

Problemen oplossen met een niet-reagerende Cisco Secure Firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Problemen oplossen](#)

[Stap 1: Visuele inspectie \(voorpaneel\)](#)

[Stap 2: Visuele inspectie \(achterpaneel\)](#)

[Stap 3: Ventilatorcontroles](#)

[Stap 4: Fysieke omgevingscontroles](#)

[Stap 5: Controles van console- en beheerpoorten](#)

[Stap 6: IP-connectiviteitstest voor beheer](#)

[Stap 7: Controles van aangrenzende apparaten](#)

[Stap 8: Controles van HA/clusterapparaat](#)

[Stap 9: Consolelogboeken verzamelen](#)

[Stap 10: Een koude reboot uitvoeren](#)

[Stap 11: Grafieken van de gezondheidsmonitor verzamelen bij de FMC](#)

[Stap 12: Controleren op schijfproblemen](#)

[Stap 13: Loganalyse](#)

[Stap 14: Opnamen](#)

[Stap 15: Aanvullende informatie voor Cisco TAC](#)

[Veelvoorkomende problemen](#)

[Fout: Time-out voor communicatie met DME](#)

[Schijffout: ontbrekend of inoperabel](#)

[Bericht ter plaatse: FN72077 - FPR9300 en FPR4100](#)

[Schijfgebruik 100%](#)

[CSF 3100 komt niet naar boven na een stroomstoring](#)

[Beveiligingstoestellen uit de Cisco Firepower 2100-reeks: sommige apparaten kunnen geheugenfouten ondervinden](#)

[Referenties](#)

Inleiding

In dit document worden de aanbevolen stappen beschreven voor het oplossen van problemen met een FTD (Cisco Secure Firewall Threat Defense) die niet reageert op hardwareplatforms van 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx en 93xx.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisprincipes van Cisco Secure FTD (installatie/configuratie).

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firewall Threat Defense
- Cisco Secure Firewall Management Center
- Cisco Firepower Extensible Operating System (FXOS)

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In sommige gevallen kan een Cisco FTD-apparaat niet meer reageren. Typische symptomen zijn:

- Geen toegang tot SSH.
- Geen toegang tot console.
- Consoletoegang werkt, maar inloggegevens niet.
- Transitverkeer gaat niet door het apparaat.
- Interfaces zijn down (gegevens en/of beheer).
- LED's zijn uit of amberkleurig (knipperend of vast).
- Beveiligde module (4100, 9300) reageert niet meer.

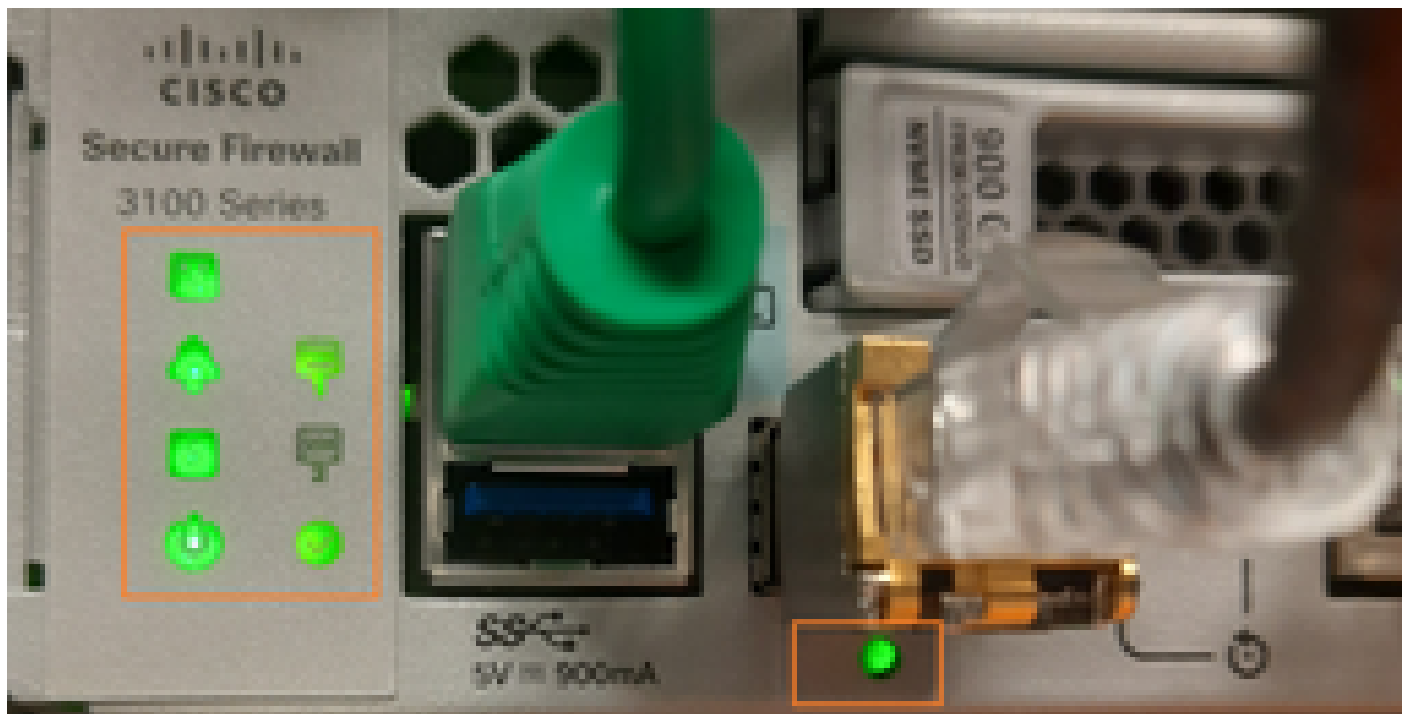
Houd er rekening mee dat, afhankelijk van de situatie, sommige van hen niet aanwezig zullen zijn. U kunt bijvoorbeeld doorgaand verkeer hebben, maar alleen beheerstoegang werkt niet.

