收集数据以分析安全防火墙中软件回溯/崩溃的根本原因

目录

简介

本文档介绍在软件回溯的情况下收集数据的步骤。

先决条件

要求

基本的产品知识。

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙1200、3100、4200
- Firepower 1000、4100、9300
- 思科安全可扩展操作系统(FXOS)2.16(0.136)
- 思科安全防火墙威胁防御(FTD)7.6.1.291
- 思科安全防火墙管理中心(FMC)7.6.1.291
- 自适应安全设备(ASA)9.22.2.9

背景

FTD或ASA软件可以回溯并通常由于不同原因重新加载，例如：

- 软件缺陷，包括操作系统和第三方组件中的缺陷。
- 硬件异常，例如低级内存或CPU错误。
- 在某些情况下，由于缺少系统资源（例如内存）。
- 用户在TAC监督下出于诊断目的手动触发：

```
<#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
```

在追溯(也称为crash)的情况下，根据进程，通常会生成crashinfo、core或minidump文件:

- crashinfo包含来自进程内存的最低诊断数据。
- 核心文件是在回溯时进程内存的完整转储。
- minidump文件特定于Snort3，包含来自进程内存的诊断数据。

在Secure Firewall软件中，具有回溯的进程可以位于以下任何组件中：

- Firepower 1000、2100、4100、9300、安全防火墙1200、3100、4200机箱。
- Firepower 4100、9300安全模块。

除了core和crashinfo文件以外，回溯的根本原因分析(RCA)还需要其他信息，例如故障排除和show-tech文件、系统日志消息等。

核心和crashfinfo文件分析由TAC和思科作为服务请求（案例）的一部分处理。

数据收集

继续执行以下步骤，为回溯的RCA收集必要数据。由于存在文件轮转导致数据丢失的风险，请尽快提供请求的数据。

1. 明确以下项目：

1a。确切的硬件。

1b。软件版本。

1c。安全防火墙软件类型（ASA或FTD）。

1d。部署模式（本地或多实例模式）。

有关详细的验证步骤，请参阅验证Firepower软件版本和验证Firepower、实例、可用性、可扩展性配置。

2.澄清最近是否发生了任何环境变化，例如：

2a.增加流量。

2b。包括命令在内的主要配置更改。

确保尽可能准确地包含时间戳和时区。

3.如果在使用特定命令更改配置后发生回溯，请收集终端会话输出。如果在ASA上配置了命令授权，请从远程服务器（例如身份服务引擎[ISE]）收集命令授权报告。

4.在接下来的步骤中，确保使用最新的时间戳验证crashinfo、core或minidump文件，并记下每个文件的完整路径。如如何从Secure Firewall收集Crashinfo、核心转储和小型转储文件？部分。

ASA

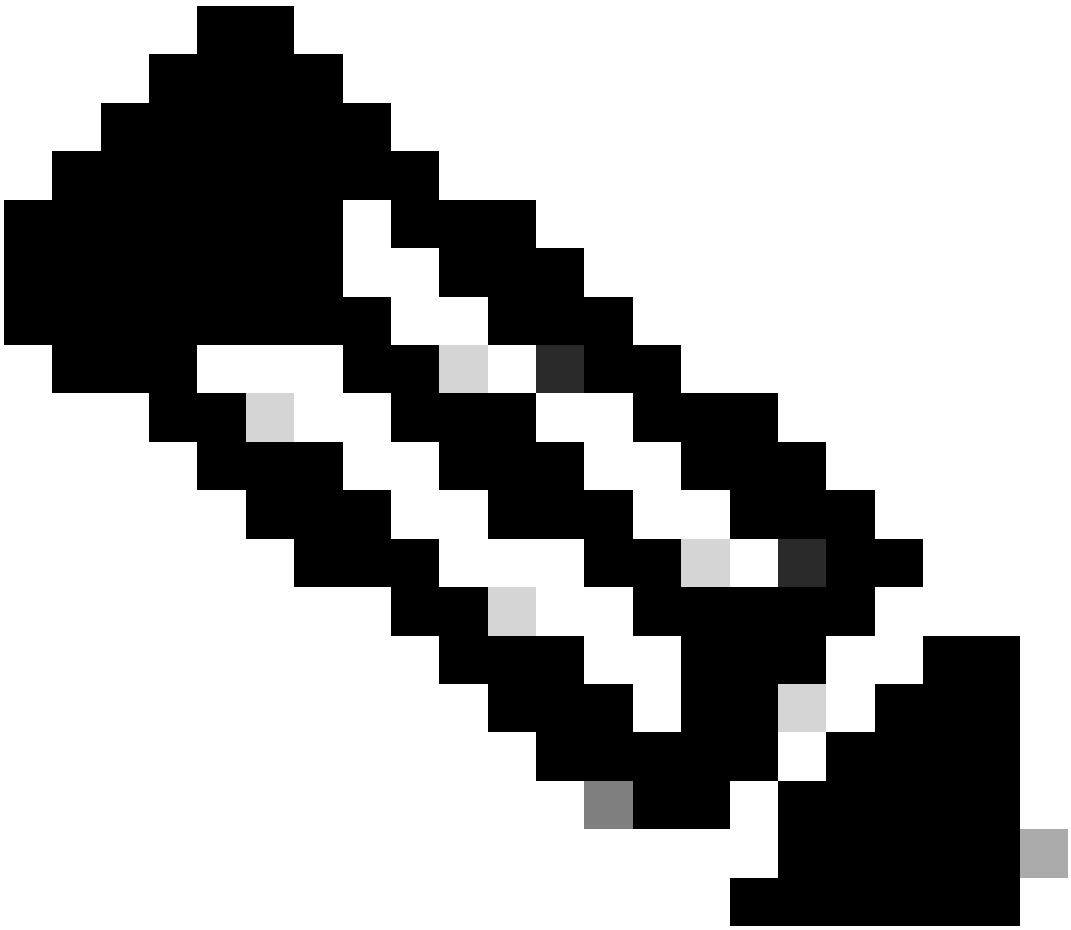
4.1.验证是否存在crashinfo文件。要查看最新的crashinfo，请运行show crashinfo命令。crashinfo文件可在dir命令的输出中找到。

```
<#root>

asa#

dir


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

crashinfo_lina.14664.20250813.205102
```

