Verfügbarkeit und Clustering Screenshots aller betroffenen Einheiten sammeln:



9. Sammeln Sie unformatierte Syslog-Meldungen der Lina-Engine von Syslog-Servern, die mindestens 30 Minuten vor dem Traceback eingehen. Das Rohformat ist für die interne Verarbeitung durch das TAC und technische Werkzeuge unerlässlich.

Sammeln Sie bei wiederkehrendem Traceback die Rohmeldungen zu einigen Vorfällen. Bei hoher Verfügbarkeit und Clustering zudem die Rohsyslogs aller betroffenen Einheiten.

Verifizierung auf der ASA/FTD CLI:

<#root>

```
ftd#
```

show run logging

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

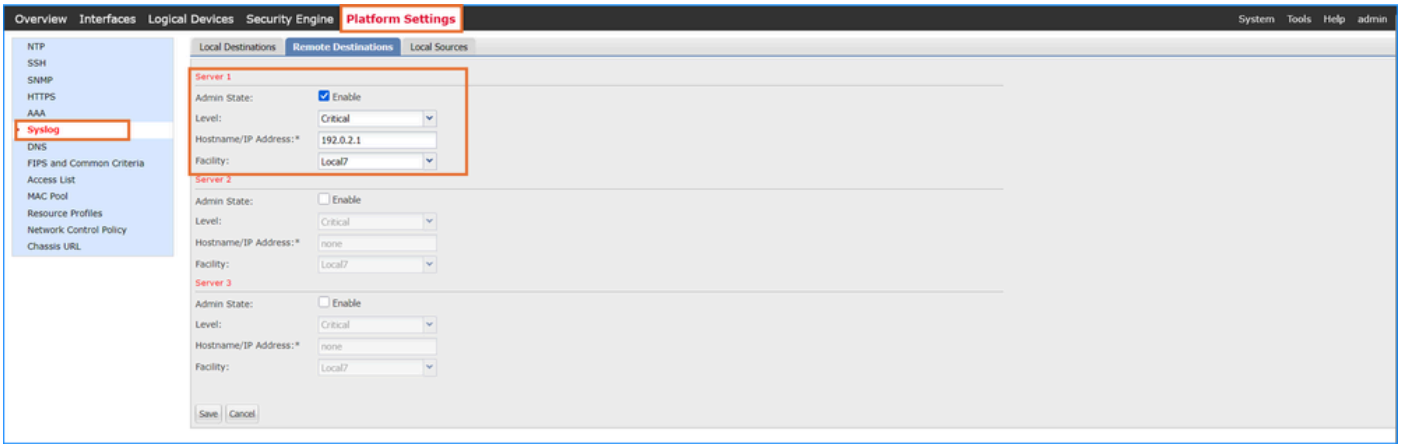
192.0.2.1

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

10. Im Fall von Firepower 4100 und 9300 sollten Sie unformatierte (nicht analysierte) FXOS-Meldungen von Syslog-Servern mindestens 10 Minuten vor dem Traceback sammeln. Das Rohformat ist für die interne Verarbeitung durch das TAC und technische Werkzeuge unerlässlich.

Bei hoher Verfügbarkeit und Clustering sollten zudem die Raw-Syslogs aus allen betroffenen Chassis erfasst werden.

Überprüfung der Benutzeroberfläche von FirePOWER Chassis Manager (FCM):



Überprüfung auf der 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. Erfassen Sie ASA- oder FTD-CPU-, Arbeitsspeicher- und Schnittstellendaten, einschließlich Traps, von den konfigurierten SNMP-Servern. Stellen Sie sicher, dass die Daten mindestens 30 Minuten vor der Rückverfolgung eingeschlossen sind.

Sammeln Sie im Falle eines wiederkehrenden Tracebacks die Rohmeldungen zu einigen Vorfällen. Sammeln Sie zudem bei hoher Verfügbarkeit und Clustering Rohnachrichten von allen betroffenen Chassis.

