Coletar dados para análise da causa raiz do rastreamento/travamento do software no firewall seguro

Contents

Introdução

Este documento descreve as etapas para coletar dados no caso de um retorno de rastreamento de software.

Pré-requisitos

Requisitos

Conhecimento básico do produto.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

As informações neste documento são baseadas nestas versões de software e hardware:

- Firewall seguro 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
- Dispositivo de segurança adaptável (ASA) 9.22.2.9

Background

O software FTD ou ASA pode rastrear e normalmente recarregar devido a diferentes motivos, como:

- Defeitos de software, incluindo defeitos no sistema operacional e componentes de terceiros.
- Exceções de hardware, como erros de memória de baixo nível ou de CPU.
- Em alguns casos, devido à falta de recursos do sistema, como memória.
- Disparado manualmente pelo usuário para fins de diagnóstico sob supervisão do 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
```

No caso de um traceback também conhecido como travamento, dependendo do processo, geralmente são gerados arquivos crashinfo, core ou minidespejo:

- crashinfo contém o mínimo de dados de diagnóstico da memória do processo.
- o arquivo de núcleo é um dump completo da memória do processo no momento do traceback.
- o arquivo minidump é específico do Snort3 e contém dados de diagnóstico da memória do processo.

No software Secure Firewall, o processo que teve um traceback pode estar em qualquer um destes componentes:

- Chassi Firepower 1000, 2100, 4100, 9300, Secure Firewall 1200, 3100, 4200.
- Módulos de segurança Firepower 4100, 9300.

Além dos arquivos principais e de informação de travamento, a análise de causa raiz (RCA) de um retorno de rastreamento requer informações adicionais, como arquivos de solução de problemas e show-tech, mensagens de syslog e assim por diante.

A análise do arquivo principal e crashfinfo é tratada pelo TAC e pela Cisco como parte de uma solicitação de serviço (caso).

Levantamento de dados

Continue com estas etapas para coletar os dados necessários para a RCA do traceback. Devido ao risco de perda de dados causada por rotações de arquivos, forneça os dados solicitados o mais rápido possível.

1. Esclareça estes itens:

1-A. Hardware exato.

1-B. Versão de software.

1 quater. Software de firewall seguro (ASA ou FTD).

1d. Modo de implantação (modo nativo ou de várias instâncias).

Consulte Verificação das versões do software Firepower e Verificação do Firepower, Instância, Disponibilidade, Configuração de escalabilidade para obter etapas de verificação detalhadas.

2. Clarificar se houve alterações ambientais recentes, tais como:

2a. Adição de tráfego.

2-B. Grandes alterações de configuração, incluindo comandos.

Certifique-se de incluir os carimbos de data/hora e o fuso horário o mais precisamente possível.

3. Se o retorno de rastreamento ocorreu após alterações de configuração usando comandos específicos, colete as saídas da sessão do terminal. Se a autorização de comando estiver configurada no ASA, colete os relatórios de autorização de comando do servidor remoto, como o Identity Services Engine (ISE).

4. Nas próximas etapas, certifique-se de verificar os arquivos crashinfo, core ou minidump com os timestamps mais recentes e tome nota do caminho completo para cada arquivo. Os caminhos completos são necessários para a coleta dos arquivos conforme mostrado em Como coletar arquivos de informação de travamento, coredump e minidespejo do Secure Firewall? seção.

ASA

4.1. Verifique a presença de um arquivo crashinfo. Para exibir as informações de travamento mais

recentes, execute o comando show crashinfo. Os arquivos crashinfo podem ser encontrados na saída do comando dir.

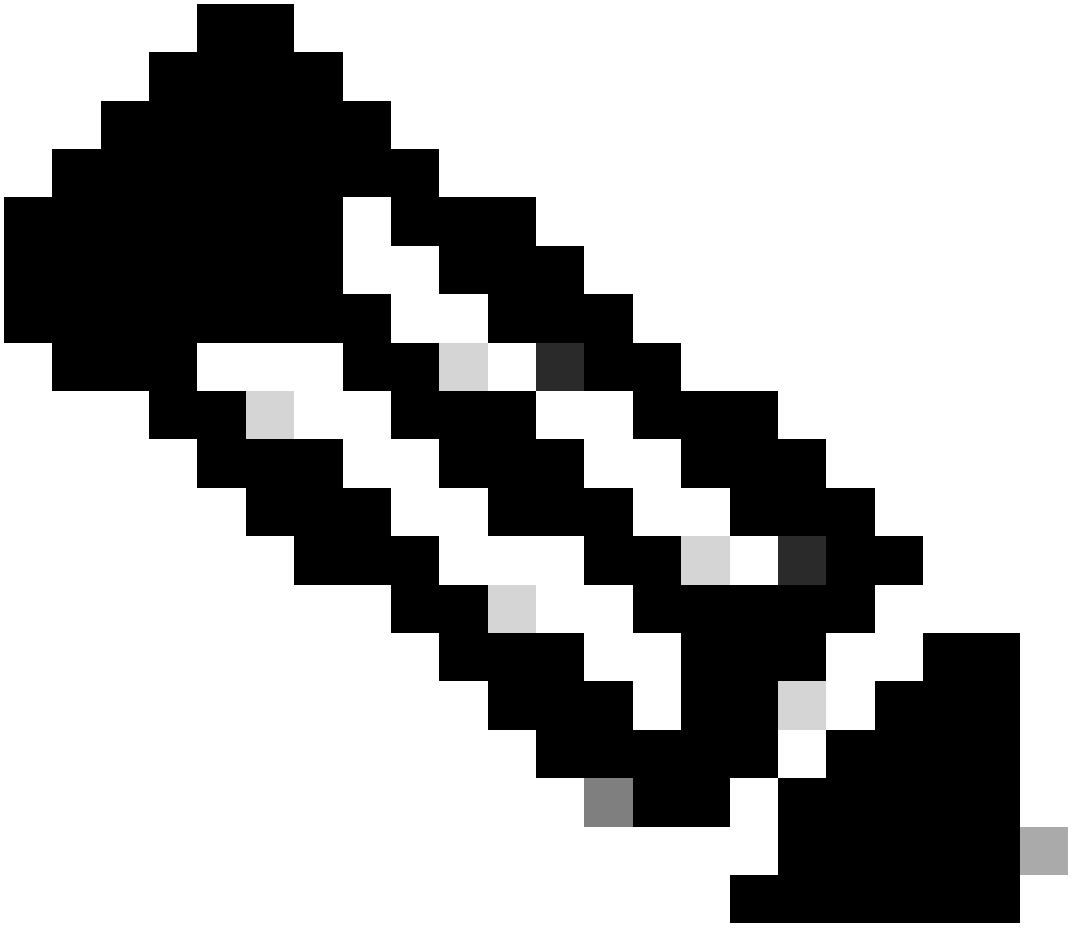
<#root>