Problemen oplossen

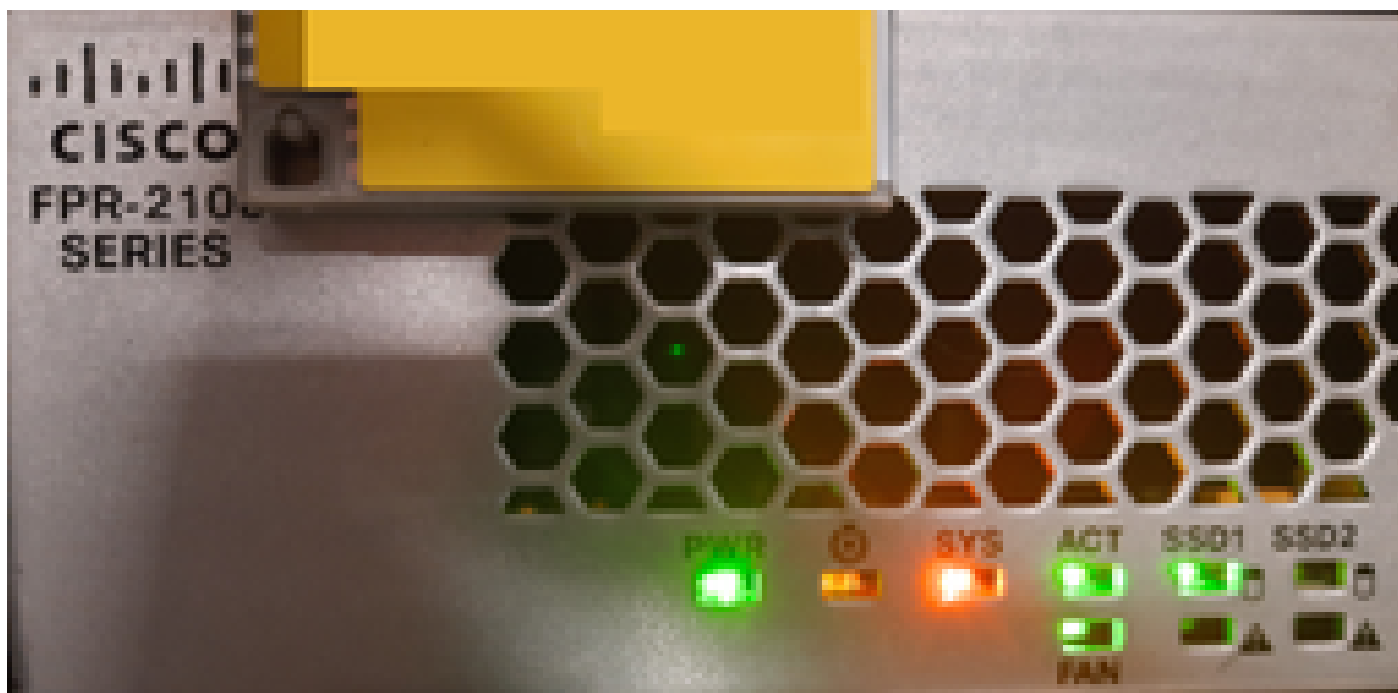
In dit gedeelte worden de aanbevolen stappen en acties beschreven die u moet uitvoeren. U kunt deze informatie aan Cisco TAC verstrekken voor verdere analyse.