Verifizierung auf der ASA/FTD CLI:

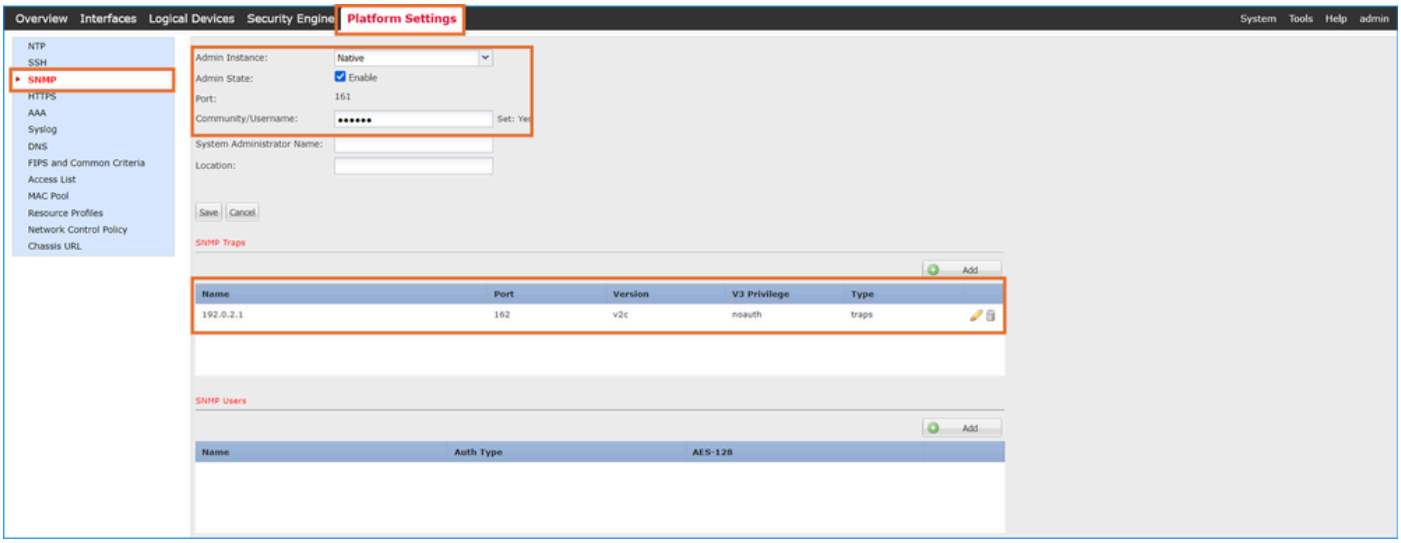
<#root>

```
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. Bei Firepower 4100 und 9300: Erfassen Sie CPU-, Speicher- und Schnittstellendaten einschließlich Traps von den konfigurierten SNMP-Servern. Stellen Sie sicher, dass die Daten mindestens 30 Minuten vor der Rückverfolgung eingeschlossen sind.

Sammeln Sie im Falle eines wiederkehrenden Tracebacks die Rohmeldungen zu einigen Vorfällen. Sammeln Sie zudem bei hoher Verfügbarkeit und Clustering Rohnachrichten von allen betroffenen Chassis.

Verifizierung auf der FCM-UI:



Überprüfung auf der 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. Traffic-Profil von den Netflow Collectors sammeln. Stellen Sie sicher, dass die Daten mindestens 30 Minuten vor der Rückverfolgung eingeschlossen sind.

Bei wiederkehrendem Traceback sollten Sie Daten zu einigen Vorfällen sammeln. Zudem müssen bei hoher Verfügbarkeit und Clustering Daten von allen betroffenen Chassis gesammelt werden.

Verifizierung auf der ASA/FTD CLI:

<#root>

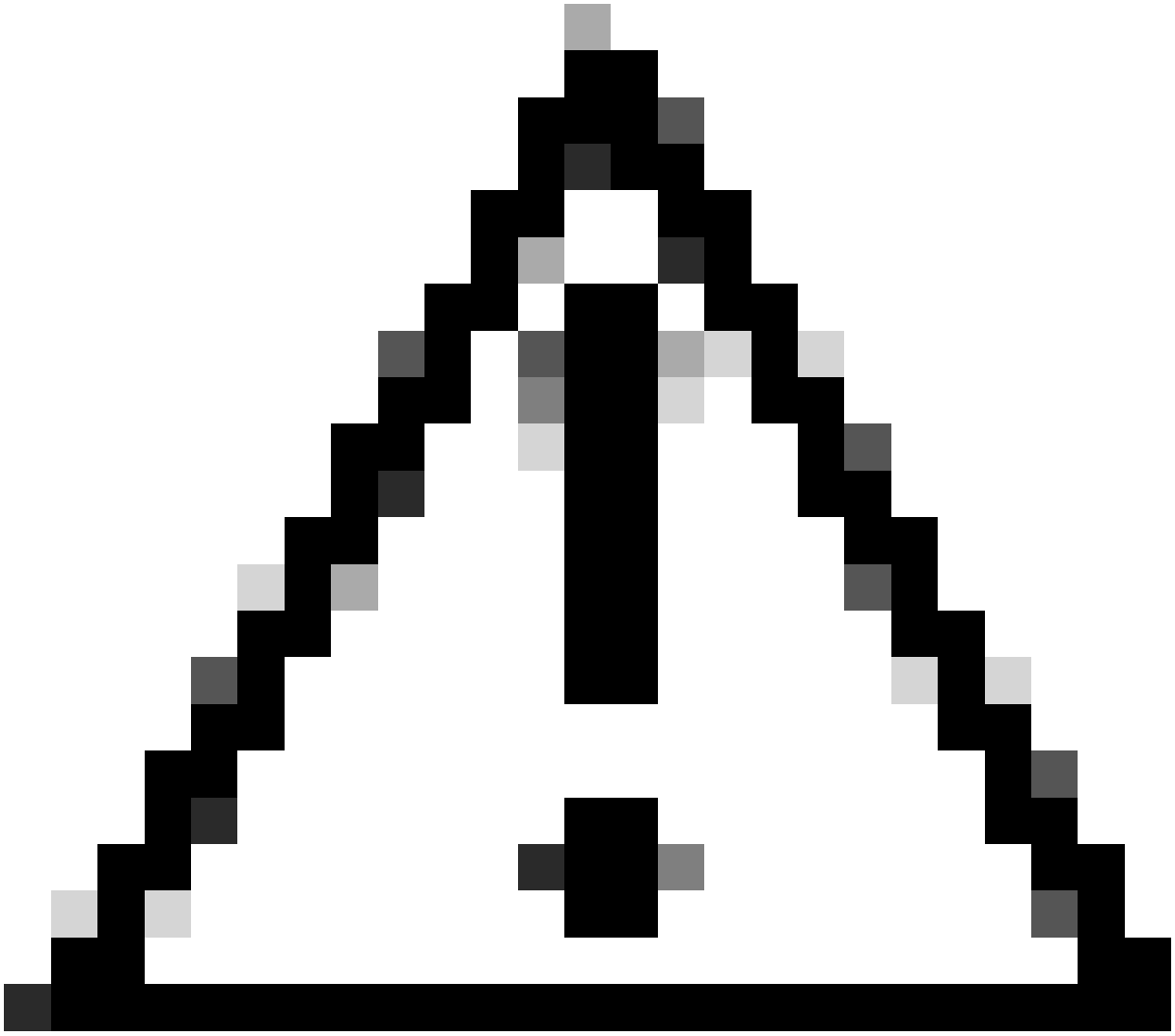
```
ftd#
show run flow-export


