Fehlerbehebung bei Problemen mit hoher Verfügbarkeit von Firepower Threat Defense

Inhalt

Einleitung

In diesem Dokument werden der Betrieb, die Verifizierung und die Fehlerbehebung für Hochverfügbarkeit (HA) in Firepower Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- FTD- und ASA-Plattformen
- Paketerfassung auf FTD-Appliances

Es wird dringend empfohlen, den Firepower-Konfigurationsleitfaden Configure FTD High Availability on Firepower Appliances zu lesen, um die in diesem Dokument beschriebenen Konzepte besser zu verstehen.

Verwendete Komponenten

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

- FTD von Cisco
- Cisco FirePOWER Management Center (FMC)

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

Die Informationen und Beispiele basieren auf FTD, die meisten Konzepte sind jedoch auch vollständig auf die Adaptive Security Appliance (ASA) anwendbar.

Ein FTD unterstützt zwei Hauptverwaltungsmodi:

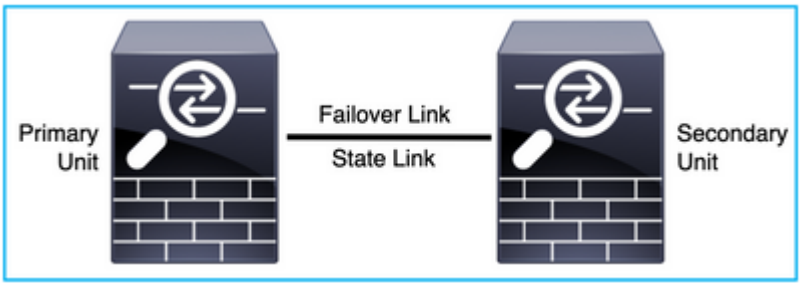
- Offbox über FMC - auch bekannt als Remote-Management
- On-Box über FirePOWER Device Manager (FDM) - auch bekannt als lokales Management

---

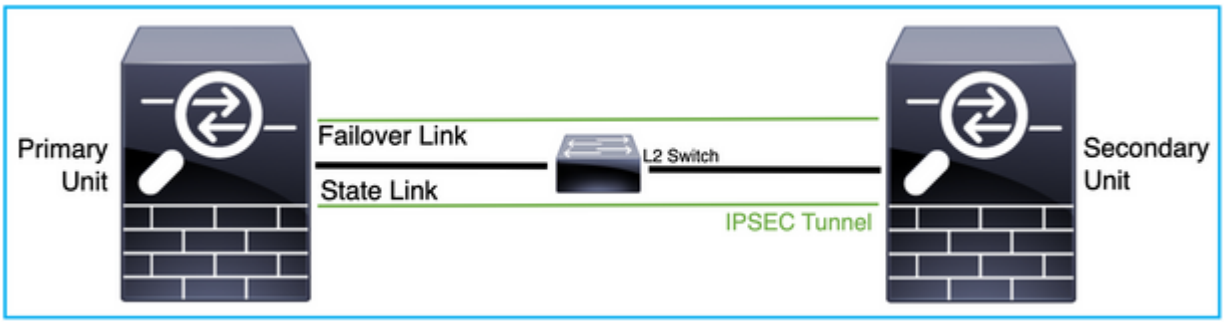
Hinweis: FTD, die über FDM verwaltet wird, kann in Hochverfügbarkeit ab Firepower Version 6.3.0 hinzugefügt werden.

Designoptionen

Aus der Sicht des Designs des FTD kann es direkt angeschlossen werden, wie in diesem Bild gezeigt:



Die Verbindung kann auch über einen Layer-2-Switch (L2) hergestellt werden, wie in der folgenden Abbildung gezeigt:



HA-Terminologie

Aktiv	Die aktive ASA empfängt alle Datenflüsse und filtert den gesamten Netzwerkverkehr. Die Konfigurationsänderungen werden auf der aktiven ASA vorgenommen.
HA-Link	Die beiden Geräte in einem Failover-Paar kommunizieren ständig über eine Failover-Verbindung, um den Betriebsstatus der einzelnen Geräte zu ermitteln und Konfigurationsänderungen zu synchronisieren. Die über den Link geteilten Informationen sind: • Der Gerätestatus (aktiv oder Standby) • Begrüßungsmeldungen (keep-alive) • Status der Netzwerkverbindung • MAC-Adressenaustausch • Konfigurationsreplikation und -synchronisierung
Primary	Dies ist die Einheit, die normalerweise zuerst konfiguriert wird, wenn Sie eine hohe Verfügbarkeit erstellen. Dies bedeutet, dass das primäre System die aktive Rolle übernimmt, wenn beide Geräte einer ASA HA zum selben Zeitpunkt zusammenkommen.
Sekundär	Dies ist die Einheit, die normalerweise an zweiter Stelle konfiguriert wird, wenn Sie eine hohe Verfügbarkeit erstellen. Dies bedeutet, dass das sekundäre Gerät die Standby-Funktion übernimmt, wenn beide Geräte einer ASA HA genau zum gleichen Zeitpunkt zusammenkommen.
Standby	Die Standby-ASA verarbeitet keinen Live-Datenverkehr, sie synchronisiert die Verbindungen und die Konfiguration vom aktiven Gerät und übernimmt die aktive Rolle bei einem Failover.
Zustandsverknüpfung	Die aktive Einheit gibt über die Statusverbindung Informationen zum Verbindungsstatus an das Standby-Gerät weiter. Daher kann das Standby-Gerät bestimmte Verbindungstypen verwalten und hat keine Auswirkungen auf Sie. Diese Informationen helfen dem Standby-Gerät, die Verbindungen aufrechtzuerhalten, die bei einem Failover vorhanden sind. Hinweis: Wenn Sie denselben Link für Failover und Stateful Failover verwenden, sparen Sie

	Schnittstellen am besten. Bei umfangreichen Konfigurationen und Netzwerken mit hohem Datenverkehrsaufkommen muss jedoch eine dedizierte Schnittstelle für die Status- und Failover-Verbindung in Betracht gezogen werden. Wir empfehlen, dass die Bandbreite der Stateful Failover-Verbindung mit der größten Bandbreite der Datenschnittstellen auf dem Gerät übereinstimmt.

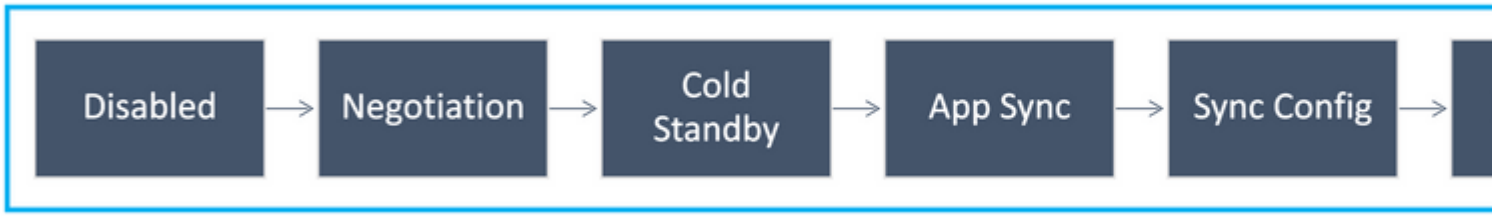
Hochverfügbarkeitsstatus

Aktiv	Das Gerät verarbeitet derzeit den Live-Datenverkehr im Netzwerk, und alle erforderlichen Konfigurationsänderungen müssen auf diesem Gerät durchgeführt werden.
App-Synchronisierung	Das Gerät in diesem Zustand synchronisiert die Konfiguration des aktiven Geräts.
Massensynchronisierung	Das Gerät in diesem Zustand synchronisiert die Konfiguration des aktiven Geräts.
Deaktiviert	Der Failover auf der Einheit wurde deaktiviert (Befehl: no failover).
Verhandlung	Das Gerät überprüft die Verfügbarkeit des aktiven Geräts und übernimmt die aktive Rolle, wenn das aktive Gerät nicht als einsatzbereit erkannt wird.
Standby-fähig	Das Gerät verarbeitet derzeit keinen Datenverkehr, übernimmt jedoch die aktive Rolle, wenn beim aktiven Gerät Probleme mit der Integritätsprüfung auftreten.
Konfiguration synchronisieren	Die Konfiguration wird vom aktiven Gerät auf das Standby-Gerät repliziert.
Cold Standby	Das Gerät übernimmt bei Failover die Funktion aktiv, repliziert jedoch keine Verbindungsereignisse.

