

応答しないCisco Secure Firewallのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[トラブルシュート](#)

[ステップ1: 目視検査 \(前面パネル\)](#)

[ステップ2: 目視検査 \(背面パネル\)](#)

[ステップ3: ファンの確認](#)

[ステップ4: 物理環境の確認](#)

[ステップ5: コンソールおよび管理ポートのチェック](#)

[ステップ6: 管理IP接続テスト](#)

[ステップ7: 隣接デバイスの確認](#)

[ステップ8: HA/クラスタデバイスの確認](#)

[ステップ9: コンソールログの収集](#)

[ステップ10: コールドリブートを実行する](#)

[ステップ11: FMCからヘルスモニタグラフを収集します](#)

[手順12: ディスクの問題を確認する](#)

[ステップ13: ログ分析](#)

[ステップ14: キャプチャ](#)

[ステップ15: Cisco TACに提供する追加情報](#)

[一般的な問題](#)

[エラー: DMEとの通信がタイムアウトしました](#)

[ディスクエラー: 見つからないか、操作できません](#)

[フィールド通知: FN72077 - FPR9300およびFPR4100](#)

[ディスク使用率100%](#)

[停電後、CSF 3100が起動しない](#)

[Cisco Firepower 2100シリーズセキュリティアプライアンス: 一部のユニットでメモリ障害が発生する可能性があります](#)

[参考資料](#)

はじめに

このドキュメントでは、1xxx、12xx、21xx、31xx、41xx、42xx、および93xxハードウェアプラットフォームで応答しないCisco Secure Firewall Threat Defense(FTD)のトラブルシューティングに推奨される手順について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco Secure FTDの基本 (インストール/設定)

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall脅威対策
- Cisco Secureファイアウォール管理センター
- Cisco Firepower eXtensibleオペレーティングシステム(FXOS)

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

場合によっては、Cisco FTDデバイスが応答しなくなることがあります。通常は次の症状が生じます。

- SSHアクセスなし。
- コンソールアクセスなし。
- コンソールアクセスは機能しているが、ログインクレデンシャルが機能していない。
- トランジットトラフィックはデバイスを通過しません。
- インターフェイスがダウンしている (データまたは管理) 。
- LEDは消灯またはオレンジ (点滅または点灯) です。
- セキュアモジュール(4100、9300)が応答しなくなります。

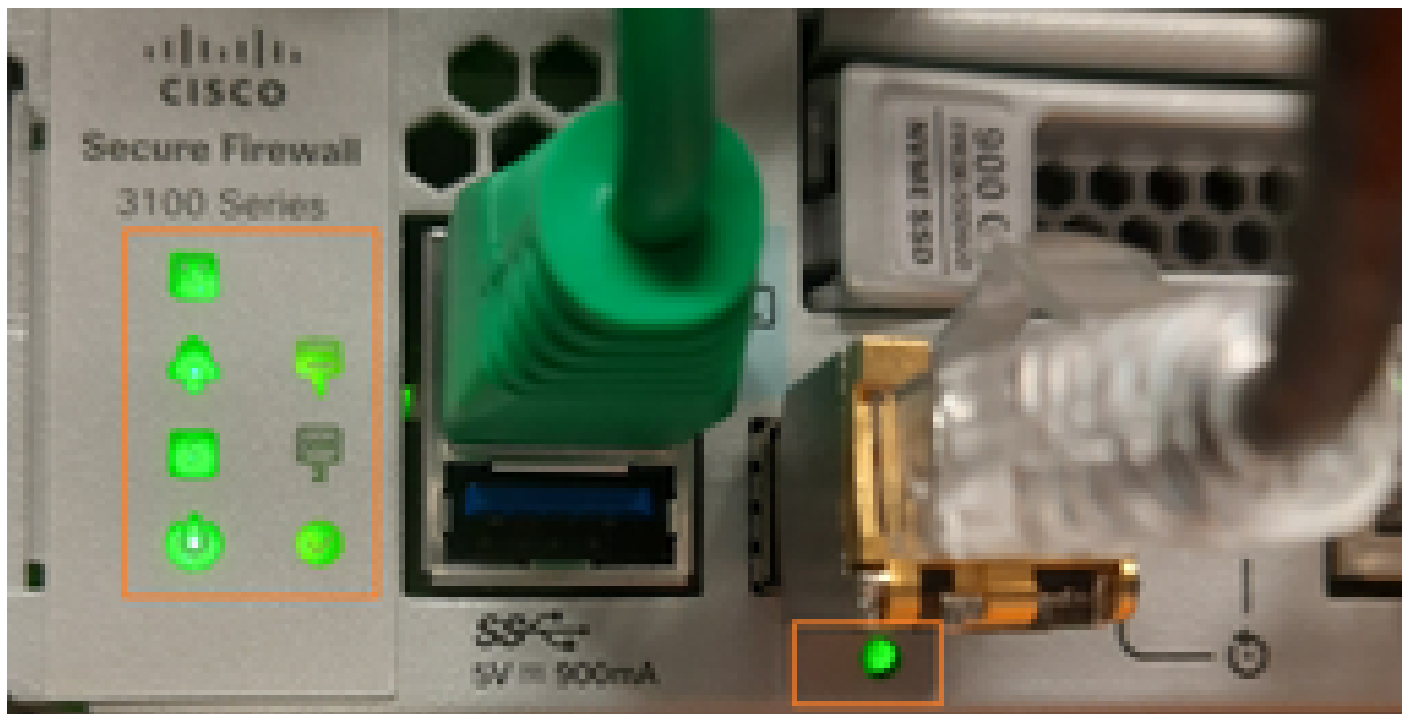
状況によっては、一部の参加者が出席しないことがあります。たとえば、通過トラフィックは通過させても、管理アクセスだけが機能しない場合があります。