4.2.使用dir coredumpfsys命令验证是否存在ASA核心文件：

```
<#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
```



注意：在虚拟ASA上，核心转储功能默认处于禁用状态：

```
<#root>
ciscoasa#
show coredump
```

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

要启用核心转储功能，请参阅Cisco安全防火墙ASA系列命令参考，A-H命令中的核心转储启用部分。

FTD

4.1.验证是否存在FTD crashinfo文件。要查看最新的crashinfo，请运行show crashinfo命令。crashinfo文件可在dir命令的输出中找到。

<#root>

```
ftd#
dir

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

在FTD上，可以在expert mode /mnt/disk0/目录中找到crashinfo文件：

<#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
```

在FTD故障排除文件中，crashinfo文件位于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.验证是否存在FTD核心文件。在FTD上，可以在expert模式/ngfw/var/data/cores/和/ngfw/var/common/ 目录中访问核心文件：

```
<#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
```

在FTD故障排除文件中，核心文件名称位于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
```

FTD Snort3特定核心转储

本节仅适用于运行Snort3引擎的FTD。

4.1.验证是否存在Snort3引擎crashinfo文件snort3-crashinfo.*在专家模式/ngfw/var/log/crashinfo/目录。

<#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

在FTD故障排除文件中，相同文件位于dir-archives/var-log/crashinfo/中。

4.2.验证/ngfw/var/data/cores/中是否存在Snort3小型转储文件minidump_*:

<#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

在FTD故障排除文件中，小型转储文件位于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

Firepower 4100和9300安全模块

本节仅适用于Firepower 4100和9300模块。

4.1.验证是否存在crashinfo和核心文件：

```
<#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.在Firepower 1000、2100和安全防火墙1200、3100、4200机箱上，使用local-mgmt shell中的dir workspace:/cores和dir workspace:/cores_fxos命令验证是否存在核心文件。

如果安装了ASA应用，则使用connect fxos admin命令连接到FXOS外壳：

```
<#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
```

机箱故障排除文件中的/opt/cisco/platform/logs/prune_cores.log文件中也提到了核心文件：

```
<#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.在Firepower 4100和9300机箱上，使用local-mgmt shell中的dir workspace:/cores命令验证是否存在核心文件：

```
<#root>

firewall(local-mgmt)#

dir workspace:/cores


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

核心文件名可以在机箱故障排除文件中找到，位于文件*_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo中的show cores 命令输出中，其中*是故障排除文件名的一部分，例如20250311123356_ FW_BC1_all.tar。

5.验证crashinfo、coredump和minidump文件是否与事件相关。

- 比较文件时间戳与事故的时间戳，或……
- 使用Linux date命令将纪元时间戳从文件名转换为日期。

对于核心和小型转储文件，纪元时间戳可以使用任何Linux主机上的date转换为日期时间：

<#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.

