对意外安全防火墙和Firepower重新启动进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

缩写

背景信息

故障排除工作流程

故障排除步骤

- 在本地模式下运行FTD或运行ASA的Firepower 1000、2100、安全防火墙1200、3100和4200
- 在容器模式下运行FTD的安全防火墙3100、4200
- Firepower 4100/9300
- 运行FTD的虚拟平台
- 在本地模式下运行FTD或运行ASA的Firepower 4100/9300安全模块
- 在容器模式下运行FTD的Firepower 4100/9300安全模块

分析正常运行时间

分析FTD消息文件

分析安全模块或机箱消息文件

分析ssp-pm.log文件

分析ssp-shutdown.log文件

分析机箱重置原因

分析硬件错误或异常

分析其他平台日志文件

分析SEL/OBFL文件

分析ASA/FTD控制台日志

分析电源电压和电源问题

参考

简介

本文档介绍意外重新加载安全防火墙/Firepower防火墙的故障排除步骤。

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

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。

缩写

缩写	说明
FXOS	Firepower可扩展操作系统：在Firepower 1000、2100、3100、4100、4200和9300平台上运行的底层操作系统。
应用	任何在FXOS平台（ASA或安全防火墙威胁防御）上运行的应用。
SSP	安全服务平台：此术语是指运行FXOS的思科安全硬件平台。
OBFL	板载故障记录：存储故障相关数据的日志文件；例如，内存错误、总线错误、中断。该文件位于CIMC中。
CMC	机箱管理控制器。
CIMC	思科集成管理控制器。

SEL	系统事件日志(SEL):系统事件日志驻留在NVRAM中安全模块的CIMC上。
PSU	电源设备。
PDU	配电装置。
PECI	平台环境控制接口总线：这是主板管理控制器(BMC)与CPU和平台控制器集线器(PCH)之间的总线。PECI用于从CPU、DIMM等收集数据。
BMC	主板管理控制器。
NPU	网络处理器单元。
FPGA	现场可编程门阵列。
SAM	FXOS管理是提供机箱管理功能的进程集合，也统称为SAM（服务器阵列管理器）。
ECC	纠错码内存是一种计算机内存，能检测和纠正存储或检索数据时的错误。
PCIe	PCI Express、外围组件互联Express。
PBTN（电源按钮）：	PBTN表示按物理电源按钮。

背景信息

在本文档中，“reboot”、“reload”和“restart”可互换使用。从用户的角度来看，意外重启大致可定义为任何重启，但以下几种情况除外，这些情况是众所周知的、有文档记录的或预期的：

1. 由于软件安装或升级而重新启动。
2. 由于用户触发的操作(例如从命令行界面(CLI)重新启动、图形用户界面(UI)或手动关闭/打开操作)而重新启动。

根据触发器，重新启动可以是正常的，也可以是不正常的：

1. 平稳重启通常是指重新启动系统、设备或服务，使所有当前进程能够正确完成，并在重启之前保存所有文件或数据。这有助于避免数据丢失或损坏。正常重启的示例包括：
    - 由于软件安装或升级而重新启动。
    - 由于用户触发的操作（例如从CLI或GUI重新启动）而重新启动。
    - 在某些情况下，需要软件回溯。

---

2. 不平稳重启与平稳重启相反，当系统不平稳重启时，即没有平稳地终止进程。不正常的重新启动可能会导致数据丢失或损坏。触发器的示例包括：
    - 通过断开所有电源线或切换电源按钮意外关闭和打开电源。
    - 电源短缺，机箱电源设备出现问题。
    - 硬件、FPGA、环境等方面的各种问题，会导致突然重启。

重新启动的常见原因：

- 用户从CLI或管理UI执行的操作。
- 软件升级或降级。
- 软件回溯。
- 由操作系统/系统关键进程出于软件中回溯以外的原因触发。
- 硬件问题，例如SSD损坏、内存错误、CPU异常、内部FPGA等。
- 环境问题，例如断电、过热等。
- 第三方组件中的软件缺陷或其他问题。
- 磁盘空间使用率较高。

在基于机箱的平台中，必须考虑重新引导的范围，特别是重新引导的具体内容：

- ASA/FTD应用。
- 安全模块(Firepower 4100/9300)。
- 机箱

默认行为包括：

- 如果在本地模式下运行的FTD上重新启动，则触发Firepower 1000/2100上的ASA或安全防火墙3100/4200;机箱也会重新启动。
- 如果在本地模式下运行的FTD、Firepower 4100/9300上的ASA或安全模块上触发重启，安全模块也会重启。机箱不受影响。
- 如果在Firepower 4100/9300安全模块上触发FTD多实例模式重新启动，则只有该实例重新启动，安全模块和机箱不会受到影响。
- 如果在安全防火墙3100和4200上触发FTD多实例模式重新启动，则只有该实例重新启动，机箱不受影响。

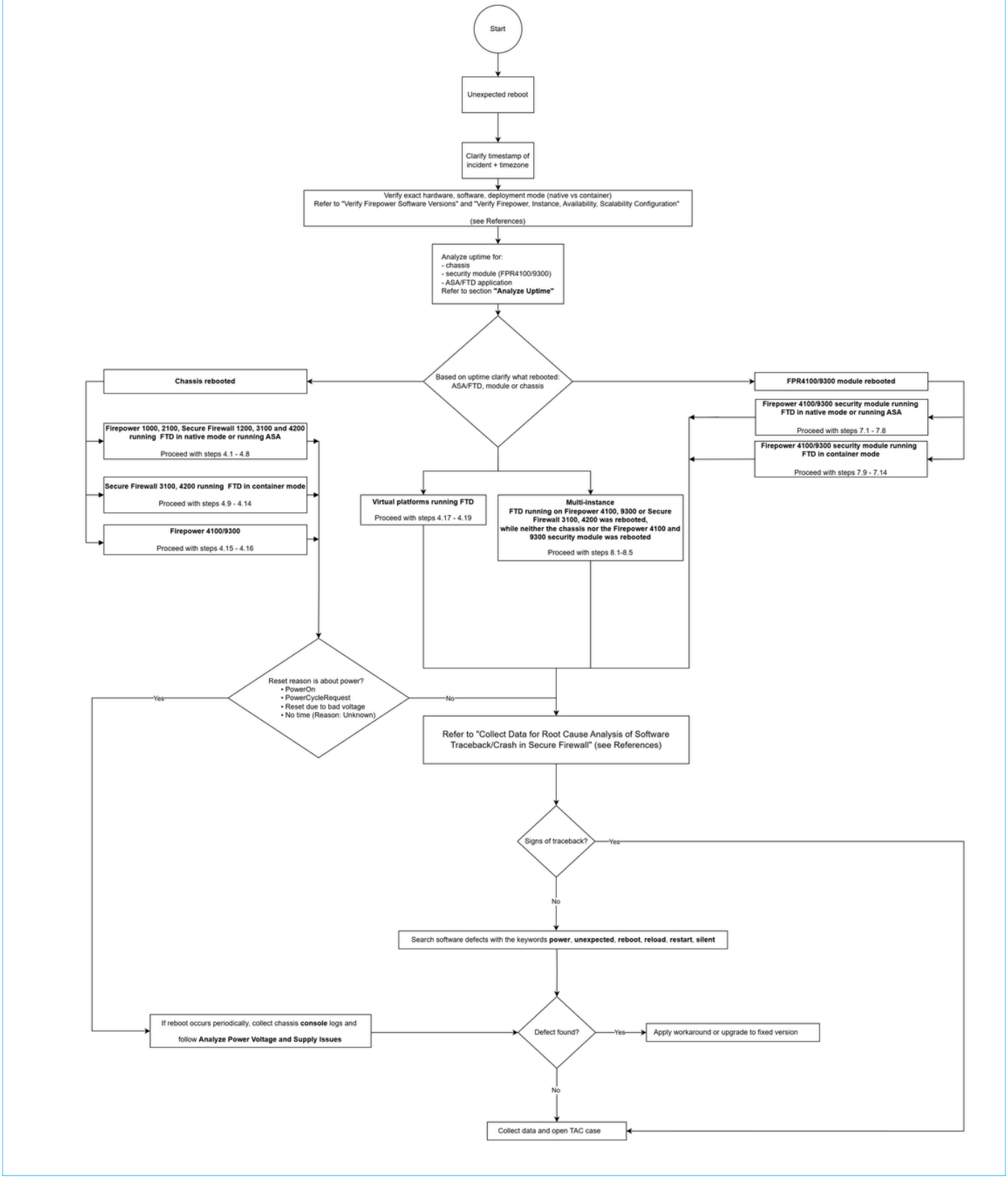
- Firepower 4100/9300安全模块上的重新启动也会重新启动，受影响的模块上运行的所有应用程序与本机多实例模式无关。
- 在机箱上重新启动也会重新启动所有安全模块和所有应用。