HA-Zustandsflussdiagramm

Primär (ohne verbundenen Peer):

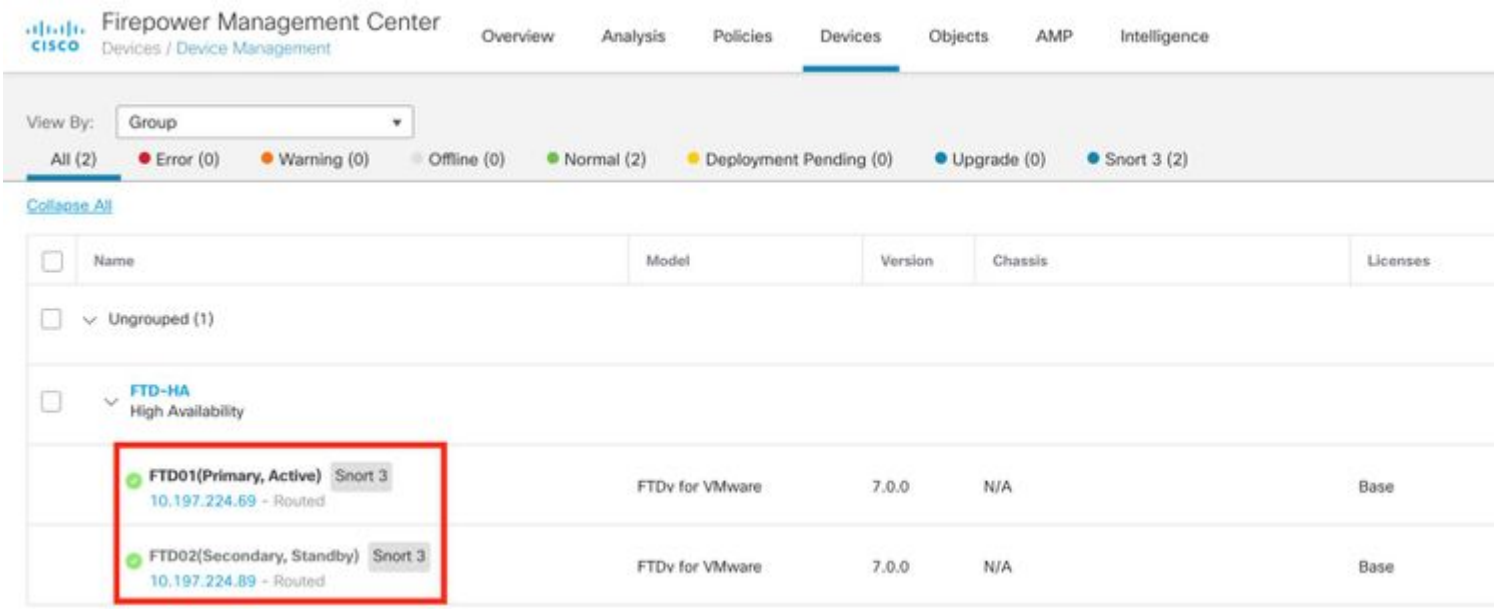
Sekundär (mit einem aktiven verbundenen Peer):



