

Solucionar problemas de um Cisco Secure Firewall que não responde

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshooting](#)

[Passo 1: Inspeção visual \(painel frontal\)](#)

[Passo 2: Inspeção visual \(painel traseiro\)](#)

[Passo 3: Verificações do ventilador](#)

[Passo 4: Verificações de ambiente físico](#)

[Passo 5: Verificações de console e de portas de gerenciamento](#)

[Passo 6: Teste de conectividade IP de gerenciamento](#)

[Passo 7: Verificações de dispositivos adjacentes](#)

[Passo 8: Verificações de dispositivo de alta disponibilidade/cluster](#)

[Etapa 9: Coletar logs do console](#)

[Etapa 10: Execute uma reinicialização a frio](#)

[Etapa 11: Coletar gráficos do Monitor de Integridade do FMC](#)

[Etapa 12: Verificar problemas de disco](#)

[Passo 13: Análise de log](#)

[Passo 14: Capturas](#)

[Etapa 15: Informações adicionais a serem fornecidas ao Cisco TAC](#)

[Problemas comuns](#)

[Erro: Tempo limite de comunicação com o DME](#)

[Erro de disco: ausente ou inoperante](#)

[Nota de campo: FN72077 - FPR9300 e FPR4100](#)

[Utilização do disco 100%](#)

[O CSF 3100 não é ativado após uma queda de energia](#)

[Dispositivos de segurança Cisco Firepower 2100 Series: Algumas Unidades Podem Apresentar Falhas De Memória](#)

[Referências](#)

Introdução

Este documento descreve as etapas recomendadas para solucionar problemas de um Cisco Secure Firewall Threat Defense (FTD) que não esteja respondendo nas plataformas de hardware 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx e 93xx.

Pré-requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conceitos básicos do Cisco Secure FTD (instalação/configuração).

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Defesa contra ameaças do Cisco Secure Firewall
- Cisco Secure Firewall Management Center
- Sistema operacional extensível Cisco Firepower (FXOS)

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Em alguns casos, um dispositivo FTD da Cisco pode deixar de responder. Os sintomas típicos incluem:

- Sem acesso SSH.
- Sem acesso ao console.
- O acesso ao console está funcionando, mas as credenciais de login não.
- O tráfego de trânsito não está passando pelo dispositivo.
- As interfaces estão inoperantes (dados e/ou gerenciamento).
- Os LEDs estão apagados ou âmbar (piscando ou estável).
- O módulo seguro (4100, 9300) não responde.

Observe que, dependendo da situação, alguns deles não estarão presentes. Por exemplo, você pode ter tráfego de trânsito passando, mas apenas o acesso de gerenciamento não está funcionando.