某些关键进程的终止（无论是正常还是不正常）都可能导致重新启动。例如：

- 如果数据平面进程(也称为lina)因回溯而终止，防火墙将重新启动。例外是ASA 9.20(x)和FTD 7.4.1中为特定平台引入了“数据平面快速重新加载”功能的软件版本。
- 如果进程管理器pm终止，防火墙将重新启动。

故障排除工作流程

查看参考故障排除步骤的故障排除工作流程：



故障排除步骤

1. 尽可能准确地记录事件时间戳，确保考虑时区。

2. 验证确切的硬件，保护防火墙软件类型（ASA或FTD）、软件版本和部署模式（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、验证Firepower、实例、可用性、可扩展性配置。

3. 请参阅分析运行时间部分，以关联ASA/FTD应用、安全模块（仅限Firepower 4100/9300）和机箱的运行时间。目标是明确重新启动范围、应用、安全模块或机箱。
4. 如果机箱已重新启动，请继续执行以下步骤：

在本地模式下运行FTD或运行ASA的Firepower 1000、2100、安全防火墙1200、3100和4200

4.1.检查分析FTD消息文件部分（仅限FTD）。

4.2.检查分析ssp-pm.log文件部分。

4.3.检查分析ssp-shutdown.log文件部分。

4.4.检查分析ASA/FTD控制台日志部分。

4.5.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

4.6.检查分析机箱重置原因部分。

4.7.检查分析硬件错误或例外部分。

4.8.检查分析平台日志文件部分。

在容器模式下运行FTD的安全防火墙3100、4200

4.9.检查分析ssp-pm.log文件部分。

4.10.检查分析ssp-shutdown.log文件部分。

4.11.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

4.12.检查分析机箱重置原因部分。

4.13.检查分析硬件错误或例外部分。

4.14.检查分析平台日志文件部分。

Firepower 4100/9300

4.15.检查分析机箱重置原因部分。

4.16.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

运行FTD的虚拟平台

4.17.检查分析FTD消息文件部分。

4.18.检查分析ASA/FTD控制台日志部分。

4.19.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

---

5. 如果在分析机箱重置原因部分找到诸如此类的重置原因，请参阅分析电源电压和电源问题:

- 开机
- PowerCycleRequest
- 由于电压不正常而重置
- 没有时间(原因：未知)