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. Bei wiederkehrendem Traceback die Ausgabe der Konsolensitzungen sammeln.

15. Öffnen Sie ein TAC-Ticket, und stellen Sie alle Daten bereit.

Wie sammle ich Crashinfo-, Coredump- und Minidump-Dateien von einer sicheren Firewall?

Fahren Sie mit den folgenden Schritten crashinfo, coredump und minidump Dateien von Secure Firewall:



Vorsicht: Warnung: Benennen Sie keine Core-, Crashfo- oder Minidump-Dateien um.

ASA

Hochladen von Dateien von der ASA CLI auf den Remote-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

Option 1: Sammeln von Dateien über die Lina CLI

1. Wenn der Remote-Server über das Lina-Modul erreichbar ist, kopieren Sie Dateien nach /mnt/disk0, und laden Sie Dateien aus der Lina-CLI hoch:

<#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. Wenn die Dateien vom Remote-Server heruntergeladen werden, stellen Sie sicher, dass Sie die kopierten Dateien aus /mnt/disk0/ auf FTD löschen:

<#root>

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

cd /mnt/disk0/

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

sudo rm core.lina.11.13050.1755081050.gz

Option 2 - Sammeln von Dateien über die Expertenmodus-CLI

Die TFTP-, SFTP- oder SCTP-Clients von Linux laden die Dateien aus dem Expertenmodus auf den Remote-Server hoch:

<#root>

```
>
```

expert

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

cd /ngfw/var/data/cores/

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

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

Option 3: Sammeln von Dateien über die FXOS-CLI für die lokale Verwaltung

Im nativen Modus können FTD im Firepower 1000-, 2100- und Secure Firewall 1200-, 3100- und 4200-Chassis die Core- und Minidump-Dateien von der CLI von FXOS local-mgmt erfasst werden:

<#root>

```
firepower#
connect local-mgmt

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

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


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

?

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

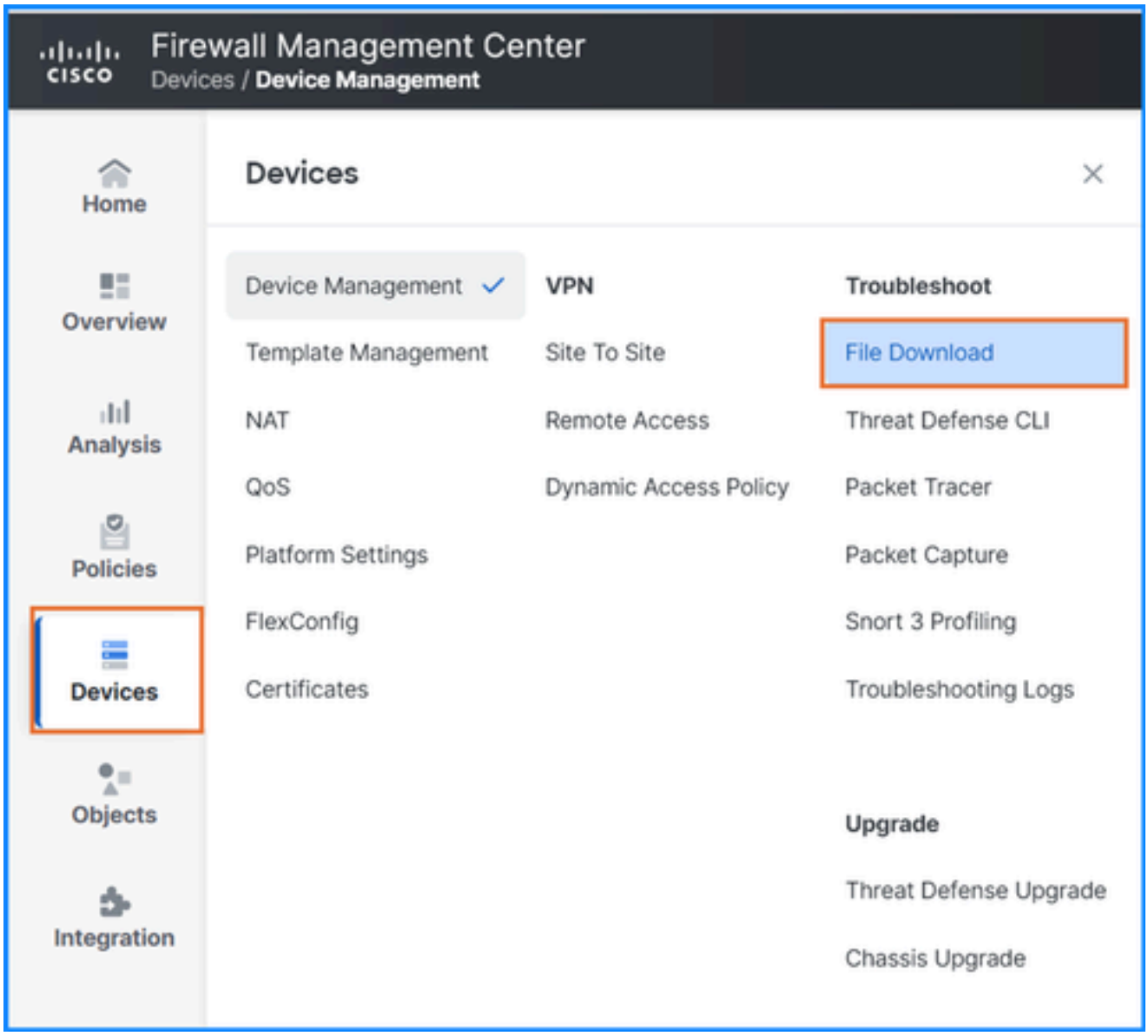
Option 4: Sammeln von Dateien über die FMC-Benutzeroberfläche