```
asa#
dir

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

4.2. Verifique a presença de arquivos de núcleo do ASA usando o 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
```



Note: No ASA virtual, o recurso de dump central está desabilitado por padrão:

```
<#root>

ciscoasa#

show coredump


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

Para habilitar o recurso coredump, consulte a seção coredump enable na Referência de Comandos do Cisco Secure Firewall ASA Series, Comandos A-H.

FTD

4.1. Verifique a presença de um arquivo de informações de travamento de FTD. Para exibir as informações de travamento mais recentes, execute o comando show crashinfo. Os arquivos crashinfo podem ser encontrados na saída do comando dir.

<#root>

```
ftd#
dir

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

No FTD, os arquivos de informação de travamento podem ser encontrados no diretório do modo especialista /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
```

No arquivo de solução de problemas do FTD, os arquivos crashinfo estão em dir-archives/var-log/mnt-disk0/:

<#root>

```
$
ls -l

/dir-archives/mnt-disk0

total 9456
-rw-r--r-- 1 root root  453024 Aug  8 23:51
```

```
crashinfo_lina.13949.20250808.235100
```

4.2. Verificar a presença dos arquivos principais do FTD. No FTD, os arquivos principais estão acessíveis nos diretórios 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
```

No arquivo de solução de problemas de FTD, os nomes dos arquivos principais estão no arquivo 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
```

Coredump específico do FTD Snort3

Esta seção é aplicável apenas ao FTD que executa o mecanismo Snort3.

4.1. Verifique a presença de arquivos de informação de travamento do mecanismo Snort3 snort3-crashinfo.* no diretório /ngfw/var/log/crashinfo/ do modo especialista.

```
<#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
```

No arquivo de solução de problemas do FTD, os mesmos arquivos estão em dir-archives/var-log/crashinfo/.

4.2. Verifique a presença dos arquivos de minidespejo do Snort3 minidump_* em /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
```

No arquivo de solução de problemas do FTD, os arquivos de minidespejo estão em file-contents/ngfw/var/data/cores/:

<#root>

```
$
ls -l file-contents/ngfw/var/data/cores/

total 1904
-rw------- 1 root root 977760 Aug 22 19:10
minidump_1755889805_firepower_snort3_17455.dmp
```

Módulos de segurança Firepower 4100 e 9300

Esta seção se aplica somente aos módulos Firepower 4100 e 9300.

4.1. Verifique a presença de informações de travamento e arquivos principais:

<#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. Nos chassis do Firepower 1000, 2100 e do Secure Firewall 1200, 3100, 4200, verifique a presença de arquivos de núcleo usando os comandos dir workspace:/cores e dir workspace:/cores_fxos no shell local-mgmt.

Se o aplicativo ASA estiver instalado, conecte-se ao shell FXOS usando o 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
```

Os arquivos principais também são mencionados nos arquivos /opt/cisco/platform/logs/prune_cores.log no arquivo de solução de problemas de chassi:

```
<#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. Nos chassis do Firepower 4100 e 9300, verifique a presença de arquivos de núcleo usando os comandos dir workspace:/cores no shell local-mgmt:

```
<#root>
firewall(local-mgmt)#
dir workspace:/cores

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

Os nomes dos arquivos principais podem ser encontrados dentro do arquivo de solução de problemas de chassi, nas saídas do comando show cores no arquivo *_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo, onde * é a parte do nome do arquivo de solução de problemas, por exemplo, 20250311123356_ FW_BC1_all.tar.

5. Verifique se os arquivos crashinfo, coredump e minidump são relevantes para o incidente.

- Compare os timestamps de arquivo com o timestamp do incidente, ou..
- Converta o timestamp epoch do nome do arquivo até a data usando o comando Linux date.

Para arquivos de núcleo e minidespejo, os carimbos de data e hora de época podem ser convertidos para data e hora usando a data em qualquer 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.

