

對無響應的思科安全防火牆進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[疑難排解](#)

[步驟 1:外觀檢查 \(前面板\)](#)

[步驟 2:外觀檢查 \(後面板\)](#)

[步驟 3:風扇檢查](#)

[步驟 4:物理環境檢查](#)

[步驟 5:控制檯和管理埠檢查](#)

[步驟 6:管理IP連通性測試](#)

[步驟 7:相鄰裝置檢查](#)

[步驟 8:HA/集群裝置檢查](#)

[步驟 9:收集控制檯日誌](#)

[步驟 10:執行冷重新啟動](#)

[步驟 11:從FMC收集運行狀況監視器圖形](#)

[步驟 12:檢查磁碟問題](#)

[步驟 13:日誌分析](#)

[步驟 14:擷取](#)

[步驟 15:要提供給Cisco TAC的其他資訊](#)

[常見問題](#)

[錯誤：與DME通訊超時](#)

[磁碟錯誤：丟失或無法操作](#)

[公告：FN72077 - FPR9300和FPR4100](#)

[磁碟利用率100%](#)

[停電後，CSF 3100無法啟動](#)

[Cisco Firepower 2100系列安全裝置：某些裝置可能會遇到記憶體故障](#)

[參考資料](#)

簡介

本文檔介紹對1xxx、12xx、21xx、31xx、41xx、42xx和93xx硬體平台上無響應的思科安全防火牆威脅防禦(FTD)進行故障排除的建議步驟。

必要條件

思科建議您瞭解以下主題：

- Cisco Secure FTD基礎知識 (安裝/配置)。

需求

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦
- 思科安全防火牆管理中心
- Cisco Firepower可擴充作業系統(FXOS)

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在某些情況下，Cisco FTD裝置可能會變得無響應。典型症狀包括：

- 無SSH訪問。
- 沒有控制檯訪問。
- 控制檯訪問正在工作，但登入憑據未工作。
- 傳輸流量不通過裝置。
- 介面關閉 (資料和/或管理)。
- 指示燈熄滅或呈琥珀色 (閃爍或呈穩定亮起)。
- 安全模組(4100、9300)變為無響應。

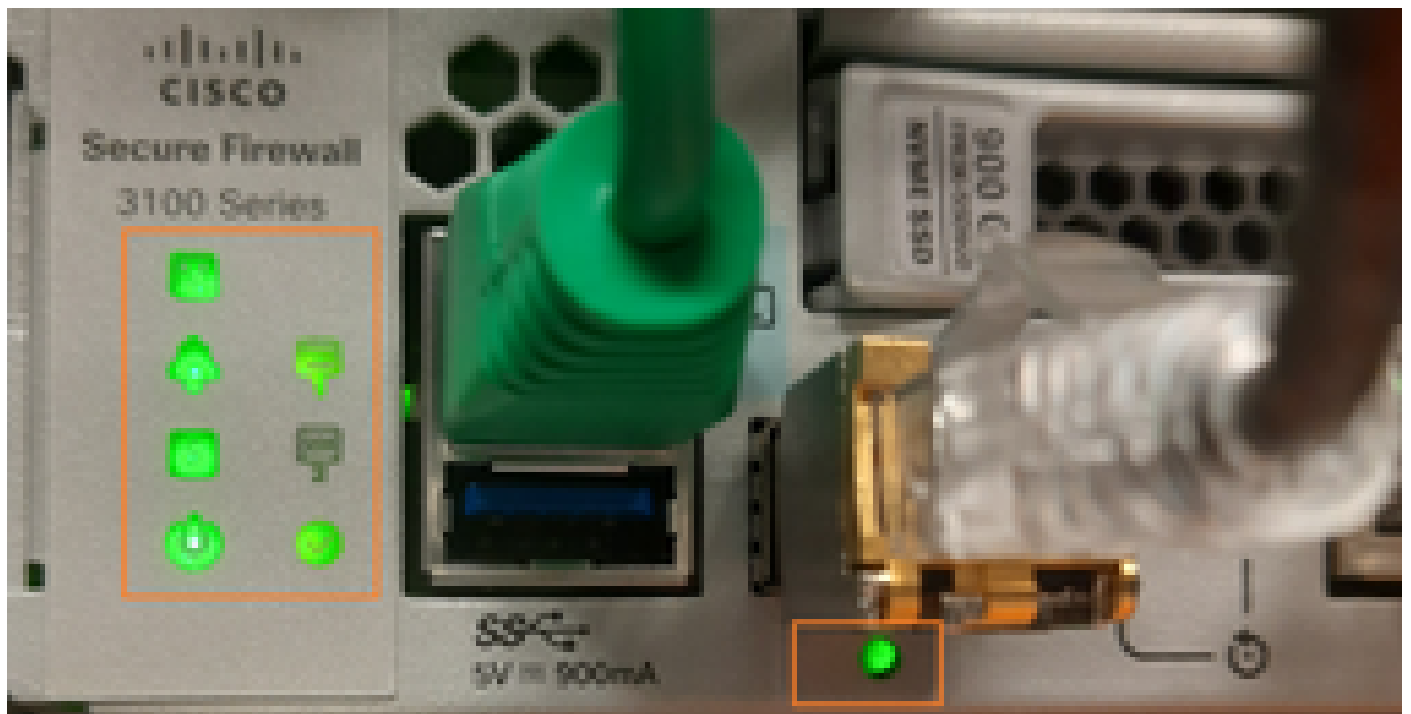
請注意，根據具體情況，其中某些產品將不顯示。例如，可以有傳輸流量通過，但只有管理訪問不起作用。