---

6. 如果机箱重新启动是重复进行的，请收集控制台日志。

7. 如果重新启动安全模块，请对Firepower 4100/9300执行以下步骤：

在本地模式下运行FTD或运行ASA的Firepower 4100/9300安全模块

7.1.检查分析FTD消息文件部分（仅限FTD）。

7.2.检查分析ssp-pm.log文件部分。

7.3.检查分析ssp-shutdown.log文件部分。

7.4.检查分析ASA/FTD控制台日志部分。

7.5.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

7.6.检查分析硬件错误或例外部分。

7.7.检查分析SEL/OBFL文件部分。

7.8.检查分析平台日志文件部分。

在容器模式下运行FTD的Firepower 4100/9300安全模块

7.9. 检查分析ssp-pm.log文件部分。

7.10.检查分析ssp-shutdown.log文件部分。

7.11.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

7.12.检查分析硬件错误或例外部分。

7.13.检查分析SEL/OBFL文件部分。

7.14.检查分析平台日志文件部分。

---

8. 如果重新引导了在Firepower 4100、9300或安全防火墙3100、4200上运行的多实例FTD，但

机箱和Firepower 4100及9300安全模块均未重新启动，请继续执行以下步骤：

8.1.检查分析FTD消息文件部分。

8.2.检查分析ssp-pm.log文件部分。

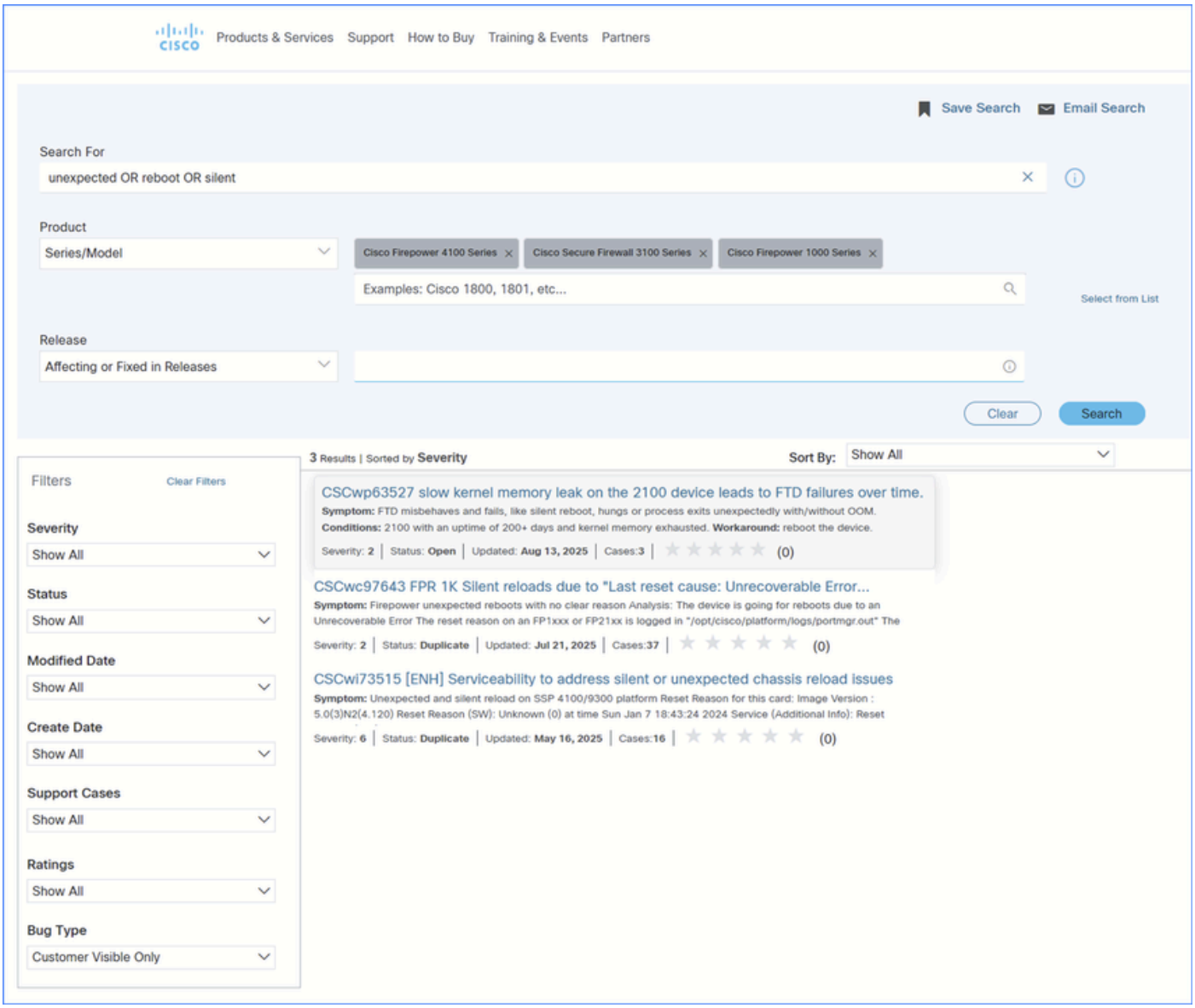
8.3.检查分析ssp-shutdown.log文件部分。

8.4.检查分析ASA/FTD控制台日志部分。

8.5.继续执行收集数据以进行安全防火墙中的软件回溯/崩溃的根本原因分析中的步骤，以验证软件回溯的症状和数据收集。

9.如果由于软件回溯而出现重新启动的迹象，请打开TAC案例并提供收集的数据。

10.使用关键字unexpected、reboot、power、reload、restart、restart和silent搜索软件缺陷：



如果找到匹配的缺陷：

- 确保]症状和条件与缺陷中描述的相符。
- 应用解决方法（如果有）。
- 升级到固定版本（如果有）。

11.通过数据收集部分打开TAC案例。

分析正常运行时间

本部分的目的是检查ASA/FTD应用、安全模块（仅限Firepower 4100/9300）和机箱的运行时间。

1. 在ASA上检查运行show version命令的防火墙引擎正常运行时间，在FTD上检查show version system命令：

```
<#root>

>

show version system


---------------[ firewall-FTD ]---------------
Model                     : Cisco Firepower 4112 Threat Defense (76) Version 7.6.1 (Build 291)
UUID                      : e9460e12-674c-11f0-97e5-d5ad3617d287
LSP version               : lsp-rel-20241211-1948
VDB version               : 408
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.22(1)21
SSP Operating System Version 2.16(0.3007)

Compiled on Thu 29-May-25 01:38 GMT by fpbesprd
System image file is "disk0:/fxos-lfbff-k8.2.16.0.136.SPA"

Config file at boot was "startup-config"

firewall-FTD up 5 days 0 hours
```

在FTD故障排除文件中，检查文件command-outputs/'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output':

```
<#root>

/command-outputs$

less 'usr-local-sf-bin-sfcli.pl show_tech_support asa_lina_cli_util.output'


…
firewall-FTD up 5 days 0 hours
…
```

对于ASA，请在show-tech文件中检查正常运行时间。

2. 对于在虚拟平台上以本机模式运行的FTD，Firepower 1000、2100、安全防火墙1200、3100和4200;在专家模式下检查操作系统的正常运行时间(天、小时和分钟)。在这种情况下，机箱正常运行时间与操作系统正常运行时间大致相同：

<#root>

>

expert

admin@firepower:/ngfw/Volume/home/admin$

uptime

 06:30:40

 up 6 days, 8:01

, 1 user, load average: 5.14, 5.45, 5.48

在FTD故障排除文件中，检查文件dir-archives/var-log/top.log:

<#root>

dir-archives/var-log$

less top.log

```
================================================================================================
Tue Jul 22 04:02:11 UTC 2025
top - 04:02:11
up 6 days, 13:57
,  4 users,  load average: 2.23, 2.42, 2.59
Tasks: 167 total,   2 running, 165 sleeping,   0 stopped,   0 zombie
%Cpu(s): 26.6 us,  7.8 sy,  1.6 ni, 64.1 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   7629.8 total,   2438.4 free,   4559.6 used,    631.8 buff/cache
MiB Swap:   5369.2 total,   3713.7 free,   1655.5 used.   2849.9 avail Mem
```

---

3. 对于安全防火墙3100或4200上多实例模式下的FTD，以及运行在Firepower 1000、2100、安全防火墙1200、3100和4200上的ASA，没有可用于检查机箱正常运行时间的命令。

您可以检查刀片正常运行时间：

```
<#root>

>

connect fxos


…
firewall#

scope ssa


firewall /ssa #

show slot detail expand



Slot:
    Slot ID: 1
    …


      Blade Uptime: up 16 hours, 2 min
```

在机箱故障排除文件中，检查opt/cisco/platform/logs/sysmgr/sam_logs/topout.log文件中的运行时间：

```
<#root>

opt/cisco/platform/logs/sysmgr/sam_logs/topout.log $

less topout.log


[Jul 23 13:15:22]
top - 13:15:22

up 16:02

,  1 user,  load average: 12.24, 11.85, 11.75
```

---

4. 对于Firepower 4100/9300，请在FXOS CLI中检查机箱和安全模块的运行时间。

机箱正常运行时间：

<#root>

```
firewall /ssa #

connect fxos


firewall(fxos)#

show system uptime


System start time:          Tue Jul 22 21:57:44 2025
System uptime:              6 days, 9 hours, 49 minutes, 50 seconds
Kernel uptime:              6 days, 9 hours, 45 minutes, 58 seconds
Active supervisor uptime:   6 days, 9 hours, 49 minutes, 50 seconds
```

安全模块正常运行时间：

<#root>

```
firewall#

scope ssa


firewall /ssa #

show slot detail expand


Slot:
    Slot ID: 1
    …
         Blade Uptime: up 5 days, 37 min
```

在机箱故障排除文件中，运行文件*_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo中show system uptime命令的输出，并在文件*_BC1_all/FPRM_A_TechSupport/sam_techsupportinfo中运行show slot expand detail expand命令，其中*是故障排除文件名的一部分，例如20250311123356_ FW_BC1_all。

分析FTD消息文件

本节介绍如何分析FTD messages文件，该文件包含与关机、重新启动和潜在触发器相关的日志。

在所有平台上运行的FTD

该文件包含与关闭、重新启动及其在FTD上运行的潜在触发器相关的日志：

- 虚拟平台、Firepower 1000、2100和安全防火墙1200、3100、4200机箱。
- Firepower 4100和9300安全模块。

可在以下位置访问该文件：

- expert模式下的FTD CLISH:/ngfw/var/log/messages
- FTD故障排除文件：dir-archives/var-log/messages

要查找关闭或重新启动的触发器，请检查FTD故障排除文件中的消息文件中包含Defense的消息。确保检查所有消息文件，包括messages.1、messages.2等。这些消息清楚地表明正常关闭：

- 正在停止思科安全防火墙……或正在停止思科Firepower..
- ...威胁防御正在关闭

<#root>

```
root@CSF1220-2:/ngfw/var/log#
```

grep -a Defense /ngfw/var/log/messages

```
messages:Jul 22 21:07:10 firepower-1220 SF-IMS[36894]: [36894] S11audit-startup-shutdown:start [INFO] C
messages:Jul 22 21:12:37 firepower-1220 SF-IMS[62594]: [62594] sensor:CLI Start [INFO] Starting Cisco S
messages:Jul 22 21:13:03 firepower-1220 SF-IMS[65410]: [65410] S99sensor:CLI Start [INFO] Starting Cisc
```

messages:Jul 23 12:56:43 CSF1220-2 SF-IMS[61878]: [61878] K01sensor:CLI Stop [INFO] Stopping Cisco Secur

messages:Jul 23 12:57:03 CSF1220-2 SF-IMS[62749]: [62749] K69audit-startup-shutdown:stop [INFO] Cisco Se

```
messages:Jul 23 13:00:21 CSF1220-2 SF-IMS[10866]: [10866] S11audit-startup-shutdown:start [INFO] Cisco S
```

```
messages:Jul 23 13:00:36 CSF1220-2 SF-IMS[13443]: [13443] S99sensor:CLI Start [INFO] Starting Cisco Secu
```