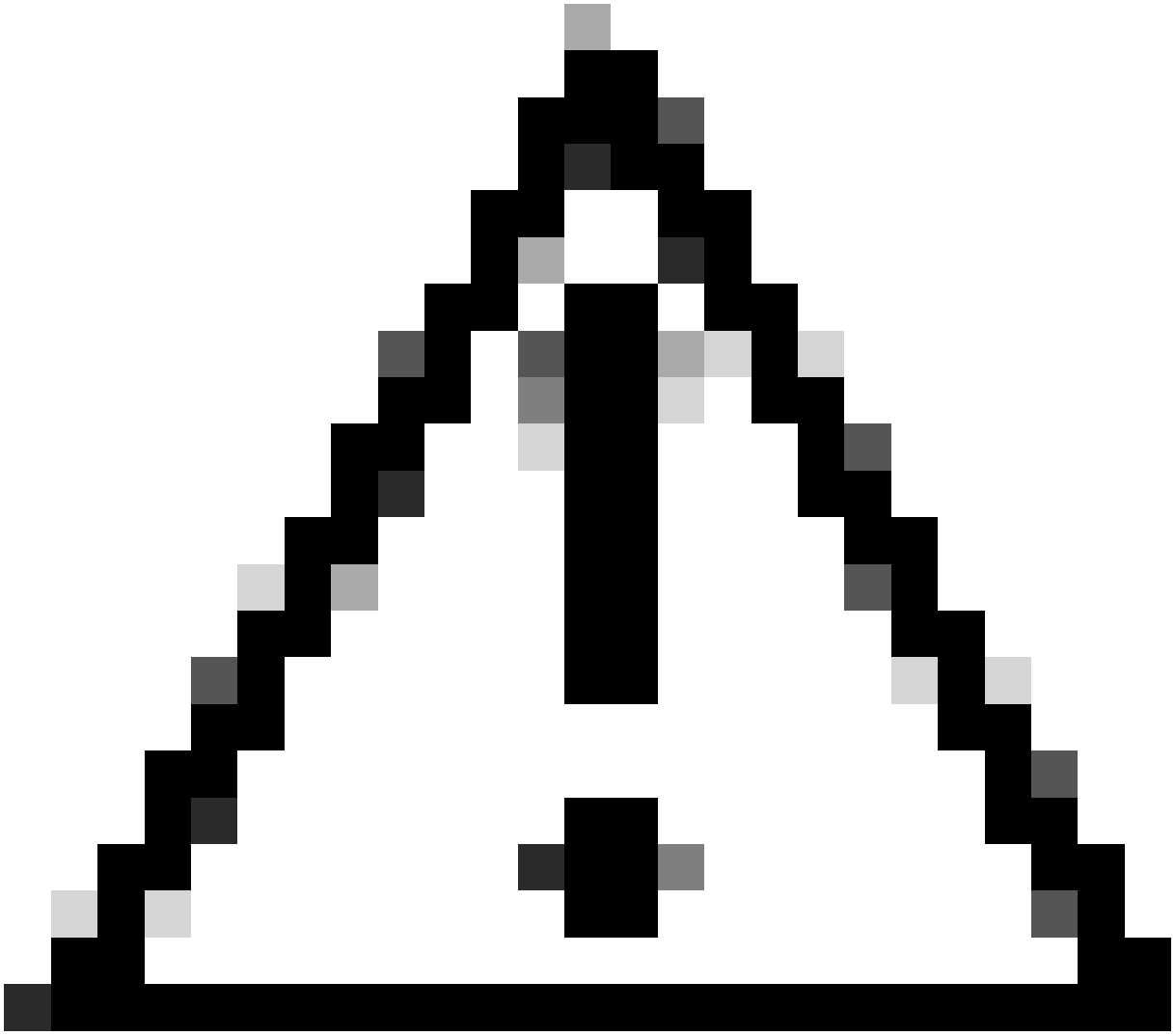
gz

linux $

date -d @1753342057

Thu Jul 24 07:27:37 UTC 2025

6. Consulte a seção Como Coletar Arquivos Crashinfo, Coredump e Minidump do Secure Firewall? para baixar os arquivos crashinfo, minidump e core das etapas 4-5.



Caution: Não renomeie os arquivos core, crashinfo ou minidump.

---

7. Continue com as etapas em Troubleshooting de Procedimentos de Geração de Arquivos do Firepower para coletar arquivos show-tech e de solução de problemas:

7-A. Arquivo de show-tech do ASA.

7-B. Arquivo de solução de problemas do FTD.

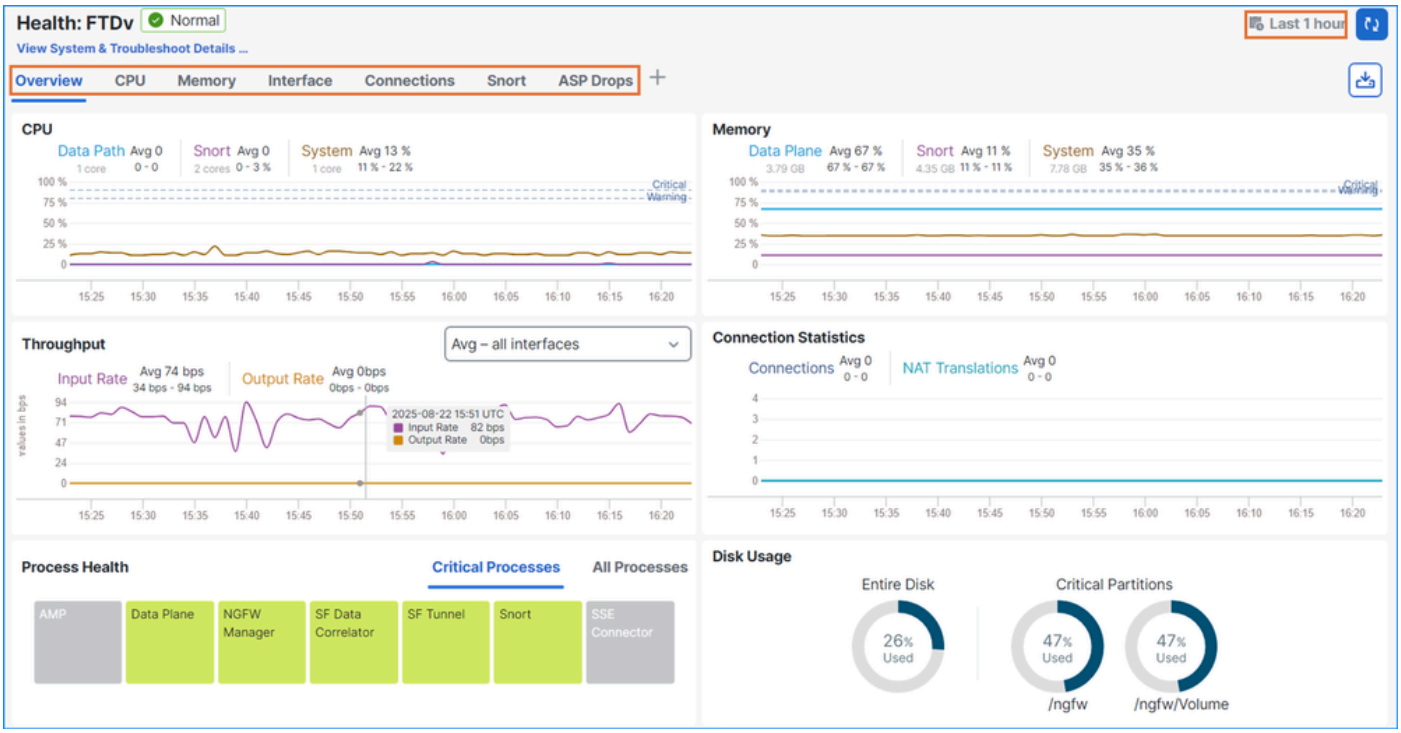
7-C. Arquivo show-tech do módulo de segurança Firepower 4100 e 9300.