トラブルシューティング

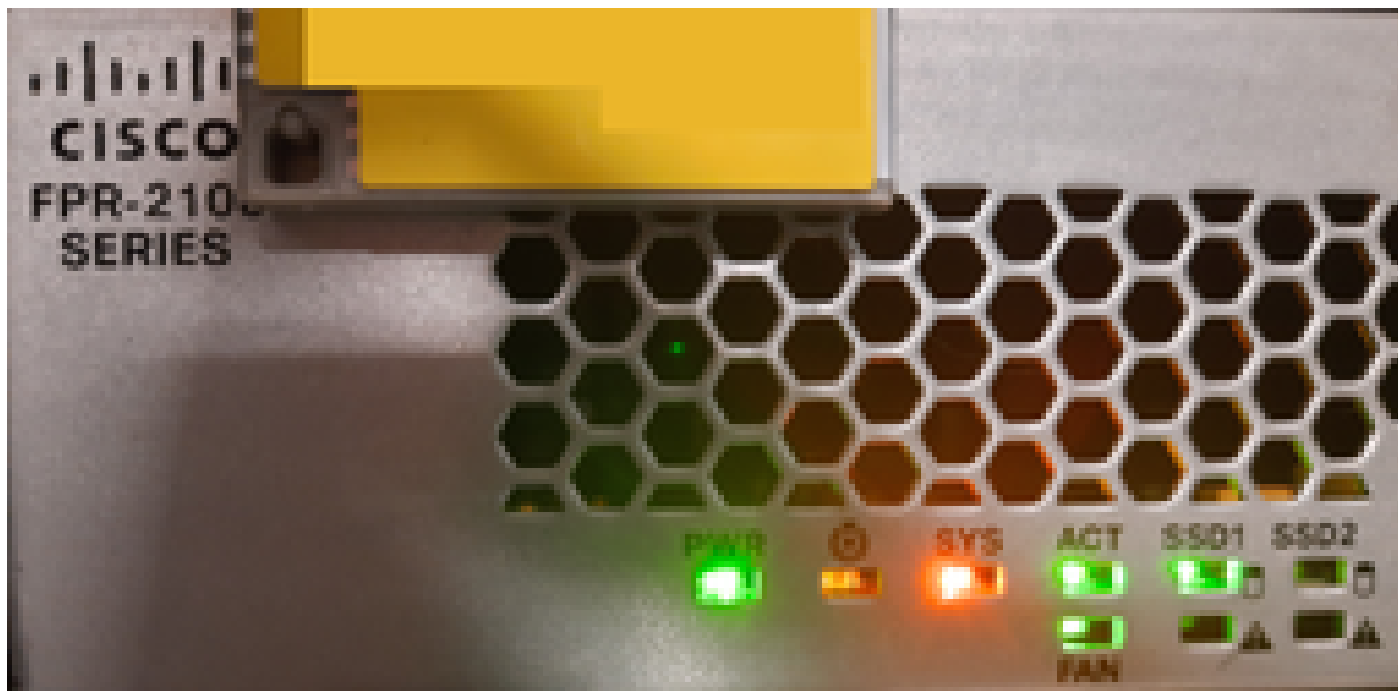
このセクションでは、推奨される手順と実行する必要があるアクションについて説明します。この情報をCisco TACに提供して、さらなる分析を行うことができます。