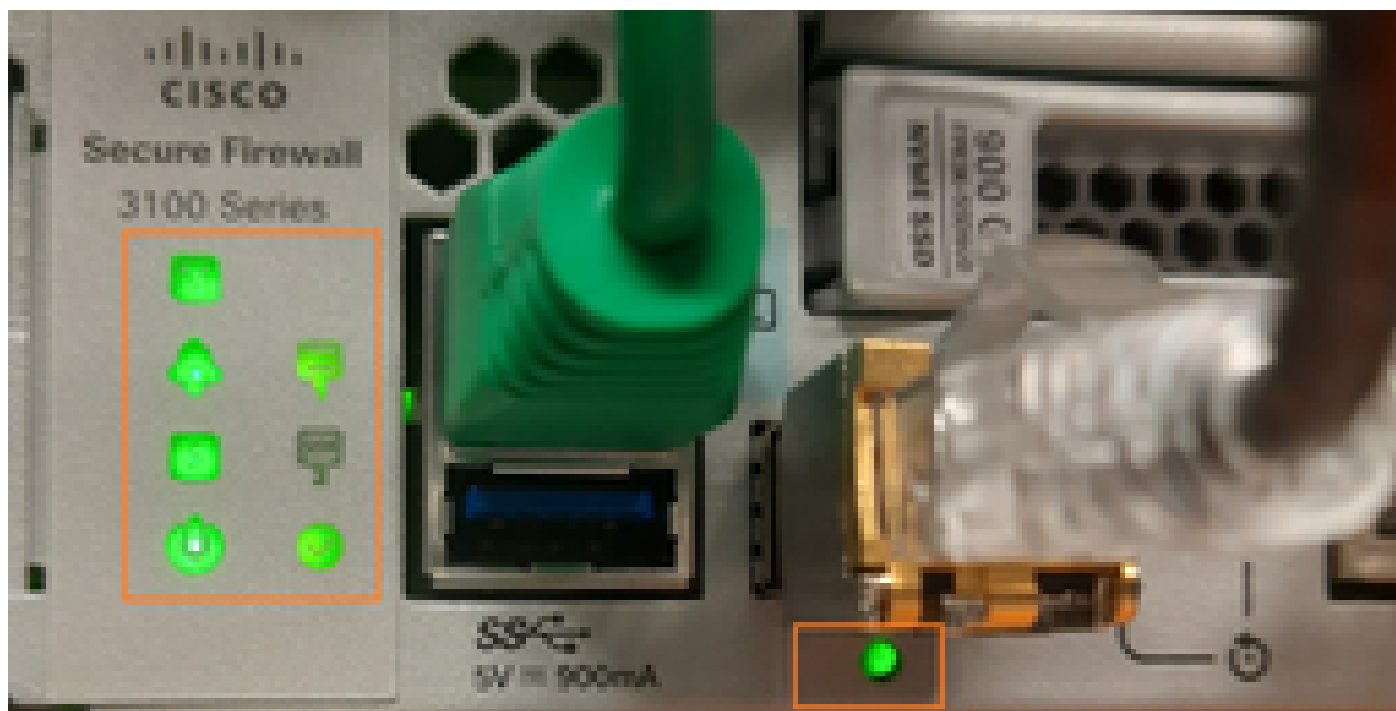
Troubleshooting

Esta seção aborda as etapas e ações recomendadas que você precisa executar. Você pode fornecer essas informações ao TAC da Cisco para análise adicional.

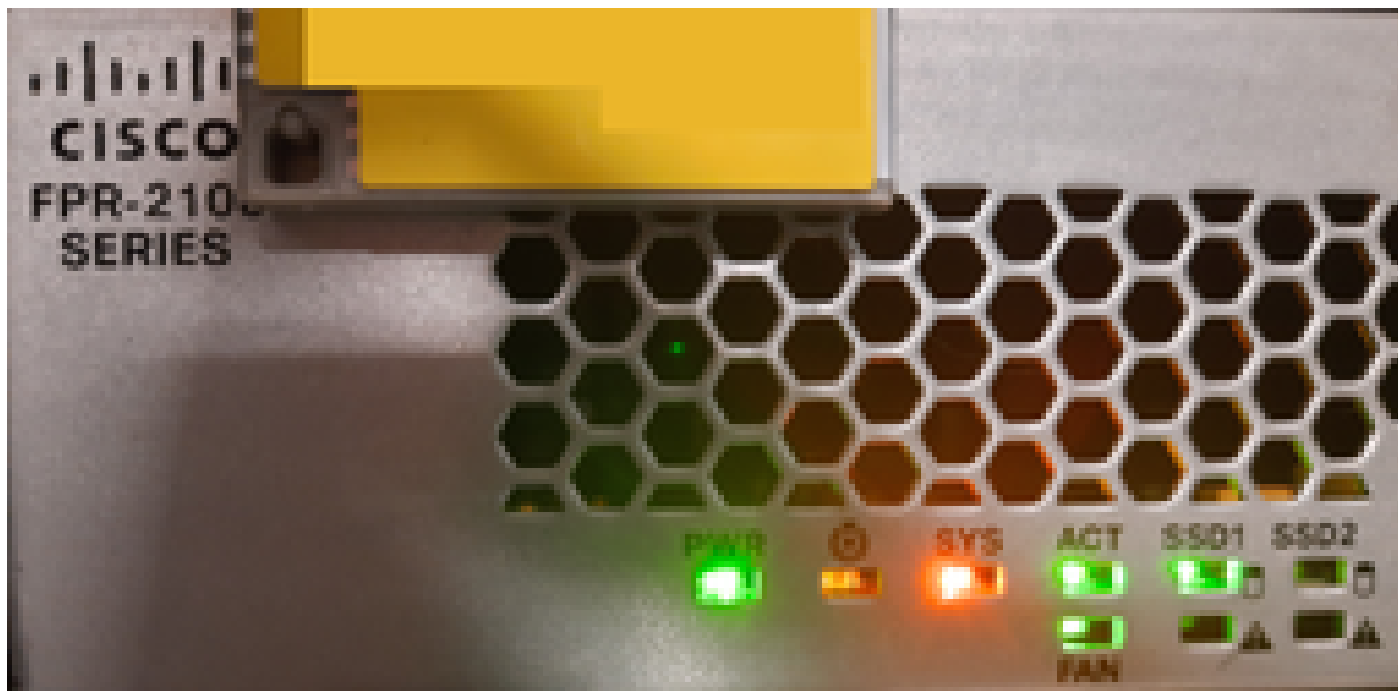
Passo 1: Inspeção visual (painel frontal)