7-D. Arquivo show-tech de chassi Firepower 4100 e 9300.

7-E. Arquivo show-tech de chassi Firepower 1000, 2100 e Secure Firewall 1200, 3100 e 4200. Os arquivos de solução de problemas de chassi do Secure Firewall 3100 e 4200 no modo de contêiner podem ser baixados através da opção FMC > Devices > [chassis] > 3 pontos > Troubleshoot Files.

8. No caso do DTF, recolher capturas de tela das guias de monitorização da saúde no CVP, abrangendo pelo menos 30 minutos antes do retorno de rastreamento. Assegurar-se de incluir as capturas de tela de todas as guias destacadas. No caso de retorno de rastreamento recorrente, recolher capturas de tela que cubram alguns incidentes.

Além disso, no caso de alta disponibilidade e clustering, colete capturas de tela para todas as unidades afetadas:



9. Colete as mensagens de syslog do mecanismo Lina bruto (não analisado) dos servidores syslog cobrindo pelo menos 30 minutos antes do retorno de rastreamento. O formato bruto é essencial para o processamento interno pelo TAC e ferramentas de engenharia.

No caso de um retorno de rastreamento recorrente, colete as mensagens brutas que cobrem alguns incidentes. Além disso, no caso de alta disponibilidade e clustering, colete syslogs brutos de todas as unidades afetadas.

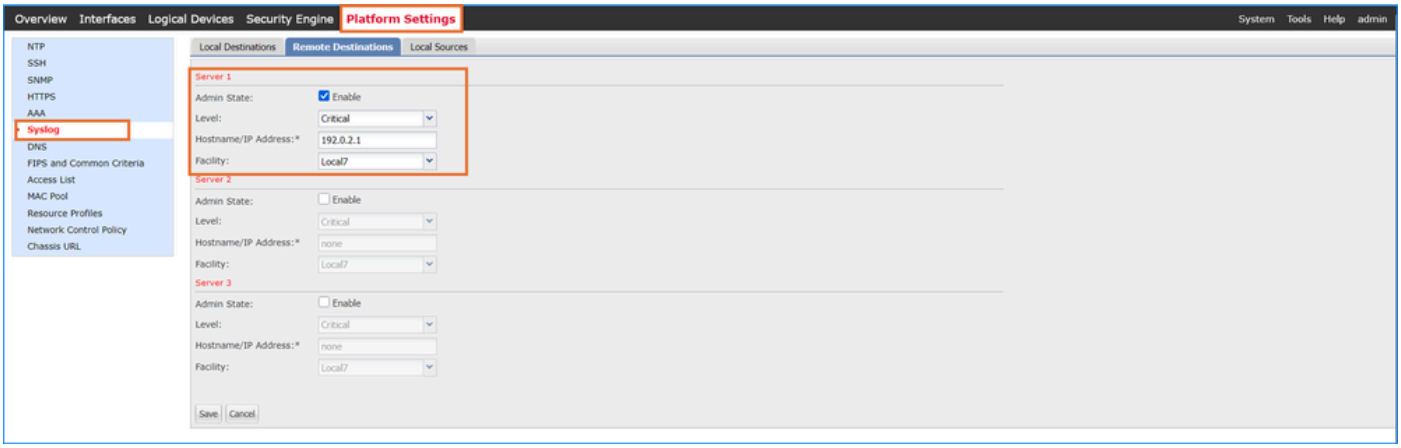
Verificação na CLI do ASA/FTD:

```
<#root>

ftd#

show run logging


logging enable
logging trap informational
logging host inside

192.0.2.1

<-- syslog server address
```

10. No caso do Firepower 4100 e 9300, colete mensagens FXOS brutas (não analisadas) de servidores syslog pelo menos 10 minutos antes do retorno de rastreamento. O formato bruto é essencial para o processamento interno pelo TAC e ferramentas de engenharia.

Além disso, no caso de alta disponibilidade e clustering, colete syslogs brutos de todos os chassis afetados.

Verificação da interface do usuário do Firepower Chassis Manager (FCM):



Verificação na CLI 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. Colete CPU, memória e dados de interface ASA ou FTD, incluindo interceptações, dos servidores SNMP configurados. Certifique-se de incluir dados que abranjam pelo menos 30 minutos antes do retorno de rastreamento.

Em caso de retorno de rastreamento recorrente, colete as mensagens brutas que cobrem alguns incidentes. Além disso, no caso de alta disponibilidade e clustering, colete mensagens brutas de todos os chassis afetados.

