Failover-Statusmeldungen für FTD verstehen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Failover-Statusmeldungen zu Secure Firewall Threat Defense (FTD) verstehen.

Voraussetzungen

Anforderungen

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

- Hochverfügbarkeit für Cisco Secure FTD
- Grundlegende Benutzerfreundlichkeit des Cisco Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco FMC v7.2.5
- Cisco Firepower der Serie 9300 v7.2.5

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

Übersicht: Failover-Zustandsüberwachung:

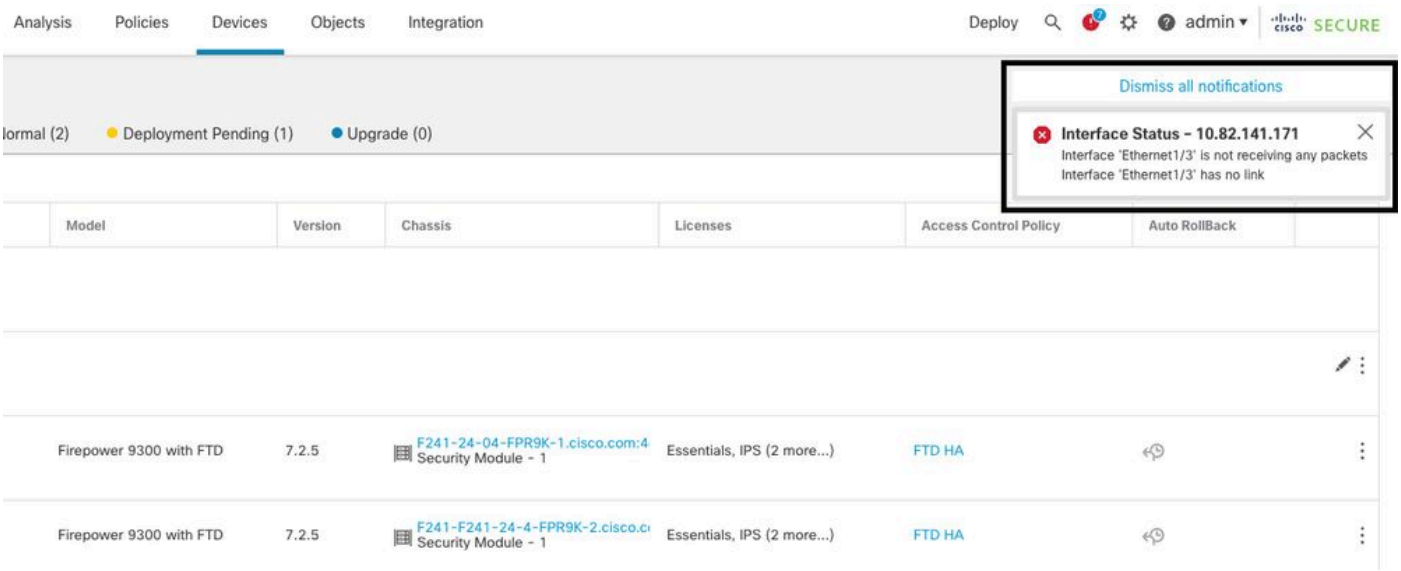
Das FTD-Gerät überwacht die einzelnen Geräte auf ihren Gesamtzustand und auf den Zustand der Schnittstelle. Das FTD führt Tests durch, um den Status der einzelnen Einheiten basierend auf der Überwachung der Integrität der Einheiten und der Schnittstellenüberwachung zu bestimmen. Wenn ein Test zur Bestimmung des Zustands der einzelnen Einheiten im HA-Paar fehlschlägt, werden Ausfallereignisse ausgelöst.

Failover-Statusmeldungen

Anwendungsfall: Datenverbindung unterbrochen ohne Failover

Wenn die Schnittstellenüberwachung auf der FTD HA nicht aktiviert ist und eine Datenverbindung ausfällt, wird kein Failover-Ereignis ausgelöst, da die Integritätsüberwachungstests für die Schnittstellen nicht durchgeführt werden.

