

排除ASA或FTD意外重新加载故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[跨所有平台和逻辑设备检查的常见事项](#)

[确认设备（逻辑或机箱）已重新启动或已崩溃](#)

[在ASA SoftwareLina\(on FTD\)崩溃的情况下检查Crashinfo](#)

[ASA平台上要检查的内容](#)

[运行ASA映像的所有ASA平台](#)

[支持运行FTD映像的ASA平台](#)

[在Firepower平台上检查的事项](#)

[FP9300/FP4100 FXOS](#)

[在运行FTD的FP9300/FP4100上](#)

[在运行ASA的FP9300/FP4100上](#)

[在FP2100 FXOS/ASA/FTD上](#)

[在FP1000 FXOS/ASA/FTD上](#)

[下载核心文件](#)

[要检查的其他事项（特定于Firepower 4100和9300平台）](#)

[查看模块内的核心文件](#)

[与系统崩溃相关的已知漏洞](#)

简介

本文档介绍如何对Firepower威胁防御(FTD)或自适应安全设备(ASA)设备无明显原因重新加载的场景进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解Firepower和ASA硬件平台的基础知识
- 了解Firepower平台上的逻辑设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带ASA软件版本9.x的ASA 5500-X
- ASA 5500-X，搭配FTD软件版本6.2.3及更高版本
- 带ASA软件版本9.x的Firepower 1000、1100、2100、4100和9300系列
- 具有FTD软件版本6.2.3及更高版本的Firepower 1000、1100、2100、4100和9300系列

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。

背景信息

在本文档中，设备是指重新命名为Cisco安全防火墙的ASA或Firepower下一代防火墙(NGFW)，它们作为逻辑设备运行ASA或FTD映像。

思科安全防火墙包括各种硬件和软件版本。ASA系列包括5500-X系列防火墙，而Firepower系列包括FPR 1000、2100、4100和9300系列设备。本文档讨论从开始的方法，以便确定设备或软件在所有上述平台上崩溃的级别，以及崩溃是否真实。它还列出所有要收集的工件、在何处找到这些工件，以及如何使用它们来查找崩溃的根本原因。

跨所有平台和逻辑设备检查的常见事项

确认设备（逻辑或机箱）已重新启动或已崩溃

对于ASA，请在配置模式下使用命令以检查设备的正常运行时间：`# show version | in Up`

在Firepower硬件上，使用以下命令检查设备正常运行时间和机箱正常运行时间（FXOS级别）：

```
FP4100-3# connect fxos
FP4100-3(fxos)# show system uptime
```

```
System start time:          Thu Oct 31 22:50:09 2019
System uptime:              391 days, 19 hours, 30 minutes, 45 seconds
Kernel uptime:             391 days, 19 hours, 34 minutes, 34 seconds
Active supervisor uptime:  391 days, 19 hours, 30 minutes, 45 seconds
```



注：如果您观察到设备在问题发生后即启动，这将确认设备已重新启动。

检查并确认是否存在任何可能导致设备突然重新启动的电源相关问题。

如果正常运行时间与网络中断（或故障切换或设备离开集群）的时间戳无关，则意味着问题不会因设备重新加载而发生，并且诊断必须完全按照不同的方向导航。


在ASA SoftwareLina(on FTD)崩溃的情况下检查Crashinfo

系统崩溃是指系统检测到不可恢复的错误并且已重新启动自己的情况。当防火墙崩溃时，它会创建一个特殊的文本格式文件，称为 `crashinfo` 文件。此文件提供有助于确定崩溃根本原因分析的诊断信息和日志。对于ASA，`crashinfo` 文件是存储在中的纯文本 `Flash:` 并包含存储器寄存器内容和其他信息的长列表 — 软件版本、收集的数据等。

输入 `show crashinfo` 命令。您可以在任何文本编辑器中甚至在ASA控制台本身上查看输出。

```
show flash | in crash
```

在服务请求中与思科技术支持中心(TAC)共享此输出，他们可以使用内部工具对其进行解码。此输出提供了有关进程和线程的有用信息，可帮助开发人员查看崩溃并将它与设备内的其他事件关联。

