

排除无响应的Cisco安全防火墙故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[故障排除](#)

[步骤 1：目视检查（前面板）](#)

[步骤 2：目视检查（后面板）](#)

[步骤 3：风扇检查](#)

[步骤 4：物理环境检查](#)

[步骤 5：控制台和管理端口检查](#)

[步骤 6：管理IP连通性测试](#)

[步骤 7：相邻设备检查](#)

[步骤 8：HA/集群设备检查](#)

[步骤 9：收集控制台日志](#)

[步骤 10：执行冷重启](#)

[步骤 11：从EMC收集运行状况监控器图形](#)

[步骤 12：检查磁盘问题](#)

[步骤 13：日志分析](#)

[步骤 14：捕获](#)

[步骤 15：提供给Cisco TAC的其他信息](#)

[常见问题](#)

[Error:与DME通信超时](#)

[磁盘错误：丢失或不可操作](#)

[Field Notice：FN72077 - FPR9300和FPR4100](#)

[磁盘利用率100%](#)

[断电后，CSF 3100无法启动](#)

[Cisco Firepower 2100系列安全设备：某些单元可能会遇到内存故障](#)

[参考](#)

简介

本文档介绍对1xxx、12xx、21xx、31xx、41xx、42xx和93xx硬件平台上无响应的思科安全防火墙威胁防御(FTD)进行故障排除的建议步骤。

先决条件

Cisco 建议您了解以下主题：

- Cisco Secure FTD基础知识 (安装/配置)。

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御
- 思科安全防火墙管理中心
- Cisco Firepower可扩展操作系统(FXOS)

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。

背景信息

在某些情况下，思科FTD设备可能会变得无响应。典型症状包括：

- 无SSH访问。
- 无控制台访问。
- 控制台访问正在工作，但登录凭证未工作。
- 中转流量不通过设备。
- 接口关闭 (数据和/或管理)。
- 指示灯熄灭或呈琥珀色 (闪烁或呈稳定亮起)。
- 安全模块(4100、9300)变为无响应。

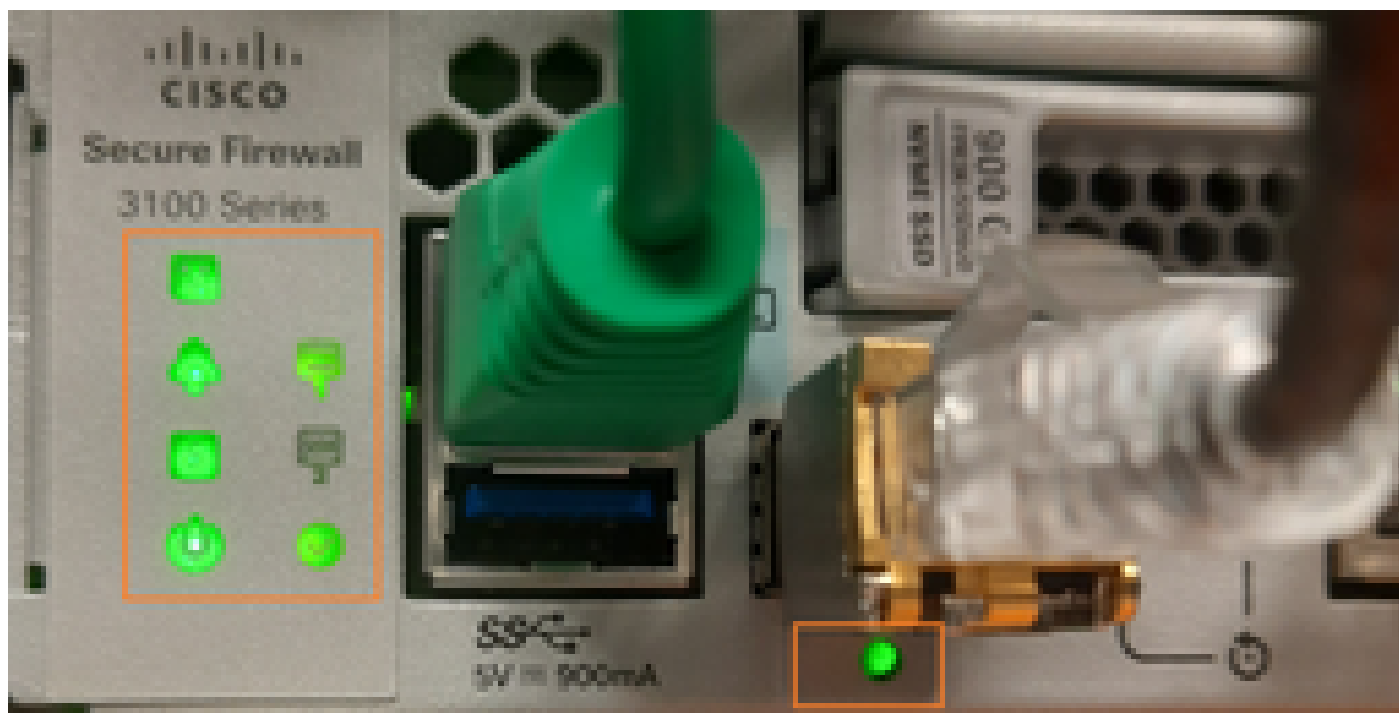
请注意，根据具体情况，有些设备不会出现。例如，您可以让中转流量通过，但只有管理访问不起作用。