ステップ1：目視検査 (前面パネル)

前面パネルのLEDのビデオまたは画像を撮影します。すべてのLEDがはっきり見える例を次に示します。



次の写真では、SYS LEDがデバイスの問題を示しています。



デバイスモデルのハードウェアガイドを参照して、LEDに関する追加情報を取得できます。次に例を示します。

モデル	LED情報
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overvi
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/over
1210CE、 1210CP、 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-12
1230、 1240、 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/n
4110、 4120、 4140、	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/

4150	
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/m
9300	https://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300/

ステップ2：目視検査（背面パネル）

背面パネルのLEDのビデオまたは写真を撮影します。例：



電源LEDが点灯していない場合：

- 可能な限り、電源モジュールを取り付け直します。
- 可能であれば、電源を交換してみてください。

ステップ3：ファンの確認

アプライアンスの背面にあるファンが動作しているかどうかを確認します。

ステップ4：物理環境の確認

デバイスから異音や異臭が聞こえるかどうかを確認します。

ステップ5：コンソールおよび管理ポートのチェック

コンソールと管理ポートが正しく接続されていることを確認します。問題が管理ポートでのみ発生する場合は、SFP（該当する場合）とネットワークケーブルを変更してみてください。

ステップ6：管理IP接続テスト

デバイスの管理IPにping(ICMP)を試行します。

ステップ7：隣接デバイスの確認

隣接デバイスのポートステータスを確認します。次に例を示します。