 **注：**通常，当您收集 `show tech-support` 来自ASA或Lina的输出（在FTD上），`show crashinfo` 理想地存在于输出中。但是，与直接运行相比，输出多次不同或不完整 `show crashinfo` 命令。因此，建议始终输入 `show crashinfo` 命令。

除了要检查的常见细节外，还需要收集更多取决于可能发生崩溃的不同级别的信息和人为因素。在ASA平台上，只能发生单一级别的崩溃。但是，Firepower平台可能会出现逻辑设备（FTD或ASA软件）级崩溃或机箱级(FXOS)崩溃。

在正常运行时间确认设备已崩溃后，`coredump` 文件生成，思科TAC需要进一步审核。此 `coredump` 根据软件的哪个组件崩溃，文件可以有不同的类型。此 `coredump` 文件还会根据崩溃的组件保存到磁盘的不同目录/部分。

ASA平台上要检查的内容

ASA平台只有一个组件，可以是ASA或FTD。

运行ASA映像的所有ASA平台

此 `corefiles` 与崩溃相关的信息存储在内部闪存驱动器的 `disk0` 下。为了检查 `corefiles`，输入 `dir disk0:/coredumpfsys` 指令：

```
<#root>
```

```
ciscoasa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2021 sysdebug  
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core_lina.1227726922.258.11.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2021 lost+found
```

```
1 file(s) total size: 87580218 bytes
```

```
16106127360 bytes total (15749222400 bytes free/97% free)
```

输入 `show coredump filesystem` 命令，以便显示 `coredump` 文件系统，其中还显示磁盘空间。建议将 `coredump` 在方便时提交文件，因为后续文件可能会 `coredump` 可以删除之前的 `coredump(s)` 以适应当前的核心。

```
<#root>
```

```
ciscoasa# show coredump filesystem
```

```
Coredump Filesystem Size is 100 MB
```

```
Filesystem type is FAT for disk0
```

Filesystem	1k-blocks	Used	Available	Use%	Mounted on
/dev/loop0	102182	75240	26942	74%	/mnt/disk0/coredumpfsys

```
Directory of disk0:/coredumpfsys/
```

```
246 -rwx 20205386 19:16:44 Nov 26 2021
```

```
core_lina.1227726922.258.11.gz
```

```
247 -rwx 36707919 19:21:56 Nov 26 2021
```

```
core_lina.1227727222.258.6.gz
```

```
248 -rwx 20130838 19:26:36 Nov 26 2021
```

```
core_lina.1227727518.258.11.gz
```

如果您没有看到 `coredump` 文件 `disk0`，则极可能会 `coredump` 未启用，这意味着无法针对此事件完成审阅。为了启用 `coredump` 对于将来出现的情况，请输入以下命令：

```
ciscoasa(config)#coredump enable
```

```
WARNING: Enabling coredump on an ASA5505 platform will delay the reload of the system in the event of software forced reload. The exact time depends on the size of the coredump generated.
```

```
Proceed with coredump filesystem allocation of 60 MB  
on 'disk0:' (Note this may take a while) ? [confirm]
```

```
Making coredump file system image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Coredump file system image created & mounted successfully
```

```
/dev/loop0 on /mnt/disk0/coredumpfsys type vfat
(rw, fmask=0022, dmask=0022, codepage=cp437, iocharset=iso8859-1)
```

支持运行FTD映像的ASA平台

ASA平台5506-X、ASA 5508-X、ASA 5512-X、ASA 5515-X、ASA 5516-X、ASA 5525-X、ASA 5545-X和ASA 5555-X支持运行FTD映像，并使其成为下一代防火墙。

在运行FTD映像的所有这些受支持的ASA平台上，corefiles 位于 /var/data/cores 或 /ngfw/var/data/cores 通过专家模式。它们也镜像在 disk0:/coredumpfsys Lina闪存的目录。

```
<#root>
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 59660
-rw-r--r-- 1 root root 4815651 Mar 14 17:07
core.SFDataCorrelato.2035.1552608478.gz

-rw-r--r-- 1 root root 56198339 Mar 14 16:47
core.lina.2113.1552607243.gz
```

```
root@firepower:/var/data/cores#
```

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/

2498562 -rw- 56198339 23:47:26 Mar 14 2019
core.lina.2113.1552607243.gz

2498563 -rw- 4815651 00:07:58 Mar 15 2019
core.SFDataCorrelato.2035.1552608478.gz
```