<#root>

```
root@1140-2:/ngfw/var/log#
```

```
grep -a Defense /ngfw/var/log/messages
```

```
messages:Jul 22 09:20:42 FPR1140-2 SF-IMS[6012]: [6012] S11audit-startup-shutdown:start [INFO] Cisco Fi
messages:Jul 22 09:21:35 FPR1140-2 SF-IMS[9050]: [9050] S99sensor:CLI Start [INFO] Starting Cisco Firep
```

```
messages:Jul 22 11:32:37 FPR1140-2 SF-IMS[15129]: [15129] K01sensor:CLI Stop [INFO] Stopping Cisco Firep
```

```
messages:Jul 22 11:32:55 FPR1140-2 SF-IMS[15940]: [15940] K69audit-startup-shutdown:stop [INFO] Cisco Fi
```

```
messages:Jul 22 11:36:38 FPR1140-2 SF-IMS[5980]: [5980] S11audit-startup-shutdown:start [INFO] Cisco Fir
```

```
messages:Jul 22 11:36:53 FPR1140-2 SF-IMS[7594]: [7594] S99sensor:CLI Start [INFO] Starting Cisco Firepo
```

分析安全模块或机箱消息文件

本节介绍如何分析包含与操作系统内核相关的日志的安全模块或机箱消息文件。

该文件包含与关闭、重新启动及其在FTD上运行的潜在触发器相关的日志：

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

可在以下位置访问该文件：

- 在本地模式下运行的基于硬件的FTD:/opt/cisco/platform/log/messages。
- 对本机模式下运行的基于硬件的FTD的文件进行故障排除：dir-archives/opt-cisco-platform-logs/messages。
- Firepower 1000、2100和安全防火墙1200、3100、4200机箱故障排除文件：/opt/cisco/platform/log/messages。
- Firepower 4100/9300安全模块显示技术文件：/opt/cisco/platform/log/messages。

以下是此文件中日志的关键点：

- 确保检查所有消息文件，包括messages.1、messages.2等。
- 操作系统内核启动时，内核日志会写入此文件。在硬件平台和安全模块上，日志最初以UTC时区写入，直到在引导期间应用自定义时区。

因此，同一文件中的不同日志可以具有不同时区的不同时间戳。

考虑以下来自Firepower 4100安全模块的UTC+2时区示例：

<#root>

2025-08-18T14:54:16+02:00 Firepower-module1/2 root: FXOS shutdown log started: pid = 52994 cmdline = /bi

2025-08-18T14:54:16+02:00 Firepower-module1/2 root: FXOS shutdown log completed: pid = 52994

2025-08-18T14:54:17+02:00 Firepower-module1/2 syslog-ng[1230]: syslog-ng shutting down; version='3.36.1'

2025-08-18T12:57:11+00:00 intel-x86-64/1 syslog-ng[1237]: syslog-ng starting up; version='3.36.1' <--- s

2025-08-18T12:57:11+00:00 intel-x86-64/1 kernel: [0.000000] Linux version 5.10.200-yocto-standard (
2025-08-18T12:57:11+00:00 intel-x86-64/1 kernel: [0.000000] Command line: rw console=ttyS0,38400 lo
…
2025-08-18T12:58:34+00:00 intel-x86-64/1 csp-console: Adi not started yet, trying to bring up
2025-08-18T12:58:34+00:00 intel-x86-64/1 ssp_tz[12159]: INFO: Lina is started
2025-08-18T12:58:34+00:00 intel-x86-64/1 SMA: INFO ExecProcessorMain [140588852127296]: finished proces
2025-08-18T12:58:34+00:00 intel-x86-64/1 ssp_tz[12167]: INFO: notify TZ to ASA LINA <---- Time zone cha
2025-08-18T14:58:35+02:00 intel-x86-64/1 ssp_tz[12192]: INFO: successfully notified TZ to ASA LINA, wai
2025-08-18T14:58:36+02:00 intel-x86-64/1 csp-console: Adi not started yet, trying to bring up

```
2025-08-18T14:58:39+02:00 intel-x86-64/1 csp-console[1237]: Last message 'Adi not started yet,' repeate
```

分析ssp-pm.log文件

本部分介绍对包含与ASA/FTD应用关闭或重新启动相关的日志的/opt/cisco/platform/logs/ssp-pm.log文件的分析。

该文件包含在上运行的ASA/FTD应用的关闭或重新启动日志：

- Firepower 1000、2100和安全防火墙1200、3100、4200机箱。
- Firepower 4100和9300安全模块（不是机箱）。

该文件只能在以下位置访问：

- FTD本地模式（非多实例）expert模式中的CLISH:opt/cisco/platform/logs/ssp-pm.log。
- FTD本地模式故障排除文件：dir-archives/opt-cisco-platform-logs/ssp-pm.log。
- Firepower 1000、2100和安全防火墙1200、3100、4200上的机箱故障排除文件：/opt/cisco/platform/logs/ssp-pm.log。

要识别平稳关机或重新启动，请查找与重新启动/关机时间戳匹配的SHUTDOWN WARNING等行。确保检查所有ssp-pm.log文件，包括ssp-pm.log.1、ssp-pm.log.2等。这些消息清楚地表明正常关闭：

<#root>

```
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Beginning System Shutdown request for CSP Ap
```

```
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-GetShutdownMaxForceQuitTimer: acquiring max
```

```
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Upgrade process ready for reboot
```

```
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-GetShutdownMaxForceQuitTimer: No force_quit_
```

```
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING: Continue System Shutdown request for CSP App

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: corre

cisco-asa.9.22.2.9__asa_001_JMX2324G1DJ947ECO1.conf

Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: corre

...cspCfg_cisco-asa.9.22.2.9__asa_001_JMX2324G1DJ947ECO1.xml.allocated_cpu_core

…
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: stopp
Fri Jul 25 10:28:51 UTC 2025 -(PM_UTILS)- SHUTDOWN WARNING:-SysShutdown_HeimdallSvcDownAllCspApps: Stopp
```

分析ssp-shutdown.log文件

本节介绍对/opt/cisco/platform/logs/ssp-shutdown.log文件的分析，这些文件包含机箱/安全模块关闭或重新启动时生成的日志。

该文件包含以下项的关闭或重新启动日志：

- Firepower 1000、2100和安全防火墙1200、3100、4200机箱。
- Firepower 4100和9300安全模块（不是机箱）。

该文件只能在以下位置访问：

- FTD本地模式（非多实例）expert模式中的CLISH:opt/cisco/platform/logs/ssp-shutdown.log。
- FTD本地模式故障排除文件：dir-archives/opt-cisco-platform-logs/ssp-shutdown.log。
- firepower 1000、2100和安全防火墙1200、3100、4200的机箱故障排除文件：/opt/cisco/platform/logs/ssp-shutdown.log。

- Firepower 4100/9300安全模块故障排除文件：opt/cisco/platform/logs/ssp-shutdown.log。

有关如何生成FTD、机箱和安全模块故障排除文件，请参阅排除Firepower文件生成过程故障。

要查找正常关机或重新启动的触发因素，请完成以下步骤：

1. 检查FXOS shutdown started等行是否与重新启动/关闭时间戳匹配。确保检查所有ssp-shutdown.log文件，包括ssp-shutdown.log.1、ssp-shutdown.log.2等。

```
#### Wed Jul 23 12:56:42 UTC 2025: FXOS shutdown started: pid = 61677 cmdline = /bin/sh/sbin/fxos_log_s
```