Dieses Bild beschreibt die Warnungen bei einem Verbindungsausfall, es werden jedoch keine Failover-Warnungen ausgelöst.



Warnung bei Verbindungsabbruch

Um den Status und Status der Datenverbindungen zu überprüfen, verwenden Sie folgenden Befehl:

- show failover - Zeigt die Informationen zum Failover-Status der einzelnen Geräte und Schnittstellen an.

```
Monitored Interfaces 1 of 1291 maximum
...
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Waiting)
Interface INSIDE (172.16.10.1): No Link (Not-Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Waiting)
Interface INSIDE (172.16.10.2): Normal (Waiting)
Interface OUTSIDE (192.168.20.2): Normal (Waiting)
Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
```

Wenn der Status der Schnittstelle "Waiting" lautet, bedeutet dies, dass die Schnittstelle aktiv ist, aber noch kein hello-Paket von der entsprechenden Schnittstelle auf der Peer-Einheit empfangen hat.

Andererseits bedeutet der Status "Keine Verbindung (nicht überwacht)", dass die physische Verbindung für die Schnittstelle ausgefallen ist, jedoch nicht durch den Failover-Prozess überwacht wird.

Um einen Ausfall zu vermeiden, wird dringend empfohlen, den Schnittstellenzustandsmonitor an allen sensiblen Schnittstellen mit den entsprechenden Standby-IP-Adressen zu aktivieren.

Um die Schnittstellenüberwachung zu aktivieren, navigieren SieDevice > Device Management > High Availability > Monitored Interfaces.

Das folgende Bild zeigt die Registerkarte "Überwachte Schnittstellen":

überwachte Schnittstellen

Führen Sie den folgenden Befehl aus, um den Status der überwachten Schnittstellen und Standby-IP-Adressen zu überprüfen:

- show failover - Zeigt die Informationen zum Failover-Status der einzelnen Geräte und Schnittstellen an.

```
Monitored Interfaces 3 of 1291 maximum
...
```

```
This host: Primary - Active
Active time: 3998 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.1): Normal (Monitored)
Interface INSIDE (172.16.10.1): No Link (Monitored)
Interface OUTSIDE (192.168.20.1): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
...
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)
Interface DMZ (192.168.10.2): Normal (Monitored)
Interface INSIDE (172.16.10.2): Normal (Monitored)
Interface OUTSIDE (192.168.20.2): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting)
```