Stap 1: Visuele inspectie (voorpaneel)

Maak een video of een foto van de LED's op het voorpaneel. Hier zijn enkele voorbeelden waarbij alle LED's duidelijk zichtbaar zijn:



In de volgende foto geeft de SYS-LED een apparaatprobleem aan:



U kunt de hardwaregids van uw apparaatmodel raadplegen voor aanvullende informatie over de LED, bijvoorbeeld:

Model	LED-info
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

Stap 2: Visuele inspectie (achterpaneel)

Maak bijvoorbeeld een video of een foto van de LED's op het achterpaneel:



Als u geen LED's ziet branden:

- Probeer de voedingseenheden te herstellen (indien van toepassing).
- Probeer indien mogelijk de stroomvoorziening te vervangen.

Stap 3: Ventilatorcontroles

Controleer of de ventilatoren aan de achterzijde van het toestel actief zijn.

Stap 4: Fysieke omgevingscontroles

Controleer of er geluid of geur afkomstig is van het apparaat.

Stap 5: Controles van console- en beheerpoorten

Zorg ervoor dat de console- en beheerpoorten goed zijn aangesloten. Als het probleem zich alleen op de beheerpoort bevindt, probeert u de SFP (indien van toepassing) en de netwerkkabel te wijzigen.

Stap 6: IP-connectiviteitstest voor beheer

Probeer het IP-beheer van het apparaat te pingen (ICMP).