Tire um vídeo ou uma foto dos LEDs do painel frontal. Aqui estão alguns exemplos onde todos os

LEDs são claramente visíveis:



Na próxima foto, o LED SYS indica um problema no dispositivo:



Você pode consultar o guia de hardware do modelo do seu dispositivo para obter informações adicionais sobre o LED, por exemplo:

Modelo	Informações do LED
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.html
1230, 1240, 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-1230.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/m-3100.html
4110, 4120, 4140,	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/overview.html

4150	
4112, 4115, 4125, 4145	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.htm
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/b

Passo 2: Inspeção visual (painel traseiro)

Tire um vídeo ou uma foto dos LEDs no painel traseiro, por exemplo:



Se você não vir nenhum LED de energia aceso:

- Tente recolocar as fontes de alimentação (sempre que aplicável).
- Se possível, tente substituir a fonte de alimentação.

Passo 3: Verificações do ventilador

Verifique se os ventiladores na parte traseira do equipamento estão em execução.

Passo 4: Verificações de ambiente físico

Verifique se há algum ruído ou cheiro vindo do dispositivo.

Passo 5: Verificações de console e de portas de gerenciamento

Verifique se o console e as portas de gerenciamento estão conectados corretamente. Se o problema estiver apenas na porta de gerenciamento, tente alterar o SFP (sempre que aplicável) e o cabo de rede.

Passo 6: Teste de conectividade IP de gerenciamento

Tente fazer ping (ICMP) no IP de gerenciamento do dispositivo.