```
<#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

ステップ8:HA/クラスタデバイスの確認

ハイアベイラビリティ(HA)またはクラスタセットアップの場合は、ピアデバイスからトラブルシューティングバンドルを収集します。

ステップ9：コンソールログの収集

ラップトップをコンソールポートに接続し、表示されているメッセージをすべてコピーします。画面上のすべてのメッセージを表示するには、上/下のキーボードキーまたはPageUpキーを押します。

ステップ10：コールドリブートを実行する

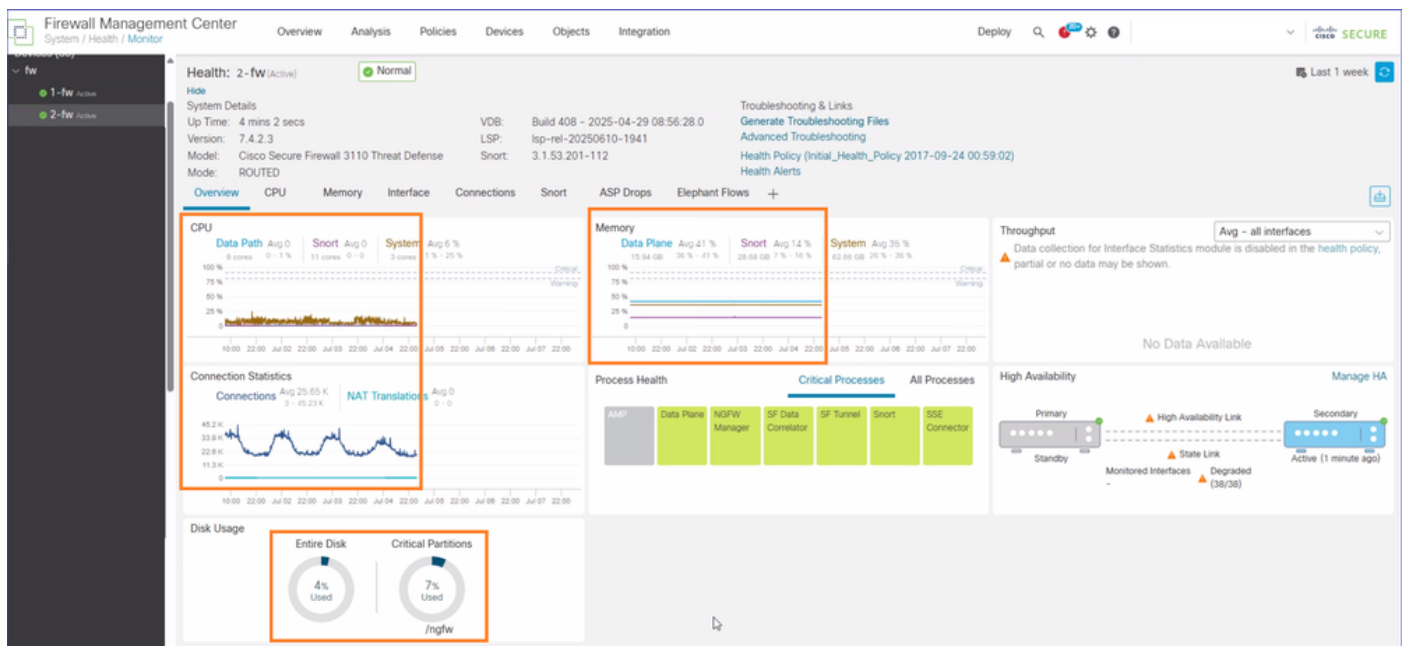
コンソールポートにラップトップを接続した場合：

1. すべての電源ケーブルのプラグを抜き、数分待ってからプラグを差し戻します。
2. フェールオーバーセットアップまたはクラスタセットアップの場合に、アクティブ/アクティブまたはクラスタが不安定になるリスクを最小限に抑えるため、HAまたはCCLリンクを含む、影響を受けるユニットのすべてのデータインターフェイスを、隣接するスイッチデバイスから取り外すか、シャットダウンすることができます。
3. 次に、電源ケーブルを接続し直し、デバイスの電源を入れます。
4. 5分待ちます。
5. コンソール出力を収集します。

デバイスが正常にシャットダウンされず、デバイスが動作可能な場合（前面パネルのLEDが点灯している場合）は、コールドリブートによってデータベースが破損する可能性があることに注意してください。コールドリブートによってデバイスが起動した場合は、トラブルシューティングバンドルを収集し、Cisco TACに連絡してください。

ステップ11:FMCからヘルスマニタグラフを収集します

デバイスが回復し、FMCによって管理されている場合は、System> Health > Monitorに移動して、デバイスを選択します。強調表示されたグラフに注目して、デバイスが応答しなくなる前のステータス（メモリの増加、CPUの使用率の上昇、ディスクの使用率の上昇など）を把握します。



手順12：ディスクの問題を確認する

非稼働シナリオ(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
```