Stap 7: Controles van aangrenzende apparaten

Controleer de poortstatus van de aangrenzende apparaten, bijvoorbeeld:

```
<#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

Stap 8: Controles van HA/clusterapparaat

In het geval van een hoge beschikbaarheid (HA) of een clusteropstelling, verzamelt u een bundel voor probleemoplossing van het (de) peer-apparaat(en).

Stap 9: Consolelogboeken verzamelen

Sluit een laptop aan op de consolepoort en kopieer de getoonde berichten. Probeer de toetsen omhoog/omlaag of PageUp in te drukken om alle berichten op het scherm te zien.

Stap 10: Een koude reboot uitvoeren

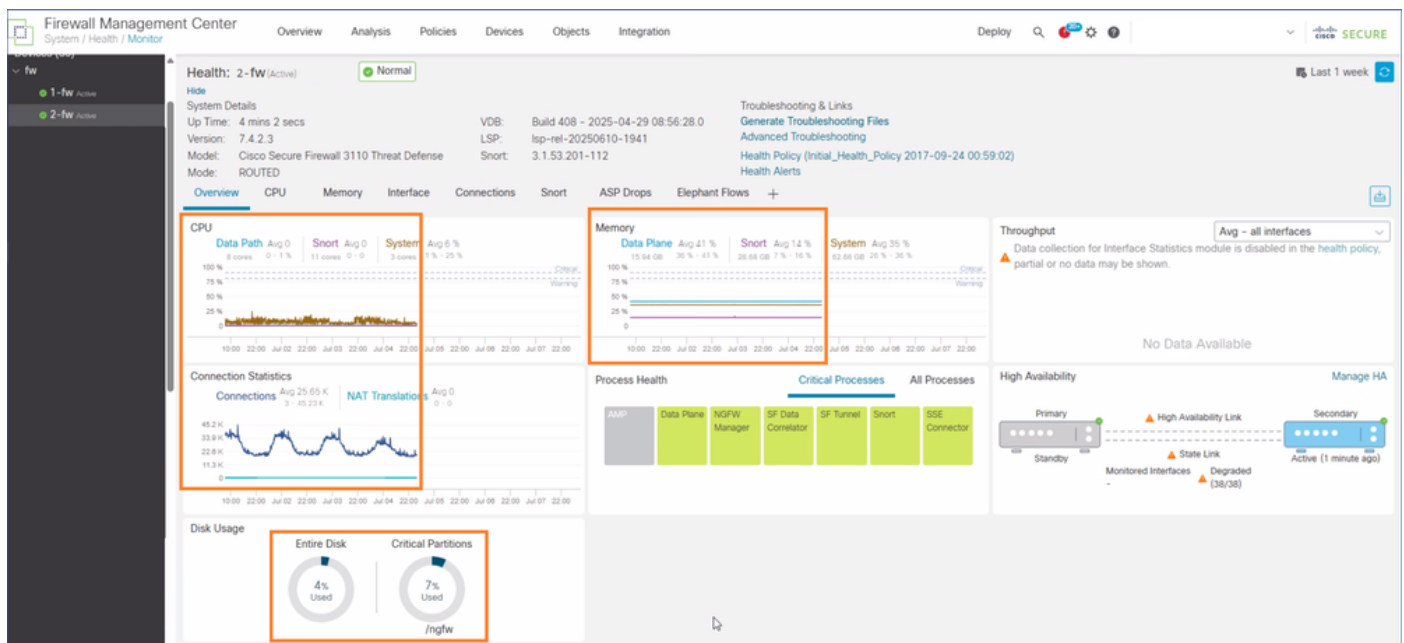
Met een laptop aangesloten op de consolepoort:

1. Koppel alle voedingskabels los en wacht een paar minuten voordat u ze weer aansluit.
2. In het geval van een failover-installatie of een clusterconfiguratie kunt u, om het risico op Active/Active of Cluster-instabiliteit te minimaliseren, alle gegevensinterfaces van het desbetreffende switch, inclusief de HA- of CCL-koppelingen, loskoppelen of afsluiten van het aangrenzende clusterapparaat.
3. Sluit vervolgens de voedingskabels opnieuw aan en zet het apparaat aan.
4. Wacht ~5 minuten.
5. Verzamel de console-uitvoer.

Merk op dat als het apparaat niet sierlijk werd afgesloten en het apparaat operationeel was (de LED's op het voorpaneel waren ingeschakeld), de koude reboot een databasecorruptie kan veroorzaken. Als de koude reboot brengt het apparaat, het verzamelen van een troubleshoot bundel en contact opnemen met Cisco TAC.

Stap 11: Grafieken van de gezondheidsmonitor verzamelen bij de FMC

Als het apparaat herstelt en wordt beheerd door een FMC, gaat u naar Systeem > Gezondheid > Monitor en selecteert u het apparaat. Focus op de gemarkeerde grafieken om te begrijpen wat de status van het apparaat was voordat het niet reageerde (bijvoorbeeld hoog geheugen, hoge CPU, hoog schijfgebruik, enzovoort).



Stap 12: Controleren op schijfproblemen

Niet-werkend scenario (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
```