Passo 7: Verificações de dispositivos adjacentes

Verifique o status da porta dos dispositivos adjacentes, por exemplo:

```
<#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

Passo 8: Verificações de dispositivo de alta disponibilidade/cluster

Em caso de alta disponibilidade (HA) ou configuração de cluster, colete um pacote de solução de problemas dos dispositivos pares.

Etapa 9: Coletar logs do console

Conecte um laptop à porta do console e copie as mensagens mostradas. Tente pressionar as teclas para cima/para baixo ou PageUp para ver todas as mensagens na tela.

Etapa 10: Execute uma reinicialização a frio

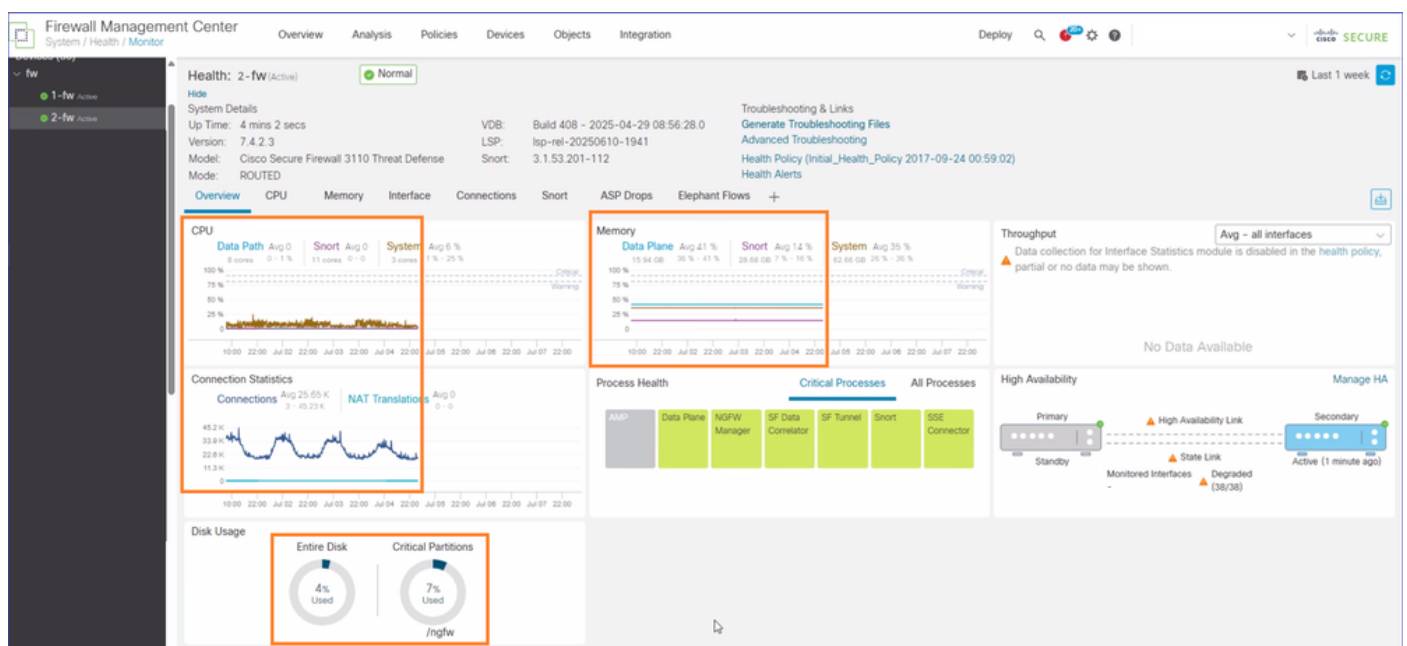
Com um laptop conectado à porta de console:

1. Desconecte todos os cabos de alimentação e aguarde alguns minutos antes de conectá-los novamente.
2. No caso de uma configuração de failover ou de cluster, para minimizar qualquer risco de instabilidade Ativo/Ativo ou de Cluster, você pode desconectar ou desligar do dispositivo de switch adjacente todas as interfaces de dados da unidade afetada, incluindo os links HA ou CCL.
3. Em seguida, reconecte os cabos de alimentação e ligue o dispositivo.
4. Aguarde aproximadamente 5 minutos.
5. Colete a saída do console.

Observe que se o dispositivo não foi desligado normalmente e estava operacional (os LEDs do painel frontal estavam acesos), a reinicialização a frio pode causar uma corrupção do banco de dados. Se a reinicialização a frio ativar o dispositivo, colete um pacote de solução de problemas e entre em contato com o TAC da Cisco.

Etapa 11: Coletar gráficos do Monitor de Integridade do FMC

Se o dispositivo se recuperar e for gerenciado por um FMC, navegue para System > Health > Monitor e selecione o dispositivo. Concentre-se nos gráficos destacados para entender qual era o status do dispositivo antes de não responder (por exemplo, alta memória, alta utilização da CPU, alta utilização do disco etc.).



Etapa 12: Verificar problemas de disco

Cenário de não funcionamento (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
```