故障排除

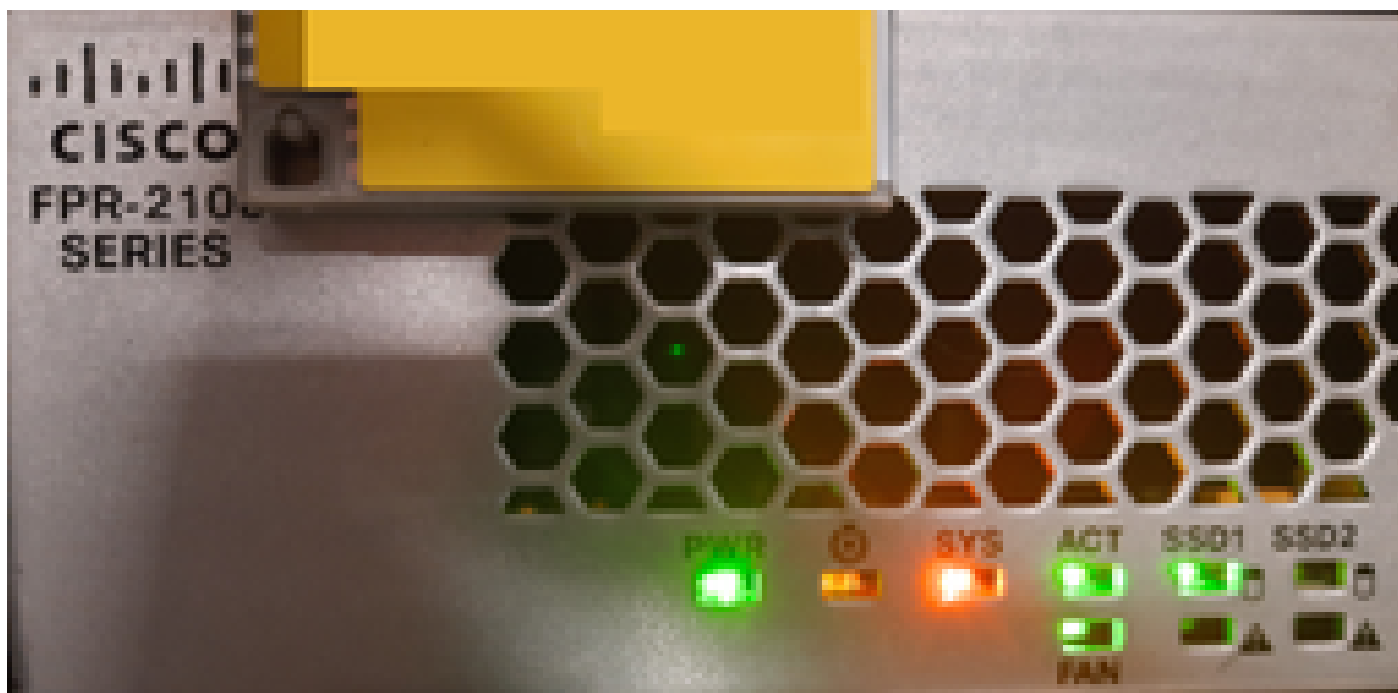
本节介绍您需要采取的推荐步骤和操作。您可以将此信息提供给思科TAC进行进一步分析。