Voorbeelduitvoer van 3100 waar schijf operationeel is:

```
<#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

Voorbeelduitvoer van 4100 waar schijf operationeel is:

<#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

Stap 13: Loganalyse

Als het firewallapparaat herstelt en u de back-endlogs wilt analyseren, genereert u een bundel voor probleemoplossing en controleert u de bestanden die in de tabel worden vermeld. Let op:

- Op 1xxx-, 12xx-, 21xx- (toestelmodus), 31xx- en 42xx-platforms bevat de FTD-probleemoplossingspakket ook de FPRM-bundel (chassis) van FXOS in het \dir-archives\var-common-platform_ts\pad. U moet de inhoud van de FPRM-bundel extraheren.
- Op de 3100/4200 in Multi-Instance (MI)-modus kunt u het TS-chassisbestand van de FMC UI of de CLI van het chassis verzamelen (toon details van het formulier voor technische ondersteuning van de opdrachtregel voor lokale beheer), zoals beschreven in <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>.
- Op 41xx- en 93xx-platforms moet u de chassisbundel afzonderlijk genereren van de chassis-gebruikersinterface of de FXOS CLI, zoals beschreven in <https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-h1d-2132091400>.
- Voor 4100- en 9300-apparaatplatforms moet u FXOS- en FTD-probleemoplossingspakketten verzamelen. Voor alle andere platforms is de FTD-probleemoplossingsbundel voldoende, omdat deze ook de FXOS-probleemoplossingsbundel bevat.
- Voor ASA is de 'show tech-support' commando uitvoer na het herstel niet erg behulpzaam. U moet vertrouwen op de FXOS-probleemoplossingsbundel.
- Vergeleken met andere platforms, hebt u op 41xx, 93xx twee pakketten voor probleemoplossing: chassis (BC1) en module bundel.
- De chassisbundel (BC1) op 41xx, 93xx, bevat onder andere de FPRM- en CIMC-bundels.
- De modulebundel op 41xx, 93xx bevat voornamelijk FXOS-logs van de blade.
- Als u een ASA hebt geïnstalleerd, moet u alleen vertrouwen op het chassis, de FPRM- en modulebundels (indien van toepassing) en de opdrachtregel 'show tech-support' van ASA.
- Afhankelijk van het platform en het incident zullen niet alle bestanden aanwezig zijn.

Bestandspad in de bundel Problemen oplossen	Beschri
FTD TS-bundel: /dir-archieven/var-log/berichten*	De string shutting getoon sierlijke De teke 'syslog- wordt w wannee wordt g