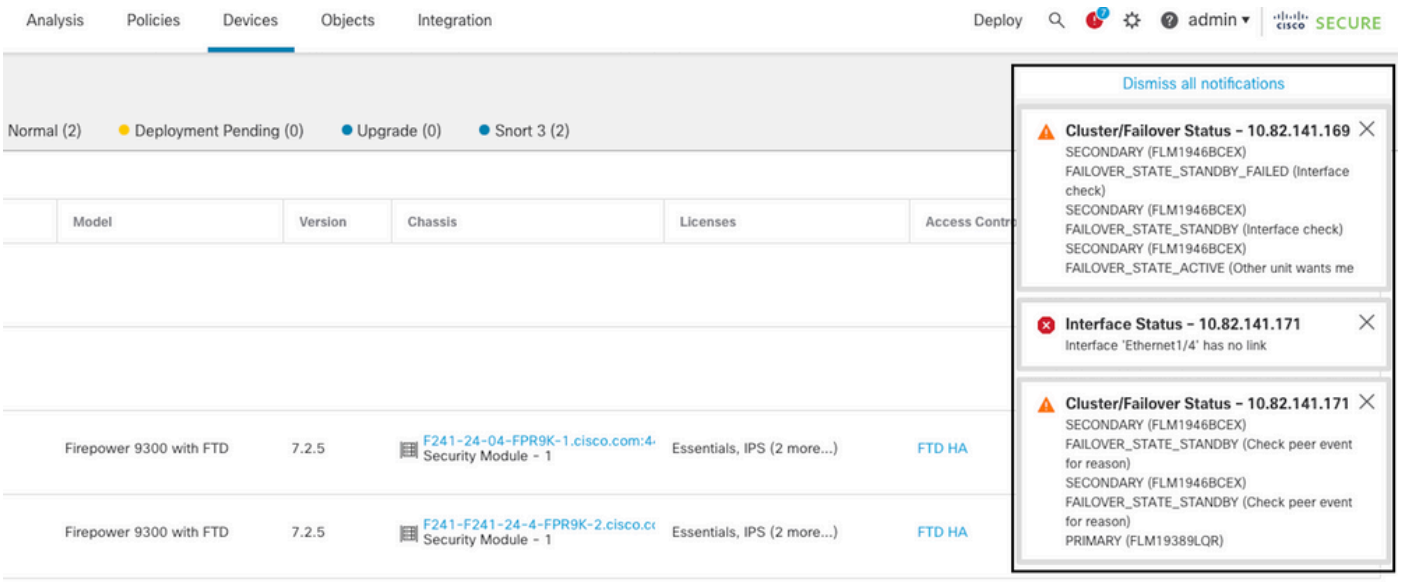
Anwendungsfall - Schnittstellenfehler

Wenn eine Einheit 15 Sekunden lang keine Hello-Nachrichten von einer überwachten Schnittstelle empfängt und der Schnittstellentest an einer Einheit fehlschlägt, aber an der anderen Einheit funktioniert, gilt die Schnittstelle als fehlgeschlagen.

Wenn der Schwellenwert für die Anzahl der ausgefallenen Schnittstellen erreicht ist und die aktive Einheit mehr ausgefallene Schnittstellen als die Standby-Einheit aufweist, tritt ein Failover auf.

Navigieren Sie zum Ändern des Schnittstellengrenzwerts zu Devices > Device Management > High Availability > Failover Trigger Criteria.

Dieses Bild beschreibt die Warnungen, die bei einem Schnittstellenausfall generiert werden:



Failover-Ereignis mit Verbindungsunterbrechung

Verwenden Sie die folgenden Befehle, um die Ursache des Fehlers zu überprüfen:

- show failover state - Dieser Befehl zeigt den Failover-Status beider Einheiten und den letzten

gemeldeten Grund für das Failover an.

<#root>

```
firepower#
```

show failover state

```
This host - Primary
            Active        Ifc Failure          19:14:54 UTC Sep 26 2023
Other host - Secondary
             Failed       Ifc Failure          19:31:35 UTC Sep 26 2023
                          OUTSIDE: No Link
```

- **show failover history** - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderung an.