---

2. 在进程树中查找包含fxos_log_shutdown或shutdown的行 reboot.sh。

   示例 1：重新引导的请求来自UUID 068f09e6-3825-11ee-a72c-e78d34d303cc和IP地址192.0.2.100（即FMC）的对等设备：

```
<#root>
root     61074  4593  2 12:56 ?        00:00:00          |   \_ /usr/bin/perl /ngfw/usr/local/sf/bin/ex

192.0.2.100 068f09e6-3825-11ee-a72c-e78d34d303cc

 SF::System::
Privileged::RebootSystem
root     61097 61074  0 12:56 ?        00:00:00          |       \_ /bin/sh /ngfw/usr/local/sf/bin/rebo
root     61670 61097  0 12:56 ?        00:00:00          |

\_ /bin/sh /sbin/shutdown -r now


root     61671 61670  0 12:56 ?        00:00:00          |               \_ /bin/sh /sbin/exec_fxos_log
root     61676 61671  0 12:56 ?        00:00:00          |                   \_ /usr/bin/timeout 15 /sb
root     61677 61676  0 12:56 ?        00:00:00          |                       \_ /bin/sh /sbin/fxos_
root     61685 61677  0 12:56 ?        00:00:00          |                           \_ /bin/ps -ef -fo

>

show managers


Type                      : Manager

Host                      : 192.0.2.100
```

```
Display name              : 192.0.2.100
Version                   : 7.6.1 (Build 291)

Identifier                : 068f09e6-3825-11ee-a72c-e78d34d303cc


Registration              : Completed
Management type           : Configuration and analytics
```

示例 2：由于软件升级而重新启动：

<#root>

```
root      2432     1  0 03:59 ?        00:00:00 /bin/bash /isan/bin/kp_reboot.sh Reboot requested for So



root      2694  2432  0 03:59 ?        00:00:00  \_ /bin/sh /isan/bin/sam_reboot.sh Reboot requested for



root      3774  2694  0 04:00 ?        00:00:00      \_ /usr/bin/sudo /sbin/shutdown -r now Reboot reque



root      3777  3774  0 04:00 ?        00:00:00          \_ /bin/sh /sbin/shutdown -r now Reboot request


root      3778  3777  0 04:00 ?        00:00:00              \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root      3783  3778  0 04:00 ?        00:00:00                  \_ /usr/bin/timeout 15 /sbin/fxos_log_
root      3784  3783  0 04:00 ?        00:00:00                      \_ /bin/sh /sbin/fxos_log_shutdown
root      3790  3784  0 04:00 ?        00:00:00                          \_ /bin/ps -ef -forest
```

示例 3：管理员用户通过运行CLISH reboot命令请求重新启动：

<#root>

```
root     22189     1  0 Jul23 ?        00:00:01 sshd: /usr/sbin/sshd [listener] 0 of 10-100 startups
root     20963 22189  0 06:55 ?        00:00:00  \_ sshd: admin [priv]
admin    20970 20963  0 06:55 ?        00:00:00  |   \_ sshd: admin@pts/0
admin    20975 20970  0 06:55 pts/0    00:00:00  |       \_ /isan/bin/ucssh --ucs-mgmt -p admin -c conn
admin    21077 20975  0 06:55 pts/0    00:00:00  |           \_ /ngfw/usr/bin/clish
admin    36022 21077  0 07:23 pts/0    00:00:00  |               \_ /ngfw/usr/bin/clish
admin    36023 21077  0 07:23 pts/0    00:00:00  |               \_ /bin/sh /tmp/klish.fifo.21077.1Hwyq
admin    36024 36023  8 07:23 pts/0    00:00:01  |
```

```
\_ /usr/bin/perl /usr/local/sf/bin/sfcli.pl reboot system


root     36083 36024  0 07:23 pts/0    00:00:00  |

\_ /usr/bin/sudo /ngfw/usr/local/sf/bin/reboot.sh


root     36088 36083  0 07:23 pts/0    00:00:00  |                          \_ /bin/sh /usr/local/sf/b
root     36433 36088  0 07:23 pts/0    00:00:00  |

\_ /bin/sh /sbin/shutdown -r now


root     36434 36433  0 07:23 pts/0    00:00:00  |                                \_ /bin/sh /sbin/e
root     36439 36434  0 07:23 pts/0    00:00:00  |                                    \_ /usr/bin/ti
root     36440 36439  0 07:23 pts/0    00:00:00  |                                        \_ /bin/sh
root     36448 36440  0 07:23 pts/0    00:00:00  |                                            \_ /bi
```

示例 4：通过单击电源按钮触发了关闭。PBTN表示按物理电源按钮。按计算机上的电源按钮将触发此事件。该脚本使用此事件启动关闭进程，通常是因为用户希望安全地关闭防火墙：

```
<#root>

root      1310     1  0 00:14 ?        00:00:00 /usr/sbin/acpid -c /etc/acpi/events

root     50700  1310  0 00:32 ?        00:00:00  \_ /bin/sh /etc/acpi/acpi_handler.sh button/power PBTN


root     50701 50700  0 00:32 ?        00:00:00

\_ /bin/sh /sbin/shutdown -h now


root     50702 50701  0 00:32 ?        00:00:00          \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     50707 50702  0 00:32 ?        00:00:00              \_ /usr/bin/timeout 15 /sbin/fxos_log_shut
root     50708 50707  0 00:32 ?        00:00:00                  \_ /bin/sh /sbin/fxos_log_shutdown
root     50715 50708  0 00:32 ?        00:00:00                      \_ /bin/ps -ef -forest
```

示例 5：内部npu_accel_mgr进程请求重启：

```
<#root>

root     12649  5280  0 13:59 ?        00:01:06  \_
```

```
npu_accel_mgr


root     19030 12649  0 18:22 ?        00:00:00  |

\_ /bin/sh /sbin/shutdown -r now


root     19031 19030  0 18:22 ?        00:00:00  |       \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     19036 19031  0 18:22 ?        00:00:00  |           \_ /usr/bin/ timeout 15 /sbin/fxos_log_shu
root     19037 19036  0 18:22 ?        00:00:00  |               \_ /bin/sh /sbin/fxos_log_shutdown
root     19043 19037  0 18:22 ?        00:00:00  |                   \_ /bin/ps -ef -forest
```

示例 6：内部poshd进程请求了关闭：

<#root>

```
root       643     1  0 13:00 ?        00:00:00

/usr/bin/poshd


root     13207   643  0 13:43 ?        00:00:00

\_ /bin/sh /sbin/shutdown -h -P now


root     13208 13207  0 13:43 ?        00:00:00      \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     13213 13208  0 13:43 ?        00:00:00          \_ /usr/bin/timeout 15 /sbin/fxos_log_shutdown
root     13214 13213  0 13:43 ?        00:00:00              \_ /bin/sh /sbin/fxos_log_shutdown
root     13221 13214  0 13:43 ?        00:00:00                  \_ /bin/ps -ef -forest
```

poshd负责在出现电源问题（通过电源按钮或外部电源因素）时正常关闭设备。

示例 7：防火墙引擎Lina的状态更改触发了重启，例如：

- 通过在ASA CLI或FTD诊断CLI中运行reload命令
- Lina引擎回溯(除了在ASA 9.20(x)和FTD 7.4.1中引入的“数据平面快速重新加载”功能的版本。)
- 从主用设备到备用设备的不完整/部分同步

<#root>

```
root     56833 56198  0 00:48 ?        00:00:00  |   \_ /ngfw/usr/local/sf/bin/consoled /ngfw/var/run/li
```

```
root     57003 56833  0 00:48 ?        00:00:00  |

\_ /bin/sh /sbin/shutdown -r now


root     59448 57003  0 00:48 ?        00:00:00  |           \_ /bin/sh /sbin/exec_fxos_log_shutdown.sh
root     59453 59448  0 00:48 ?        00:00:00  |               \_ /usr/bin/timeout 15 /sbin/fxos_log_
root     59454 59453  0 00:48 ?        00:00:00  |                   \_ /bin/sh /sbin/fxos_log_shutdown
root     59461 59454  0 00:48 ?        00:00:00  |                       \_ /bin/ps -ef -forest
```

分析机箱重置原因

本节介绍机箱重置原因的分析。在Firepower 4100/9300机箱上，重置原因仅在以下位置可用：

- FXOS CLI:

```
<#root>

#

connect fxos


(fxos)#

show system reset-reason
```

