Fehlerbehebung bei einer nicht reagierenden Cisco Secure Firewall

Inhalt

Einleitung

In diesem Dokument werden die empfohlenen Schritte zur Fehlerbehebung bei einer Cisco Secure Firewall Threat Defense (FTD) beschrieben, die auf den Hardwareplattformen 1xxx, 12xx, 21xx, 31xx, 41xx, 42xx und 93xx nicht reagiert.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure FTD - Grundlagen (Installation/Konfiguration)

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall - Schutz vor Bedrohungen
- Cisco Secure Firewall Management Center
- Cisco FirePOWER Extensible Operating System (FXOS)

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In einigen Fällen reagiert ein FTD-Gerät von Cisco nicht mehr. Typische Symptome sind:

- Kein SSH-Zugriff.
- Kein Konsolenzugriff.
- Der Konsolenzugriff funktioniert, die Anmeldedaten jedoch nicht.
- Der Transit-Datenverkehr läuft nicht über das Gerät.
- Die Schnittstellen sind ausgefallen (Daten und/oder Verwaltung).
- Die LEDs leuchten nicht oder orange (blinkend oder stetig).
- Das sichere Modul (4100, 9300) reagiert nicht mehr.

Beachten Sie, dass je nach Situation einige von ihnen nicht anwesend sein werden. Es könnte beispielsweise passieren, dass Datenverkehr durch die Infrastruktur fließt, aber nur der Verwaltungszugriff funktioniert nicht.