FTD TS-bundel: /dir-archives/var-log/ASAconsole.log In het geval van ASA op 4100/9300, kunt u het bestand ook vinden in de Module bundel onder /opt/cisco/platform/logs/ASAconsole.log	Zoek na fouten, enzovo
FTD TS-bundel: /dir-archives/var-log/dmesg.log	Zoek na fouten, enzovo
FTD TS-bundel: /dir-archives/var/log/ngfwManager.log*	Zoek na fouten, enzovo Dit best informa HA/Clu gebeur
FTD TS-bundel: /command-outputs/LINA_troubleshoot/show_tech_output.txt	De outp 'show f en de 's history' inzicht volgord gebeur
FTD TS-bundel: /command-outputs/ Bestandsnamen:	Control potenti kernbes

· voor CORE in `ls opt-cisco-csp-cores _ grep core` _ do file -opt-cisco-csp-cores-_{CORE}_done.output · voor CORE in `ls var-common _ grep core` _ do file var-common-_{CORE}_ done.output · voor CORE in `ls var-data-cores _ grep core` _ do file -var-data-cores-_{CORE}_ done.output	(traceb...
FTD TS-bundel: /dir-archieven/var/log/crashinfo/snort3-crashinfo.*	Control crashin
FTD TS-bundel: /dir-archives/var/log/process_stderr.log*	Control Backtra (bijvoor bug-ID
FTD TS-bundel: /dir-archves/var/log/periodic_stats/	De dire meerde die inzi bieden momen inciden
FPRM-bundel: tech_support_brief	Control uitgang foutdeta
FPRM-bundel: /opt/cisco/platform/logs/kern.log	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/berichten*	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/mce.log Hetzelfde bestand bestaat ook in de module bundel (41xx, 93xx).	Dit is he Machin Excepti Zoek na fouten, enzovo

FPRM-bundel: /opt/cisco/platform/logs/portmgr.out	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/ssp-pm.log Hetzelfde bestand bestaat ook in de module bundel (41xx, 93xx).	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/sma.log Hetzelfde bestand bestaat ook in de module bundel (41xx, 93xx).	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/heimdall.log	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/ssp-shutdown.log Hetzelfde bestand bestaat ook in de module bundel (41xx, 93xx).	Het bev van ps, enkele dmesg opnieuw afsluite gestart. Beschik 1000/2
FPRM-bundel: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	Zoek na fouten, enzovo
FPRM-bundel: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	Zoek na fouten, enzovo
CIMC-bundel (41xx, 93xx):	Zoek na fouten,

/OBFL/OBFL-log*	enzovo
CIMC-bundel (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*	Zoek na fouten, enzovo Speciaa CATER
Module bundel (41xx, 93xx): /tmp/mount_media.log/mount_media.log	Zoek na fouten, enzovo