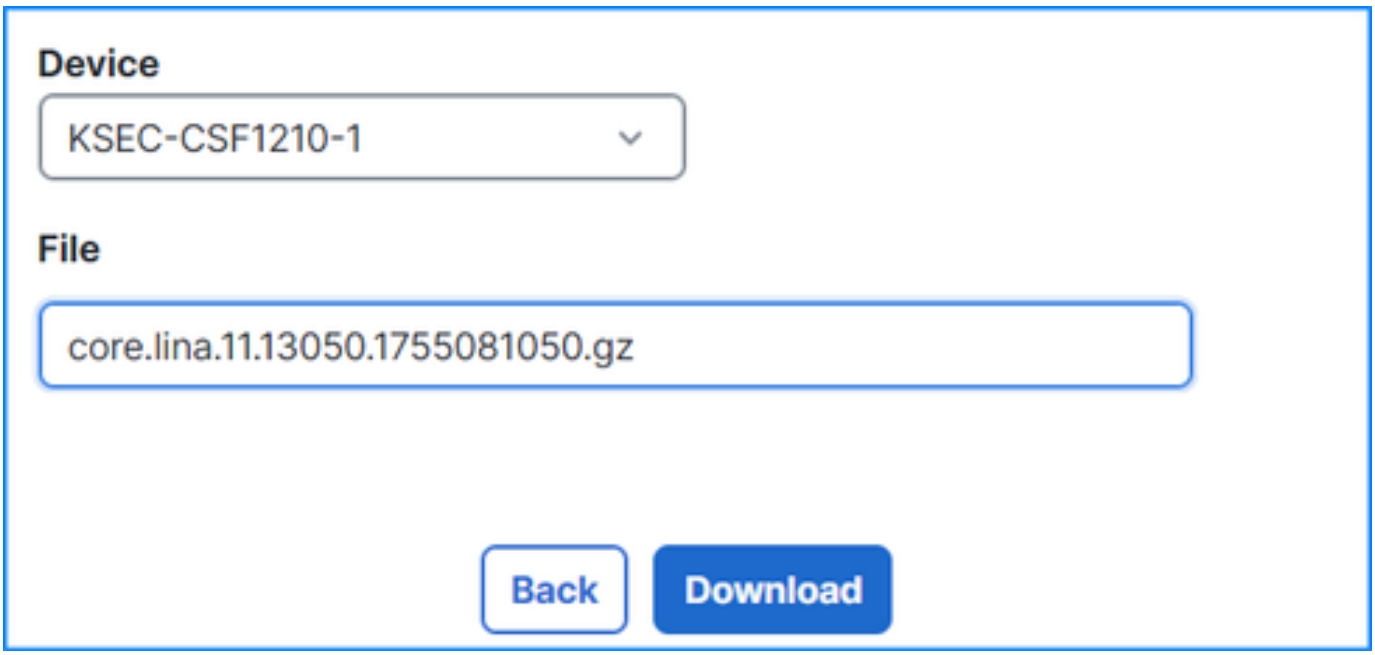
Kopieren Sie die Dateien nach /ngfw/var/common:

<#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. Laden Sie die Datei über die FMC-Benutzeroberfläche mit der Option Geräte > Datei-Download herunter:





3. Wenn die Dateien vom Remote-Server heruntergeladen werden, stellen Sie sicher, dass Sie die

kopierten Dateien aus /ngfw/var/common/ auf FTD löschen:

<#root>

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

cd

/ngfw/var/common/

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

sudo rm core.lina.11.13050.1755081050.gz

Sicherheitsmodule für Firepower 4100 und 9300

1. Stellen Sie eine Verbindung mit dem Modul her, und sammeln Sie die Core- und Crashfo-Dateien im Rahmen des Moduls 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
```