步骤 1：目视检查 (前面板)

拍摄前面板LED的视频或图片。以下是所有LED都清晰可见的一些示例：



在下一张照片中，SYS LED指示设备问题：



您可以参考设备型号的硬件指南，以获取有关LED的其他信息，例如：

型号	LED信息
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overview.html
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/overview.html
1210CE、 1210CP、 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-1210-20.html
1230、 1240 和 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-1230-40-50.html
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/overview.html
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/migration.html
4110、 4120、 4140、 4150	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/overview.html

4112、 4115、 4125、 4145	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.html
4200	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/4200/fw-4200-install.html
9300	https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html

步骤 2：目视检查（后面板）

拍摄后面板上的LED的视频或图片，例如：



如果您看不到任何电源LED：

- 尝试重新拔插电源（如果适用）。
- 如果可能，请尝试更换电源。

步骤 3：风扇检查

验证设备背面的风扇是否正在运行。

步骤 4：物理环境检查

验证是否有来自设备的噪音或气味。

步骤 5：控制台和管理端口检查

确保控制台和管理端口连接正确。如果问题仅出现在管理端口上，请尝试更改SFP（只要适用）和网络电缆。

步骤 6：管理IP连通性测试

尝试ping(ICMP)设备的管理IP。

步骤 7：相邻设备检查

检查相邻设备的端口状态，例如：

```
<#root>

switch#
show interface description | i FW-4215-1

Gi7/1                up                up                FW-4215-1 ETH1/1
Gi7/2                up                up                FW-4215-1 ETH1/2
Gi7/3                up                up                FW-4215-1 MGMT
```