Stap 14: Opnamen

Als een specifieke interface niet meer reageert, legt u de firewall en het aangrenzende apparaat vast. U kunt dit document raadplegen voor meer informatie:

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

Zorg er bovendien voor dat de ARP- en CAM-tabellen van de aangrenzende apparaten correct zijn ingevuld.

Stap 15: Aanvullende informatie voor Cisco TAC

Naast de hierboven genoemde zaken is het sterk aan te raden om ook deze informatie te verstrekken:

15 bis. Als het apparaat is hersteld, verzamelt u een bundel voor probleemoplossing (controleer stap 13 voor meer informatie).

15 ter. Als het apparaat nog steeds niet reageert, geeft u deze informatie op:

- Informatie over hardware (model).
- Software-informatie.
- FMC-softwaregegevens (indien van toepassing).
- Implementatie (standalone/HA/cluster).

15 quater. Geschatte tijd (datum/tijd) waarop het apparaat niet meer reageert.

15d. Geschatte uptime van het apparaat voordat het niet meer reageert.

15 sexies. Is dit een nieuwe of een bestaande?

15 septies. Wat was de laatste actie die werd uitgevoerd voordat het apparaat niet meer reageerde?

15 g. Firewall data plane (LINA)-syslogs vanaf het moment dat het apparaat niet meer reageerde (probeer logs te starten ~5 minuten voor het incident). Als beste praktijk wordt aanbevolen om syslogs te configureren op niveau 6 (Informatief).

15.00 uur Als u een syslog-server op het chassis hebt geconfigureerd (FXOS op 4100/9300), geeft u de logboeken op (vanaf ~5 minuten voor het incident).

15 decies. Syslogs van de aangrenzende apparaten uit de tijd van het incident.

15j. Een topologiediagram dat de fysieke verbindingen tussen het firewallapparaat en de aangrenzende apparaten toont.

Veelvoorkomende problemen

Fout: Time-out voor communicatie met DME

Als u verbinding maakt met de console en zie:

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

Meestal duidt dit op een softwareprobleem.

Aanbevolen actie: Neem contact op met Cisco TAC

Schijffout: ontbrekend of inoperabel

Deze uitvoer is afkomstig van een 4100/9300-hardwareapparaat waarbij een schijfgerelateerde fout wordt gegenereerd:

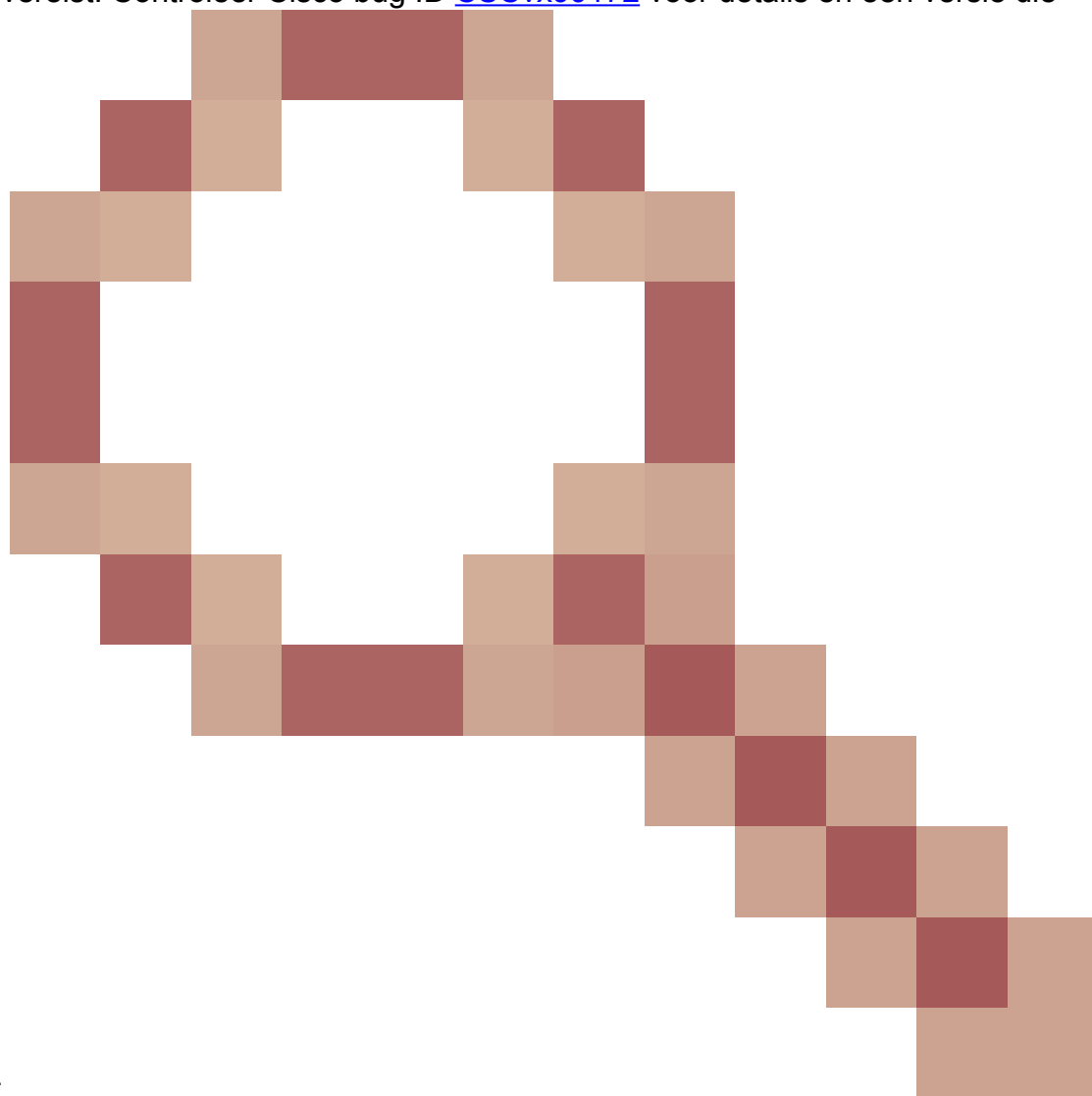
Overview Interfaces Logical Devices Security Engine Platform Settings			
Hardware State	Service State	Power	Application
 Up	 Fault	 On	Cisco Firepower Threat Defense