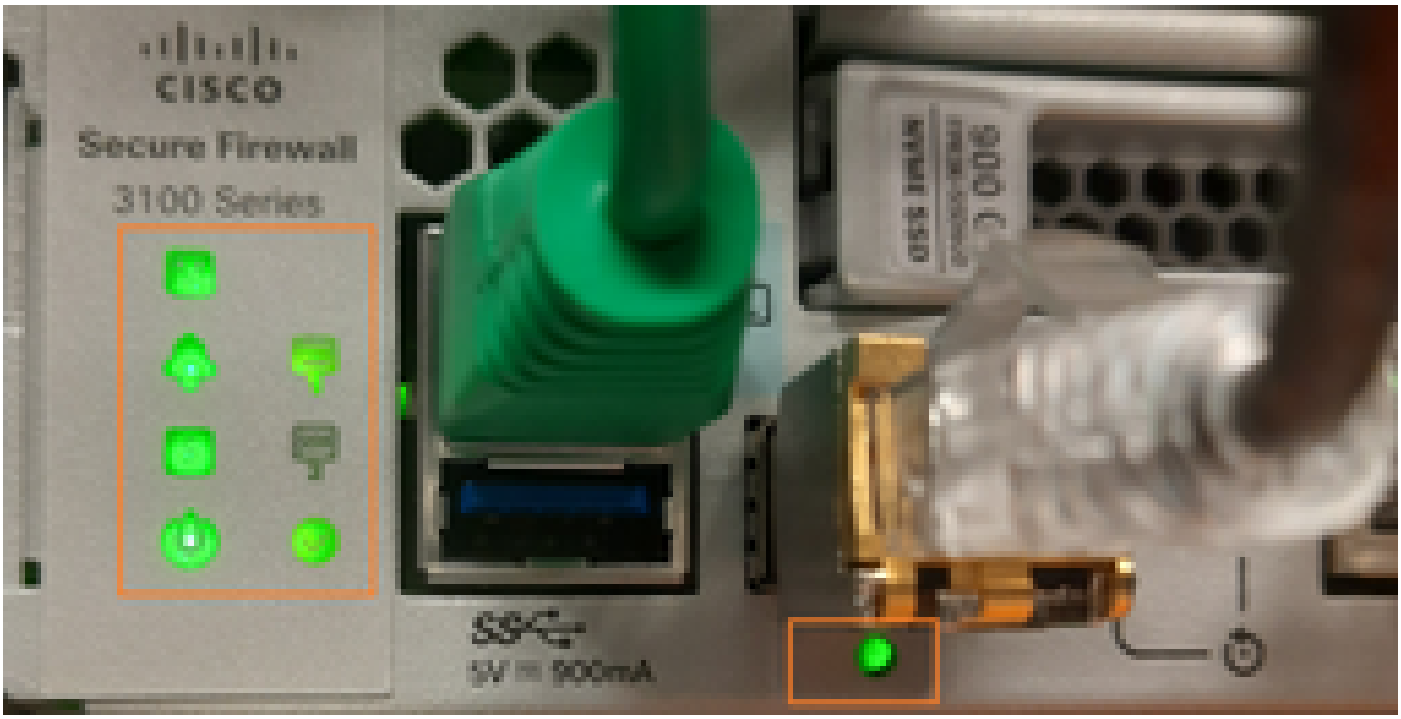
Fehlerbehebung

In diesem Abschnitt werden die empfohlenen Schritte und Aktionen beschrieben, die Sie durchführen müssen. Sie können diese Informationen dem Cisco TAC zur weiteren Analyse zur Verfügung stellen.

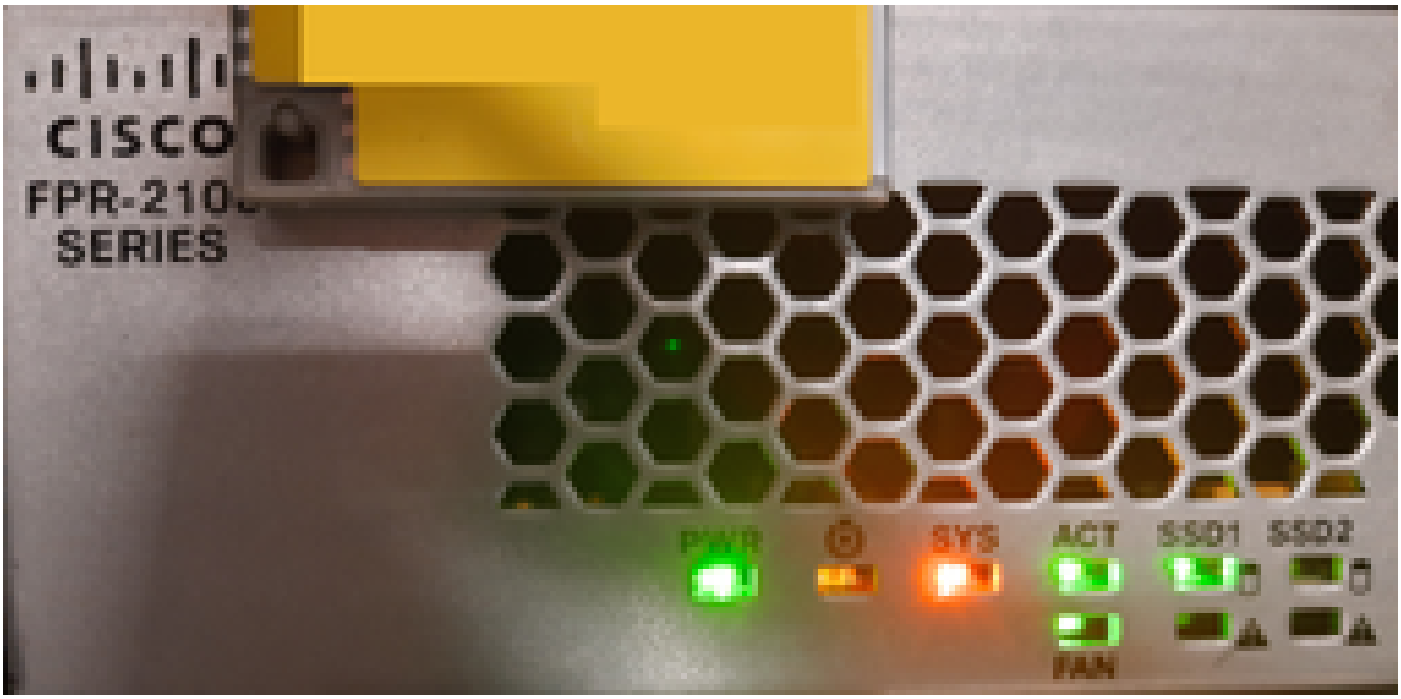
Schritt 1: Sichtprüfung (Vorderseite)

Nehmen Sie ein Video oder ein Bild der LEDs auf der Vorderseite auf. Hier einige Beispiele, bei

denen alle LEDs deutlich sichtbar sind:



Auf dem nächsten Foto zeigt die SYSTEM-LED ein Geräteproblem an:



Im Hardware-Handbuch Ihres Gerätemodells finden Sie weitere Informationen über die LED, z. B.:

Modell	LED-Info
1010	https://www.cisco.com/c/en/us/td/docs/security/firepower/1010/hw/guide/hw-install-1010/overvie
1100	https://www.cisco.com/c/en/us/td/docs/security/firepower/1100/hw/guide/hw-install-11001/overvi
1210CE, 1210CP, 1220CX	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1210-20/hw-install-121
1230, 1240, 1250	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/1230-40-50/hw-install-1
2100	https://www.cisco.com/c/en/us/td/docs/security/firepower/2100/hw/guide/b_install_guide_2100/ov
3100	https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/hardware/3100/fw-3100-install/m-
4110, 4120, 4140, 4150	https://www.cisco.com/c/en/us/td/docs/security/firepower/4100/hw/guide/b_install_guide_4100/ov

+1 4112 4115 4125	https://www.cisco.com/c/en/us/td/docs/security/firepower/41x5/hw/guide/install-41x5/overview.ht
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

Phase 2: Sichtprüfung (Rückseite)

Nehmen Sie ein Video oder ein Bild der LEDs auf der Rückseite auf, zum Beispiel:

Wenn keine LEDs zum Ein-/Ausschalten angezeigt werden:

- Versuchen Sie, die Netzteile wieder einzusetzen (falls zutreffend).
- Versuchen Sie, wenn möglich, das Netzteil auszutauschen.

Schritt 3: Lüfterprüfungen

Überprüfen Sie, ob die Lüfter auf der Rückseite der Appliance ausgeführt werden.

Schritt 4: Prüfungen der physischen Umgebung

Prüfen Sie, ob Geräusche oder Gerüche vom Gerät ausgehen.

Schritt 5: Überprüfung von Konsolen- und Management-Ports

Stellen Sie sicher, dass die Konsolen- und Management-Ports ordnungsgemäß angeschlossen sind. Wenn das Problem nur beim Management-Port auftritt, versuchen Sie, den SFP (sofern zutreffend) und das Netzwerkkabel zu ändern.

Schritt 6: Management-IP-Verbindungstest

Versuchen Sie, einen Ping (ICMP) an die Management-IP-Adresse des Geräts zu senden.

Schritt 7: Prüfungen benachbarter Geräte

Überprüfen Sie den Port-Status der benachbarten Geräte, z. B.:

<#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
```

Schritt 8: Überprüfung von HA-/Cluster-Geräten

Im Fall einer Hochverfügbarkeit oder einer Cluster-Konfiguration holen Sie ein Fehlerbehebungspaket von den Peer-Geräten ein.

Schritt 9: Konsolenprotokolle erfassen

Schließen Sie einen Laptop an den Konsolenport an, und kopieren Sie alle angezeigten Meldungen. Drücken Sie die Tasten Nach oben/Nach unten oder PageUp, um alle Meldungen auf dem Bildschirm anzuzeigen.

Phase 10: Kaltstart durchführen

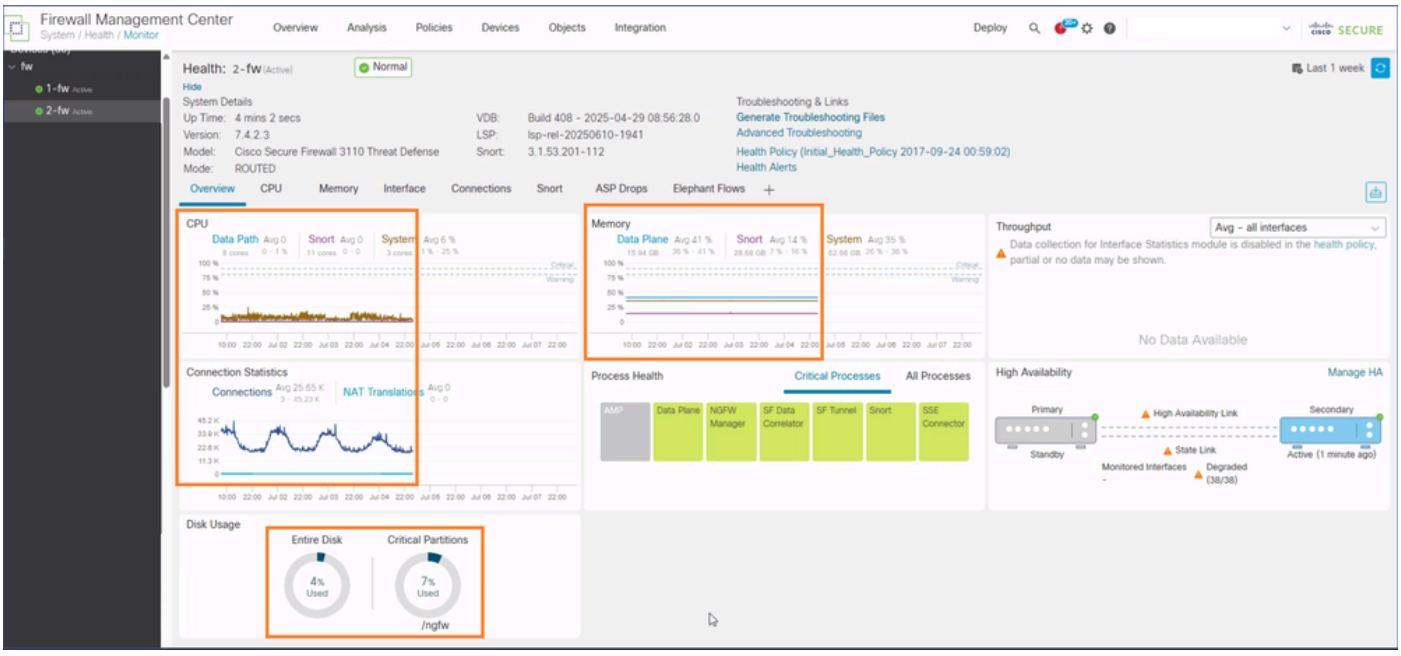
Mit einem Laptop, der an den Konsolenport angeschlossen ist:

1. Ziehen Sie alle Netzkabel ab, und warten Sie einige Minuten, bevor Sie sie wieder anschließen.
2. Im Falle einer Failover- oder Cluster-Konfiguration können Sie zur Minimierung des Risikos einer Active/Active- oder Cluster-Instabilität alle Datenschnittstellen des betroffenen Geräts einschließlich der HA- oder CCL-Verbindungen vom benachbarten Switch-Gerät trennen oder herunterfahren.
3. Schließen Sie dann die Netzkabel wieder an, und schalten Sie das Gerät ein.
4. Warten Sie ca. 5 Minuten.
5. Sammeln Sie die Konsolenausgabe.

Beachten Sie, dass der Kaltstart zu einer Datenbankbeschädigung führen kann, wenn das Gerät nicht ordnungsgemäß heruntergefahren wurde und das Gerät betriebsbereit war (die LEDs auf der Vorderseite waren eingeschaltet). Wenn der Kaltstart das Gerät aktiviert, nehmen Sie ein Fehlerbehebungspaket mit und wenden Sie sich an Cisco TAC.

Phase 11: Erfassen von Health Monitor-Diagrammen von FMC

Wenn das Gerät wiederhergestellt und von einem FMC verwaltet wird, navigieren Sie zu System > Health > Monitor, und wählen Sie das Gerät aus. Konzentrieren Sie sich auf die hervorgehobenen Diagramme, um den Status des Geräts zu ermitteln, bevor Sie nicht reagieren (z. B. hoher Arbeitsspeicher, hohe CPU, hohe Festplattenauslastung usw.).



Phase 12: Überprüfen Sie, ob Probleme mit dem Datenträger vorliegen.

Nichterfüllung (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
```

Beispielausgabe von 3100, wenn die Festplatte betriebsbereit ist:

<#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
```

Beispielausgabe von 4100, wenn die Festplatte betriebsbereit ist:

<#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
```

Phase 13: Protokollanalyse

Wenn das Firewall-Gerät wiederhergestellt wird und Sie die Backend-Protokolle analysieren möchten, erstellen Sie ein Fehlerbehebungspaket, und überprüfen Sie die in der Tabelle genannten Dateien. Beachten Sie, dass:

- Auf den Plattformen 1xxx, 12xx, 21xx (Appliance-Modus), 31xx, 42xx enthält das FTD-Problemlösungspaket auch das Chassis-Paket (FPRM) von FXOS im Pfad \dir-archives\var-common-platform_ts\. Sie müssen den Inhalt des FPRM-Pakets extrahieren.
- Sammeln Sie auf 3100/4200 im Multi-Instance (MI)-Modus die TS-Datei des Chassis von der FMC-Benutzeroberfläche oder der CLI des Chassis (zeigen Sie Details des technischen Supports aus dem local-mgmt-Befehlsbereich), wie unter https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400 beschrieben.
- Auf 41xx- und 93xx-Plattformen müssen Sie das Chassis-Paket separat von der Chassis-UI oder der FXOS-CLI generieren, wie in https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#toc-hId-2132091400 beschrieben.
- Für 4100- und 9300-Geräteplattformen müssen Sie FXOS- und FTD-Fehlerbehebungspakete sammeln. Für alle anderen Plattformen ist das FTD-Fehlerbehebungspaket ausreichend, da es auch das FXOS-Fehlerbehebungspaket enthält.
- Für ASA ist die Befehlsausgabe "show tech-support" nach der Wiederherstellung nicht sehr hilfreich. Verlassen Sie sich auf das FXOS-Paket zur Fehlerbehebung.
- Im Vergleich zu anderen Plattformen stehen für 41xx und 93xx zwei Pakete zur Fehlerbehebung zur Verfügung: Chassis (BC1) und Modulpaket.
- Das Chassis-Paket (BC1) auf 41xx, 93xx enthält unter anderem die FPRM- und CIMC-Pakete.
- Das Modulpaket auf 41xx, 93xx enthält hauptsächlich FXOS-Protokolle vom Blade.
- Wenn Sie eine ASA installiert haben, müssen Sie sich (sofern zutreffend) nur auf das Chassis, FPRM und die Modulpakete verlassen sowie auf die Befehlsausgabe "show tech-support" von ASA.

- Je nach Plattform und Incident sind nicht alle Dateien vorhanden.

Dateipfad im Fehlerbehebungspaket	Beschr
FTD TS-Paket: /dir-archives/var-log/messages*	Die Zei "syslog down" v ordnung Herunte angeze Beim S Geräts Zeicher ng start wird ge angeze
FTD TS-Paket: /dir-archives/var-log/ASAconsole.log Bei ASA auf 4100/9300 finden Sie die Datei auch im Modul-Paket unter /opt/cisco/platform/logs/ASAconsole.log	Suchen Fehlern Fehlern
FTD TS-Paket: /dir-archives/var-log/dmesg.log	Suchen Fehlern Fehlern
FTD TS-Paket: /dir-archives/var/log/ngfwManager.log*	Suchen Fehlern Fehlern Diese D auch In über HA Ereignis
FTD TS-Paket: /command-outputs/LINA_troubleshoot/show_tech_output.txt	Die Aus "show f (Failove anzeige cluster" (Cluste

	anzeige zusätzli in die E liefern.
FTD TS-Paket: /command-outputs/ Dateinamen: · für CORE in `ls opt-cisco-csp-cores _ grep core`_ do file -opt-cisco-csp-cores-_{CORE}_ done.output · für CORE in `ls var-common _ grep core`_ do file var-common-_{CORE}_ done.output · für CORE in `ls var-data-cores _ grep core`_ do file -var-data-cores-_{CORE}_ done.output	Auf pot Dateien prüfen.
FTD TS-Paket: /dir-archives/var/log/crashinfo/snort3-crashinfo.*	Suchen Snort3 Dateien
FTD TS-Paket: /dir-archives/var/log/process_stderr.log*	Überprü Rückve vorhand Cisco E CSCwh
FTD TS-Paket: /dir-archives/var/log/periodic_stats/	Das Ve enthält Dateien in den Z Vorfalls können
FPRM-Paket: Technische_Unterstützung_Kurzbeschreibung	Prüfen Ausgab fault de
FPRM-Paket: /opt/cisco/platform/logs/kern.log	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/messages*	Suchen

	Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/mce.log Dieselbe Datei ist auch im Modulpaket (41xx, 93xx) vorhanden.	Dies ist Datei (M Excepti Sie nac Fehlern
FPRM-Paket: /opt/cisco/platform/logs/portmgr.out	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/sysmgr/logs/kp_init.log:	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/ssp-pm.log Dieselbe Datei ist auch im Modulpaket (41xx, 93xx) vorhanden.	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/sma.log Dieselbe Datei ist auch im Modulpaket (41xx, 93xx) vorhanden.	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/heimdall.log	Suchen Fehlern Fehlern
FPRM-Paket: /opt/cisco/platform/logs/ssp-shutdown.log Dieselbe Datei ist auch im Modulpaket (41xx, 93xx) vorhanden.	Es enth Ausgab und ein dmesg oder He Verfügb 1000/2
FPRM-Paket: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_dme.log*	Suchen Fehlern Fehlern

FPRM-Paket: /opt/cisco/platform/logs/sysmgr/sam_logs/svc_sam_envAG.log*	Suchen Fehlern Fehlern
CIMC-Paket (41xx, 93xx): /obfl/obfl-log*	Suchen Fehlern Fehlern
CIMC-Paket (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*	Suchen Fehlern Fehlern Speziel
Modulpaket (41xx, 93xx): /tmp/mount_media.log/mount_media.log	Suchen Fehlern Fehlern

Phase 14: Aufnahmen

Wenn eine bestimmte Schnittstelle nicht mehr reagiert, können Sie Aufzeichnungen auf der Firewall und dem benachbarten Gerät erstellen. Weitere Informationen finden Sie in diesem Dokument:

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

Stellen Sie außerdem sicher, dass die ARP- und CAM-Tabellen der benachbarten Geräte korrekt ausgefüllt sind.

Phase 15: Zusätzliche Informationen für das Cisco TAC

Zusätzlich zu den oben genannten Punkten wird dringend empfohlen, folgende Informationen bereitzustellen:

15 a) Wenn das Gerät wiederhergestellt wurde, sammeln Sie ein Fehlerbehebungspaket (weitere Informationen finden Sie in Schritt 13).

15 b. Wenn das Gerät immer noch nicht reagiert, geben Sie die folgenden Informationen an:

- Hardware-Informationen (Modell).
- Software-Informationen.

- FMC-Softwareinformationen (falls zutreffend).
- Bereitstellung (Standalone/HA/Cluster).

15 c. Ungefährer Zeitpunkt (Datum/Uhrzeit), an dem das Gerät nicht mehr reagiert.

15 d. Ungefähre Betriebszeit des Geräts, bevor es nicht mehr reagiert.

15e. Handelt es sich um ein neues oder ein vorhandenes Setup?

15 f. Welche Aktion wurde zuletzt ausgeführt, bevor das Gerät nicht mehr reagiert?

15 g Firewall Data Plane (LINA)-Syslogs ab dem Zeitpunkt, an dem das Gerät nicht mehr reagiert (Protokolleingabe etwa 5 Minuten vor dem Vorfall). Als Best Practice wird empfohlen, Syslogs auf Stufe 6 zu konfigurieren (informativ).

15 Uhr Wenn Sie einen Syslog-Server im Chassis (FXOS auf 4100/9300) konfiguriert haben, stellen Sie die Protokolle bereit (Beginn ca. 5 Minuten vor dem Vorfall).

15i Syslogs von den benachbarten Geräten zum Zeitpunkt des Incident.

15 j) Topologiediagramm, das die physischen Verbindungen zwischen dem Firewall-Gerät und den angrenzenden Geräten zeigt.

Häufige Probleme

Fehler: Zeitüberschreitung bei der Kommunikation mit DME

Wenn Sie eine Verbindung zur Konsole herstellen und Folgendes sehen:

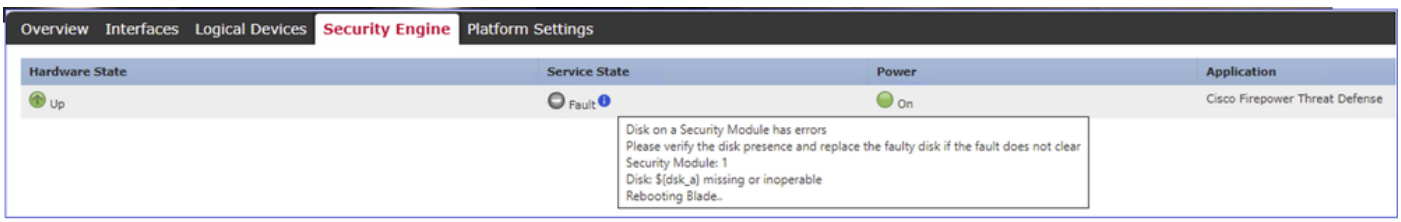
```
Software Error: Exception during execution: [Error: Timed out communicating with DME]
```

Meistens weist dies auf ein Softwareproblem hin.