ディスクが動作している場合の3100からの出力例：

```
<#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

ディスクが動作している場合の4100からの出力例：

<#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

ステップ13：ログ分析

ファイアウォールデバイスが回復し、バックエンドログを分析する場合は、トラブルシューティングバンドルを生成し、表に記載されているファイルを確認します。次の点に注意してください。

- 1xxx、12xx、21xx (アプライアンスモード)、31xx、42xxプラットフォームでは、FTDトラブルシューティングバンドルには\dir-archives\var-common-platform_ts\パスのFXOSからのシャーシ(FPRM)バンドルも含まれています。FPRMバンドルの内容を抽出する必要があります。
- Multi-Instance(MI)モードの3100/4200で、
<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>の説明に従って、FMC UIまたはシャーシCLI(local-mgmtコマンドスコープでshow tech-support fprm detailを実行)からシャーシTSファイルを収集します。
- 41xx、93xxプラットフォームでは、
<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>の説明に従って、シャーシUIまたはFXOS CLIとは別にシャーシバンドルを生成する必要があります。
- 4100および9300デバイスプラットフォームの場合は、FXOSとFTDのトラブルシューティングバンドルを収集する必要があります。その他すべてのプラットフォームでは、FTDのトラブルシューティングバンドルにはFXOSのトラブルシューティングバンドルも含まれているため、このバンドルで十分です。
- ASAの場合、リカバリ後の「show tech-support」コマンド出力は非常に役に立ちません。FXOSのトラブルシューティングバンドルを利用する必要があります。
- 他のプラットフォームと比較すると、41xxおよび93xxには、シャーシ(BC1)とモジュールの2つのトラブルシューティングバンドルがあります。
- 41xx、93xxのシャーシバンドル(BC1)には、FPRMバンドルとCIMCバンドルが含まれています。

- 41xxおよび93xxのモジュールバンドルには、主にブレードからのFXOSログが含まれています。
- ASAがインストールされている場合、依存する必要があるのは、シャーシ、FPRM、およびモジュールバンドル（該当する場合）と、ASAからのshow tech-supportコマンド出力だけです。
- プラットフォームやインシデントによっては、すべてのファイルが存在するとは限りません。

トラブルシューティングバンドルのファイルパス	説明/ヒ
FTD TSバンドル：/dir-archives/var-log/messages*	グレー ダウン syslog- down」 。 デバイ 、文字 starting ます。
FTD TSバンドル：/dir-archives/var-log/ASAconsole.log 4100/9300上のASAの場合、このファイルは/opt/cisco/platform/logs/ASAconsole.logの下のもジュールバンドルにもあります	エラー、 どを探