Disk on a Security Module has errors Please verify the disk presence and replace the faulty disk if the fault does not clear Security Module: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

Aanbevolen actie: Probeer de SSD-schijf opnieuw te herstellen. Als dit niet helpt, verzamelt u de bundel voor probleemoplossing voor het chassis en neemt u contact op met Cisco TAC.

Bericht ter plaatse: FN72077 - FPR9300 en FPR4100

- De beveiligingstoestellen uit de FPR9300- en FPR4100-reeks passeren niet langer het netwerkverkeer.
- Gebruikers met geldige referenties kunnen zich niet aanmelden bij de beheerconsole.
- CLI toont foutmelding: "Softwarefout: uitzondering tijdens uitvoering: [Fout: Time-out voor communicatie met DME]"

Aanbevolen actie: om tijdelijk van dit probleem te herstellen, is een stroomcyclus van het 4100/9300-chassis vereist. Controleer Cisco bug ID [CSCvx99172](#) voor details en een versie die

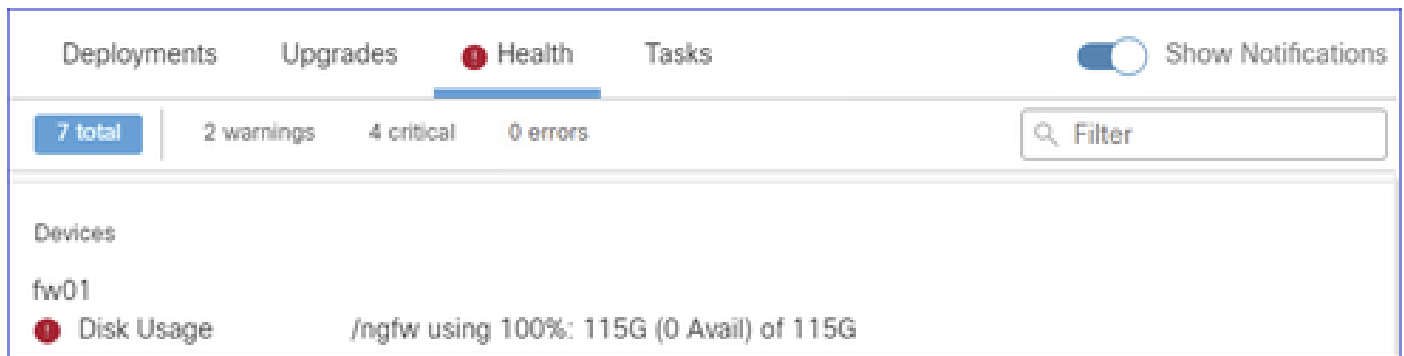


een oplossing heeft.

(Kennisgeving in het veld: FN72077 - FPR9300- en FPR4100-serie beveiligingstoestellen - Sommige apparaten kunnen na 3,2 jaar uptime het verkeer niet passeren).

Schijfgebruik 100%

Lage schijfruimte op de firewall kan het apparaat niet reageren. Als het apparaat wordt beheerd door FMC, kunt u gezondheidswaarschuwingen als volgt krijgen:



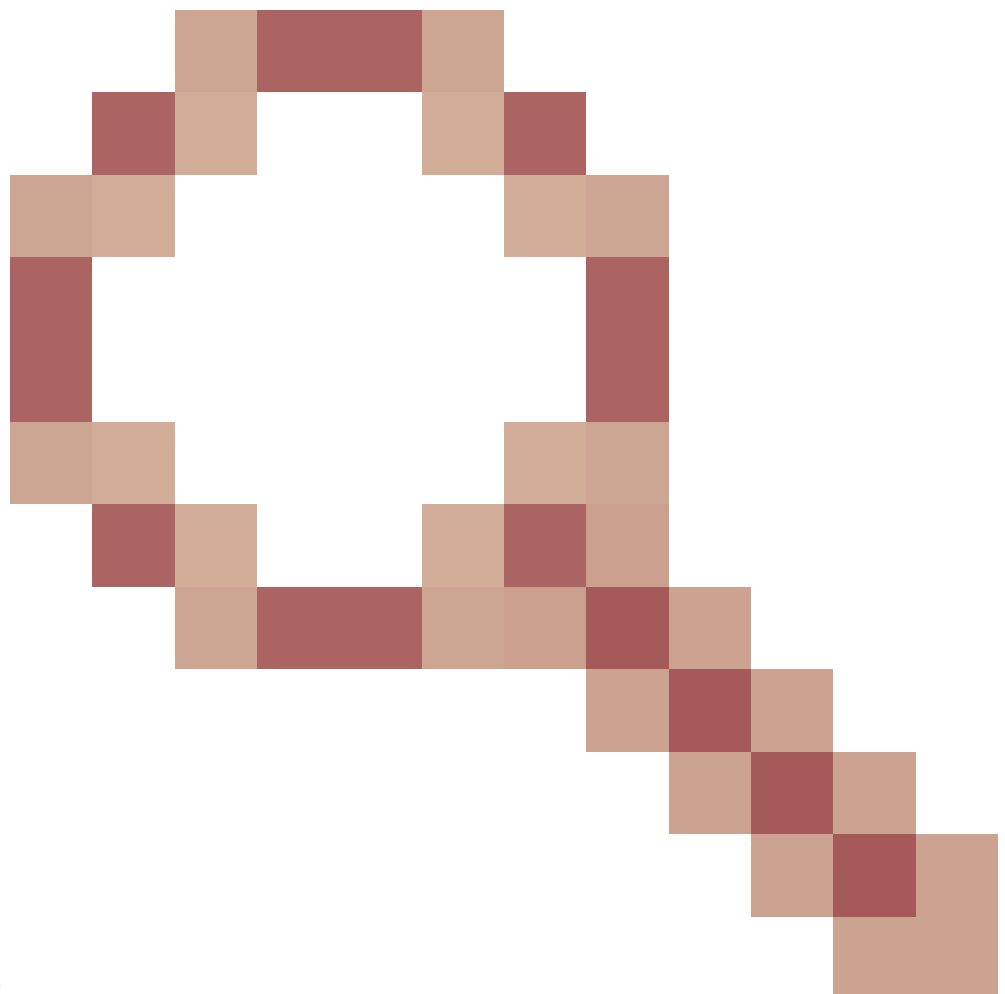
Aanbevolen actie: Als FMC en FTD op software 7.7.0 en hoger worden uitgevoerd, probeer dan wat schijfruimte vrij te maken met de procedure die is beschreven op

<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>

Als dit niet haalbaar is of niet helpt, neemt u contact op met Cisco TAC.

CSF 3100 komt niet naar boven na een stroomstoring

Aanbevolen actie: Upgrade naar een softwarerelease met een oplossing voor:



Cisco bug ID [CSCwm14729](#)

CSF 3100-serie die niet opnieuw wordt opgestart na stroomuitval, waarvoor handmatige voedingscyclus nodig is.

Beveiligingstoestellen uit de Cisco Firepower 2100-reeks: sommige apparaten kunnen geheugenfouten ondervinden

- DIMM-fouten binnen 5 jaar na levering vanwege problemen met het componentproces
- Gerelateerd FN: <https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html>
- Gerelateerde Cisco bug ID [CSCwb74948](#)

Aanbevolen actie: vervanging van DIMM-onderdelen of vervanging van het beveiligingsapparaat

Referenties

- <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>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.