<#root>

```
firepower#
```

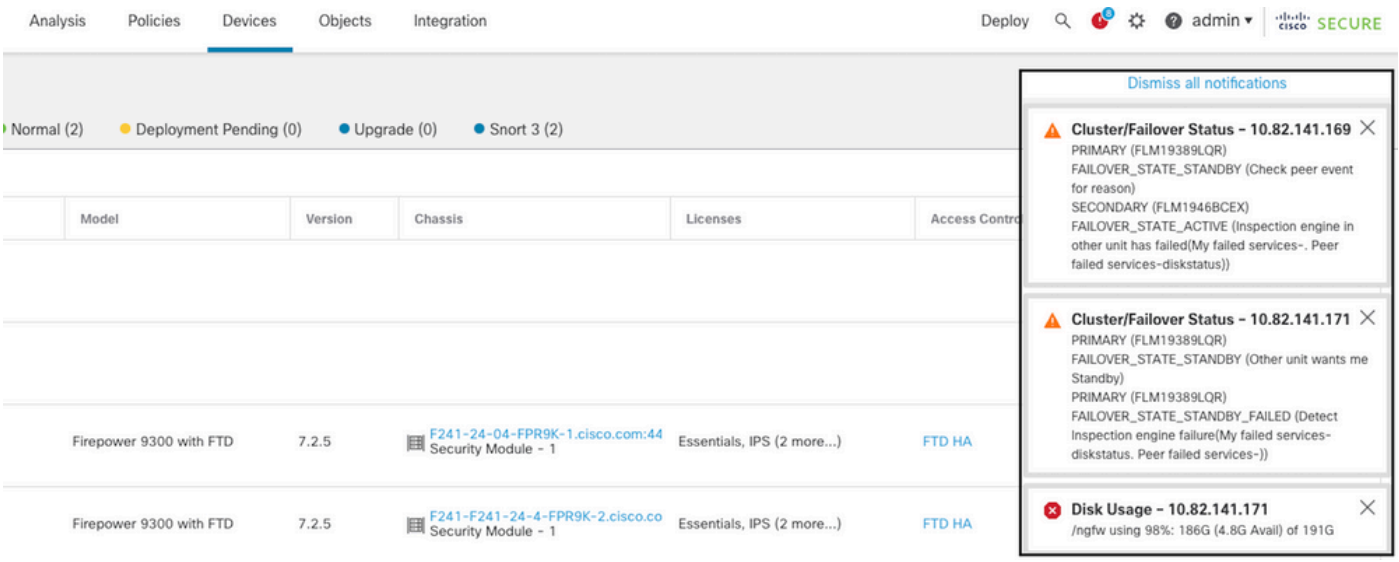
show failover history

```
==========================================================================
From State                     To State             Reason
==========================================================================
19:31:35 UTC Sep 26 2023
Active                          Failed             Interface check
                                                   This host:1
                                                   single_vf: OUTSIDE
                                                   Other host:0
```

Anwendungsfall - Hohe Festplattennutzung

Wenn der Festplattenspeicher auf dem aktiven Gerät zu mehr als 90 % belegt ist, wird ein Failover-Ereignis ausgelöst.

Dieses Bild beschreibt die Warnungen, die generiert werden, wenn der Datenträger voll ist:



Failover mit Festplattennutzung

Verwenden Sie die folgenden Befehle, um die Ursache des Fehlers zu überprüfen:

- show failover history - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderungen an.

<#root>

```
firepower#

show failover history

==========================================================================
From State                    To State                      Reason
==========================================================================
20:17:11 UTC Sep 26 2023
Active                        Standby Ready                 Other unit wants me Standby
                                                            Inspection engine in other unit ha

20:17:11 UTC Sep 26 2023.     Standby Ready                 Failed Detect Inspection engine fa
Active                                                      due to disk failure
```

- show failover - Zeigt die Informationen zum Failover-Status der einzelnen Geräte an.

<#root>

```
firepower#

show failover | include host|disk

      This host: Primary - Failed
              slot 2: diskstatus rev (1.0) status (down)
      Other host: Secondary - Active
               slot 2: diskstatus rev (1.0) status (up)
```

- df -h - Zeigt die Informationen über alle gemounteten Dateisysteme an, die die Gesamtgröße, den genutzten Speicherplatz, den Nutzungsprozentsatz und den Mount-Punkt umfassen.