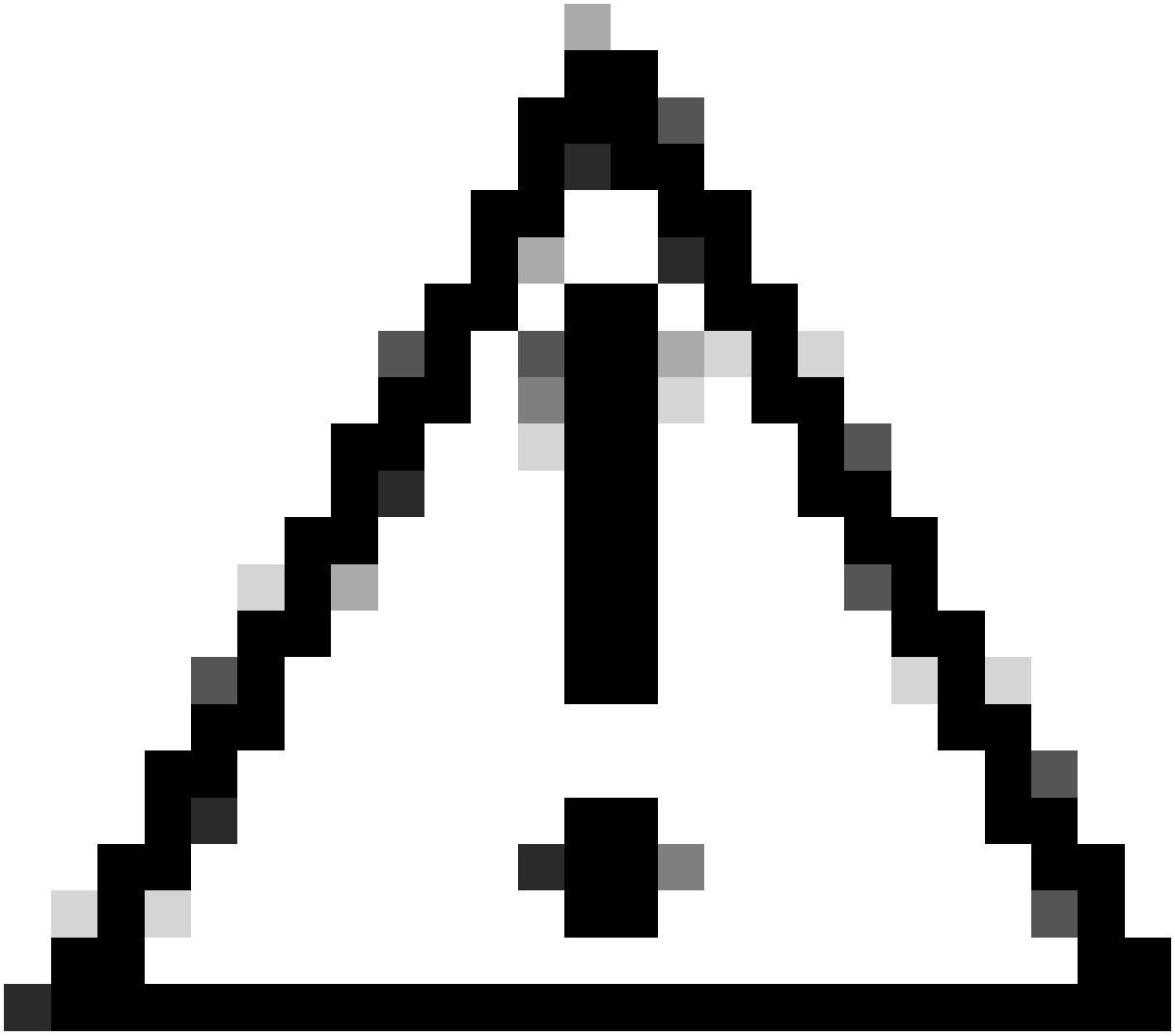
gz

linux $

date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025

6.请参阅如何从Secure Firewall收集Crashinfo、Coredump和Minidump文件？部分，从步骤4-5下载crashinfo、Minidump和core文件。