疑難排解

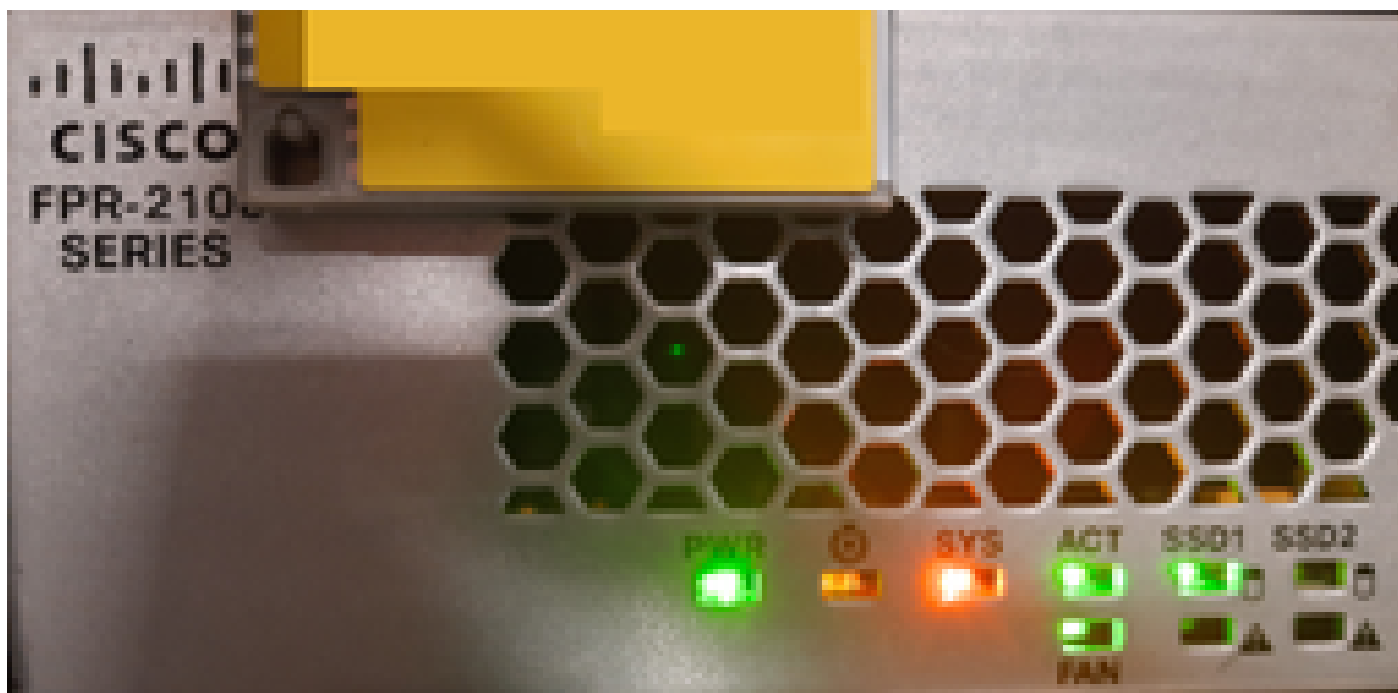
本節介紹您需要採取的推薦步驟和操作。您可以將此資訊提供給Cisco TAC，以進行進一步分析。