- 在机箱故障排除文件*_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo中，show system reset-reason 命令的输出中，其中*是故障排除文件名的一部分，例如20250311123356_FW_BC1_all

---

在Firepower 1000、2100、安全防火墙1200、3100、4200上，重置原因仅在以下位置可用：

- FTD本地模式（非多实例）expert模式中的CLISH:opt/cisco/platform/logs/portmgr.out。
- FTD本地模式故障排除文件：dir-archives/opt-cisco-platform-logs/portmgr.out。
- firepower 1000、2100和安全防火墙1200、3100、4200上的机箱故障排除文件：/opt/cisco/platform/logs/portmgr.out。

有关如何生成FTD、机箱和安全模块文件，请参阅排除Firepower文件生成过程故障。

要查找Firepower 4100/9300以外的硬件平台的重置原因，请执行以下步骤：

1. 在/opt/cisco/platform/logs/portmgr.out中，检查匹配重新启动/关闭时间戳的行，例如Last reset cause。确保检查所有portmgr.out文件，包括portmgr.out.1、portmgr.out.2等。

2. 有关常见重置原因的解释，请参阅下表：

重置原因	说明
开机	上次重置是由加电事件引起的（交流电源循环）。
LocalSoft	上次重置是由本地软件重置（软件重置为CPU）引起的。
FanFail	风扇托架缺失或风扇故障检测导致系统重新通电。
RP-Reset	此位表示软件请求重新通电。
BootRom升级	上次重置是由映像升级闪存重置引起的。
BootRomUpgradeFail	升级过程失败。
监视程序/PCH	上次重置是由FPGA中的监视器计时器超时引起的。
手动	上次重置是由手动按钮重置引起的。
SwitchOff	上次重置是由手动电源开关切换关闭引起的。
不可恢复的错误	由CPU灾难性错误信号引起。
ResetRequest	上次重置是由发出重置信号的CPU引起的。 这也可能由内核紧急事件引起。 当从CLISH、Lina或FMC手动触发FTD重新启动时，也会显示此原因。
PowerCycleRequest	上次重置/重新通电是由断言任何休眠信号的CPU引起的。

要查找Firepower 4100/9300的重置原因，请执行以下步骤：

1. 在FXOS CLI上，在FXOS命令shell中运行show system reset-reason命令。

<#root>

```
FPR4115-2 #

connect fxos



…
FPR4115-2(fxos)#

show system reset-reason



----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 612806449 usecs after Tue Jul 22 23:50:33 2025
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.141)

2) No time
    Reason: Unknown
    Service:
    Version: 5.0(3)N2(4.141)

3) No time
    Reason: Unknown
    Service:
    Version: 5.0(3)N2(4.141)

4) At 723697 usecs after Thu Oct  3 17:56:08 2024
    Reason: Reset Requested by CLI command reload
    Service:
    Version: 5.0(3)N2(4.120)
```

此命令的输出也可在机箱故障排除文件*_BC1_all/FPRM_A_TechSupport/sw_techsupportinfo中找到，其中*是故障排除文件名的一部分。例如，20250311123356_ FW_BC1_all

<#root>

```
#

pwd



20250521112103_FPR9300_BC1_all/FPRM_A_TechSupport
```

```
#

less sam_techsupportinfo
```

最常见的原因：

CLI命令reload请求重置。
上次重置是由监视器超时引起的。
由于致命系统错误而请求重置。
由于致命的模块错误而请求重置。
由于温度传感器策略触发而关闭电源。
由于电压不正常而重置。
由于致命系统错误而请求重置。
由于多个不可纠正的ASIC内存错误而重置。
由于内核死机而重置。
由于HA切换策略触发重置。
内核重新引导请求。
由于未知原因而重置。

2.步骤1中没有时间的Unknown原因通常表示突然断电或电源单元(PSU)问题。建议检查外部断电或配电装置(PDU)问题的事件。

3.此外，运行show logging onboard internal reset-reason的输出 | no-more命令。此命令的输出也可在机箱故障排除文件*_BC1_all/FPRM_A_TechSupport/sw_kernel_trace_log中找到，其中*是故障排除文件名的一部分。例如，20250311123356_ FW_BC1_all:

```
<#root>
FPR4115-2 #

connect fxos


…
KSEC-FPR4115-2(fxos)#

show logging onboard internal reset-reason | no-more


----------------------------
OBFL Data for
    Module:  1
----------------------------
Reset Reason for this card:
        Image Version : 5.0(3)N2(4.141)

        Reset Reason (SW): Unknown (0) at time Fri Jul  4 23:57:21 2025


          Service (Additional Info):

        Reset Reason (HW): FPGA  reset code: 0x0001



          FPGA Power-ON Reset at time Fri Jul  4 23:57:21 2025
```

分析硬件错误或异常

本节介绍对包含硬件错误或异常的文件进行的分析。

Firepower 1000、2100、安全防火墙1200、3100、4200、Firepower 4100/9300安全模块

相关文件包括：

- /opt/cisco/platform/logs/mce.log(计算机检查异常日志)

- /ngfw/var/log/dmesg.log（仅限FTD）
- /opt/cisco/config/var/logs/dmesg.log
- /opt/cisco/platform/logs/messages

这些文件可能包含以下项的硬件错误或异常日志：

- Firepower 1000、2100和安全防火墙1200、3100、4200机箱
- Firepower 4100和9300安全模块（非机箱）

这些文件仅在以下位置可访问：

- FTD本地模式（非多实例）expert模式中的CLISH:
  - /opt/cisco/platform/logs/mce.log
  - /ngfw/var/log/dmesg.log（仅限FTD）
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages

- FTD本地模式故障排除文件：
  - dir-archives/var-common-platform_ts/opt/cisco/platform/logs/mce.log
  - dir-archives/var-common-platform_ts/opt/cisco/platform/logs/messages
  - dir-archives/var-common-platform_ts/opt/cisco/config/var/logs/dmesg.log
  - dir-archives/var-log/dmesg.log
- Firepower 1000、2100和安全防火墙1200、3100、4200上的机箱故障排除文件：
  - /opt/cisco/platform/logs/mce.log
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages
- Firepower 4100/9300上的安全模块show-tech文件：
  - /opt/cisco/platform/logs/mce.log
  - /opt/cisco/config/var/logs/dmesg.log
  - /opt/cisco/platform/logs/messages

硬件相关错误的示例：

<#root>

```
opt/cisco/config/var/logs/ $

less dmesg.log
```

```
[Sun Apr 27 05:17:10 2025] mce: [Hardware Error]: Machine check events logged
[Sun Apr 27 05:17:10 2025] mce: [Hardware Error]: Machine check events logged

/opt/cisco/platform/logs $
```

less messages

```
Jul  9 17:39:38 fw2 kernel: [  628.949572] [Hardware Error]: Corrected error, no action required.
Jul  9 17:39:38 fw2 kernel: [  629.023798] [Hardware Error]: CPU:2 (19:1:1) MC18_STATUS[Over|CE|MiscV|A
Jul  9 17:39:38 fw2 kernel: [  629.152245] [Hardware Error]: Error Addr: 0x0000000068d06d40
Jul  9 17:39:38 fw2 kernel: [  629.152248] [Hardware Error]: PPIN: 0x02b0bc114ba60075
Jul  9 17:39:38 fw2 kernel: [  629.281830] [Hardware Error]: IPID: 0x0000009600550f00, Syndrome: 0x0004
Jul  9 17:39:38 fw2 kernel: [  629.374797] [Hardware Error]: Unified Memory Controller Ext. Error Code:
Jul  9 17:39:38 fw2 kernel: [  629.475078] [Hardware Error]: cache level: L3/GEN, tx: GEN, mem-tx: RD
Jul  9 17:44:40 fw2 kernel: [  930.967028] [Hardware Error]: Corrected error, no action required.
Jul  9 17:44:40 fw2 kernel: [  931.041247] [Hardware Error]: CPU:2 (19:1:1) MC18_STATUS[Over|CE|MiscV|A
Jul  9 17:44:40 fw2 kernel: [  931.169689] [Hardware Error]: Error Addr: 0x000000007191d0c0
Jul  9 17:44:40 fw2 kernel: [  931.237616] [Hardware Error]: PPIN: 0x02b0bc114ba60075
Jul  9 17:44:40 fw2 kernel: [  931.299275] [Hardware Error]: IPID: 0x0000009600550f00, Syndrome: 0x0000

/opt/cisco/platform/logs $
```

less mce.log

Hardware event. This is not a software error.

```
MCE 0
CPU 0 BANK 7 TSC 7b29f624ae62e
MISC 140129286 ADDR 3402b9a00
TIME 1745747035 Sun Apr 27 09:43:55 2025
MCG status:
MCi status:
Corrected error
MCi_MISC register valid
MCi_ADDR register valid
MCA: MEMORY CONTROLLER RD_CHANNEL0_ERR
```