```
2 file(s) total size: 61013990 bytes
42949672960 bytes total (39523602432 bytes free/92% free)
```

在Firepower平台上检查的事项

Firepower平台带有两个软件组件。第一个是FXOS，即机箱操作系统，第二个是应用实例，也称为逻辑设备，可以是ASA或FTD。因此，必须确定发生故障的部件，以便确定下载的位置 corefiles

如果Firepower 1000/2000/4100和9300上的应用实例崩溃，则崩溃信息和 `corefiles` 始终默认生成。但是，在某些情况下，可以禁用核心转储。

要检查4100/9300上是否启用了核心转储，请输入以下命令：

```
connect module 1 console
Firepower-module1>show platform core dumps
```

启用或禁用Firepower模块核心转储：

在Firepower模块上启用核心转储，以便在系统崩溃时帮助排除故障，或者根据请求发送至Cisco TAC。

```
Firepower# connect module 1 console
show coredump detail
```

命令输出显示当前核心转储状态信息，包括是否启用核心转储压缩。

```
<#root>
```

```
Firepower-module1>
```

```
show coredump detail
```

```
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

请使用 `config coredump` 命令，以便启用或禁用核心转储，以及在崩溃期间启用或禁用核心转储压缩。

- 输入 `config coredump enable` 命令，以便在崩溃期间创建核心转储。
- 输入 `config coredump disable` 命令，以便在崩溃期间禁用核心转储创建。
- 输入 `config coredump compress enable` 命令以启用核心转储压缩。
- 输入 `config coredump compress disable` 命令可禁用核心转储压缩。

此示例说明如何启用核心转储：


```
<#root>
```

```
Firepower-module1>
```

```
config coredump enable
```

```
Coredump enabled successfully.
```

```
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system failure. Are you
y
Firepower-module1>
```

 **注意：**核心转储文件会占用磁盘空间，如果空间不足且未启用压缩，则即使启用了核心转储也不会保存核心转储文件。

必须上传崩溃文件和核心文件才能进行完整分析，因为崩溃文件可能不包含所有数据。

FP9300/FP4100 FXOS

在FP9300/FP4100上，FXOS `corefiles` 位于 `local-mgmt cores` 目录。

```
firepower-4110# connect local-mgmt
firepower-4110(local-mgmt)# dir cores

1 9337521 Apr 30 11:28:15 2016 1462040896_0x101_snm_log.5289.tar.gz
1 1067736 Oct 09 10:38:49 2017 1507570679_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 798663 Oct 10 18:05:54 2017 1507683913_firepower-4110_BC01_MEZZ0101_mcp_log.122.tar.gz
1 348160 Feb 11 23:53:25 2019 core.21845

Usage for workspace://
3999125504 bytes total
64200704 bytes used
3730071552 bytes free
firepower-4110(local-mgmt)#
```

要将核心文件从FXOS复制到本地计算机，请输入以下命令：

```
firepower-4110(local-mgmt)# copy workspace:/cores:<file>.tar.gz scp://username@x.x.x.x
```

在运行FTD的FP9300/FP4100上

在运行FTD的FP9300/FP4100上，`corefiles` 位于 `/var/data/cores` 或 `/ngfw/var/data/cores` 通过专家模式。它们也镜像在 `disk0:/coredumpfsys Lina` 闪存的目录。

```
root@firepower:/var/data/cores# ls -l
total 59660
-rw-r--r-- 1 root root 4815651 Mar 14 17:07 core.SFDataCorrelato.2035.1552608478.gz
-rw-r--r-- 1 root root 56198339 Mar 14 16:47 core.lina.2113.1552607243.gz
root@firepower:/var/data/cores#
```

```
firepower# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/

2498562 -rw- 56198339 23:47:26 Mar 14 2019 core.lina.2113.1552607243.gz
2498563 -rw- 4815651 00:07:58 Mar 15 2019 core.SFDataCorrelato.2035.1552608478.gz

2 file(s) total size: 61013990 bytes
42949672960 bytes total (39523602432 bytes free/92% free)
```