步骤 8::HA/集群设备检查

在高可用性(HA)或集群设置的情况下，从对等设备收集故障排除捆绑包。

步骤 9：收集控制台日志

将笔记本电脑连接到控制台端口，并复制显示的所有消息。尝试按上/下键盘键或PageUp键查看屏幕上的所有消息。

步骤 10：执行冷重启

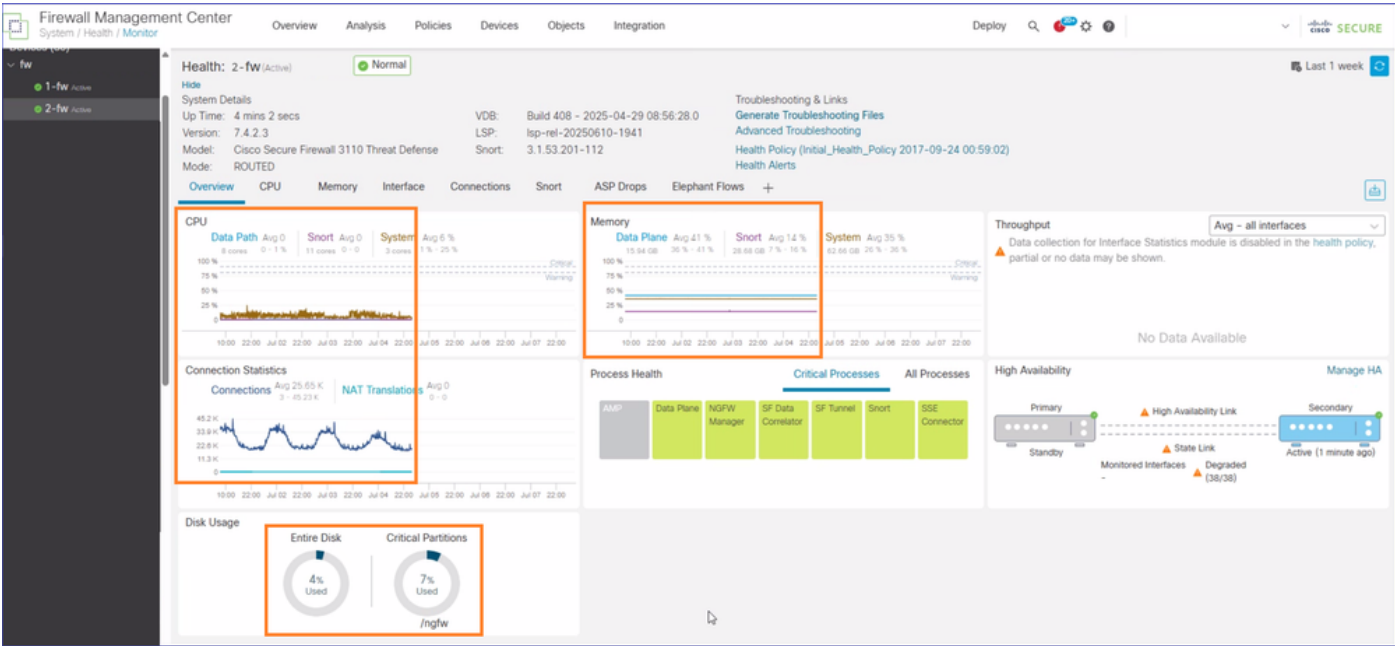
将笔记本电脑连接到控制台端口：

- 1. 拔下所有电源线，等待几分钟，然后再重新插上。
- 2. 在故障切换设置或集群设置的情况下，为了最大程度地降低主用/主用或集群不稳定的任何风险，您可以从邻接交换机设备拔出或关闭受影响单元的所有数据接口，包括HA或CCL链路。
- 3. 然后，重新插入电源线并接通设备电源。
- 4. 等待约5分钟。
- 5. 收集控制台输出。

请注意，如果设备未正常关闭且设备运行正常（前面板LED亮起），冷重新启动可能会导致数据库损坏。如果冷重启启动设备，请收集故障排除捆绑包并联系思科TAC。

步骤 11：从FMC收集运行状况监控器图形

如果设备恢复并由FMC管理，请导航到System > Health > Monitor，然后选择设备。关注突出显示的图表，了解设备在变得无响应之前所处的状态（例如，高内存、高CPU、高磁盘利用率等）。



步骤 12：检查磁盘问题

非工作场景(4100):

<#root>

FW4100#

show server storage

Server 1/1:

RAID Controller 1:

Type: SATA
Vendor: Cisco Systems Inc
Model: FPR4K-PT-01
Serial: JAD12345678
HW Revision:
PCI Addr: 00:31.2
Raid Support:
OOB Interface Supported: No
Rebuild Rate: N/A
Controller Status: Unknown

Local Disk 1:

Vendor: Micron
Model: 5300 MTFD
Serial: MSA123456AB
HW Rev:
Operability: N/A

Presence: Missing <-----

Size (MB): 200000
Drive State: Online
Power State: Active
Link Speed: 6 Gbps
Device Type: SSD

Local Disk Config Definition:

Mode: NO RAID
Description:
Protect Configuration: No

磁盘运行正常的3100的输出示例：

<#root>

FW3105#

show server storage

Server 1/1:

Disk Controller 1:

Type: SOFTRAIID
Vendor: Cisco Systems Inc
Model: FPR_SOFTRAIID
HW Revision:
PCI Addr:
Raid Support: raid1
OOB Interface Supported: No
Rebuild Rate: N/A
Controller Status: Optimal

Local Disk 1:
Presence: Equipped
Model: SAMSUNG MZQL2960HCJR-00A07
Serial: S64FNT0AB12345

Operability: Operable <---

Size (MB): 858306
Device Type: SSD
Firmware Version: GDC5A02Q

Virtual Drive 1:
Type: Raid
Blocks: 878906048
Operability: Degraded
Presence: Equipped
Size (MB): 858306
Drive State: Degraded

4100中磁盘运行正常时的输出示例：

<#root>

FW4125#

show server storage

Server 1/1:
RAID Controller 1:
Type: SATA
Vendor: Cisco Systems Inc
Model: FPR4K-PT-01
Serial: JAD1234567
HW Revision:
PCI Addr: 00:31.2
Raid Support:
OOB Interface Supported: No
Rebuild Rate: N/A
Controller Status: Unknown

Local Disk 1:
Vendor: TOSHIBA
Model: KHK61RSE
Serial: 11BS1234567AB
HW Rev: 0

Operability: Operable

Presence: Equipped
Size (MB): 800000
Drive State: Online
Power State: Active
Link Speed: 6 Gbps
Device Type: SSD

Local Disk Config Definition:
Mode: No RAID
Description:
Protect Configuration: No