步驟 1:外觀檢查 (前面板)

拍攝前面板LED的影片或圖片。以下範例顯示所有LED：



在下一張照片中，SYS LED指示裝置問題：



您可以參考裝置型號的硬體指南，以獲取有關LED的其他資訊，例如：

型號	LED資訊
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、 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

步驟 2:外觀檢查 (後面板)

拍攝後面板上的LED影片或圖片，例如：



如果您沒有看到任何電源指示燈亮起：

- 嘗試重新拔插電源 (如果適用)。
- 如果可能，請嘗試更換電源。

步驟 3:風扇檢查

驗證裝置背面的風扇是否正在運行。

步驟 4:物理環境檢查

驗證是否有來自裝置的噪音或氣味。

步驟 5:控制檯和管理埠檢查

確保控制檯和管理埠連線正確。如果問題僅出現在管理埠上，請嘗試更改SFP（如果適用）和網路電纜。

步驟 6:管理IP連通性測試

嘗試ping(ICMP)裝置的管理IP。

步驟 7:相鄰裝置檢查

檢查相鄰裝置的埠狀態，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

步驟 8:HA/集群裝置檢查

在高可用性(HA)或群集設定的情況下，從對等裝置收集故障排除捆綁包。

步驟 9:收集控制檯日誌

將筆記型電腦連線到控制檯埠，並複製顯示的所有消息。嘗試按上/下鍵盤鍵或PageUp鍵檢視螢幕上的所有消息。

步驟 10:執行冷重新啟動

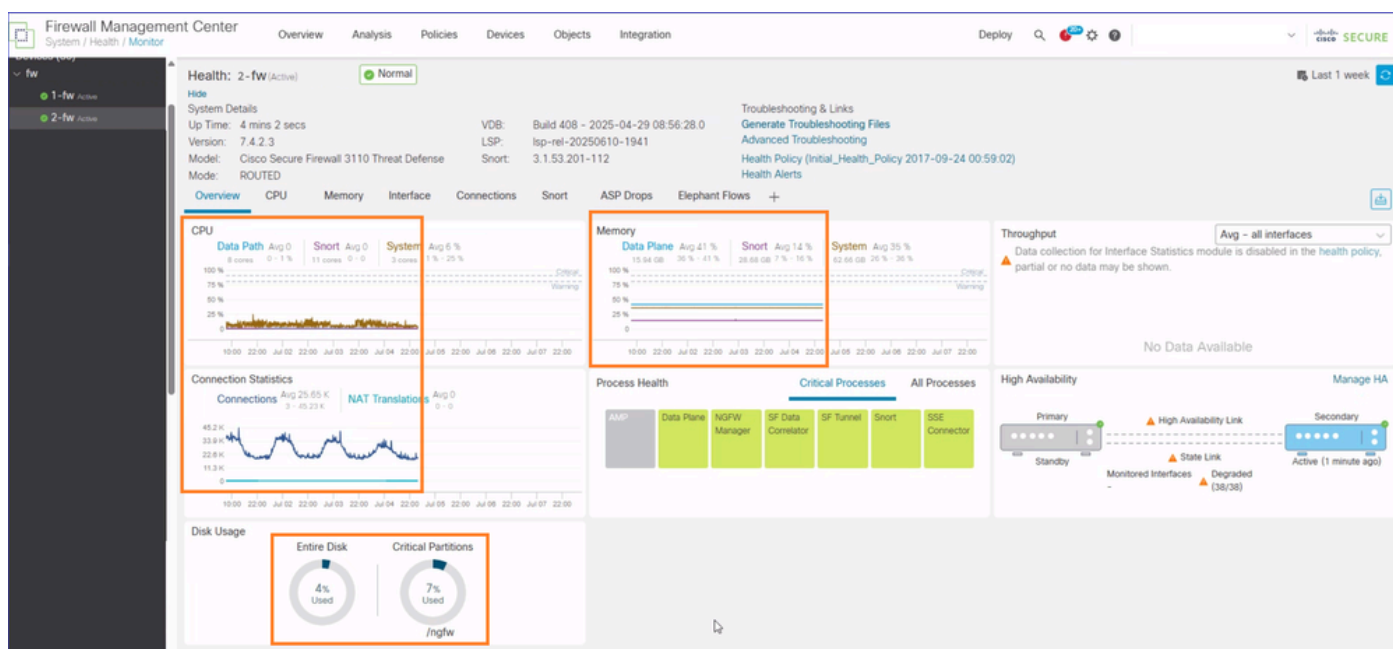
將筆記型電腦連線到控制檯埠：

1. 拔下所有電源線，等待幾分鐘，然後再重新插上。
2. 在故障轉移設定或群集設定的情況下，為了最大程度地降低主用/主用或群集不穩定的任何風險，您可以從相鄰交換機裝置拔出或關閉受影響裝置的所有資料介面，包括HA或CCL鏈路。
3. 然後，重新插入電源線並開啟裝置的電源。
4. 等待~5分鐘。
5. 收集控制檯輸出。

請注意，如果裝置未正常關閉且裝置運行正常（前面板LED指示燈亮起），冷重新啟動可能會導致資料庫損壞。如果冷重啟導致裝置啟動，請收集故障排除捆綁包並聯絡思科TAC。

步驟 11:從FMC收集運行狀況監視器圖形

如果裝置恢復並由FMC管理，請導航到System > Health > Monitor，然後選擇裝置。關注突出顯示的圖表，瞭解裝置在進入無響應狀態之前的狀態（例如，高記憶體、高CPU、高磁碟利用率等）。



步驟 12:檢查磁碟問題

非工作場景(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