Verificação na CLI do ASA/FTD:

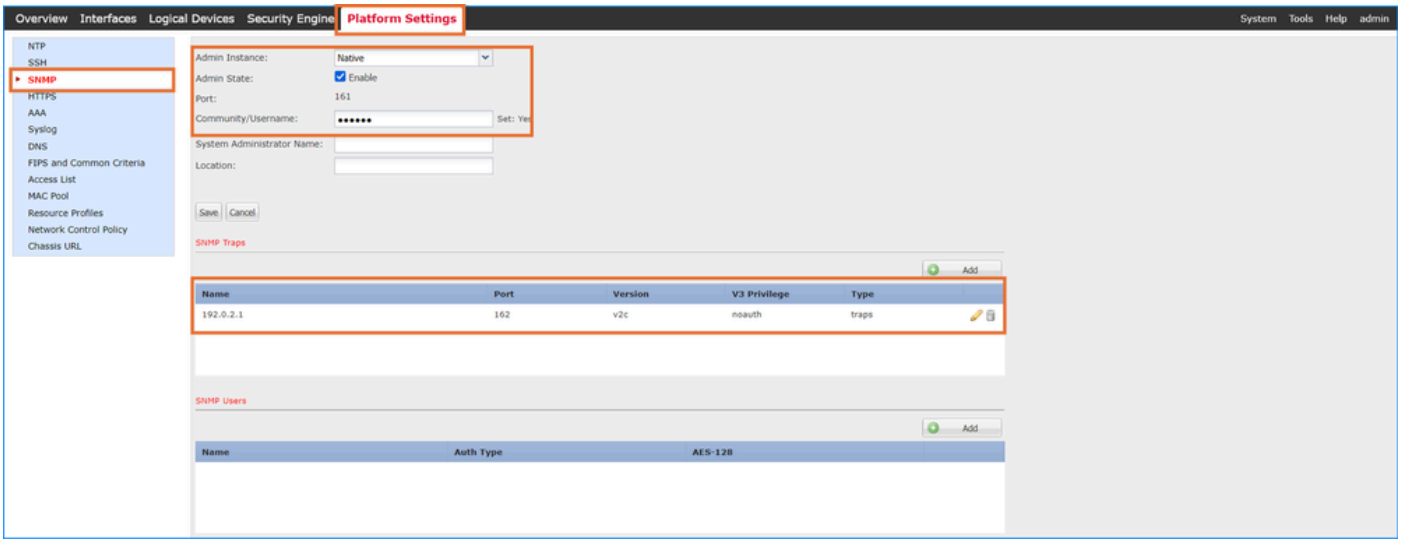
<#root>

```
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. No caso do Firepower 4100 e 9300, colete dados de CPU, memória e interface, incluindo interceptações, dos servidores SNMP configurados. Certifique-se de incluir dados que abranjam pelo menos 30 minutos antes do retorno de rastreamento.

Em caso de retorno de rastreamento recorrente, colete as mensagens brutas que cobrem alguns incidentes. Além disso, no caso de alta disponibilidade e clustering, colete mensagens brutas de todos os chassis afetados.

Verificação na interface do usuário do FCM:



Verificação na CLI 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. Colete o perfil de tráfego dos coletores do Netflow. Certifique-se de incluir dados que abranjam pelo menos 30 minutos antes do retorno de rastreamento.

Em caso de retorno de rastreamento recorrente, colete dados que abranjam alguns incidentes. Além disso, no caso de alta disponibilidade e clustering, colete dados de todos os chassis afetados.

Verificação na CLI do ASA/FTD:

<#root>

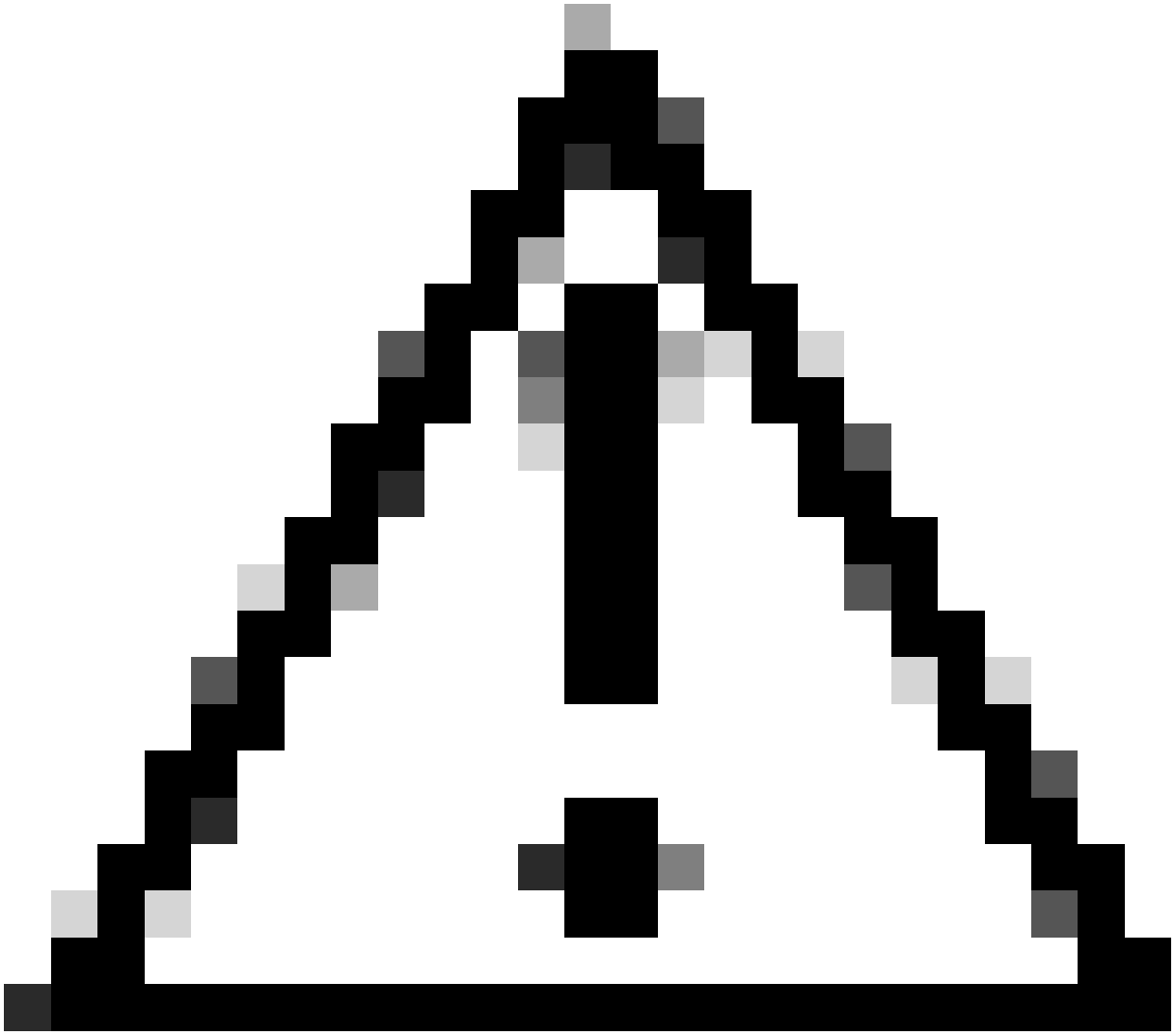
```
ftd#
show run flow-export


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. No caso de um retorno de rastreamento recorrente, colete a saída das sessões de console.