FTD TSバンドル：/dir-archives/var-log/dmesg.log	エラー、 どを探
FTD TSバンドル：/dir-archives/var/log/ngfwManager.log*	エラー、 どを探 このフ HA/クラ 関する います。
FTD TSバンドル：/command-outputs/LINA_troubleshoot/show_tech_output.txt	「show history」 cluster' から、 ケース

	わかり
FTD TSバンドル : /command-outputs/ ファイル名 ・ 'ls opt-cisco-csp-core _ grep core'_内のCOREについては、「file -opt-cisco-csp-core-_{CORE}_ done.output ・ 'ls var-common _ grep core'_のCOREについては、var-common-_{CORE}_ done.outputファイルを実行してください。 ・ 'ls var-data-core _ grep core'_のCOREについては、ファイル - var-data-core-_{CORE}_ done.outputを実行してください。	潜在的な (トレ 確認し
FTD TSバンドル : /dir-archives/var/log/crashinfo/snort3-crashinfo*	Snort3 イルを
FTD TSバンドル : /dir-archives/var/log/process_stderr.log*	バック (例 : C CSCwh
FTD TSバンドル : /dir-archives/var/log/periodic_stats/	このデ 、イン の情報 のファ います。
FPRMバンドル : tech_support_brief	「show 出力を
FPRMバンドル : /opt/cisco/platform/logs/kern.log	エラー、 どを探
FPRMバンドル : /opt/cisco/platform/logs/messages*	エラー、 どを探
FPRMバンドル : /opt/cisco/platform/logs/mce.log モジュールバンドル(41xx、93xx)にも同じファイルが存在します。	これは、 ク例外 す。エ 害など

FPRM/バンドル : /opt/cisco/platform/logs/portmgr.out	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/ssp-pm.log モジュールバンドル(41xx、93xx)にも同じファイルが存在します。	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/sma.log モジュールバンドル(41xx、93xx)にも同じファイルが存在します。	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/heimdall.log	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/ssp-shutdown.log モジュールバンドル(41xx、93xx)にも同じファイルが存在します。	リブ トダウ 際のps dmesg 力を含 1000/2 使用可