磁碟運行正常的3100的輸出示例：

<#root>

FW3105#

show server storage

Server 1/1:

Disk Controller 1:

Type: SOFTRAID
Vendor: Cisco Systems Inc
Model: FPR_SOFTRAID
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中磁碟運行正常時的輸出示例：

<#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

步驟 13: 日誌分析

如果防火牆裝置恢復，並且您想要分析後端日誌，請生成故障排除捆綁包並檢查表中提到的檔案。
請注意：

- 在1xxx、12xx、21xx (裝置模式)、31xx和42xx平台上，FTD故障排除捆綁包還包含來自FXOS的機箱(FPRM)捆綁包，路徑為\dir-archives\var-common-platform_ts\。您必須解壓FPRM套件組合的內容。
- 在多例項(MI)模式下的3100/4200上，從FMC UI或機箱CLI收集機箱TS檔案(local-mgmt命令範圍中的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-h1d-2132091400>中所述。
- 在41xx、93xx平台上，您必須從機箱UI或FXOS CLI單獨生成機箱套件，如
<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>中所述
- 對於4100和9300裝置平台，您需要收集FXOS和FTD疑難排解捆綁包。對於所有其他平台，FTD疑難排解捆綁包已足夠，因為它還包含FXOS疑難排解捆綁包。
- 對於ASA，「show tech-support」命令在恢復後輸出沒有多大幫助。您必須依靠FXOS疑難排解套件組合。
- 與其他平台相比，在41xx和93xx上，您有兩個故障排除捆綁包：機箱(BC1)和模塊套件。
- 41xx、93xx上的機箱套件(BC1)包含FPRM和CIMC套件組合。
- 41xx、93xx上的模組捆綁包主要包含來自刀片的FXOS日誌。
- 如果安裝了ASA，則只能依靠機箱、FPRM和模組捆綁包 (如果適用) 以及ASA的「show tech-support」命令輸出。
- 根據平台和突發事件，並非所有檔案都存在。

疑難排解套件組合中的檔案路徑	說明/提
FTD TS套件：/dir-archives/var-log/messages*	平滑關 「syslo down」 當裝置