15. Abra um caso de TAC e forneça todos os dados.

Como coletar arquivos Crashinfo, Coredump e Minidump do Secure Firewall?

Continue com estas etapas: crashinfo, coredump e minidespejo de arquivos do Secure Firewall:



Caution: aviso: Não renomeie os arquivos core, crashinfo ou minidump.

ASA

Carregue arquivos da CLI do ASA para o servidor remoto:

<#root>

ASA#

copy flash:/crashinfo_lina.14664.20250813.205102 ?

```
  cluster:        Copy to cluster: file system
  disk0:          Copy to disk0: file system
  flash:          Copy to flash: file system
  ftp:            Copy to ftp: file system
  running-config  Update (merge with) current system configuration
  scp:            Copy to scp: file system
```

```
  smb:            Copy to smb: file system
  startup-config  Copy to startup configuration
  system:         Copy to system: file system
  tftp:           Copy to tftp: file system
```

FTD

Opção 1 - Coletar arquivos usando o Lina CLI

1. Se o servidor remoto estiver acessível a partir do mecanismo Lina, copie os arquivos para /mnt/disk0 e carregue os arquivos da CLI do 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 os arquivos do servidor remoto forem baixados, certifique-se de excluir os arquivos copiados de /mnt/disk0/ no FTD:

```
<#root>

admin@firepower:~$

cd /mnt/disk0/


admin@firepower:/mnt/disk0/:$

 sudo rm core.lina.11.13050.1755081050.gz
```

Opção 2 - Coletar arquivos usando a CLI do modo especialista

Usando clientes Linux TFTP, SFTP ou SCTP, carregue os arquivos do modo especialista para o servidor remoto:

```
<#root>

>

expert


admin@firepower:~$

cd /ngfw/var/data/cores/
```