Empfohlene Aktion: Cisco TAC kontaktieren

Datenträgerfehler: fehlend oder funktionsunfähig

Diese Ausgabe stammt von einer 4100/9300-Hardware-Appliance, bei der ein festplattenbezogener Fehler generiert wird:



Empfohlene Aktion: Versuchen Sie, den SSD-Datenträger erneut einzusetzen. Wenn es nicht hilft, Chassis-Fehlerbehebung Paket sammeln und Cisco TAC kontaktieren.

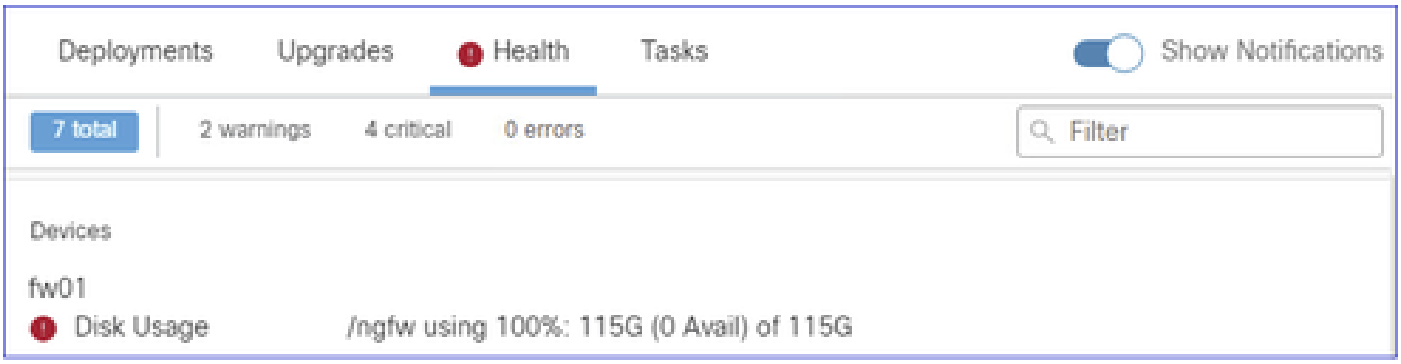
Problemhinweis: FN72077 - FPR9300 und FPR4100

- Die Sicherheits-Appliances der Serien FPR9300 und FPR4100 leiten den Netzwerkverkehr nicht mehr weiter.
- Benutzer mit gültigen Anmeldeinformationen können sich nicht bei der Verwaltungskonsole anmelden.
- CLI zeigt eine Fehlermeldung an: "Softwarefehler: Ausnahme während der Ausführung: [Fehler: Zeitüberschreitung bei der Kommunikation mit DME]

Empfohlene Aktion: Um dieses Problem vorübergehend zu beheben, muss das 4100/9300-Gehäuse aus- und wieder eingeschaltet werden. Unter der Cisco Bug-ID CSCvx99172 finden Sie weitere Informationen und eine Version, die behoben werden kann.
(Problemhinweis: FN72077 - Sicherheitslösungen der Serien FPR9300 und FPR4100 - Bei einigen Appliances kann der Datenverkehr nach 3,2 Jahren Betriebszeit nicht weitergeleitet werden.)

Festplattenauslastung 100 %

Wenn wenig Festplattenspeicher in der Firewall vorhanden ist, reagiert das Gerät möglicherweise nicht mehr. Wenn das Gerät vom FMC verwaltet wird, können Sie Statusmeldungen wie diesen erhalten:



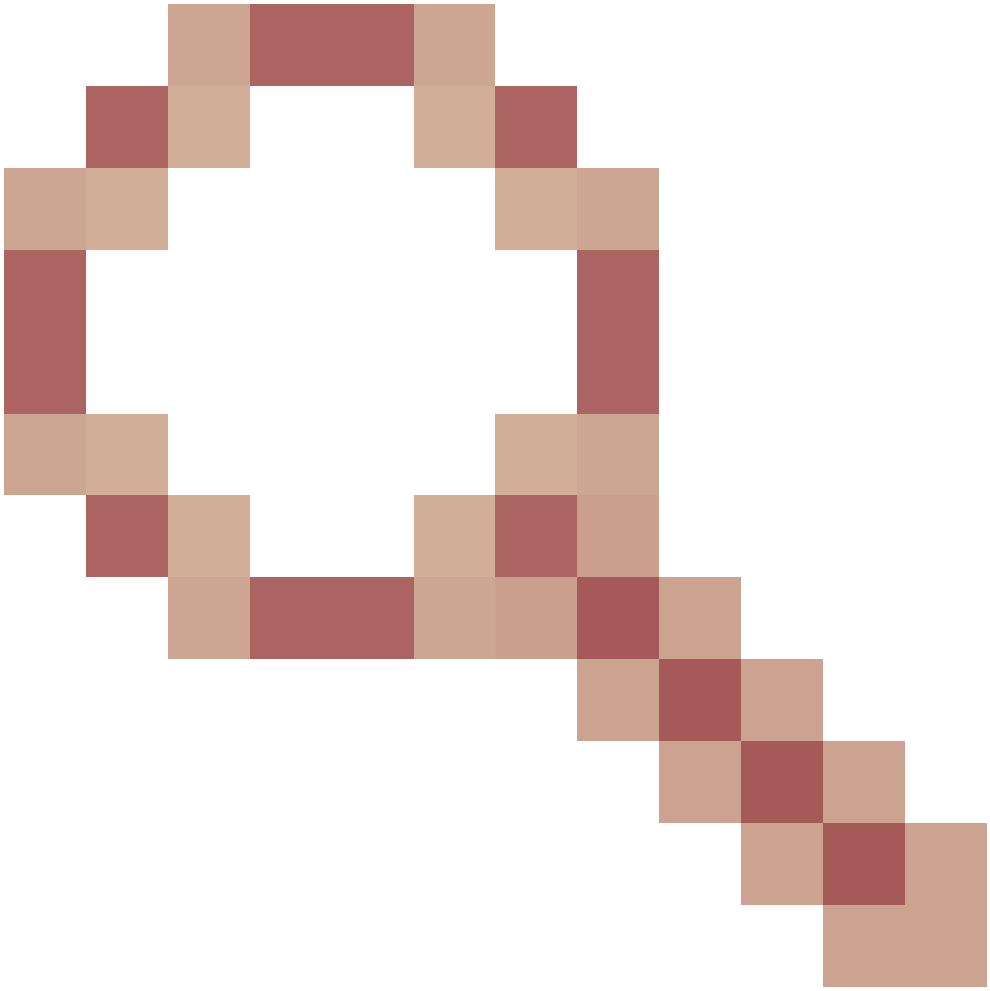
Empfohlene Aktion: Wenn FMC und FTD auf der Software 7.7.0 und höher ausgeführt werden, versuchen Sie, einen Teil des Festplattenspeichers mithilfe des unter https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-

center/admin/770/management-center-admin-77/health-troubleshoot.html#clear-disk-space dokumentierten Verfahrens zu löschen.

Wenn dies nicht möglich ist oder nicht weiterhilft, wenden Sie sich an Cisco TAC.

Nach einem Stromausfall kommt der CSF 3100 nicht zum Einsatz

Empfohlene Aktion: Führen Sie ein Upgrade auf eine Softwareversion durch, die die folgenden Probleme behebt:



Cisco Bug-ID CSCwm14729
Die Serie CSF 3100 wird nach einem Stromausfall nicht neu gestartet und muss manuell ein- und ausgeschaltet werden.

Cisco Firepower Security Appliances der Serie 2100: Bei einigen Einheiten können Speicherfehler auftreten.

- DIMM-Fehler innerhalb von 5 Jahren nach Serviceausfall aufgrund von Problemen mit Komponentenprozessen
- Zugehörige FN: https://www.cisco.com/c/en/us/support/docs/field-notices/741/fn74199.html
- Zugehörige Cisco Bug-ID CSCwb74948

Empfohlene Aktion: Austausch von DIMM-Komponenten oder Austausch der Sicherheits-Appliance

Referenzen

- 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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.