	串「sysup」。
FTD TS套件：/dir-archives/var-log/ASAconsole.log 如果是4100/9300上的ASA，您還可以在/opt/cisco/platform/logs/ASAconsole.log下的模組捆綁包中找到該檔案	查詢錯誤等。
FTD TS套件：/dir-archives/var-log/dmesg.log	查詢錯誤等。
FTD TS套件：/dir-archives/var/log/ngfwManager.log*	查詢錯誤等。 此檔案在HA/Cluster中。
FTD TS套件：/command-outputs/LINA_troubleshoot/show_tech_output.txt	「show history cluster」可以提及其他見解
FTD TS套件：/command-outputs/ 檔名： ·對於「ls opt-cisco-csp-cores _ grep core」_ do file -opt-cisco-csp-cores-_{CORE}_ done.output ·對於'ls var-common _ grep core'_ do file var-common-_{CORE}_ done.output中的CORE ·對於「ls var-data-cores _ grep core」_ do file -var-data-cores-_{CORE}_ done.output中的CORE	檢查可能（回溯）
FTD TS套件：/dir-archives/var/log/crashinfo/snort3-crashinfo.*	檢查Snort3檔案。
FTD TS套件：/dir-archives/var/log/process_stderr.log*	檢查反饋 Cisco錯誤 CSCwh
FTD TS套件：/dir-archives/var/log/periodic_stats/	該目錄

	，可在 見解。
FPRM搭售方案：tech_support_brief	檢查「s detail」
FPRM搭售方案：/opt/cisco/platform/logs/kern.log	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/messages*	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/mce.log 模組捆綁包(41xx、93xx)中也存在相同的檔案。	這是電 (mce)檔 故障、
FPRM搭售方案：/opt/cisco/platform/logs/portmgr.out	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/ssp-pm.log 模組捆綁包(41xx、93xx)中也存在相同的檔案。	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/sma.log 模組捆綁包(41xx、93xx)中也存在相同的檔案。	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/heimdall.log	查詢錯誤 等。
FPRM搭售方案：/opt/cisco/platform/logs/ssp-shutdown.log 模組捆綁包(41xx、93xx)中也存在相同的檔案。	重新啟 包含dm 幾行輸 1000/2 供。

FPRM搭售方案：/opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	查詢錯誤等。
FPRM搭售方案：/opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	查詢錯誤等。
CIMC套件(41xx、93xx): /obfl/obfl-log*	查詢錯誤等。
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*	查詢錯誤等。 尤其適
模組套件(41xx、93xx): /tmp/mount_media.log/mount_media.log	查詢錯誤等。

步驟 14:擷取

如果特定介面在防火牆和相鄰裝置上變為無響應Take捕獲。如需詳細資訊，請參閱本檔案：

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

此外，請確保正確填充相鄰裝置的ARP表和CAM表。

步驟 15:要提供給Cisco TAC的其他資訊

除上述專案外，強烈建議還提供以下資訊：

15a. 如果裝置已恢復，請收集故障排除捆綁包（有關詳細資訊，請檢視步驟13）。

15b. 如果裝置仍然沒有響應，請提供以下資訊：

- 硬體資訊（型號）。
- 軟體資訊。
- FMC軟體資訊（如果適用）。
- 部署（獨立/HA/集群）。

15c. 裝置變得無響應時的近似時間（日期/時間）。

15天。裝置變得無響應之前的大致正常運行時間。

15e。這是新設定還是現有設定？

15f。在裝置變得無響應之前執行的最後一個操作是什麼？

15克。防火牆資料平面(LINA)自裝置沒有回應時開始系統日誌（嘗試取得事件前5分鐘開始的日誌）。作為一種最佳實踐，建議將系統日誌配置為第6級（資訊性）。

15小時。如果您在機箱上配置了系統日誌伺服器（4100/9300上的FXOS），請提供日誌（從事件之前約5分鐘開始）。

15i。從事件發生時開始從相鄰裝置發出syslog。

15j。顯示防火牆裝置和相鄰裝置之間的物理連線的拓撲圖。

常見問題

錯誤：與DME通訊超時

如果您連線到主控台並參閱：

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

大多數情況下，這表示存在軟體問題。

建議的操作：聯絡Cisco TAC

磁碟錯誤：丟失或無法操作

此輸出來自生成磁碟相關故障的4100/9300硬體裝置：

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..				