警告：请勿重命名core、crashinfo或minidump文件。

7.继续执行Firepower文件生成过程故障排除中的步骤，以收集show-tech文件并排除文件故障：

7a。ASA show-tech文件。

7b。FTD故障排除文件。

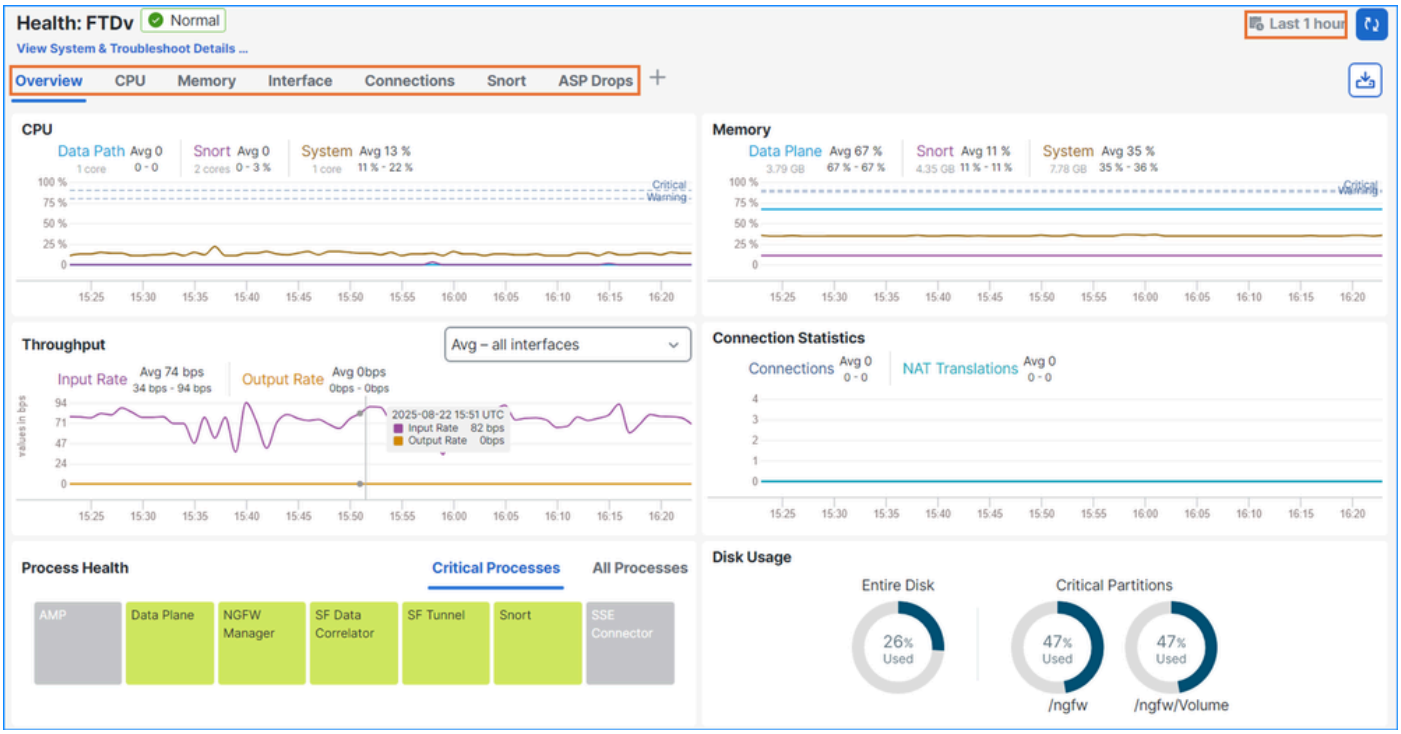
7c。Firepower 4100和9300安全模块show-tech文件。

7d。Firepower 4100和9300机箱显示技术文件。

7e。Firepower 1000、2100和安全防火墙1200、3100、4200机箱show-tech文件。容器模式下安全防火墙3100、4200的机箱故障排除文件可以通过FMC > Devices > [机箱] > 3 dots > Troubleshoot Files选项下载。

8.对于FTD，请收集FMC上的运行状况监控选项卡的屏幕截图，该屏幕截图在回溯之前至少有30分钟。确保包括所有突出显示的选项卡的屏幕截图。对于重复回溯，请收集一些事件的屏幕截图。

此外，对于高可用性和集群，请收集所有受影响设备的屏幕截图：



9.收集来自syslog服务器的原始（未分析）Lina引擎syslog消息，这些消息在回溯之前至少覆盖30分钟。原始格式对于TAC和工程工具的内部处理至关重要。

在重复回溯的情况下，收集覆盖少数事件的原始消息。此外，在高可用性和集群的情况下，收集所有受影响单元的原始系统日志。

在ASA/FTD CLI上进行验证：

<#root>

ftd#

show run logging

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

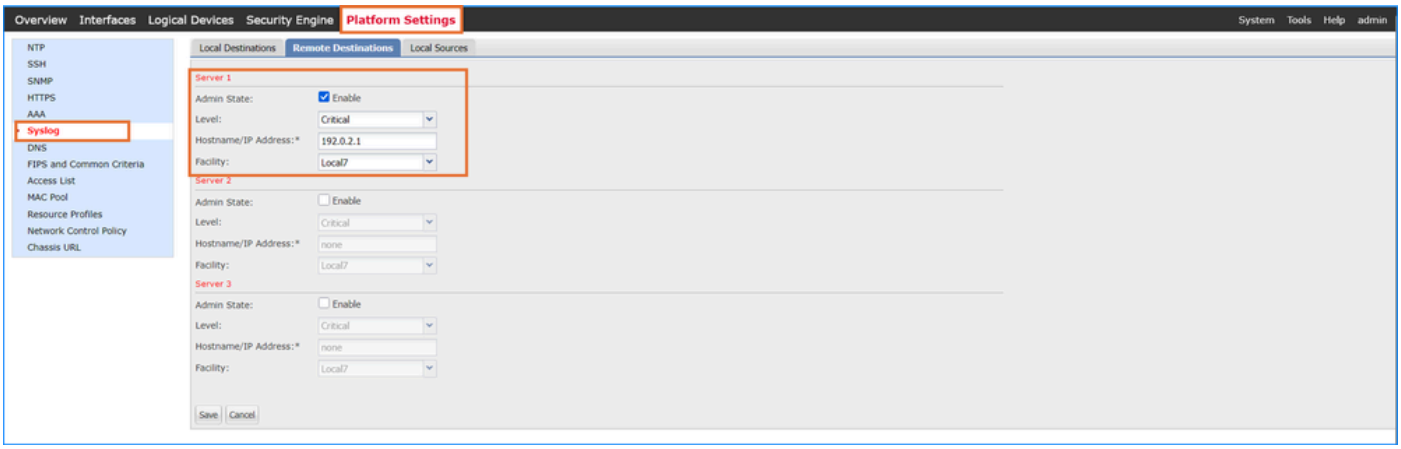
192.0.2.1

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

10.对于Firepower 4100和9300，请在回溯之前至少10分钟从系统日志服务器收集原始（未解析的）FXOS消息。原始格式对于TAC和工程工具的内部处理至关重要。

此外，对于高可用性和集群，请从所有受影响的机箱收集原始系统日志。

在Firepower机箱管理器(FCM)用户界面(UI)上验证：



在FXOS CLI上进行验证：

<#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.从已配置的SNMP服务器收集ASA或FTD CPU、内存、接口数据（包括陷阱）。确保包含的数据至少覆盖回溯前30分钟。