Überprüfung der Benutzeroberfläche

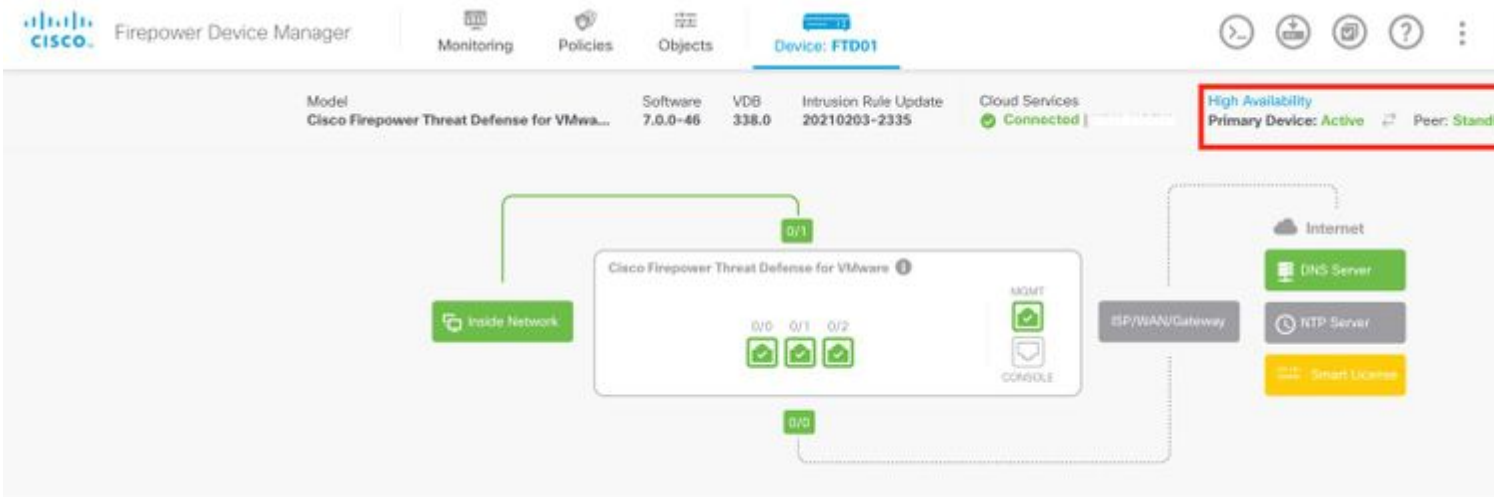
FirePOWER Management Center Managed FTD HA

Der FTD HA-Status kann über die FMC-Benutzeroberfläche überprüft werden, wenn Sie zu **Gerät > Gerätemanagement** navigieren, wie in diesem Bild gezeigt:



FDM-verwaltete FTD HA

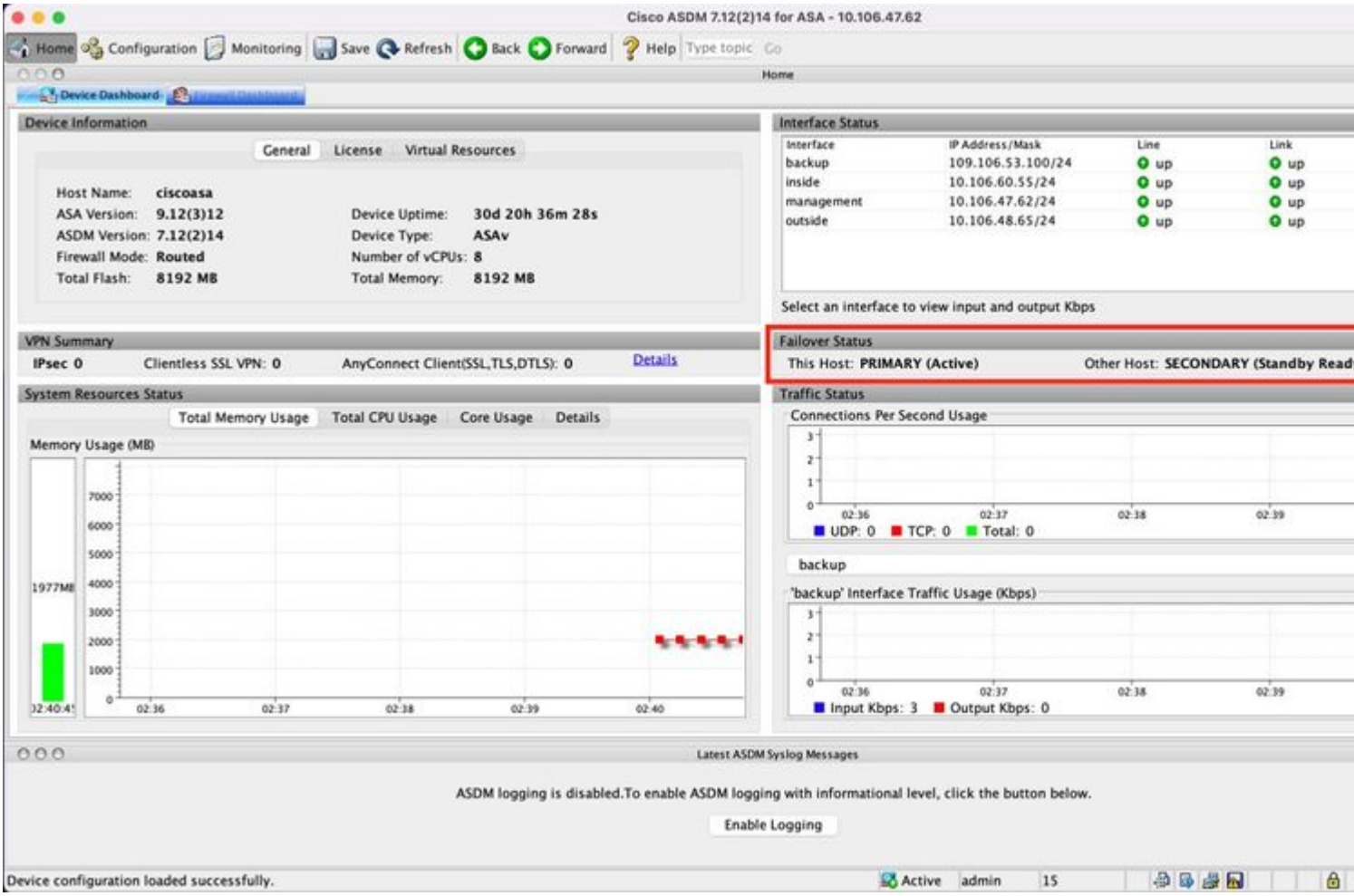
Seite "Primary FDM Overview":