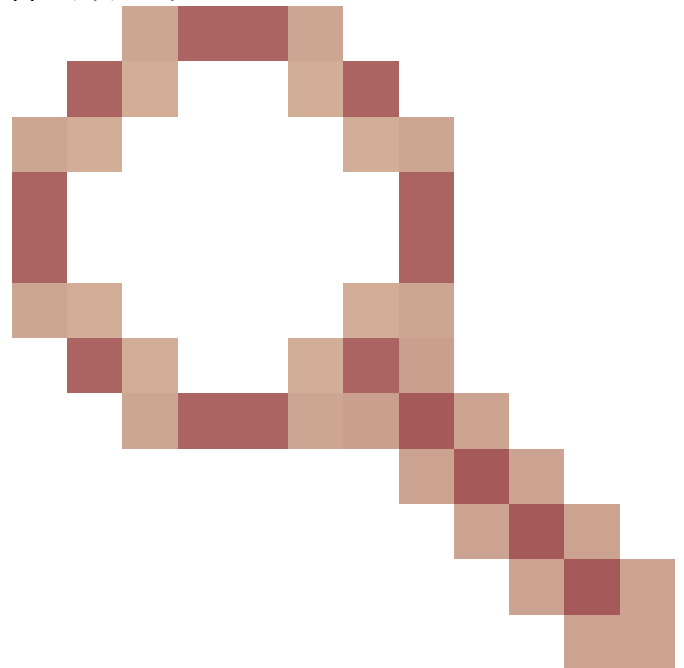
建議的操作：嘗試重新拔插SSD磁碟。如果沒有幫助，請收集機箱故障排除捆綁包並聯絡思科TAC。

公告：FN72077 - FPR9300和FPR4100

- FPR9300和FPR4100系列安全裝置不再傳遞網路流量。
- 具有有效憑據的使用者無法登入到管理控制檯。

- CLI顯示錯誤消息："軟體錯誤：執行過程中出現異常：[錯誤：與DME通訊超時]