如果出现重复回溯，请收集涵盖几个事故的原始邮件。此外，在高可用性和群集的情况下，收集来自所有受影响机箱的原始消息。

在ASA/FTD CLI上进行验证：

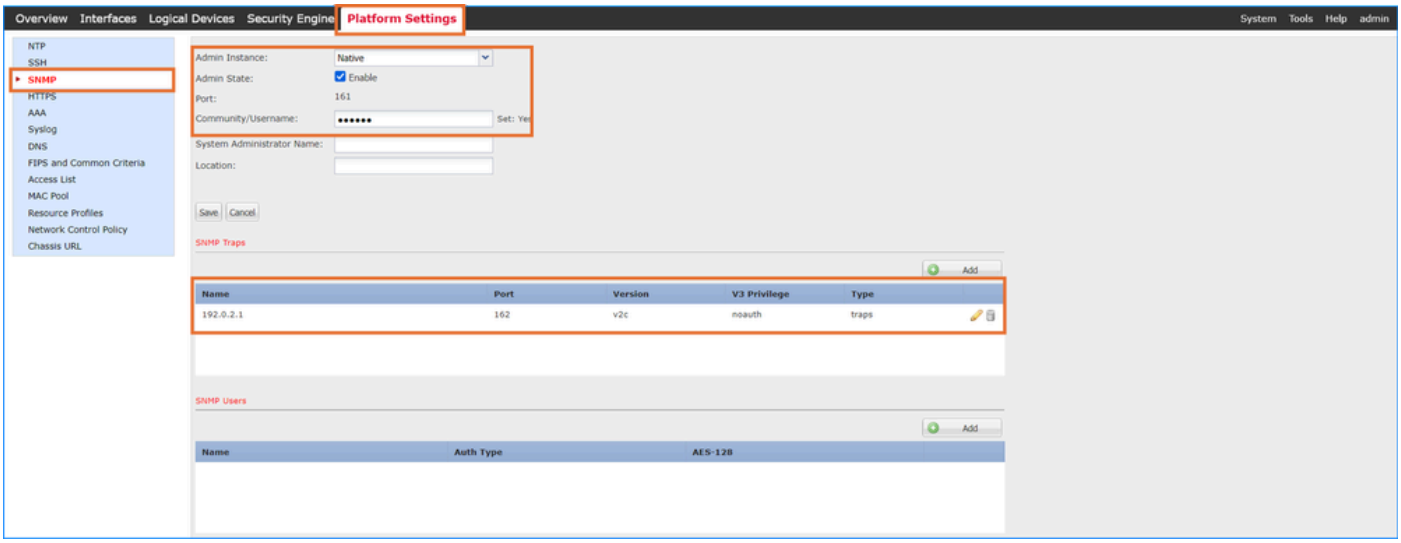
<#root>

```
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.对于Firepower 4100和9300，从配置的SNMP服务器收集CPU、内存和接口数据，包括陷阱。确保包含的数据至少覆盖回溯前30分钟。

如果出现重复回溯，请收集涵盖几个事故的原始邮件。 此外，在高可用性和群集的情况下，收集来自所有受影响机箱的原始消息。

在FCM UI上的验证：



在FXOS CLI上进行验证：

<#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.从Netflow收集器收集流量量变曲线。确保包含的数据至少覆盖回溯前30分钟。

在重复回溯的情况下，收集覆盖少数事件的数据。 此外，在高可用性和群集的情况下，请从所有受影响的机箱收集数据。

在ASA/FTD CLI上进行验证：