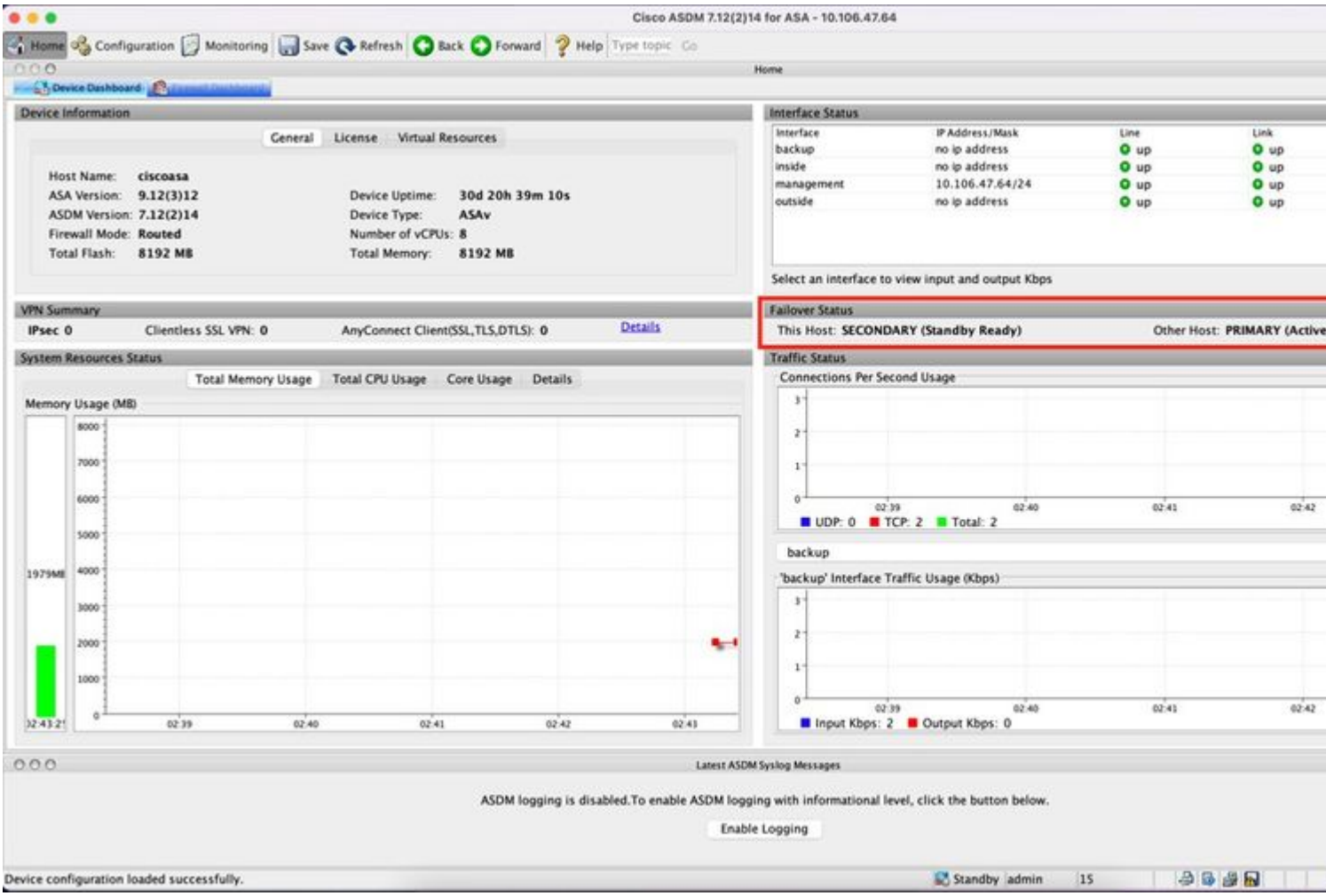
Seite "Secondary FDM Overview":