Exemplo de saída do 3100 onde o disco está operacional:

```
<#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

Exemplo de saída do 4100 onde o disco está operacional:

<#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

Passo 13: Análise de log

Se o dispositivo de firewall se recuperar e você quiser analisar os logs de back-end, gere um pacote de solução de problemas e verifique os arquivos mencionados na tabela. Observe que:

- Nas plataformas 1xxx, 12xx, 21xx (modo de dispositivo), 31xx, 42xx, o pacote de solução de problemas de FTD também contém o pacote de chassi (FPRM) de FXOS no caminho \dir-archives\var-common-platform_ts\. Você precisa extrair o conteúdo do pacote FPRM.
- No 3100/4200, no modo Multi-Instance (MI), colete o arquivo TS do chassi da interface do usuário do FMC ou da CLI do chassi (show tech-support fprm detail do escopo do comando local-mgmt), conforme descrito em <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>.
- Nas plataformas 41xx, 93xx, você precisa gerar o pacote de chassi separadamente da interface do usuário do chassi ou da CLI FXOS, conforme descrito em <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>.
- Para plataformas de dispositivos 4100 e 9300, você precisa coletar pacotes de solução de problemas FXOS e FTD. Para todas as outras plataformas, o pacote de solução de problemas de FTD é suficiente, pois também contém o pacote de solução de problemas de FXOS.
- Para o ASA, a saída do comando 'show tech-support' após a recuperação não é muito útil. Você precisa confiar no pacote de solução de problemas FXOS.
- Em comparação com outras plataformas, em 41xx, 93xx você tem dois pacotes de solução de problemas: chassi (BC1) e conjunto de módulos .
- O pacote do chassi (BC1) em 41xx, 93xx contém, entre outros, os pacotes FPRM e CIMC.
- O pacote de módulos em 41xx, 93xx contém principalmente logs FXOS do blade.
- Se você tiver um ASA instalado, precisará confiar apenas no chassi, no FPRM e nos pacotes de módulos (sempre que aplicável) e na saída do comando "show tech-support" do

ASA.

- Dependendo da plataforma e do incidente, nem todos os arquivos estarão presentes.

Caminho do arquivo no pacote de solução de problemas	Descrição
Pacote de FTD TS: /dir-archives/var-log/messages*	A string shutting mostrac um des energia A string starting mostrac disposi
Pacote de FTD TS: /dir-archives/var-log/ASAconsole.log No caso do ASA em 4100/9300, você também pode encontrar o arquivo no pacote de módulos em /opt/cisco/platform/logs/ASAconsole.log	Procura falhas,