步骤 13：日志分析

如果防火墙设备恢复并且您想要分析后端日志，请生成故障排除捆绑包并检查表中提到的文件。请注意：

- 在1xxx、12xx、21xx (设备模式)、31xx、42xx平台上，FTD故障排除捆绑包还包含\dir-archives\var-common-platform_ts\路径中FXOS的机箱(FPRM)捆绑包。您必须提取FPRM包的内容。
- 在3100/4200上的多实例(MI)模式下，从FMC UI或机箱CLI收集机箱TS文件(local-mgmt命令范围内的show tech-support fprm detail)，如
<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hld-2132091400>中所述。
- 在41xx、93xx平台上，您必须单独从机箱UI或FXOS CLI生成机箱套件，如
<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hld-2132091400>中所述。
- 对于4100和9300设备平台，您需要收集FXOS和FTD疑难解答程序包。对于所有其他平台，FTD疑难解答程序包就足够了，因为它还包含FXOS疑难解答程序包。
- 对于ASA，在恢复后show tech-support命令输出不是很有用。您必须依靠FXOS故障排除捆绑包。
- 与其他平台相比，在41xx、93xx上，您有两个故障排除捆绑包：机箱(BC1)和模块捆绑包。
- 41xx、93xx上的机箱捆绑包(BC1)包含FPRM和CIMC捆绑包等。
- 41xx、93xx上的模块捆绑包主要包含来自刀片的FXOS日志。
- 如果您安装了ASA，则只能依赖机箱、FPRM和模块捆绑包 (只要适用) 以及ASA的“show tech-support”命令输出。
- 根据平台和突发事件，并非所有文件都会显示。

故障排除捆绑包中的文件路径	说明/提
FTD TS套件：/dir-archives/var-log/messages*	在正常 符串“sy down”。 设备启 “syslog up”。

FTD TS套件：/dir-archives/var-log/ASAconsole.log 如果是4100/9300上的ASA，您也可以在/opt/cisco/platform/logs/ASAconsole.log下的模块捆绑包中找到该文件	查找错误等。
FTD TS套件：/dir-archives/var-log/dmesg.log	查找错误等。
FTD TS套件：/dir-archives/var/log/ngfwManager.log*	查找错误等。 此文件收集事件。
FTD TS套件：/command-outputs/LINA_troubleshoot/show_tech_output.txt	show fa “show c 输出可以 序的其他
FTD TS套件：/command-outputs/ 文件名： ·对于“ls opt-cisco-csp-cores _ grep core”_ do file -opt-cisco-csp-cores-_{CORE}_ done.output”中的CORE ·对于“ls var-common _ grep core”_ do file var-common-_{CORE}_ done.output”中的CORE ·对于“ls var-data-cores _ grep core”_ do file -var-data-cores-_{CORE}_ done.output”中的CORE	检查潜在（回溯
FTD TS套件：/dir-archives/var/log/crashinfo/snort3-crashinfo.*	检查Sn件。
FTD TS套件：/dir-archives/var/log/process_stderr.log*	检查回Bug ID
FTD TS套件：/dir-archives/var/log/periodic_stats/	该目录，可在见解。
FPRM捆绑包：tech_support_brief	检查“shdetail”输

FPRM捆绑包：/opt/cisco/platform/logs/kern.log	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/messages*	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/mce.log 模块捆绑包(41xx、93xx)中也存在相同的文件。	这是计划(mce)文档故障、
FPRM捆绑包：/opt/cisco/platform/logs/portmgr.out	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/ssp-pm.log 模块捆绑包(41xx、93xx)中也存在相同的文件。	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/sma.log 模块捆绑包(41xx、93xx)中也存在相同的文件。	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/heimdall.log	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/ssp-shutdown.log 模块捆绑包(41xx、93xx)中也存在相同的文件。	重新启动包含dm几行输入在1000/2提供。
FPRM捆绑包：/opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	查找错误等。
FPRM捆绑包：/opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	查找错误等。

CIMC套件(41xx、93xx): /obfl/obfl-log*	查找错误等。
CIMC套件(41xx、93xx): /CIMC1_TechSupport.tar.gz/CIMC1_TechSupport.tar/tmp/techsupport_pid*/CIMC1_TechSupport-nvram.tar.gz/CIMC1_TechSupport-nvram.tar/nv/etc/log/eng-repo/messages*	查找错误等。 尤其对
模块套件(41xx、93xx): /tmp/mount_media.log/mount_media.log	查找错误等。