Transaction: Memory read error

```
STATUS 8c00004000010090 MCGSTATUS 0
MCGCAP 1000c16 APICID 0 SOCKETID 0
PPIN afeebaf20487b95
MICROCODE 700000d
CPUID Vendor Intel Family 6 Model 86 Step 3
```

mcelog: failed to prefill DIMM database from DMI data

Firepower 4100/9300安全模块上的灾难性错误(CATERR)

CATERR是处理器断言的异常。CATERR可能表示CPU崩溃或使刀片无法访问的低级问题。机箱管

理引擎重新启动遇到过CATERR的安全模块。CATERR日志位于CIMC<X>_TechSupport/obfl/和CIMC<X>_TechSupport/var/log/sel中的Firepower 4100/9300故障排除文件内，其中<X>代表模块编号。

机箱故障排除文件示例
*_BC1_all/CIMC<X>_TechSupport.tar.gz/CIMC<X>_TechSupport.tar/obfl/obfl-log，其中*是故障排除文件名的一部分。例如，20250311123356_ FW_BC1_all和<X >是安全模块ID:

<#root>

2022 Mar 25 22:33:13 CET:4.1(30b):selparser:1950: selparser.c:727: # BF 06 00 00 01 02 00 00 19 35 3E 6

Processor CATERR

_N #0x81 |

Predictive Failure asserted | Asserted

当前数据管理引擎(DME)登录
*_BC1_all/FPRM_A_TechSupport.tar.gz\FPRM_A_TechSupport.tar\var\sysmgr\sam_logs\svc_sam_dme.lo
重新启动
*_BC1_all/FPRM_A_TechSupport.tar.gz/FPRM_A_TechSupport.tar/opt/sam_logs.tgz/sam_logs.tar/sam_lo
前的日志包含因CATERR而具有重新通电刀片X的行，其中X是刀片ID。

在CATERR的情况下，可以生成故障转储。故障转储位于
*_BC1_all/CIMC<X>_TechSupport.tar.gz/CIMC<X>_TechSupport.tar/techsupport_pidxxxx/nv/etc/log/eng-repo/caterrlog.first中。

示例内容：

```
CRASH DUMP START TIME = Mon Dec 19 00:42:40 2022
               SERVER: presidio
               GetCpuID: CPUID = 0x00050654
               PresidioCatErrHandler: CPU TYPE : Skylake
               handleCaterr_Purley: ---
               PECI BUS : LOCKED
               CPU Socket 1 : Populated
               CPU Socket 2 : Populated
               Stage1Dump: ---
               MC0: IFU - Instruction Fetch Unit and Instruction Cache
               CPU1 (0x30): ThreadID 0 : IA32_MC0_CTL (0x400) : 0x0000000000000fff
               CPU1 (0x30): ThreadID 0 : IA32_MC0_STATUS (0x401) : 0x0000000000000000
               CPU1 (0x30): ThreadID 0 : IA32_MC0_ADDR (0x402) : 0x0000000000000000
```

分析其他平台日志文件

本节介绍对包含平台日志的文件进行的分析。根据硬件，其中一些文件可能包含与特定组件触发的重新启动相关的日志。

Firepower 1000、2100、安全防火墙1200、3100、4200、Firepower 4100/9300安全模块

这些文件包含下列机箱日志：

- Firepower 1000、2100和安全防火墙1200、3100、4200机箱
- Firepower 4100和9300安全模块（非机箱）

这些文件仅在以下位置可访问：

- FTD本地模式（非多实例）在/opt/cisco/platform/logs/
- FTD本机模式故障排除文件dir-archives/var-common-platform_ts/opt/cisco/platform/logs/
- Firepower 1000、2100和安全防火墙1200、3100、4200 in/opt/cisco/platform/logs/上的机箱故障排除文件
- Firepower 4100/9300 in/opt/cisco/platform/logs/上的安全模块show-tech文件

要查找与重新启动相关的潜在日志，请搜索包含关键字(如reboot、restart、power、shut、reload)的行。



注意：这是尽力而为的方法，因为搜索的结果可以返回大量匹配行（用户必须分析匹配行）。

示例 1：

<#root>

```
admin@firewall:/opt/cisco/platform/logs$
```

```
grep -Ei "power|reboot|reload|restart|shut" *
```

```
...
npu_accel_fatal_err_stats.log:nic_top_inb_q_restart_drop_cnt = 0
npu_accel_fatal_err_stats.log:nic_top_norm_q_restart_drop_cnt = 0
npu_accel_fatal_err_stats.log:nic_top_inb_q_restart_drop_cnt = 0

npu_accel_mgr.log:2025 Oct 03 14:29:16 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 09 18:13:09 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 17 17:11:23 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 17 17:31:55 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

npu_accel_mgr.log:2025 Oct 17 19:29:29 NPU ACCEL MGR: FATAL - NPU Accelerator FAILED - REBOOTING the dev

ntp.log:27 Sep 02:21:16 ntpd[1580]: 0.0.0.0 c016 06 restart
ntp.log:27 Sep 02:23:27 ntpd[10193]: 0.0.0.0 c016 06 restart
...
```

在这种情况下，重新启动因安全防火墙4200的网络处理单元(NPU)加速器故障而触发。

分析SEL/OBFL文件

本节介绍如何分析Firepower 4100/9300安全模块上包含安全事件日志(SEL)和板载故障日志(OBFL)的文件。这些文件包含模块硬件事件和电源状态更改，并且位于Firepower 4100/9300故障排除文件内，位于CIMC<X>_TechSupport/obfl/和CIMC<X>_TechSupport/var/log/sel中，其中<X>代表模块编号。查找具有不区分大小写的stop、shutdown、power off、reset和critical的线路。

示例 1：

<#root>

```
2023 Sep 21 13:53:13:4.1(30b):cipmi:1088: [[xxxCVxxx]]:oem_command.c:457:IPMI Request Message --> Chan:

2023 Sep 21 13:53:13:4.1(30b):selparser:1203: [[xxxCVxxx]]:selparser.c:727: # A9 04 00 00 01 02 00 00 49
```

```
2023 Sep 21 13:53:14:4.1(30b):cipmi:1088: peci.c:278:Error: Failed to read local PCI config after 3 ret
2023 Sep 21 13:53:15:4.1(30b):kernel:-:<5>[platform_reset_cb_handler]:75:Platform Reset ISR -> ResetSta
2023 Sep 21 13:53:15:4.1(30b):cipmi:1088: ocmds_intel_me.c:251:Intel ME Operating State:[MO without UMA
2023 Sep 21 13:53:15:4.1(30b):cipmi:1088: ocmds_intel_me.c:261:Intel ME is initializing.
```