FPRM/バンドル : /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	エラー、 どを探
FPRM/バンドル : /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	エラー、 どを探
CIMC/バンドル(41xx、93xx): /obfl/obfl-log*	エラー、 どを探
CIMC/バンドル(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*	エラー、 どを探 特にCA

モジュールバンドル(41xx、93xx):

/tmp/mount_media.log/mount_media.log

エラー、
どを探

ステップ14：キャプチャ

特定のインターフェイスが応答しなくなった場合は、ファイアウォールと隣接デバイスでキャプチャを実行します。詳細については、次のドキュメントを参照してください。

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

さらに、隣接するデバイスのARPおよびCAMテーブルにデータが正しく入力されていることを確認します。

ステップ15: Cisco TACに提供する追加情報

上記の項目に加えて、次の情報も提供することを強く推奨します。

15a. デバイスが復旧したら、トラブルシューティングバンドルを収集します (詳細については、ステップ13を参照してください)。

150億それでもデバイスが応答しない場合は、次の情報を提供します。

- ハードウェア情報 (モデル)。
- ソフトウェア情報。
- FMCソフトウェア情報 (該当する場合)
- 導入 (スタンドアロン/HA/クラスタ)

15c. デバイスが応答しなくなったおおよその時刻 (日時)。

15d. 応答しなくなった前のデバイスの稼働時間のおおよその時間。

15e. これは新しい設定ですか、それとも既存の設定ですか。

15f. デバイスが応答しなくなる前に実行した最後のアクションは何ですか。

15g. デバイスが応答しなくなった時点からのファイアウォールデータプレーン(LINA)syslog (インシデントの5分前から開始するログの取得を試みる)。 ベストプラクティスとして、syslogをレベル6 (情報) に設定することを推奨します。

15時間シャーシ (4100/9300のFXOS) にsyslogサーバを設定している場合は、ログを提供します (インシデントの5分前から開始)。

15i. インシデント発生時からの隣接デバイスからのsyslog

15j. ファイアウォールデバイスと隣接デバイス間の物理接続を示すトポロジ図。

一般的な問題

エラー：DMEとの通信がタイムアウトしました

コンソールに接続すると、次のように表示されます。

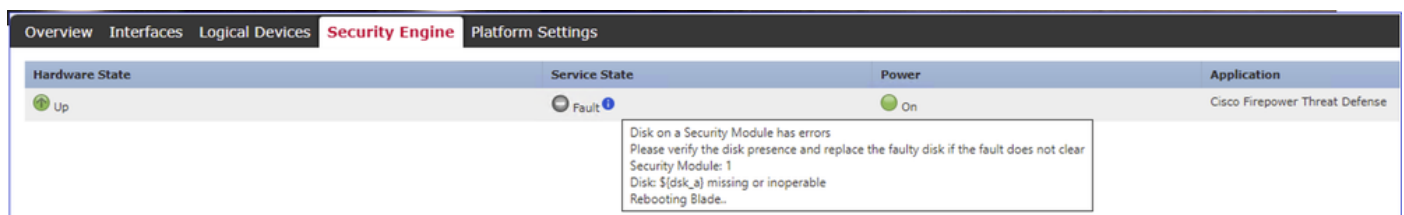
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

ほとんどの場合、これはソフトウェアの問題を示します。

推奨処置：Cisco TACに連絡してください

ディスクエラー：見つからないか、操作できません