```
<#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
```

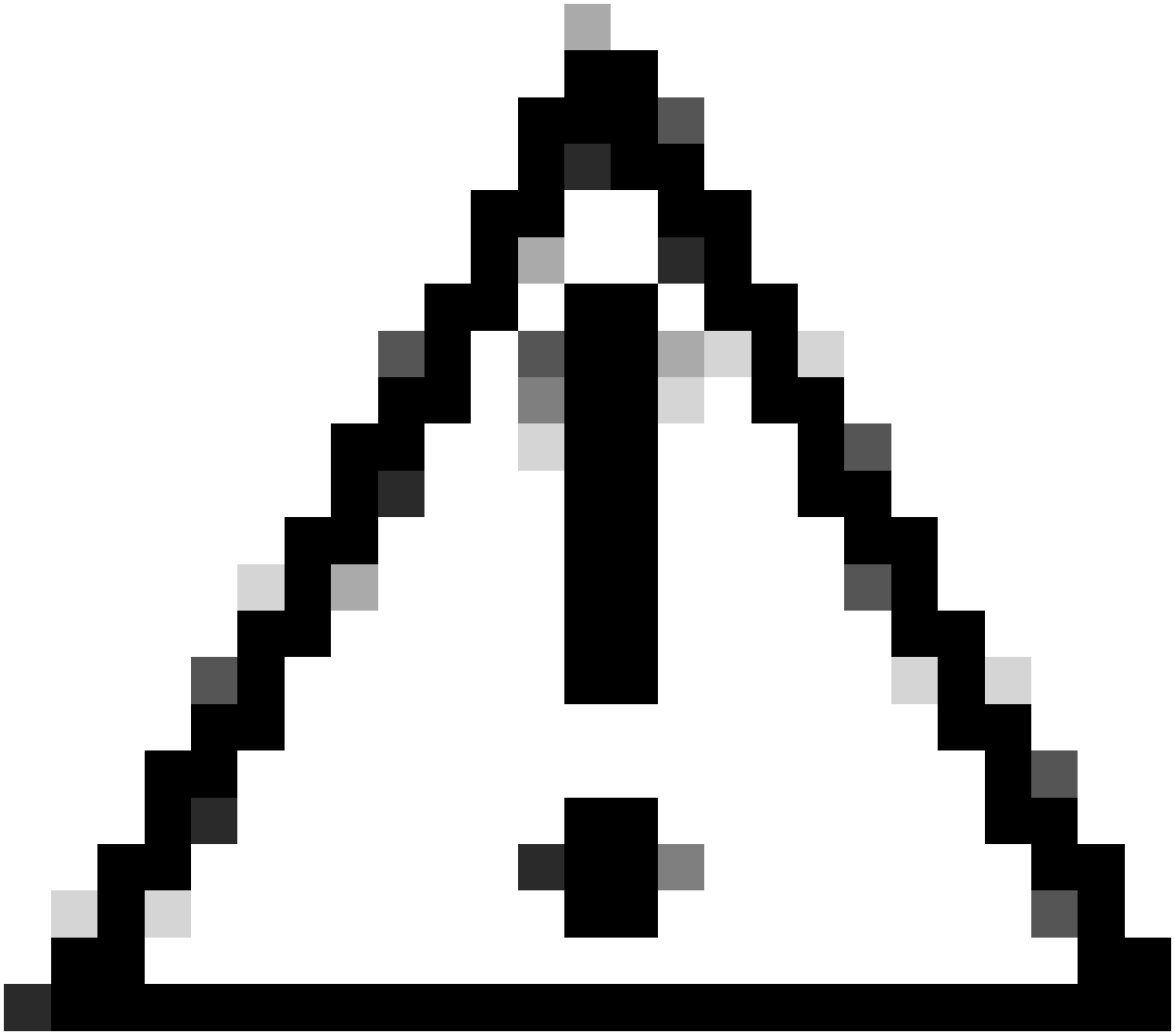
```
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP


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.如果是重复回溯，请收集控制台会话的输出。

15.创建TAC案例并提供所有数据。

如何从Secure Firewall收集Crashinfo、Coredump和Minidump文件？

继续从Secure Firewall中执行crashinfo、coredump和minidump Files这些步骤：



警告：警告：请勿重命名core、crashinfo或minidump文件。

ASA

将文件从ASA CLI上传到远程服务器：

<#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

选项1 — 使用Lina CLI收集文件

1. 如果可以从Lina引擎访问远程服务器，请将文件复制到/mnt/disk0，并从Lina CLI上传文件：

```
<#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. 从远程服务器下载文件时，请确保从FTD上的/mnt/disk0/删除复制的文件:

<#root>

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

cd /mnt/disk0/

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

sudo rm core.lina.11.13050.1755081050.gz

选项2 — 使用专家模式CLI收集文件

使用Linux TFTP、SFTP或SCTP客户端将文件从专家模式上传到远程服务器：

<#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
```

选项3 — 使用FXOS本地管理CLI收集文件

在Firepower 1000、2100和安全防火墙1200、3100、4200机箱上运行的本地模式FTD上，核心和小型转储文件可以从FXOS本地管理CLI收集：

```
<#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
```