<#root>

admin@firepower:/ngfw/Volume/home$

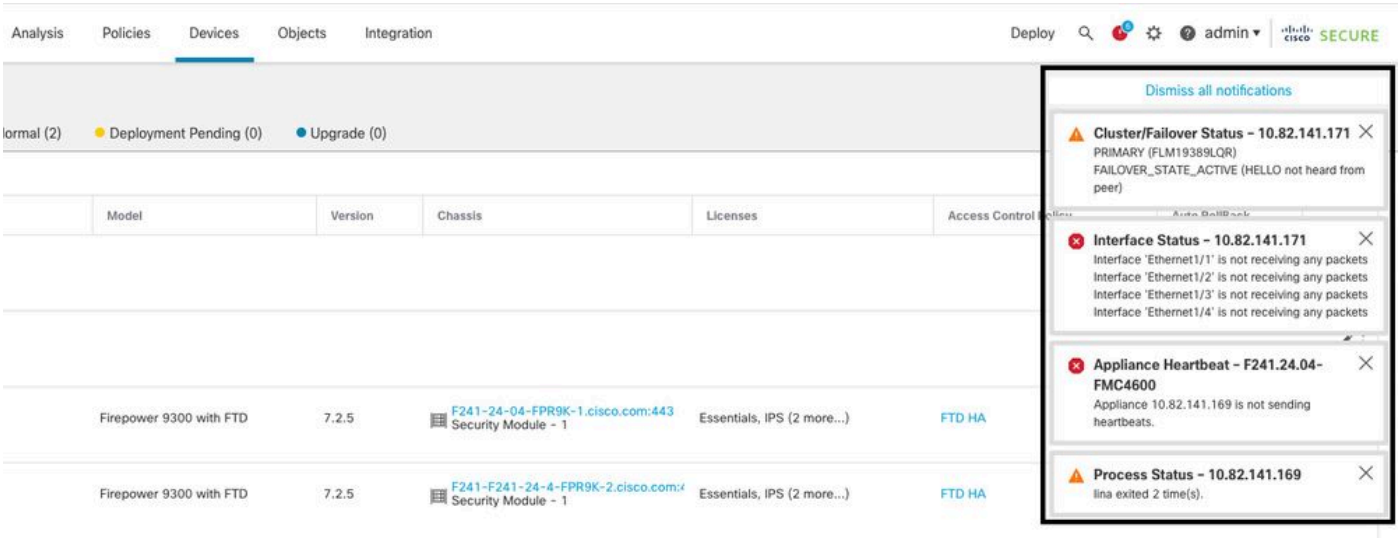
df -h /ngfw

```
Filesystem Size Used Avail Use% Mounted on
/dev/sda6  191G 186G 4.8G  98%  /ngfw
```

Anwendungsfall - Lina Traceback

Bei einem Lina-Traceback kann ein Failover-Ereignis ausgelöst werden.

Dieses Bild beschreibt die Alarme, die im Fall von lina traceback generiert werden:



Failover mit lina traceback

Verwenden Sie die folgenden Befehle, um die Ursache des Fehlers zu überprüfen:

- show failover history - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderung an.

<#root>

firepower#

show failover history

```
==========================================================================
From State                     To State                       Reason
==========================================================================
8:36:02 UTC Sep 27 2023
```

```
Standby Ready                  Just Active                    HELLO not heard from peer
                                                              (failover link up, no response from pee
18:36:02 UTC Sep 27 2023
Just Active                    Active Drain                   HELLO not heard from peer
                                                              (failover link up, no response from pee

18:36:02 UTC Sep 27 2023
Active Drain                   Active Applying Config         HELLO not heard from peer
                                                              (failover link up, no response from pee

18:36:02 UTC Sep 27 2023
Active Applying Config          Active Config Applied         HELLO not heard from peer
                                                              (failover link up, no response from pee

18:36:02 UTC Sep 27 2023
Active Config Applied           Active                        HELLO not heard from peer
                                                              (failover link up, no response from pee
```

Im Fall von lina traceback verwenden Sie diese Befehle, um nach den Core-Dateien zu suchen:

<#root>

```
root@firepower:/opt/cisco/csp/applications#
```

cd /var/data/cores

```
root@firepower:/var/data/cores#
```

ls -l

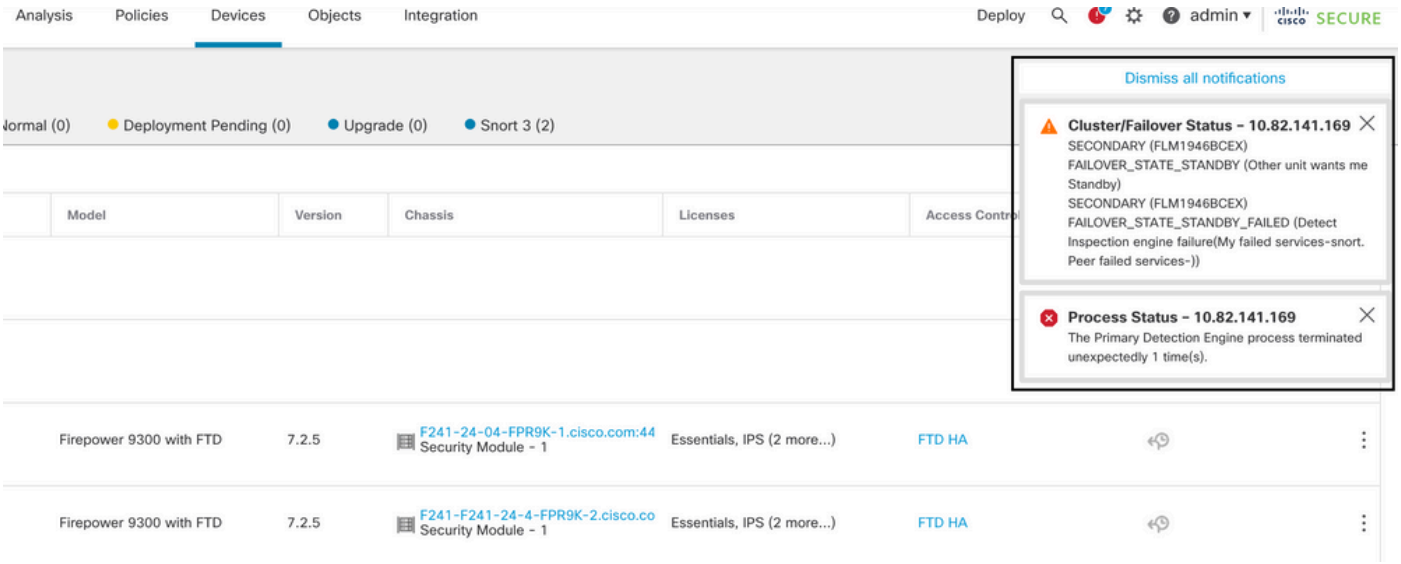
```
total 29016
-rw------- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

Im Fall von Lina Traceback wird dringend empfohlen, die Fehlerbehebungsdateien zu sammeln, die Core-Dateien zu exportieren und sich an Cisco TAC zu wenden.

Anwendungsfall - Snort-Instanz nicht verfügbar

Wenn mehr als 50 % der Snort-Instanzen auf dem aktiven Gerät ausgefallen sind, wird ein Failover ausgelöst.

In diesem Bild werden die Warnungen beschrieben, die bei einem Snort-Fehler generiert werden:



Failover mit Snort-Traceback

Um Überprüfen Sie den Grund für den Fehler. Verwenden Sie hierzu die folgenden Befehle:

- show failover history - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderung an.

<#root>

```
firepower#

show failover history

==========================================================================
From State                     To State                       Reason
==========================================================================
21:22:03 UTC Sep 26 2023
Standby Ready                  Just Active                    Inspection engine in other unit has failed
                                                              due to snort failure

21:22:03 UTC Sep 26 2023
                               Just Active                    Active Drain Inspection engine in other unit
                                                              due to snort failure

21:22:03 UTC Sep 26 2023
                               Active Drain                   Active Applying Config Inspection engine in o
                                                              due to snort failure

21:22:03 UTC Sep 26 2023
                               Active                         Applying Config Active Config Applied Inspect
                                                              due to snort failure
```

- show failover - Zeigt die Informationen zum Failover-Status des Geräts an.

<#root>