ASDM-verwaltete ASA HA

ASDM-Startseite zur primären ASA:

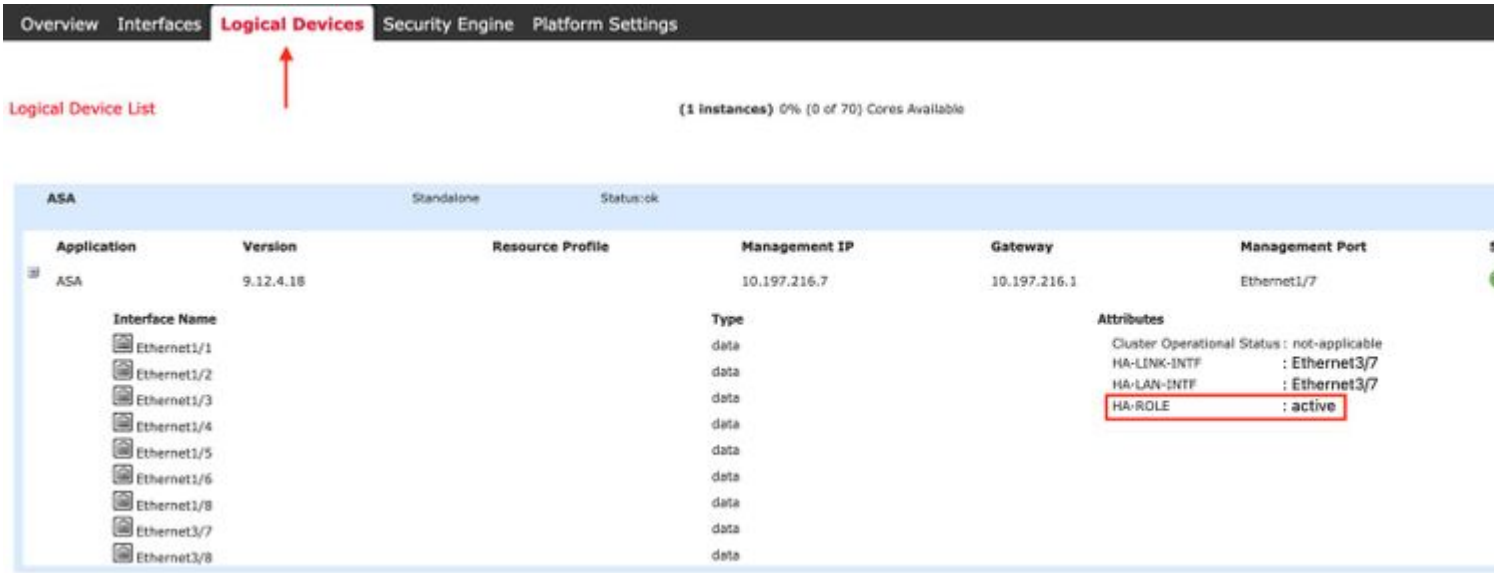


ASDM-Startseite zur sekundären ASA:

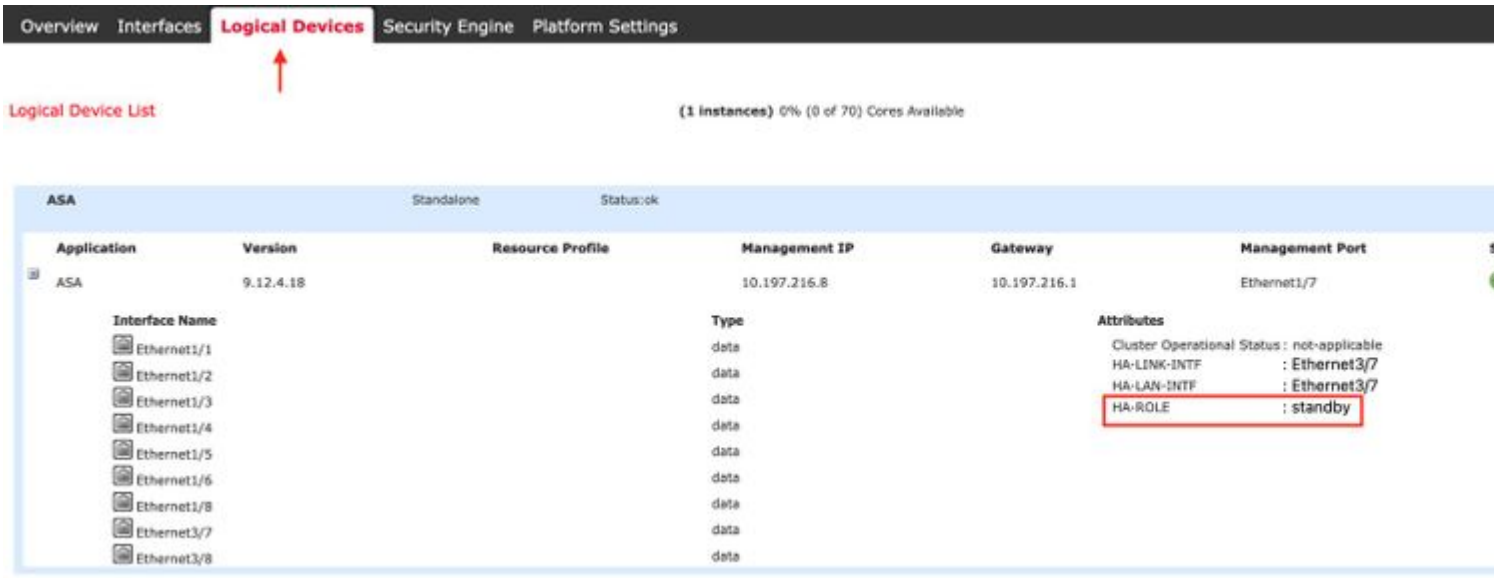


Firepower Chassis Manager für 4100/9300 mit FTD/ASA HA

Seite "Logisches FCM-Gerät":



Seite "Sekundäres logisches FCM-Gerät":



CLI überprüfen

<#root>

>

show running-config failover

```
failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

Dabei sind folgende Punkte zu beachten:

Failover
Failover-LAN-Einheit sekundär â€”> ob es sich um eine primäre oder sekundäre Einheit handelt
Failover LAN-Schnittstelle Failover-Link GigabitEthernet0/2 â€”> physische Schnittstelle der Failover-Verbindung auf dem Gerät
Failover-Replikation http
Failover-Verbindung Failover-Link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 â€”> primäre und die IP-Adressen der Standby-Device-Failover-Verbindung.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
```

```
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.2): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)
    Other host: Primary - Active
        Active time: 707216 (sec)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.1): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
    Link : failover-link GigabitEthernet0/2 (up)
    Stateful Obj        xmit       xerr          rcv          rerr
    General             95752       0           115789          0
    sys cmd             95752       0            95752          0
    up time               0         0              0            0
    RPC services          0         0              0            0
    TCP conn              0         0              0            0
    UDP conn              0         0              0            0
    ARP tbl               0         0            20036          0
    Xlate_Timeout         0         0              0            0
    IPv6 ND tbl           0         0              0            0
    VPN IKEv1 SA          0         0              0            0
    VPN IKEv1 P2          0         0              0            0
    VPN IKEv2 SA          0         0              0            0
    VPN IKEv2 P2          0         0              0            0
    VPN CTCP upd          0         0              0            0
    VPN SDI upd           0         0              0            0
    VPN DHCP upd          0         0              0            0
    SIP Session           0         0              0            0
    SIP Tx                0         0              0            0
    SIP Pinhole           0         0              0            0
    Route Session         0         0              0            0
    Router ID             0         0              0            0
    User-Identity         0         0              1            0
    CTS SGTNAME           0         0              0            0
    CTS PAC               0         0              0            0
    TrustSec-SXP          0         0              0            0
    IPv6 Route            0         0              0            0
    STS Table             0         0              0            0
    Rule DB B-Sync        0         0              0            0
    Rule DB P-Sync        0         0              0            0
    Rule DB Delete        0         0              0            0

    Logical Update Queue Information
       Cur   Max    Total
```

```
Recv Q: 0     5     504656
Xmit Q: 0     1     95752
```