示例 2：操作系统级别关闭：

<#root>

```
2025 Jul 30 23:31:02 UTC:4.1(30b):cipmi:1052: [[xxxCVxxx]]:oem_command.c:457:IPMI Request Message --> C
2025 Jul 30 23:31:02 UTC:4.1(30b):selparser:1169: [[xxxCVxxx]]:selparser.c:727: # 48 03 00 00 01 02 00
2025 Jul 30 23:31:04 UTC:4.1(30b):kernel:-:<5>[platform_reset_cb_handler]:75:Platform Reset ISR -> Rese
2025 Jul 30 23:31:05 UTC:4.1(30b):kernel:-:<4>[peci_ioctl]:293:non-responsive controller, resetting pec
2025 Jul 30 23:31:05 UTC:4.1(30b):cipmi:1052: ocmds_intel_me.c:251:Intel ME Operating State:[MO without
2025 Jul 30 23:31:05 UTC:4.1(30b):cipmi:1052: ocmds_intel_me.c:261:Intel ME is initializing.

2025 Jul 30 23:31:05 UTC:4.1(30b):information_logger:589: uptime.c:1219:Host Transition Ocurred. Event C
```

示例 3：主板管理控制器因监视器而重置：

<#root>

```
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:487:BMC Watchdog resetted BMC.
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:489:BMC Watchdog System Bus Debug Status R
2025 Jun 14 07:44:50 CDT:4.1(30b):kernel:-:<3>[watchdog_init]:523:BMC Watchdog resetted BMC due to OOM.
```

分析ASA/FTD控制台日志

本节介绍如何分析ASAConsole.log文件，这些文件包含来自Lina引擎的日志，可以检查是否有软件回溯或重新启动的迹象。该文件包含在虚拟平台、Firepower 1000、2100和安全防火墙1200、3100、4200以及Firepower 4100和9300安全模块（不是机箱）上运行的ASA/FTD的关闭或重新启动日志。

该文件只能在以下位置访问：

- expert模式下的FTD CLISH:/ngfw/var/log/ASAConsole.log
- FTD故障排除文件：dir-archives/opt-cisco-platform-logs/ASAConsole.log。

- Firepower 4100/9300上的安全模块故障排除文件：/opt/platform/logs/ASAConsole.log
- Firepower 1000、2100和安全防火墙1200、3100、4200机箱显示技术文件：/opt/platform/logs/ASAConsole.log

---

回溯和生成核心文件的症状：

<#root>

```
root@KSEC-CSF1210-6:/ngfw/var/log#

less ASAconsole.log


2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:11 /bin/grep: (standard input): Resource temporarily unavailable
2025-08-09 01:06:35 !! !! First Crash in tid: 14834 signo: 11
2025-08-09 01:06:35
2025-08-09 01:06:35 Writing live core file to flash. Please do not reload.
2025-08-09 01:06:35
2025-08-09 01:06:35 Coredump starting....
2025-08-09 01:06:35 Corehelper: /opt/cisco/csp/cores/core.lina.11.14550.1754701595
2025-08-09 01:06:35 Waiting for Corehelper to finish....
2025-08-09 01:06:35 Livecore: generating coredump of 14550
2025-08-09 01:06:35 [New LWP 14795]
2025-08-09 01:06:35 [New LWP 14796]
2025-08-09 01:06:35 [New LWP 14834]
2025-08-09 01:06:35 [New LWP 14835]
2025-08-09 01:06:35 [New LWP 14836]
2025-08-09 01:06:35 [New LWP 14869]
2025-08-09 01:06:35 [New LWP 14934]
2025-08-09 01:06:35 [New LWP 14939]
2025-08-09 01:06:35 [New LWP 14940]
2025-08-09 01:06:35 [New LWP 14941]
2025-08-09 01:06:35 [New LWP 14942]
2025-08-09 01:06:35 [New LWP 14943]
2025-08-09 01:06:35 [New LWP 14945]
2025-08-09 01:06:35 [New LWP 14947]
2025-08-09 01:06:35 [New LWP 14948]
```

Lina引擎启动症状（注意日志时间戳中的间隙）：

<#root>

```
root@KSEC-CSF1210-6:/ngfw/var/log#

less ASAconsole.log


2024-11-13 22:43:09 INFO: SW-DRBG health test passed.
```

```
2024-11-13 22:43:09 M_MMAP_THRESHOLD 65536, M_MMAP_MAX 82155
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 /bin/grep: (standard input): Resource temporarily unavailable
2024-11-13 22:43:10 User enable_1 logged in to firepower
2024-11-13 22:43:10 Logins over the last 1 days: 1.
2024-11-13 22:43:10 Failed logins since the last login: 0.
2024-11-13 22:43:10 Type help or '?' for a list of available commands.

2024-11-13 22:43:10 ^Mfirepower>



2025-04-04 09:11:46 System Cores 8 Nodes 1 Max Cores 24



2025-04-04 09:11:46 Number of Cores 3
2025-04-04 09:11:46 IO Memory Nodes: 1
2025-04-04 09:11:46 IO Memory Per Node: 1073741824 bytes num_pages = 262144 page_size = 4096
2025-04-04 09:11:46
2025-04-04 09:11:46 Global Reserve Memory Per Node: 2147483648 bytes Nodes=1
2025-04-04 09:11:46
2025-04-04 09:11:46 LCMB: got DMA 1073741824 bytes on numa-id=0, phys=0x00000001c0000000, virt=0x000040
2025-04-04 09:11:46 LCMB: HEAP-CACHE POOL got 2147483648 bytes on numa-id=0, virt=0x0000400080000000
2025-04-04 09:11:46
2025-04-04 09:11:46 total_reserved_mem = 1073741824
2025-04-04 09:11:46
2025-04-04 09:11:46 total_heapcache_mem = 2147483648
2025-04-04 09:11:46 total mem 5384115842 system 16318316544 kernel 21847377 image 85732792
2025-04-04 09:11:46 new 5384115842 old 1159474616 reserve 3221225472 priv new 2184737747 priv old 0
2025-04-04 09:11:46 Processor memory:   5384115842
2025-04-04 09:11:46 POST started...
2025-04-04 09:11:46 POST finished, result is 0 (hint: 1 means it failed)
2025-04-04 09:11:46
2025-04-04 09:11:46 Cisco Adaptive Security Appliance Software Version 9.22(1)1
```

分析电源电压和电源问题

如果作为分析机箱重置原因部分重置原因的一部分找到以下原因，请继续本节：

- 开机
- PowerCycleRequest
- 由于电压不正常而重置
- 未知原因:

```
No time
    Reason: Unknown
    Service:
    Version:
```

以下原因可能表明以下一个或多个方面可能存在问题：

- 电力供应短缺
- 电源装置(PSU)问题
- 电源线问题
- 机架中的配电装置(PDU)问题
- 电源问题

继续执行以下步骤：

1. 要缩小问题范围，请回答以下问题：

- 断电是一次性问题还是反复出现？
- 防火墙是否有冗余PSU?
- PSU是否连接到不同的电源和/或PDU?
- 是否有任何其他设备连接到同一电源和/或PSU?
- 连接到同一电源和/或PSU的其他设备是否也发生断电？

---

2. 如果根据第一步的问题，只有防火墙会受到影响，请确保：

- 电源线与电源和机箱紧密连接。
- 电源线未损坏，请尝试更换电源线以排除电缆的潜在问题。

---

3. 如果机箱继续意外重新启动，请在FXOS中收集以下命令的输出几次：

<#root>

scope chassis 1

show psu detail expand

scope psu 1

```
show stats history psu-stats detail expand
```

```
show stats psu-stats detail expand
```

```
exit
```

```
scope psu 2
```

```
show stats history psu-stats detail expand
```

```
show stats psu-stats detail expand
```

---

4. 收集机箱故障排除文件。

参考

1. 验证 Firepower 软件版本
2. 验证Firepower、实例、可用性、可扩展性配置
3. 收集数据以分析安全防火墙中软件回溯/崩溃的根本原因
4. 排除Firepower文件生成过程故障

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）。