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

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

Opção 3 - Coletar arquivos usando a CLI de gerenciamento local FXOS

No FTD de modo nativo em execução nos chassis Firepower 1000, 2100 e Secure Firewall 1200, 3100, 4200, os arquivos de núcleo e de minidespejo podem ser coletados na CLI de gerenciamento local 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
```

Opção 4 - Coletar arquivos usando a interface do usuário do FMC

Copie os arquivos para /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/

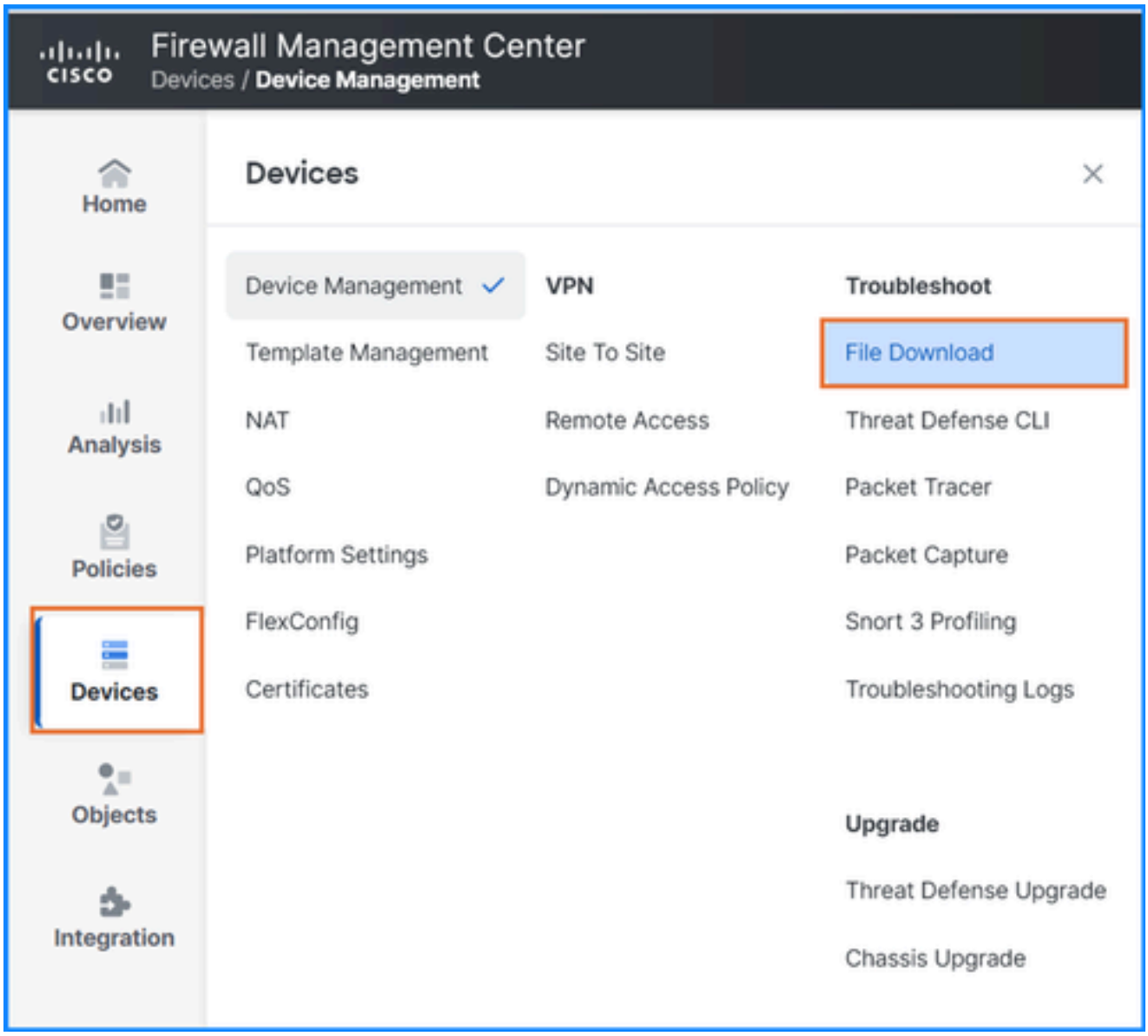
admin@firepower:~$

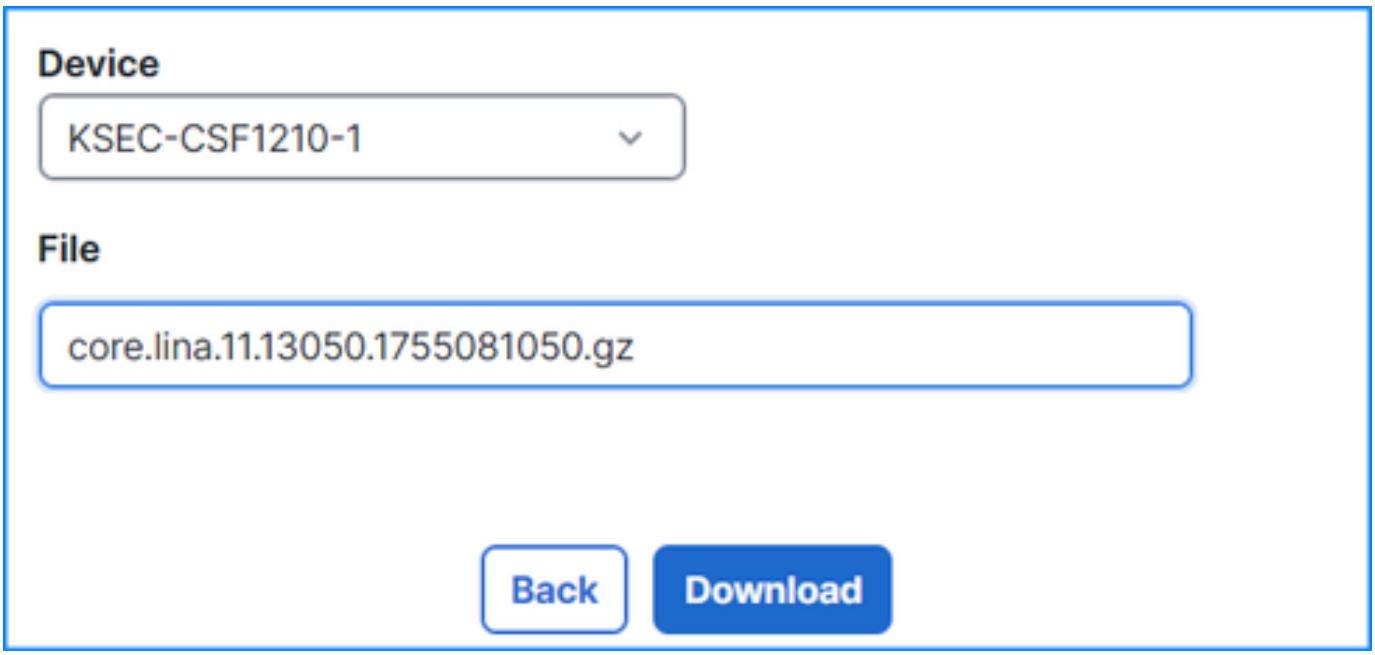
ls -l /ngfw/var/common/

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

core.lina.11.13050.1755081050.gz

2. Baixe o arquivo da interface do usuário do FMC usando a opção Devices > File Download:





3. Quando os arquivos do servidor remoto forem baixados, certifique-se de excluir os arquivos

copiados de /ngfw/var/common/ no FTD:

<#root>

admin@firepower:~$

cd

/ngfw/var/common/

admin@firepower:/mnt/disk0/:$

sudo rm core.lina.11.13050.1755081050.gz

Módulos de segurança Firepower 4100 e 9300

1. Conecte-se ao módulo e colete os arquivos do núcleo e de informação de travamento como parte do arquivo show-tech do módulo:

<#root>

firepower #

connect module 1 console

Firepower-module1>

support diagnostic

```
======= Diagnostic =======
1. Create default diagnostic archive
2. Manually create diagnostic archive
3. Exit

Please enter your choice:
```

2

```
=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

1

```
=== Add files to package | Manual Diagnostic ===
1. Platform Logs
```

```
2. Config Platform Logs
3. Crash Info files & Core dumps
4. Applications Logs
5. ASA Logs
b. Back to main menu

Please enter your choice:
```

3

```
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286  |
```

core.lina.11.13050.1755081050.gz

```
([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:
```

s

```
Type the partial name of the file to add ([*] for all, [<] to cancel)
>
```

core.lina.11.13050.1755081050.gz

```
core.lina.11.13050.1755081050.gz
Are you sure you want to add these files? (y/n)
```

y

```
=== Package Contents ===
[Added] core.lina.11.13050.1755081050.gz
========================
----------sub-dirs----------
lost+found
-----------files------------
2025-08-04 12:43:07 | 419619286  | core.lina.11.13050.1755081050.gz

([b] to go back or [m] for the menu or [s] to select files to add)
Type a sub-dir name to see its contents:
```

b

```
=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

2

```
=== Package Contents ===
core.lina.11.13050.1755081050.gz
```

```
========================

=== Manual Diagnostic ===
1. Add files to package
2. View files in package
3. Complete package
4. Exit.