次の出力は、ディスク関連の障害が生成された4100/9300ハードウェアアプライアンスから得られたものです。

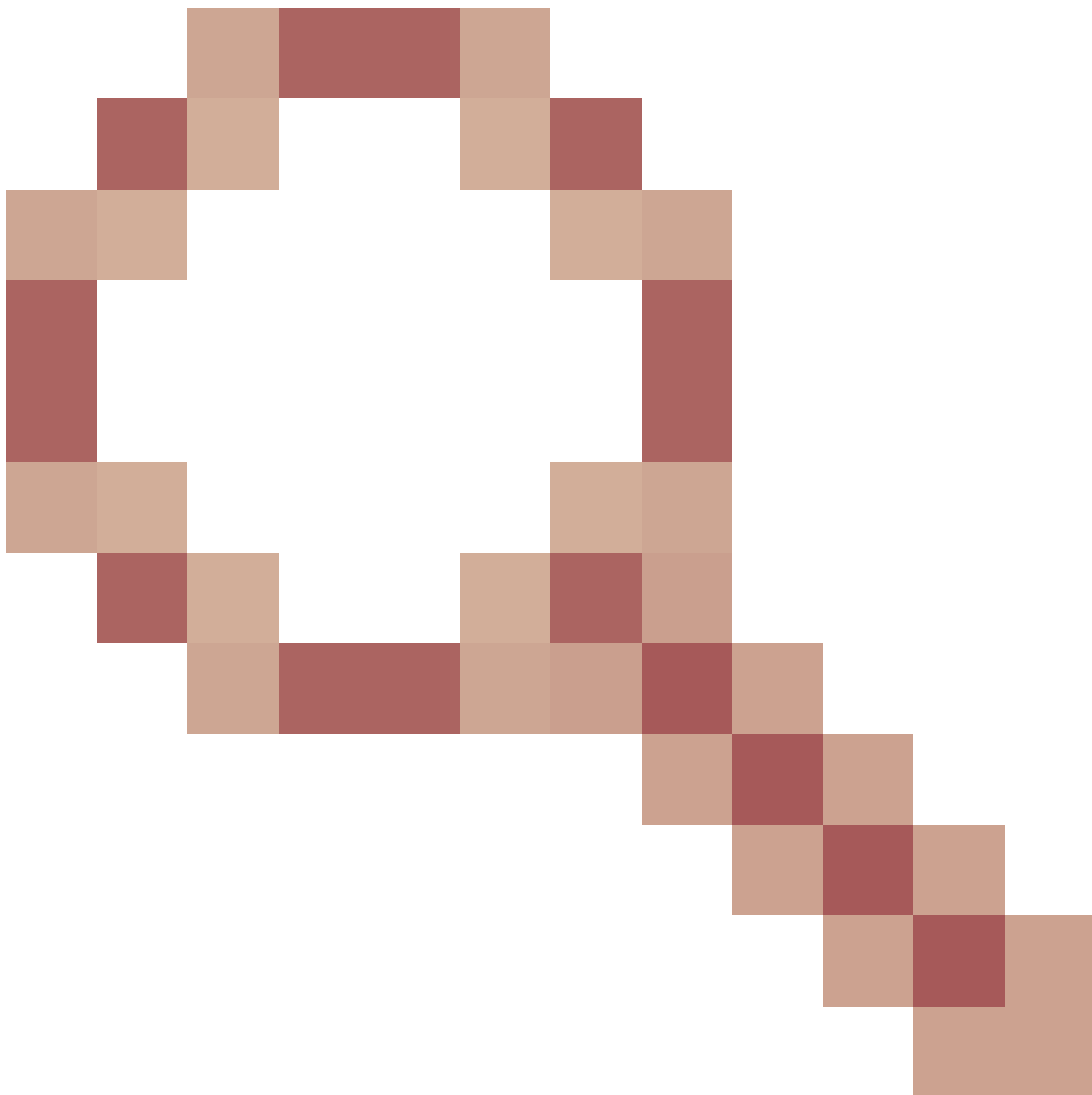


推奨処置：SSDディスクを取り付け直します。問題が解決しない場合は、シャーシのトラブルシューティングバンドルを収集し、Cisco TACに連絡してください。

フィールド通知：FN72077 - FPR9300およびFPR4100

- ネットワークトラフィックが FPR9300 および FPR4100 シリーズ セキュリティ アプライアンスを通過できなくなります。
- 有効な資格情報を持つユーザーは、管理コンソールにログインできません。
- CLIに「Software Error: Exception dme execution: [Error: Timed out communicating with DME]」というエラーメッセージが表示される

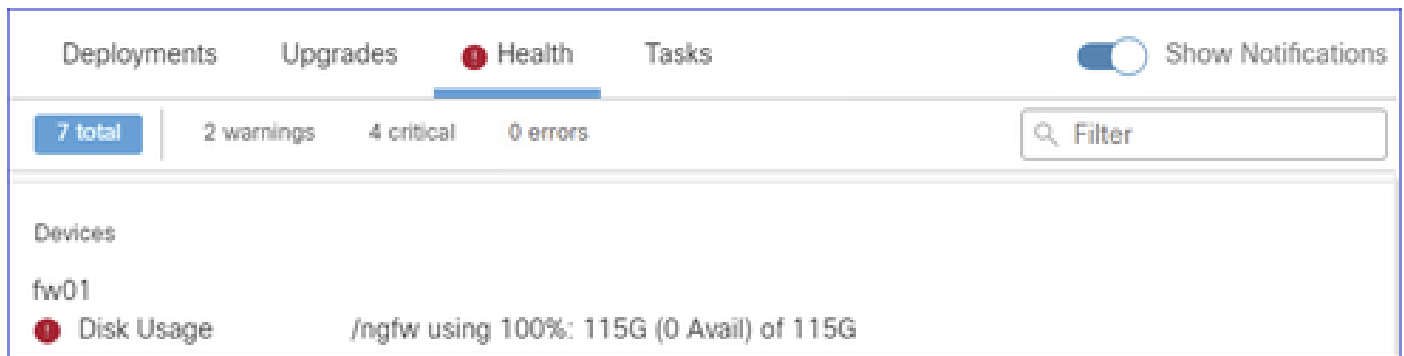
推奨処置：この問題から一時的に回復するには、4100/9300シャーシの電源を再投入する必要があります。Cisco Bug ID [CSCvx99172](#) (登録ユーザ専用) で、詳細と修正があるバージョンを確認してください。



(フィールド通知： FN72077 - FPR9300およびFPR4100シリーズセキュリティアプライアンスの一部のアプライアンスは、3.2年の稼働時間の後、トラフィックを渡さないことがある)

ディスク使用率100%

ファイアウォールのディスク領域が少ないと、デバイスが応答しなくなる可能性があります。デバイスがFMCによって管理されている場合は、次のようなヘルスアラートを受け取ることができます。

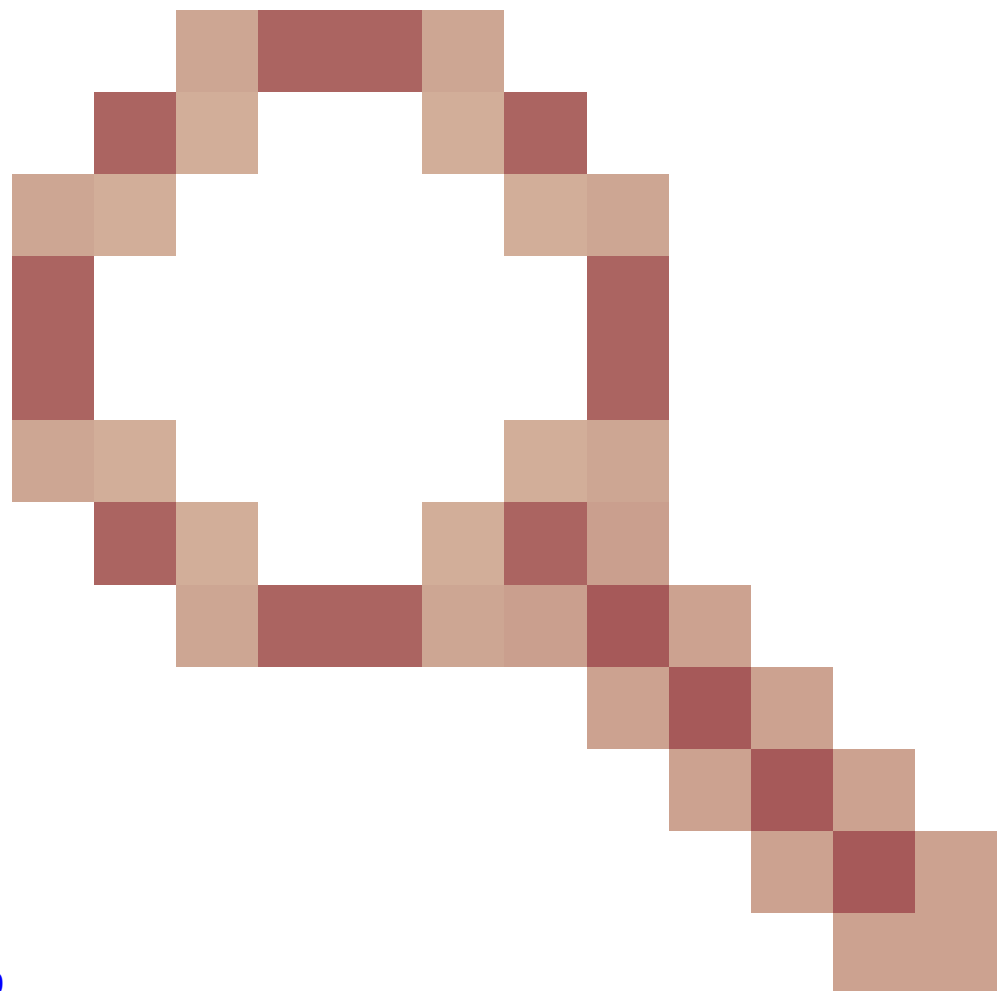


推奨処置：ソフトウェア7.7.0以降でFMCとFTDを実行している場合は、
<https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space>に記載されている手順を使用して、ディスク領域の一部をクリアしてください。

これを実行できない、または実行できない場合は、Cisco TACにお問い合わせください。

停電後、CSF 3100が起動しない

推奨処置：次の問題の修正が取り込まれたソフトウェアリリースにアップグレードしてください。
。



Cisco Bug ID [CSCwm14729](#)

CSF 3100シリーズが停電後にリブートしないため、手動で電源を再投入する必要がある

Cisco Firepower 2100シリーズセキュリティアプライアンス：一部のユニットでメモリ障害が発生する可能性があります

- コンポーネントプロセスの問題による5年以内のサービスでのDIMM障害
- 関連FN:<https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html>
- 関連するCisco Bug ID [CSCwb74948](#)

推奨処置:DIMMコンポーネントまたはセキュリティアプライアンスの交換

参考資料

- <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>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。