在运行ASA的FP9300/FP4100上

在运行ASA的FP9300/FP4100上，corefiles 位于 disk0:/coredumpfsys 目录。

```
<#root>
```

```
asa#
```

```
dir disk0:/coredumpfsys
```

```
Directory of disk0:/coredumpfsys/

11 drwx 16384 17:34:50 Sep 10 2018 lost+found
12 -rw- 317600388 16:43:40 Mar 14 2019
   core.lina.6320.1552607012.gz
```

```
1 file(s) total size: 317600388 bytes
21476089856 bytes total (21255872512 bytes free/98% free)
```

在FP2100 FXOS/ASA/FTD上

在FP2100 FXOS/ASA/FTD上，corefiles 位于 local-mgmt cores 目录使用ASA还是FTD。在FTD中，它们也在 /ngfw/var/data/cores (或 /var/data/cores)和 /ngfw/var/common/ 通过专家模式。但请注意，FP2100平台没有 disk0:/coredumpfsys 目录。

 注意：提交Cisco Bug ID [CSCvh01912](#)是为了使FP2100与FP9300/4100平台保持一致。在解决此问题之前，请使用所描述的位置查找 corefiles。

当FTD位于Firepower 2100、1000、ASA设备和ISA 3000设备时，Firepower核心文件的位置：

对于所有这些平台，请使用此过程来查找与所有Firepower进程相关的核心文件。

低于 /ngfw/var/common/:

1.通过SSH或控制台连接到设备的CLI。

2.输入此模式作为专家模式：

```
> expert
admin@firepower:~$
```

3.成为根用户。

```
<#root>
admin@firepower:~$
sudo su
Password:
root@firepower:/home/admin#
```

4.导航至 `/ngfw/var/common/` 文件夹，核心文件所在的位置。

```
root@firepower:/home/admin# cd /ngfw/var/common/
```

5.检查文件夹中的文件。

```
root@firepower:/ngfw/var/common# ls -l | grep -i core
total 21616
-rw-r--r-- 1 root root 22130788 Nov  6  2020 process.core.tar.gz
```

FP2100上的FTD：不足 `/ngfw/var/data/cores:`

```
> expert
admin@firepower:~$ sudo su
[cut]
root@firepower:/home/admin# ls -l /ngfw/var/data/cores
total 133740
-rw-r--r-- 1 root root 4761622 Jun  4 05:13 core.SFDataCorrelato.28634.1622783636.gz
-rw-r--r-- 1 root root 132014190 Jun  4 05:17 core.lina.11.1378.1622783800.gz
drwx----- 2 root root 16384 Nov  5 2019 lost+found
drwxr-xr-x 3 root root 4096 Nov  5 2019 sysdebug
```

```
> connect fxos
[cut]
firepower# connect local-mgmt
firepower(local-mgmt)# dir cores
```

```
1 4761622 Jun 04 05:13:56 2021 core.SFDataCorrelato.28634.1622783636.gz
1 132014190 Jun 04 05:17:25 2021 core.lina.11.1378.1622783800.gz
2 16384 Nov 05 22:35:15 2019 lost+found/
3 4096 Nov 05 22:36:05 2019 sysdebug/
```

```
Usage for workspace://
85963259904 bytes total
15324155904 bytes used
70639104000 bytes free
firepower(local-mgmt)#
```

FP2100上的ASA:

```
firepower-2110(local-mgmt)# dir cores
```

```
1 167408075 Jul 04 00:43:25 2018 core.lina.6.2025.1530657764.gz
2 16384 Mar 28 16:17:56 2018 lost+found/
3 4096 Mar 28 16:18:43 2018 sysdebug/
```



注意：FXOS corefiles 存储在connect的相同cores目录下 local-mgmt.

在FP1000 FXOS/ASA/FTD上

在FP1000 FXOS/ASA/FTD上，此过程与FP2100类似。此外，disk0:/coredumpfsys 目录位于Lina侧。

FP1000的FTD:

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
```

```
FP1010> ena
Password:
FP1010# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
13 -rw- 86493184 19:59:39 Jun 03 2021 core.lina.18707.1622750370.gz
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
14 -rw- 4770749 20:19:24 Jun 03 2021 core.SFDataCorrelato.7098.1622751564.gz
12 -rw- 197689 23:01:08 May 19 2021 core.top.6163.1621465268.gz
16 -rw- 4752067 20:28:03 Jun 03 2021 core.SFDataCorrelato.28195.1622752083.gz
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
15 -rw- 5048839 20:20:32 Jun 03 2021 core.SFDataCorrelato.18952.1622751632.gz
```