Pacote de FTD TS: /dir-archives/var-log/dmesg.log	Procura falhas,
Pacote de FTD TS: /dir-archives/var/log/ngfwManager.log*	Procura falhas, Esse ar também informa eventos
Pacote de FTD TS: /command-outputs/LINA_troubleshoot/show_tech_output.txt	A saída comando failover 'show c pode fo informa adicion sequên eventos

Pacote de FTD TS: /command-outputs/ Nomes de arquivo: · para CORE em `ls opt-cisco-csp-cores _ grep core` _ do file -opt-cisco-csp-cores-_{CORE}_done.output · para CORE em `ls var-common _ grep core` _ do arquivo var-common-_{CORE}_done.output · para CORE em `ls var-data-cores _ grep core` _ do file -var-data-cores-_{CORE}_done.output	Verifique o arquivo em potencial (traceback)
Pacote de FTD TS: /dir-archives/var/log/crashinfo/snort3-crashinfo.*	Verifique o arquivo do Snort
Pacote de FTD TS: /dir-archives/var/log/process_stderr.log*	Verifique (por exemplo, bug da CSCwh)
Pacote de FTD TS: /dir-archives/var/log/periodic_stats/	O diretório contém vários arquivos que podem fornecer informações sobre o momento e o tipo de incidentes
Pacote FPRM: tech_support_brief	Verifique o conteúdo de 'show'
Pacote FPRM: /opt/cisco/platform/logs/kern.log	Procure erros de falhas,
Pacote FPRM: /opt/cisco/platform/logs/messages*	Procure erros de falhas,
Pacote FPRM: /opt/cisco/platform/logs/mce.log O mesmo arquivo também existe no pacote do módulo (41xx, 93xx).	Este é o arquivo de logs do MCE (Machine Check Exception) para erros de falhas, etc.

Pacote FPRM: /opt/cisco/platform/logs/portmgr.out	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/ssp-pm.log O mesmo arquivo também existe no pacote do módulo (41xx, 93xx).	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/sma.log O mesmo arquivo também existe no pacote do módulo (41xx, 93xx).	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/heimdall.log	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/ssp-shutdown.log O mesmo arquivo também existe no pacote do módulo (41xx, 93xx).	Ele con de ps, t linhas c quando reinicia desliga iniciado Dispon 100/210
Pacote FPRM: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	Procure falhas,
Pacote FPRM: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	Procure falhas,
Pacote CIMC (41xx, 93xx): /obfl/obfl-log*	Procure falhas,
Pacote CIMC (41xx, 93xx): /CIMC1_TechSupport.tar.gz/CIMC1_TechSupport.tar/tmp/techsupport_pid*/CIMC1_TechSupport-	Procure falhas,