建議的操作：需要對4100/9300機箱重新通電，才能暫時解決此問題。檢查思科錯誤ID

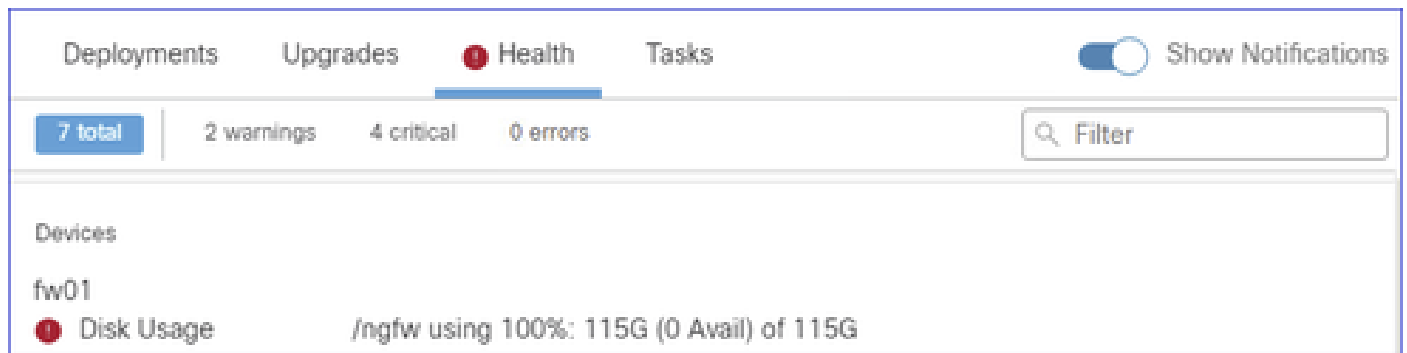


[CSCvx99172](#)以瞭解詳細資訊和有修正程式的版本。

(公告：FN72077 - FPR9300和FPR4100系列安全裝置 — 某些裝置在3.2年的正常運行時間後可能無法傳遞流量)。

磁碟利用率100%

防火牆上的磁碟空間過低可能會使裝置失去響應。如果裝置由FMC管理，您可以收到如下運行狀況警報：



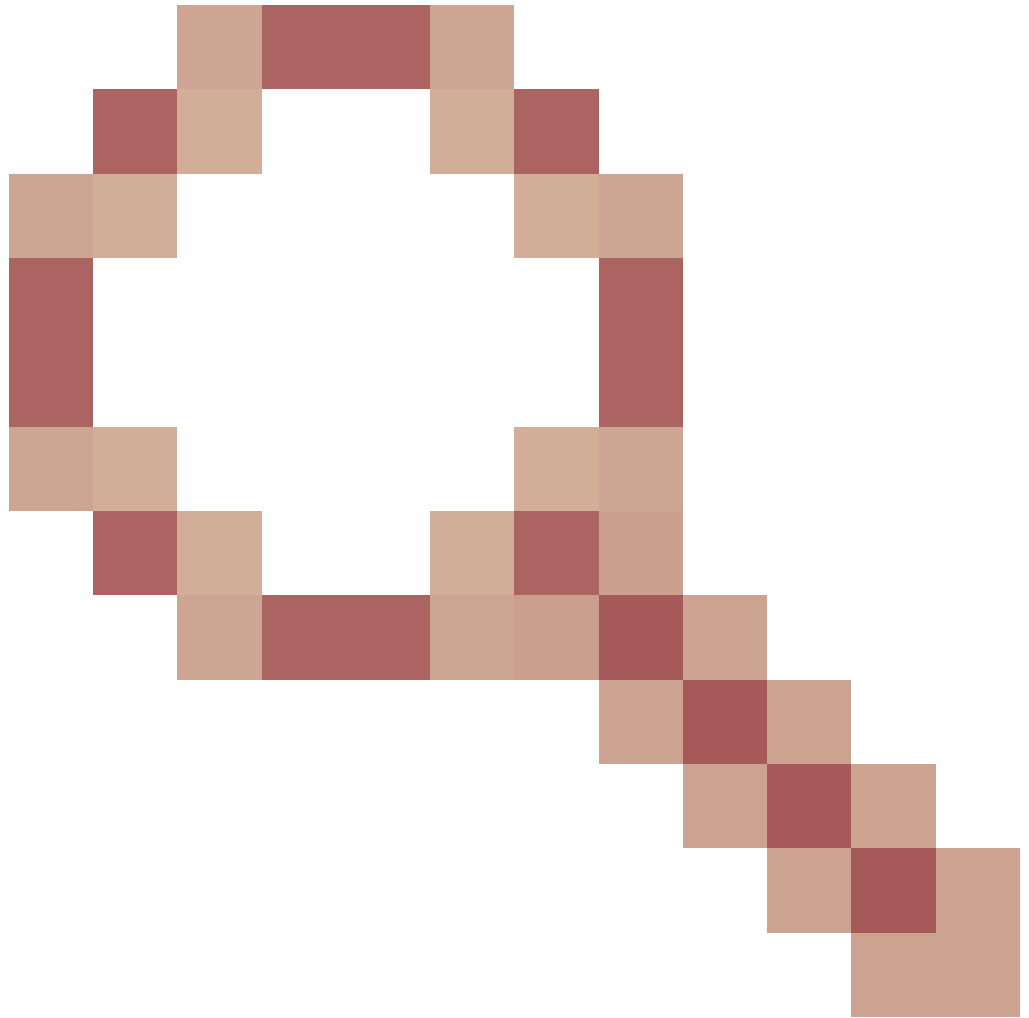
建議的操作：如果您的FMC和FTD運行在軟體7.7.0及更高版本上，請嘗試使用

<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>上記錄的步驟清除某些磁碟空間

如果此操作不可行或無效，請聯絡Cisco TAC。

停電後，CSF 3100無法啟動

建議的操作：升級至具有下列修復程式的軟體版本：



思科錯誤ID [CSCwm14729](#)

停電後，CSF 3100系列無法重新啟動，需要手動重新通電。

Cisco Firepower 2100系列安全裝置：某些裝置可能會遇到記憶體故障

- 5年內由於元件處理問題而導致DIMM故障
- 相關FN:<https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html>
- 相關思科錯誤ID [CSCwb74948](#)

建議的操作:更換DIMM元件或更換安全裝置

參考資料

- <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>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。