```
5 file(s) total size: 101262528 bytes
123418959872 bytes total (110302621696 bytes free/89% free)
```

```
> connect fxos
[cut]
```

```
FP1010# connect local-mgmt
FP1010(local-mgmt)# dir cores
```

```
1 5048839 Jun 03 20:20:32 2021 core.SFDataCorrelato.18952.1622751632.gz
1 4752067 Jun 03 20:28:03 2021 core.SFDataCorrelato.28195.1622752083.gz
1 4770749 Jun 03 20:19:24 2021 core.SFDataCorrelato.7098.1622751564.gz
1 86493184 Jun 03 19:59:39 2021 core.lina.18707.1622750370.gz
1 197689 May 19 23:01:08 2021 core.top.6163.1621465268.gz
2 16384 Aug 30 23:13:37 2019 lost+found/
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://
159926181888 bytes total
17475063808 bytes used
142451118080 bytes free
```

```
> expert
admin@FP1010:~$ sudo su
Password:
root@FP1010:/home/admin# ls -l /var/data/cores
total 99048
-rw-r--r-- 1 root root 5048839 Jun 3 20:20 core.SFDataCorrelato.18952.1622751632.gz
-rw-r--r-- 1 root root 4752067 Jun 3 20:28 core.SFDataCorrelato.28195.1622752083.gz
-rw-r--r-- 1 root root 4770749 Jun 3 20:19 core.SFDataCorrelato.7098.1622751564.gz
-rw-r--r-- 1 root root 86493184 Jun 3 19:59 core.lina.18707.1622750370.gz
-rw-r--r-- 1 root root 197689 May 19 23:01 core.top.6163.1621465268.gz
drwx----- 2 root root 16384 Aug 30 2019 lost+found
drwxr-xr-x 3 root root 4096 Aug 30 2019 sysdebug
```

FP1000上的ASA:

```
<#root>
```

```
ciscoasa# dir disk0:/coredumpfsys
Directory of disk0:/coredumpfsys/
```

```
1071057 drwx 4096 23:14:58 Aug 30 2019 sysdebug
12 -rw- 87580218 04:49:23 Jun 04 2021
```

```
core.lina.27515.1622782155.gz
```

```
11 drwx 16384 23:13:37 Aug 30 2019 lost+found
```

```
1 file(s) total size: 87580218 bytes
16106127360 bytes total (15749222400 bytes free/97% free)
```

```
ciscoasa#
```

```
connect fxos
```

```
[cut]
```

```
FP1010#
```

```
connect local-mgmt
```

```
FP1010(local-mgmt)#
```

```
dir cores
```


```
1 87580218 Jun 04 04:49:23 2021
```

```
core.lina.27515.1622782155.gz
```

```
2 16384 Aug 30 23:13:37 2019 lost+found/
```

```
3 4096 Aug 30 23:14:58 2019 sysdebug/
```

```
Usage for workspace://  
159926181888 bytes total  
5209071616 bytes used  
154717110272 bytes free
```

 注:FXOS corefiles 在连接时存储在同一个cores目录下 local-mgmt.

下载核心文件

有一个 copy 命令下 connect local-mgmt 和Lina/ASA CLI。对于FTD专家模式，请使用 scp 命令。

要检查的其他事项（特定于Firepower 4100和9300平台）

检查 show pmon state 命令下 local-mgmt 在FXOS上。此示例显示当没有进程崩溃时的期望输出。此输出不仅捕获设备级崩溃，还捕获接口模块/DME崩溃等。

```
<#root>
```

```
fp1120-v-1(local-mgmt)#
```

```
show pmon state
```

SERVICE NAME	STATE	RETRY(MAX)	EXITCODE	SIGNAL	CORE
-----	-----	-----	-----	-----	-----
svc_sam_dme	running	0(4)	0	0	no
svc_sam_dcosAG	running	0(4)	0	0	no
svc_sam_portAG	running	0(4)	0	0	no
svc_sam_statsAG	running	0(4)	0	0	no
httpd.sh	running	0(4)	0	0	no
svc_sam_sessionmgrAG	running	0(4)	0	0	no
sam_core_mon	running	0(4)	0	0	no
svc_sam_svcmonAG	running	0(4)	0	0	no
svc_sam_serviceOrchAG	running	0(4)	0	0	no
svc_sam_appAG	running	0(4)	0	0	no
svc_sam_envAG	running	0(4)	0	0	no

如果在相关的FTD/ASA目录中找不到任何核心文件，则核心文件可以存在于4100/9300上的bootCLI中。

查看模块内的核心文件

输入以下命令以连接到模块控制台：