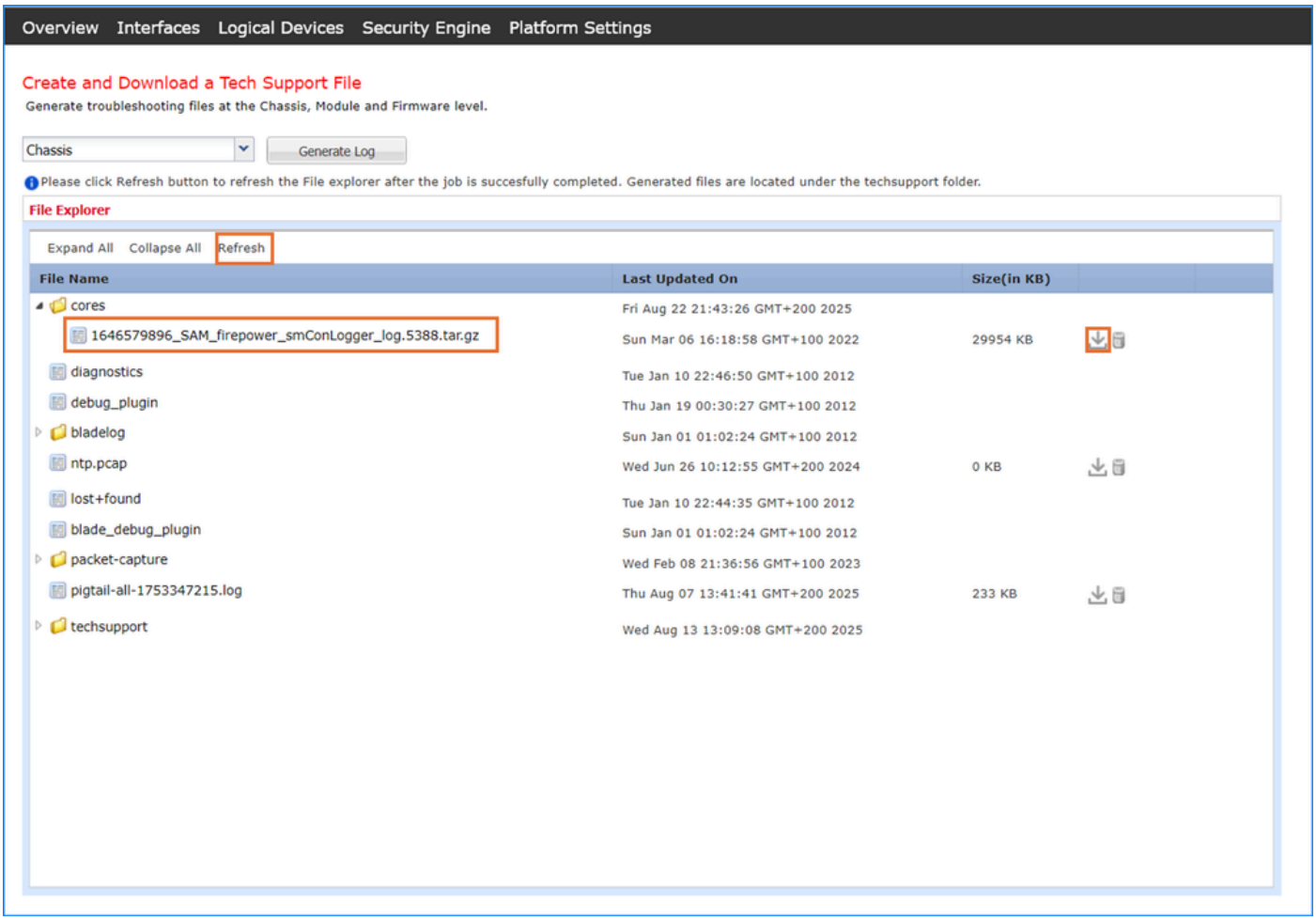
Firepower-Module1_08_04_2025_13_17_50.tar

FirePOWER-Chassis der Serien 4100 und 9300

1. Sammeln Sie Kerndateien mithilfe der FXOS-CLI für die lokale Verwaltung:

```
<#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. Alternativ dazu können Sie Dateien über Tools > Troubleshooting Logs (Tools > Fehlerbehebungsprotokolle) von der FCM-Benutzeroberfläche sammeln. Klicken Sie auf Aktualisieren, um die Dateiverzeichnisansicht und das Downloadsymbol neben der Kerndatei zu aktualisieren:



Referenzen

- FirePOWER-Softwareversionen überprüfen
- Überprüfen der FirePOWER-, Instanz-, Verfügbarkeits- und Skalierbarkeitskonfiguration
- Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung
- ASA-Befehlsreferenz

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.