```
firepower#
```

```
show failover | include host|snort


This host: Secondart - Active
slot 1: snort rev (1.0) status (up)
Other host: Primary - Failed
slot 1: snort rev (1.0) status (down)
Firepower-module1#
```

Im Fall von snort traceback verwenden Sie diese Befehle, um die Crashfo- oder Core-Dateien zu finden:

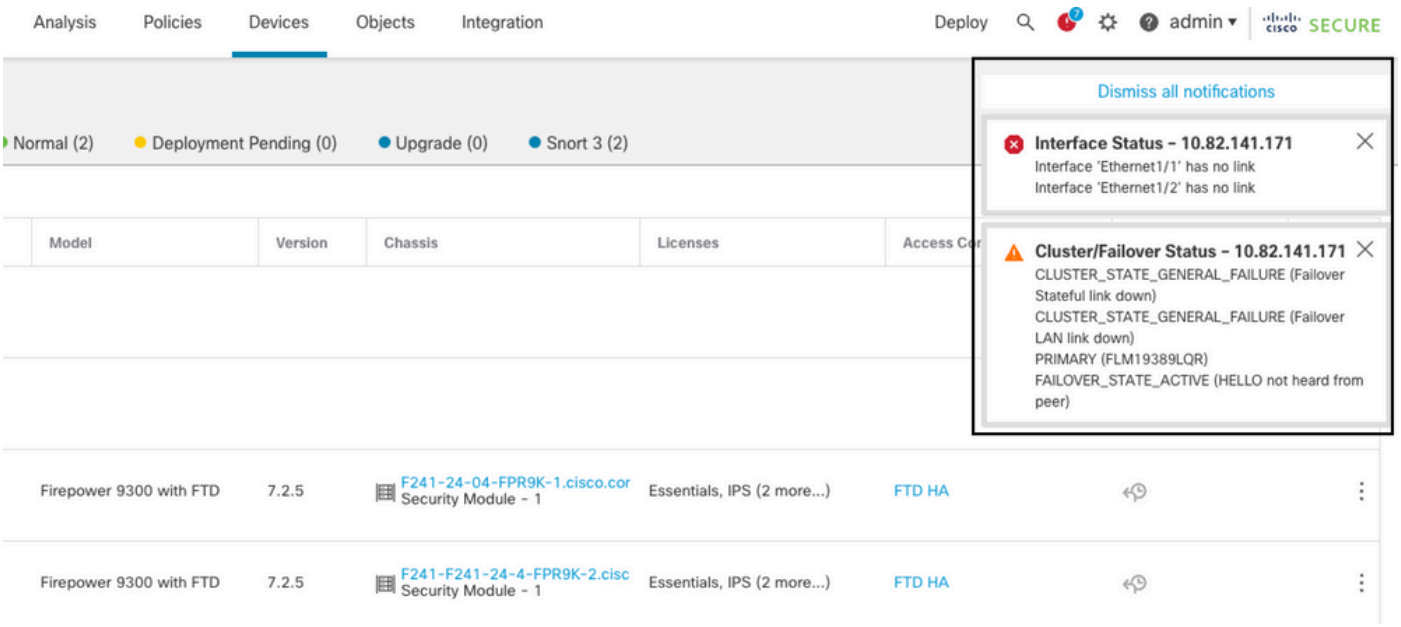
```
<#root>

For snort3:
root@firepower#

cd /ngfw/var/log/crashinfo/


root@firepower:/ngfw/var/log/crashinfo#

ls -l


total 4
-rw-r--r-- 1 root root 1052 Sep 27 17:37 snort3-crashinfo.1695836265.851283