```
<#root>
```

```
/ssa # connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
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: Transient_Core_Files
```

```
-----files-----
[No files]
([b] to go back)
Type a sub-dir name to list its contents: b
```

```
=====
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-----
2017-03-20 20:45:06 | 40639151 | core.lina.48857.1490042695.gz
2017-03-20 20:48:47 | 40638054 | core.lina.18113.1490042915.gz
2017-03-20 20:52:28 | 40638186 | core.lina.18112.1490043137.gz
2017-03-20 20:56:10 | 40638466 | core.lina.18123.1490043359.gz
```

```

2017-03-20 20:59:53 | 40638345 | core.lina.18262.1490043582.gz
2017-03-20 21:03:35 | 40638120 | core.lina.18476.1490043803.gz
2017-03-20 21:07:22 | 40638335 | core.lina.18529.1490044031.gz ([b] to go back)
Type a sub-dir name to list its contents: b =====
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: x
Firepower-module1>

```

如果bootCLI中没有核心文件，则可以检查FXOS级别的日志：

```

connect fxos
1-(fxos)# show logging onboard obfl-logs
2-(fxos)# show logging onboard stack-trace
3-(fxos)# show logging onboard kernel-trace
4-(fxos)# show logging onboard exception-log
5-(fxos)# show logging onboard internal kernel
6-(fxos)# show logging onboard internal platform
7-(fxos)#show logging onboard internal kernel | no-more
8-(fxos)#show logging onboard internal kernel-big | no-more
9-(fxos)#show logging onboard internal platform | no-more
10-(fxos)#show logging onboard internal reset-reason | no-more

```

If logging at fxos level is enabled, you can check the logs on fxos.
It contains the syslog buffer and OBFL logs stored in NVRAM

```

Connect fxos
show logging log -----This is a non-persistent syslog buffer
show logging onboard obfl-logs -----Non-volatile storage for history of boot up and reset occurrences.
show logging nvram -----Non-volatile storage for critical logs.Important for historical is

```

On FXOS CLI, at the top-level scope use following command.

```
show fault detail or show fault
```

If you want to view faults for a specific object, scope to that object and then enter the show fault command.

You can check for audit-logs which is a persistent store of user operations.

This moreover stores the sequence of user operations done.

```

firepower# scope security
firepower# /security # show audit-logs

```

有时，设备以静默方式崩溃，不会生成任何崩溃或核心文件。在这种情况下，您可以检查日志：

```

At FTD instance or device level:
#####

```

Navigate to the /ngfw/var/log or /var/log and open the messages log file. Check all the logs generated.
You can search for following messages (in /ngfw/var/log or /var/log) to confirm if device rebooted with:

```
firepower shutdown[2313]: shutting down for system reboot
Stopping Cisco Firepower 2130 Threat Defense
pm:process [INFO] Begin Process Shutdown
```

Check for syslog messages (specific to device up and down) generated when the device rebooted.
You can check for syslog messages generated 15-30 min before and after the device reboot to know if:

与系统崩溃相关的已知漏洞

有关系统崩溃的其他信息，请参阅以下页面：

- Cisco Bug ID [CSCvu84127](#) - FTD静默崩溃，不生成核心或崩溃文件
- Cisco Bug ID [CSCwa35845](#) - ASA 5516重新加载，生成核心文件
- Cisco Bug ID [CSCvw99444](#) - FTD与 `crashinfo/corefile`
- Cisco Bug ID [CSCvv86926](#) - FTD崩溃生成 `crashfile`
- 思科漏洞ID [CSCvp16482](#) - ASA崩溃生成核心文件
- Cisco Bug ID [CSCvm53545](#) - ASA可以回溯和重新加载，无需生成 `crashinfo` 文件

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）。