步骤 14：捕获

如果特定接口变得无响应，则获取防火墙和相邻设备上的捕获。有关详细信息，请参阅本文档：

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

此外，请确保正确填充邻接设备的ARP表和CAM表。

步骤 15：提供给Cisco TAC的其他信息

除上述项目外，强烈建议同时提供以下信息：

15a. 如果设备已恢复，请收集故障排除捆绑包（有关详细信息，请查看步骤13）。

15b. 如果设备仍然没有响应，请提供以下信息：

- 硬件信息（型号）。
- 软件信息。
- FMC软件信息（如果适用）。
- 部署（独立/高可用性/集群）。

15c. 设备无响应的大概时间（日期/时间）。

15d. 设备无响应前的大致正常运行时间。

15e. 这是新设置还是现有设置？

15f. 在设备变得无响应之前，最后一次执行什么操作？

15g. 防火墙数据平面(LINA)系统日志从设备无响应时开始（尝试获取事件前5分钟开始的日志）。

作为一种最佳实践，建议将系统日志配置为第6级（信息性）。

15小时。如果您已在机箱上配置系统日志服务器（4100/9300上的FXOS），请提供日志（从事故发生前约5分钟开始）。

15i。从事件发生时开始从相邻设备发送系统日志。

15j。显示防火墙设备与相邻设备之间物理连接的拓扑图。

常见问题

Error:与DME通信超时

如果连接到控制台并参阅：

```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

在大多数情况下，这表示存在软件问题。

建议操作：联系思科TAC

磁盘错误：丢失或不可操作

此输出来自生成磁盘相关故障的4100/9300硬件设备：

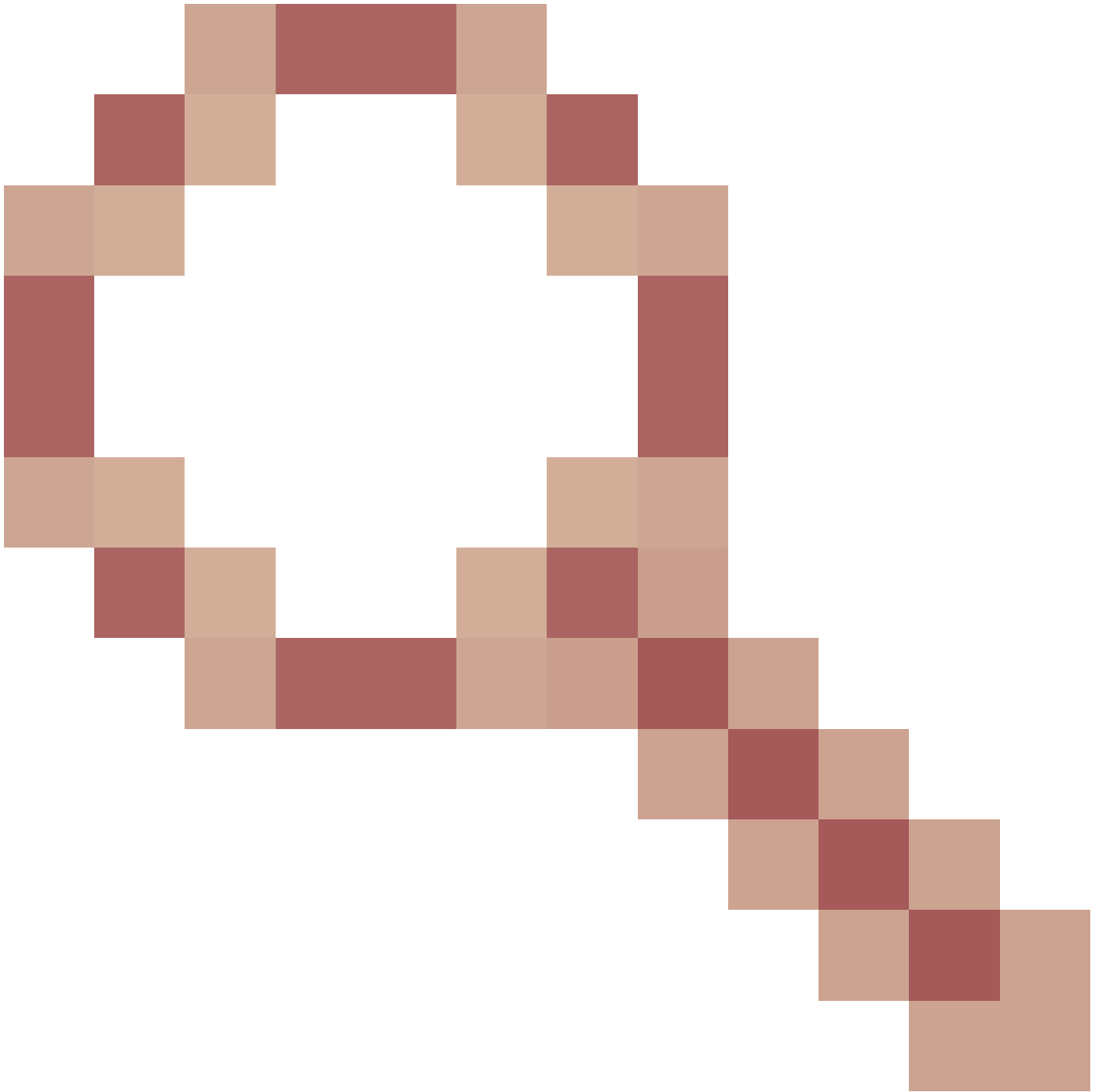
Overview	Interfaces	Logical Devices	Security Engine	Platform Settings