For snort2:
root@firepower#

cd/var/data/cores


root@firepower:/var/data/cores#

ls -al

total 256912
-rw-r--r-- 1 root root  46087443 Apr  9 13:04 core.snort.24638.1586437471.gz
```

Im Fall von Snort Traceback wird dringend empfohlen, die Fehlerbehebungsdateien zu sammeln, die Core-Dateien zu exportieren und sich an das Cisco TAC zu wenden.

Anwendungsfall: Hardware- oder Stromausfall

Das FTD-Gerät ermittelt den Zustand des anderen Geräts, indem es die Failover-Verbindung mit Hello-Meldungen überwacht. Wenn ein Gerät nicht drei aufeinander folgende Hello-Meldungen über die Failover-Verbindung empfängt und die Tests an den überwachten Schnittstellen fehlschlagen, kann ein Failover-Ereignis ausgelöst werden.

Dieses Bild beschreibt die Warnungen, die bei einem Stromausfall ausgegeben werden:



Failover mit Stromausfall

Um Überprüfen Sie den Grund für den Fehler. Verwenden Sie hierzu die folgenden Befehle:

- show failover history - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderung an.

<#root>

```
firepower#

show failover history


==========================================================================
From State                     To State                   Reason
==========================================================================
22:14:42 UTC Sep 26 2023
Standby Ready                  Just Active                HELLO not heard from peer
                                                          (failover link down)
22:14:42 UTC Sep 26 2023
Just Active                    Active Drain               HELLO not heard from peer
                                                          (failover link down
22:14:42 UTC Sep 26 2023
Active Drain                   Active Applying Config     HELLO not heard from peer
                                                          (failover link down
22:14:42 UTC Sep 26 2023
Active Applying Config         Active Config Applied      HELLO not heard from peer
                                                          (failover link down)
22:14:42 UTC Sep 26 2023
Active Config Applied          Active                     HELLO not heard from peer
                                                          (failover link down)
```

- show failover state - Dieser Befehl zeigt den Failover-Status beider Einheiten und den letzten gemeldeten Grund für das Failover an.

<#root>

```
firepower#
```

show failover state

```
              State                Last Failure Reason     Date/Time
This host  -   Primary
               Active              None
Other host -   Secondary
               Failed              Comm Failure            22:14:42 UTC Sep 26 2023
```

Anwendungsfall - MIO-Hearbeat-Fehler (Hardwaregeräte)

Die Anwendungsinstanz sendet regelmäßig Heartbeats an den Supervisor. Wenn die Heartbeat-Antworten nicht empfangen werden, kann ein Failover-Ereignis ausgelöst werden.

Um Überprüfen Sie den Grund für den Fehler. Verwenden Sie hierzu die folgenden Befehle:

- show failover history - Zeigt den Failover-Verlauf an. Der Failover-Verlauf zeigt vergangene Failover-Zustandsänderungen und den Grund für die Zustandsänderung an.

<#root>

```
firepower#
```

show failover history

```
==========================================================================
From State                     To State               Reason
==========================================================================
02:35:08 UTC Sep 26 2023
Active                         Failed                 MIO-blade heartbeat failure

02:35:12 UTC Sep 26 2023
Failed                         Negotiation            MIO-blade heartbeat recovered
.
.
.
02:37:02 UTC Sep 26 2023
Sync File                      System Bulk Sync       Detected an Active mate

02:37:14 UTC Sep 26 2023
Bulk Sync                      Standby Ready          Detected an Active mate
```

Wenn MIO-hearbeat ausfällt, wird dringend empfohlen, die Fehlerbehebungsdateien zu sammeln, technische Protokolle von FXOS anzuzeigen und sich an Cisco TAC zu wenden.

Sammeln Sie für die Firepower 4100/9300 das Chassis für den technischen Support und das Modul für den technischen Support.

Für FPR1000/2100 und Secure Firewall 3100/4200, sammeln Sie das Formular show tech-support.

Zugehörige Informationen

- Hohe Verfügbarkeit für FTD
- Konfigurieren von FTD-Hochverfügbarkeit auf Firepower-Appliances
- Fehlerbehebung bei FirePOWER-Verfahren zur Dateigenerierung
- Video - So generieren Sie Show Tech-Support-Dateien auf FXOS
- Technischer Support und Dokumentation für Cisco Systeme

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.