nvram.tar.gz/CIMC1_TechSupport-nvram.tar/nv/etc/log/eng-repo/messages*	Especialista CATER
Pacote do módulo (41xx, 93xx): /tmp/mount_media.log/mount_media.log	Procurador falhas,

Passo 14: Capturas

Se uma interface específica ficar sem resposta, faça capturas no firewall e no dispositivo adjacente. Você pode consultar este documento para obter detalhes:

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

Além disso, certifique-se de que as tabelas ARP e CAM dos dispositivos adjacentes estejam preenchidas corretamente.

Etapa 15: Informações adicionais a serem fornecidas ao Cisco TAC

Além dos itens mencionados acima, é altamente recomendável fornecer também estas informações:

15 bis. Se o dispositivo recuperado coletar um pacote de solução de problemas (verifique a etapa 13 para obter detalhes).

15-B. Se o dispositivo ainda não responder, forneça estas informações:

- Informações de hardware (modelo).
- Informações de software.
- Informações do CVP (se aplicável).
- Implantação (independente/HA/cluster).

15 quater. Hora aproximada (data/hora) em que o dispositivo parou de responder.

15-D. Tempo de atividade aproximado do dispositivo antes de ele deixar de responder.

15 sexies. Esta é uma configuração nova ou existente?

15 septies. Qual foi a última ação executada antes de o dispositivo deixar de responder?

15 octies. Os syslogs de plano de dados de firewall (LINA) a partir do momento em que o dispositivo ficou sem resposta (tente obter logs a partir de ~5 minutos antes do incidente). Como prática recomendada, é recomendável configurar syslogs no nível 6 (Informativo).

15-H. Caso você tenha configurado um Servidor syslog no chassi (FXOS em 4100/9300), forneça os logs (começando aproximadamente 5 minutos antes do incidente).

15-I. Syslogs dos dispositivos adjacentes a partir do momento do incidente.

15-J. Diagrama de topologia que mostra as conexões físicas entre o dispositivo de firewall e os dispositivos adjacentes.

Problemas comuns

Erro: Tempo limite de comunicação com o DME

Se você se conectar ao console e vir:

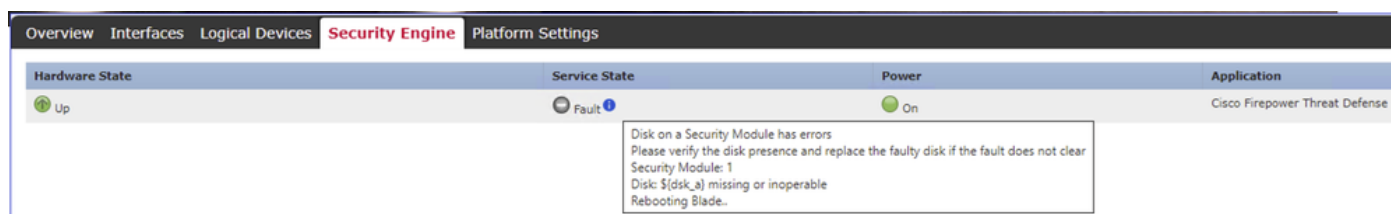
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

Na maioria das vezes, isso indica um problema de software.

Ação recomendada: Entre em contato com o Cisco TAC

Erro de disco: ausente ou inoperante

Esta saída é de um dispositivo de hardware 4100/9300 onde uma falha relacionada ao disco é gerada:

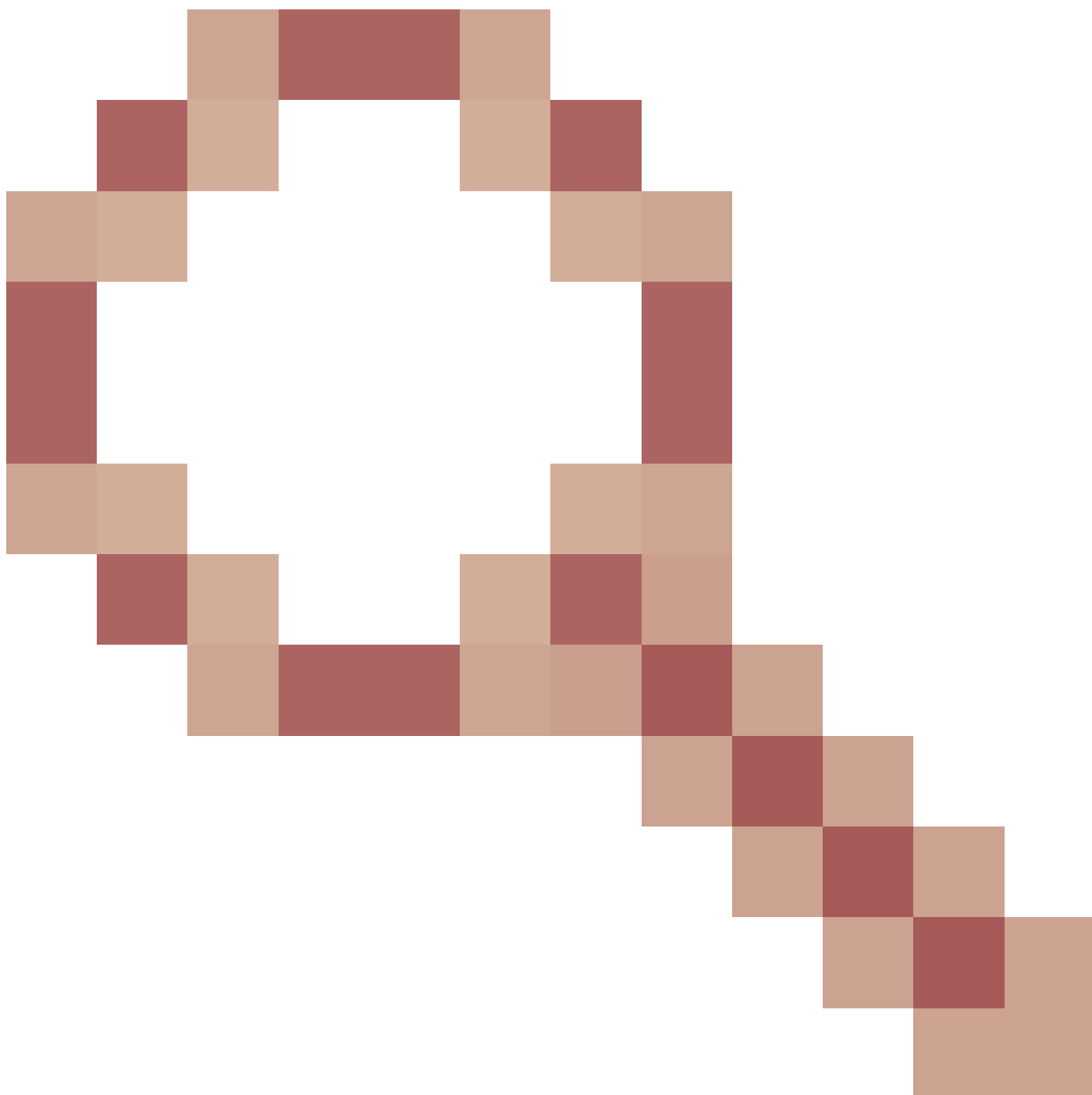


Ação recomendada: Experimente reassentar o disco SSD. Se isso não ajudar, colete o pacote de solução de problemas de chassi e entre em contato com o TAC da Cisco.

Nota de campo: FN72077 - FPR9300 e FPR4100

- Os dispositivos de segurança FPR9300 e FPR4100 Series não passam mais tráfego de rede.
- Os usuários com credenciais válidas não podem fazer login no console de gerenciamento.
- A CLI mostra uma mensagem de erro: "Erro de software: Exceção durante a execução: [Erro: Tempo limite de comunicação com DME]"

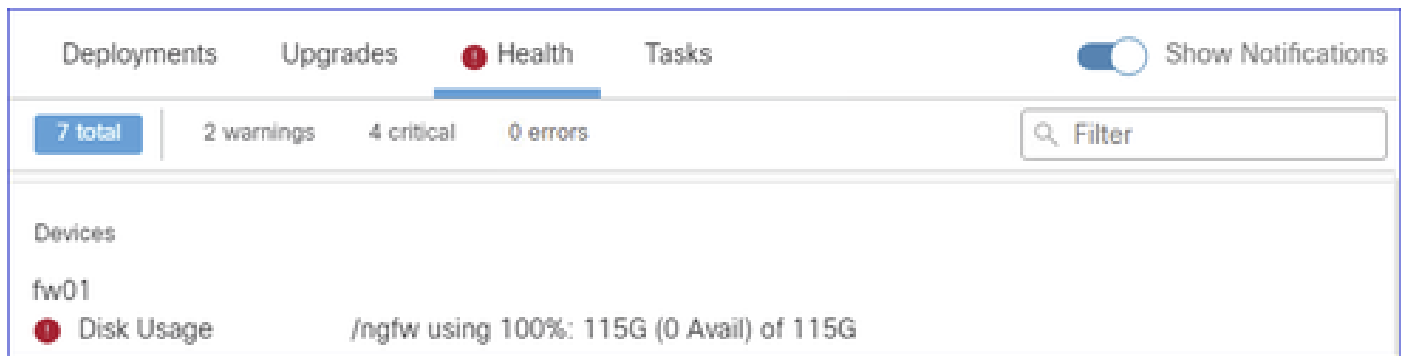
Ação recomendada: Um ciclo de energia do chassi 4100/9300 é necessário para a recuperação temporária desse problema. Verifique o bug da Cisco ID [CSCvx9172](https://tools.cisco.com/bugcenter/bug/?bugID=CSCvx9172) para obter detalhes e uma versão que tenha uma correção.



(Nota de campo: FN72077 - Dispositivos de segurança FPR9300 e FPR4100 Series - Alguns dispositivos podem falhar ao transmitir tráfego após 3,2 anos de tempo de atividade).

Utilização do disco 100%

Pouco espaço em disco no firewall pode fazer com que o dispositivo não responda. Se o dispositivo for gerenciado pelo FMC, você poderá receber alertas de integridade como este:

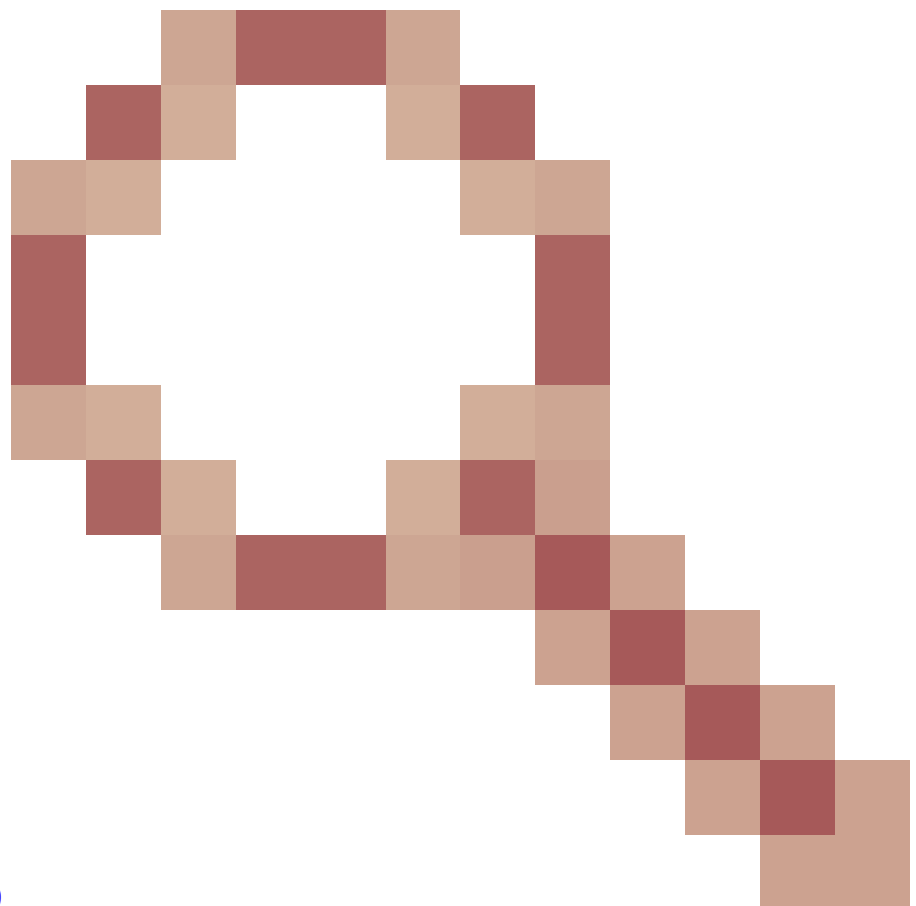


Ação recomendada: Se o FMC e o FTD estiverem sendo executados no software 7.7.0 ou posterior, tente liberar espaço em disco usando o procedimento documentado em <https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space>

Se isso não for viável ou não ajudar, entre em contato com o TAC da Cisco.

O CSF 3100 não é ativado após uma queda de energia

Ação recomendada: Atualizar para uma versão de software que tenha uma correção para:



ID de bug da Cisco [CSCwm14729](#)

A série CSF 3100 não é reiniciada após queda de energia, exigindo ciclo de energia manual.

Dispositivos de segurança Cisco Firepower 2100 Series: Algumas Unidades Podem Apresentar Falhas De Memória

- Falhas de DIMM em 5 anos de serviço devido a problemas no processo do componente
- FN relacionado: <https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html>
- ID de bug Cisco [CSCwb74948](https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html)

Ação recomendada: Substituição de componentes DIMM ou substituição do dispositivo de segurança

Referências

- <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>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.