选项4 — 使用FMC UI收集文件

将文件复制到/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/

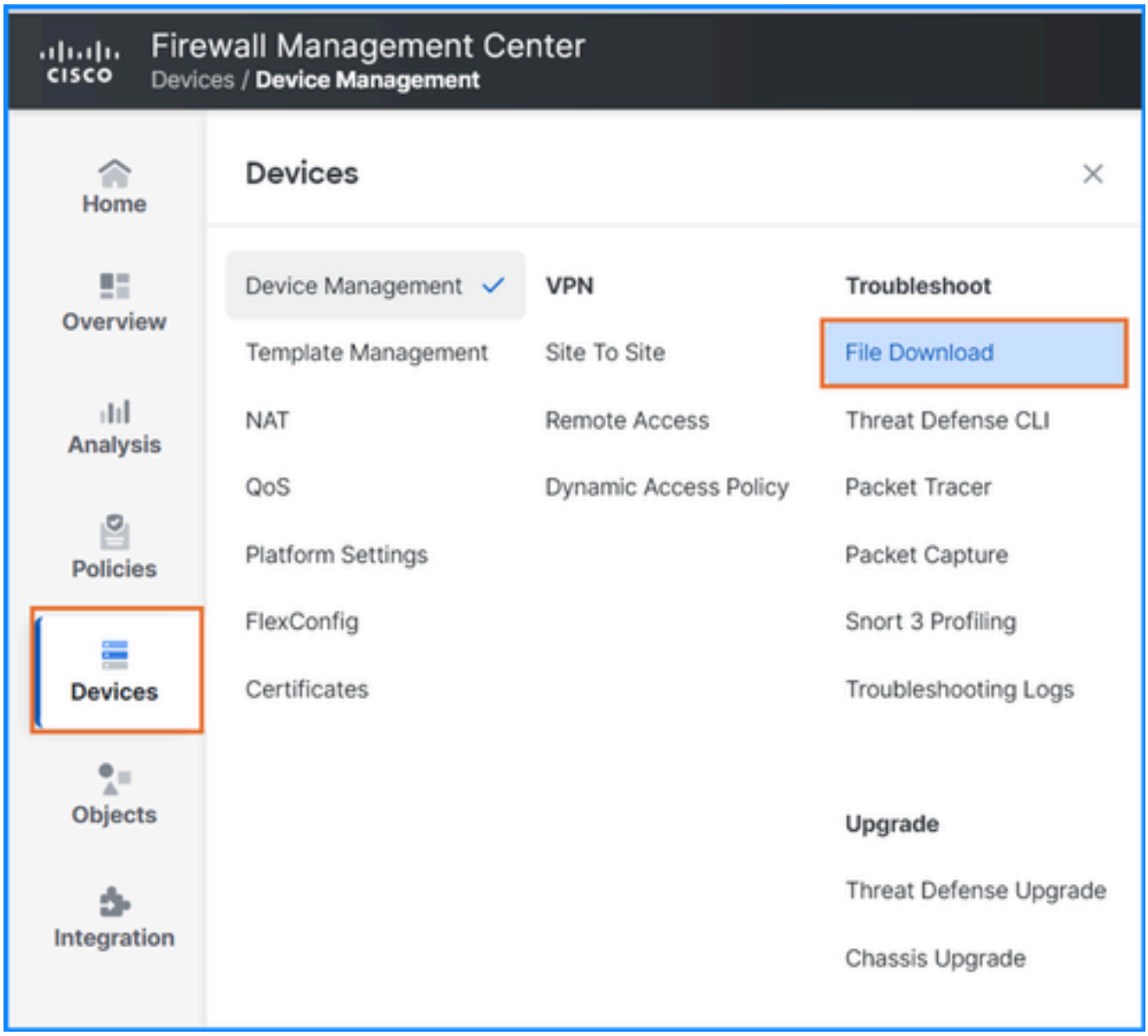
```
admin@firepower:~$
```

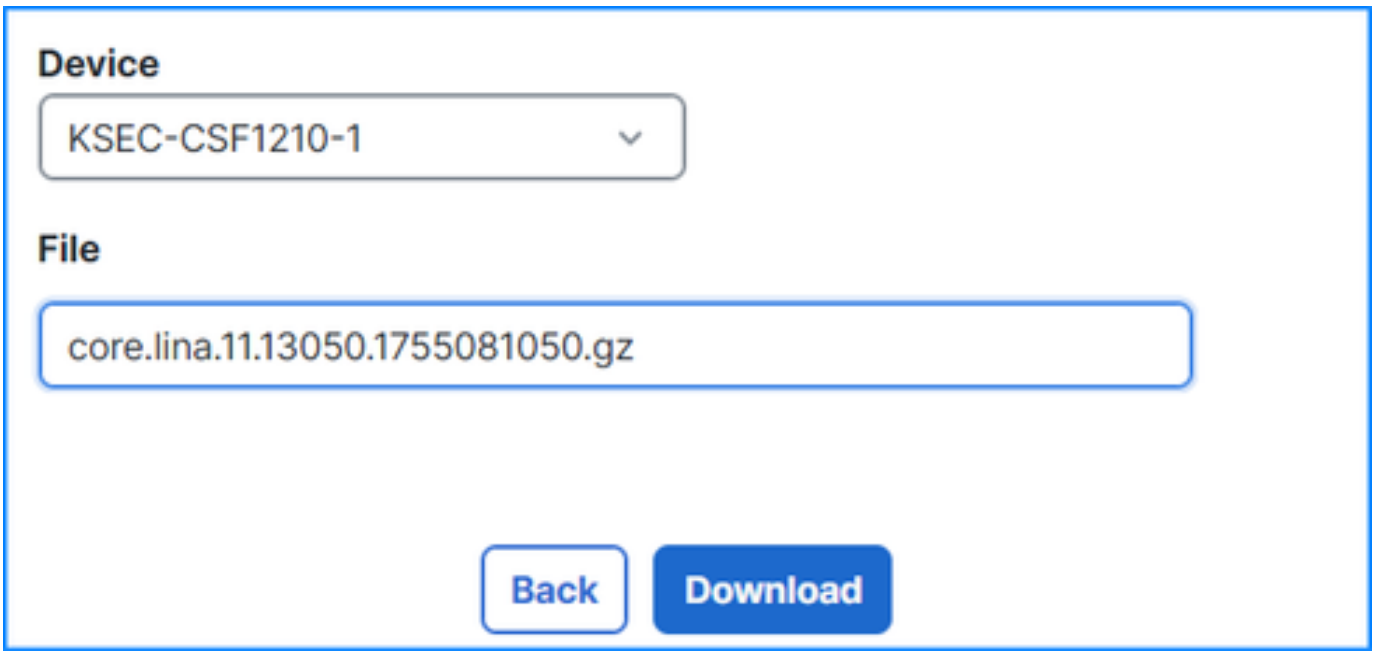
ls -l /ngfw/var/common/

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

core.lina.11.13050.1755081050.gz

2. 使用Devices > File Download选项从FMC UI下载文件：





3.从远程服务器下载文件时，请确保从FTD上的/ngfw/var/common/删除复制的文件:

<#root>

admin@firepower:~$

cd

/ngfw/var/common/

admin@firepower:/mnt/disk0/:$

sudo rm core.lina.11.13050.1755081050.gz

Firepower 4100和9300安全模块

1. 连接到模块并收集core和crashinfo文件作为模块show-tech文件的一部分：

<#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
```

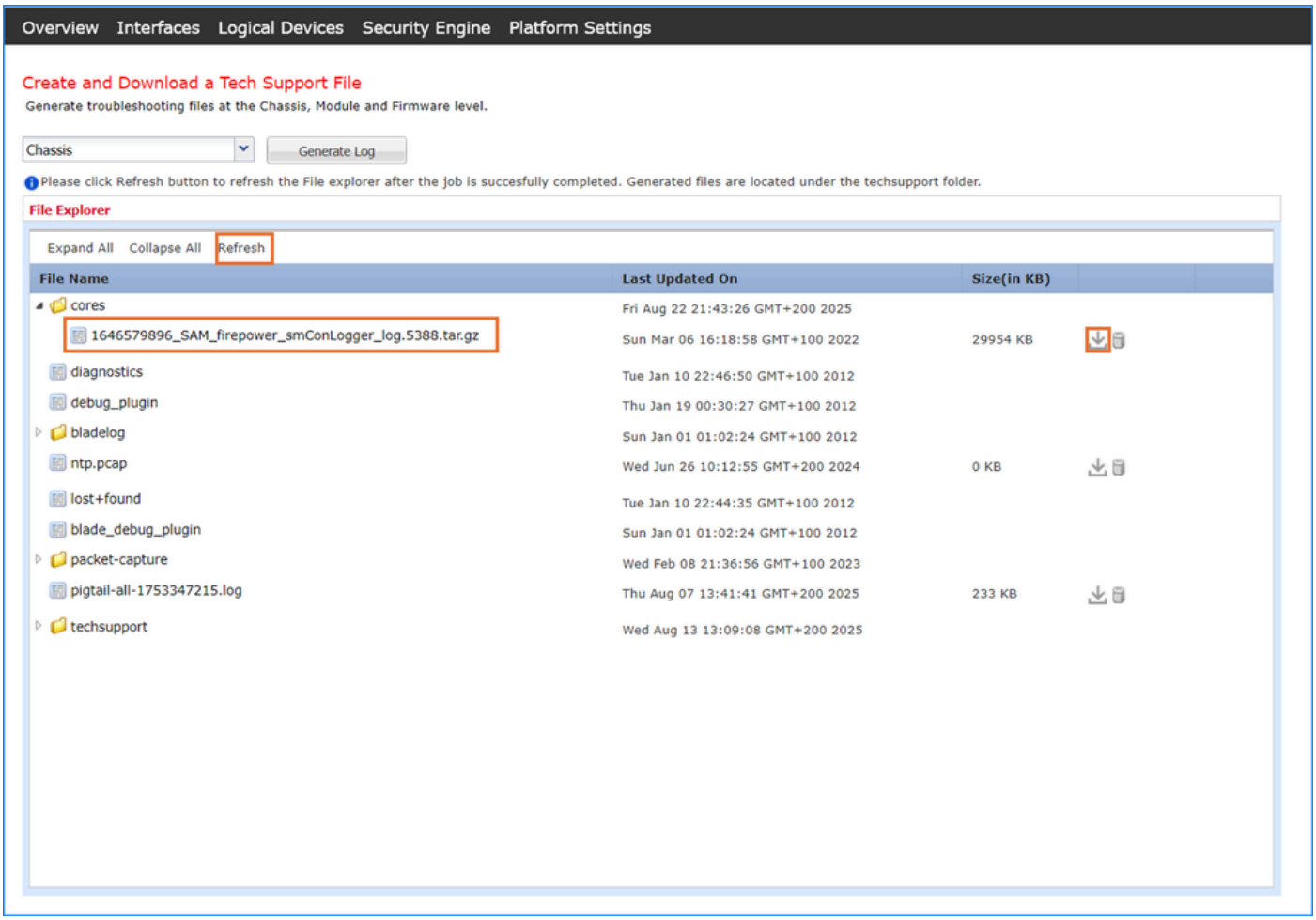
Firepower-Module1_08_04_2025_13_17_50.tar

Firepower 4100和9300机箱

1. 使用FXOS本地管理CLI收集核心文件：

```
<#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.或者，通过工具 > 故障排除日志从FCM UI收集文件。单击Refresh以更新文件目录视图和核心文件旁边的下载图标：



参考

- 验证Firepower软件版本
- 验证Firepower、实例、可用性、可扩展性配置
- 排除Firepower文件生成过程故障
- ASA命令参考

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。