Please enter your choice:
```

3

```
Creating Manual archive
Added file: core.lina.11.13050.1755081050.gz
```

Created archive file Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-module1>
```

support fileupload

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

1

```
-----------files------------
2025-08-04 13:17:50.723396 | 419624960  |
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
([s] to select files or [x] to Exit):
```

s

```
Type the partial name of the file to add, [<] to cancel
>
```

Firepower-Module1_08_04_2025_13_17_50.tar

```
Firepower-Module1_08_04_2025_13_17_50.tar
Are you sure you want to add these files? (y/n)
```

y

```
=== Package Contents ===
[Added] Firepower-Module1_08_04_2025_13_17_50.tar
=========================

Type the partial name of the file to add, [<] to cancel
>
```

<

```
Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status
Please enter your choice [x] to Exit:
```

2

```
1 : Firepower-Module1_08_04_2025_13_17_50.tar

Please choose from following:
================================
1. Archive Files
2. View selected files
3. Start upload and Exit
4. View transfer Status

Please enter your choice [x] to Exit:
```

3

Transfer of Firepower-Module1_08_04_2025_13_17_50.tar started.

```
Firepower-module1>
Firepower-module1>
Firepower-module1> ß
```

Shift + ~

```
telnet> quit
Connection closed.

firepower /ssa #
```

connect local-mgmt

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

dir workspace:/bladelog/blade-1/

```
1 152828400 Aug 04 13:26:35 2025
```

Firepower-Module1_08_04_2025_13_17_50.tar

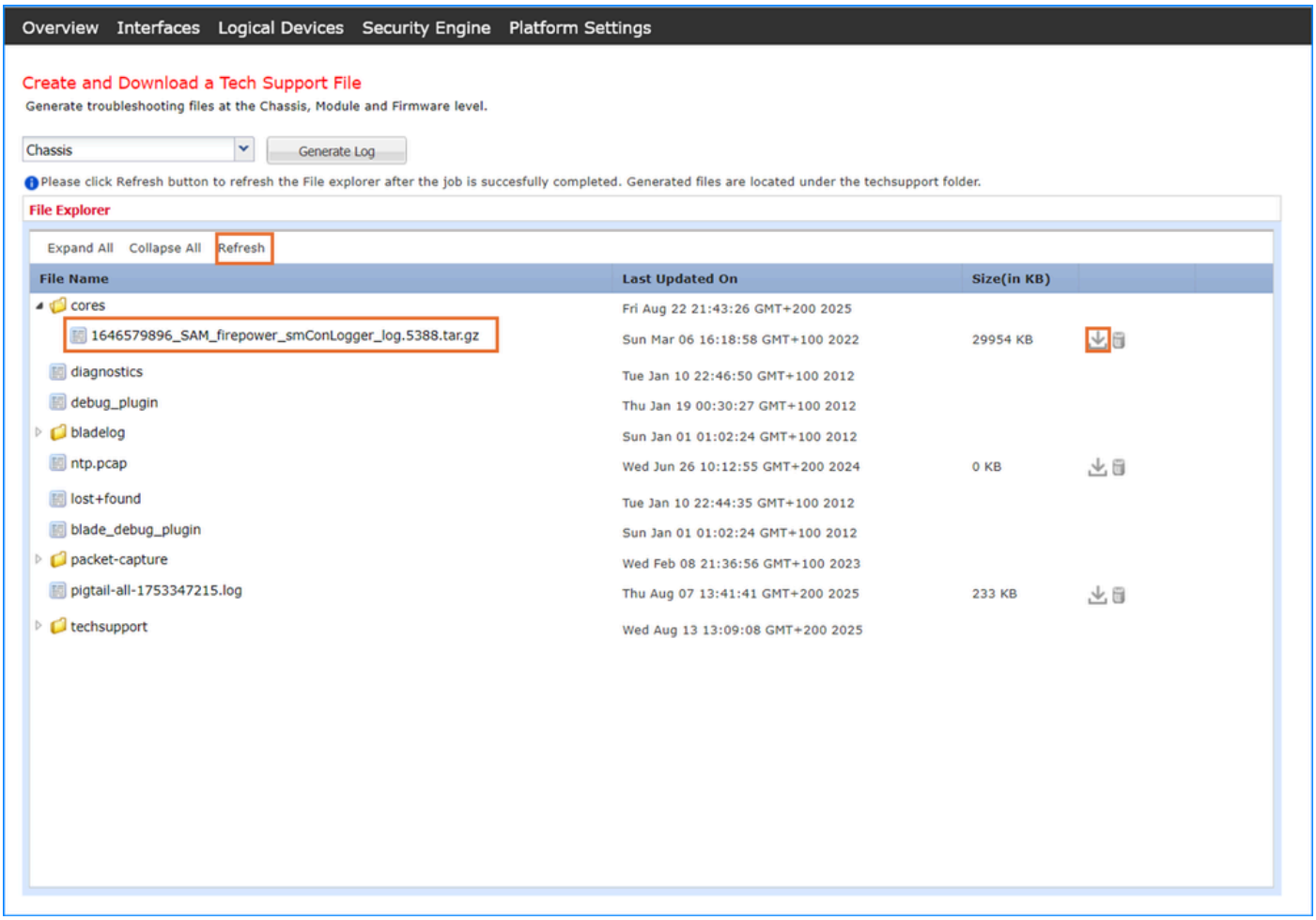
Chassis Firepower 4100 e 9300

1. Colete os arquivos principais usando a CLI de gerenciamento local 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. Como alternativa, colete arquivos da interface do usuário do FCM via Ferramentas > Logs de solução de problemas. Clique em Atualizar para atualizar a visualização do diretório de arquivos e o ícone de download ao lado do arquivo principal:



Referências

- Verificar versões do software Firepower
- Verificar a configuração do Firepower, da instância, da disponibilidade e da escalabilidade
- Solucionar problemas de procedimentos de geração de arquivos do Firepower
- Referência de comando do ASA

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.