Hardware State	Service State	Power	Application	
Up	Fault	On	Cisco Firepower Threat Defense	
Disk on a Security Module has errors Please verify the disk presence and replace the faulty disk if the fault does not clear Security Module: 1 Disk: \$(disk_a) missing or inoperable Rebooting Blade...				

建议操作：尝试重新拔插SSD磁盘。如果它不起作用，请收集机箱故障排除捆绑包并联系思科TAC。

Field Notice：FN72077 - FPR9300和FPR4100

- FPR9300和FPR4100系列安全设备不再传递网络流量。
- 具有有效凭据的用户无法登录到管理控制台。
- CLI显示错误消息："Software Error:执行过程中的异常：[Error:与DME通信超时]

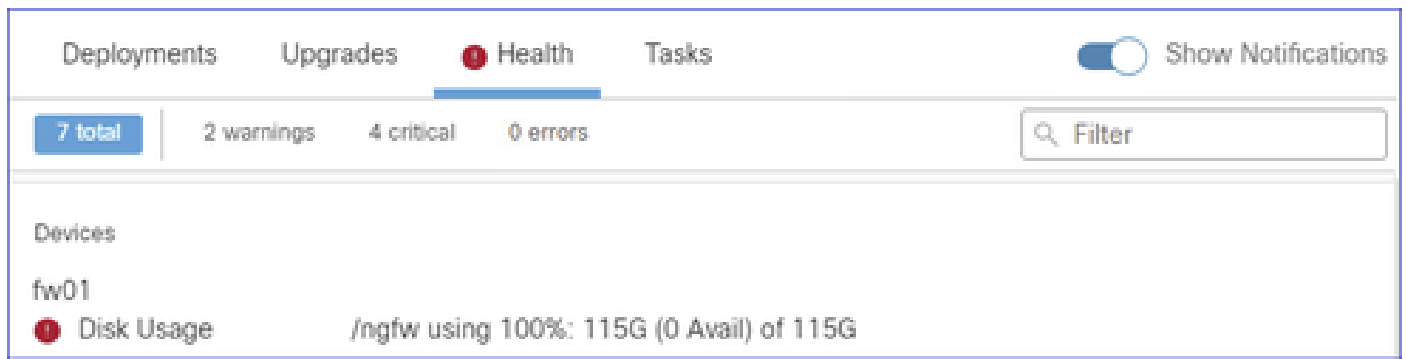
建议操作：需要对4100/9300机箱重新通电才能暂时解决此问题。有关详细信息，请查看Cisco Bug ID [CSCvx99172](#)，了解具有修复程序的版本。



(问题信息通告:FN72077 - FPR9300和FPR4100系列安全设备 — 某些设备在3.2年的正常运行时间后可能无法传递流量)。

磁盘利用率100%

防火墙上的磁盘空间过低可能导致设备无响应。如果设备由FMC管理，您可以收到如下运行状况警报：

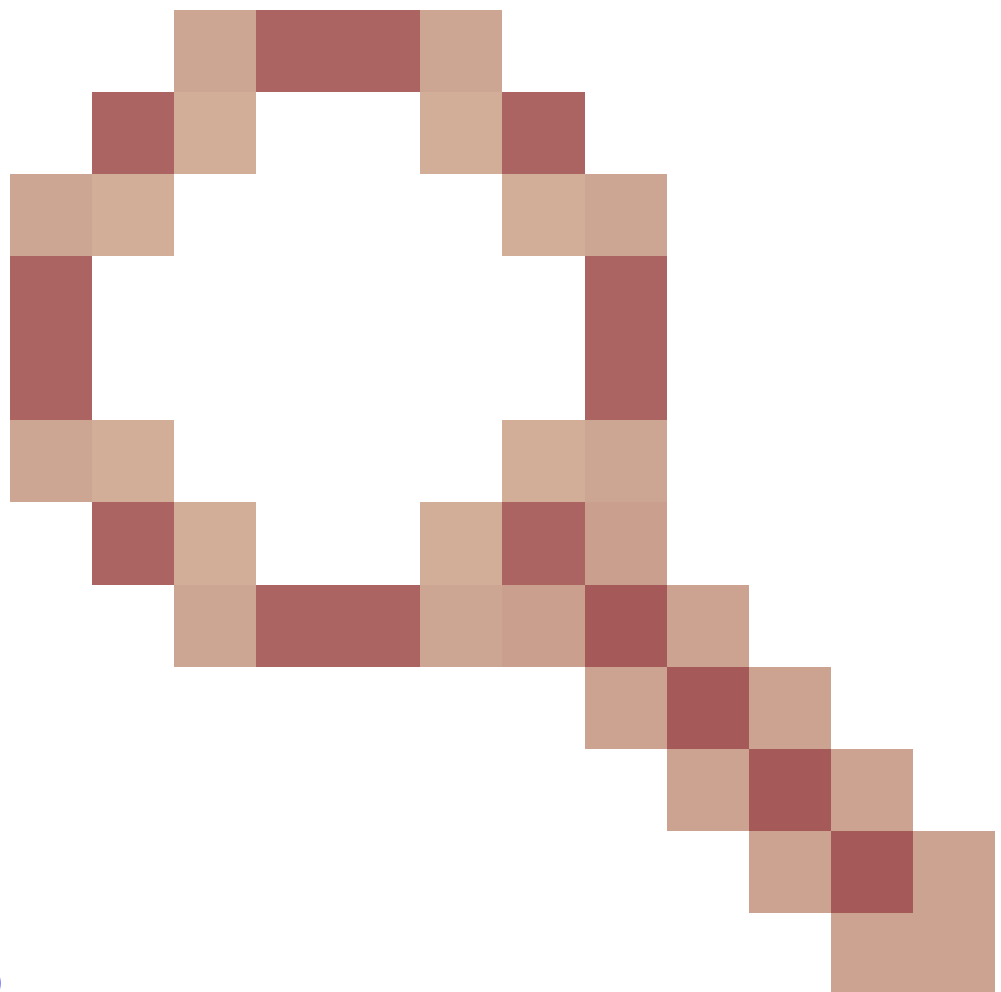


建议操作：如果您的FMC和FTD运行在软件7.7.0及更高版本上，请尝试使用<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space>上记录的过程清除一些磁盘空间

如果此操作不可行或无效，请联系思科TAC。

断电后，CSF 3100无法启动

建议操作：升级到具有以下修复程序的软件版本：



Cisco Bug ID [CSCwm14729](#)

断电后，CSF 3100系列无法重新启动，需要手动重新通电。

Cisco Firepower 2100系列安全设备：某些单元可能会遇到内存故障

- 5年服务期内由于组件流程问题导致的DIMM故障
- 相关FN:<https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html>
- 相关Cisco Bug ID [CSCwb74948](#)

建议操作：更换DIMM组件或更换安全设备

参考

- <https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>
- <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#>
- <https://www.cisco.com/c/en/us/support/docs/field-notices/720/fn72077.html>
- <https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/216245-collection-of-core-files-from-a-firepowe.html#anc6>
- <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

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）。