Failover Ein: Failover ist aktiviert oder deaktiviert.

Dieser Host: Sekundär - Standby-fähig. Die Rolle dieses Geräts und die Status der Schnittstellen.

Andere Hosts: Primär - Aktiv Das andere Gerät befindet sich in einem aktiven Zustand und kommuniziert mit dem aktuellen Gerät.

<#root>

>

show failover history

```
==========================================================================
From State                 To State                       Reason
==========================================================================
01:18:14 UTC Nov 25 2021
Not Detected               Negotiation                    No Error

01:18:27 UTC Nov 25 2021
Negotiation                Just Active                    No Active unit found

01:18:27 UTC Nov 25 2021
Just Active                Active Drain                   No Active unit found

01:18:27 UTC Nov 25 2021
Active Drain               Active Applying Config         No Active unit found

01:18:27 UTC Nov 25 2021
Active Applying Config     Active Config Applied          No Active unit found

01:18:27 UTC Nov 25 2021
Active Config Applied         Active                      No Active unit found
==========================================================================
```

Verwenden Sie diese Option, um den historischen Status der Geräte und die Gründe für diese Statusänderungen zu überprüfen:

<#root>

>

show failover state

```
             State              Last Failure Reason      Date/Time
This host -  Secondary
             Standby Ready          None
Other host - Primary
             Active                 None
```

```
====Configuration State===
    Sync Done - STANDBY
====Communication State===
    Mac set
```

Überprüfen Sie den aktuellen Status der Geräte und den Grund für das letzte Failover:

Feld	Beschreibung
Konfigurationsstatus	Zeigt den Status der Konfigurationssynchronisierung an. Mögliche Konfigurationszustände für das Standby-Gerät: • Config Syncing - STANDBY - Wird während der Ausführung der synchronisierten Konfiguration festgelegt. • Synchronisierung der Schnittstellenkonfiguration - STANDBY • Sync Done - STANDBY - Diese Einstellung wird aktiviert, wenn die Standby-Einheit eine Konfigurations-Synchronisierung von der aktiven Einheit abgeschlossen hat. Mögliche Konfigurationszustände für die aktive Einheit: • Config Syncing (Konfigurationssynchronisierung): Diese Einstellung wird auf dem aktiven Gerät festgelegt, wenn eine Konfigurations-Synchronisierung mit dem Standby-Gerät durchgeführt wird. • Synchronisierung der Schnittstellenkonfiguration • Sync Done (Synchronisierung abgeschlossen): Dieser Parameter legt fest, wann die Konfiguration des aktiven Geräts erfolgreich mit dem Standby-Gerät synchronisiert wurde. • Ready for Config Sync (Bereit für Konfigurations-Synchronisierung): Wird auf dem aktiven Gerät festgelegt, wenn das Standby-Gerät signalisiert, dass es für eine Konfigurations-Synchronisierung bereit ist.
Kommunikationsstatus	Zeigt den Status der Synchronisierung der MAC-Adressen an. • MAC-Satz - Die MAC-Adressen wurden von der Peer-Einheit mit dieser Einheit synchronisiert. • Aktualisierter Mac - Wird verwendet, wenn eine MAC-Adresse aktualisiert wird und mit der anderen Einheit synchronisiert werden muss. Wird auch zum Zeitpunkt des Übergangs verwendet, wenn die Einheit die von der Peer-Einheit synchronisierten lokalen MAC-Adressen aktualisiert.
Datum/Uhrzeit	Zeigt ein Datum und einen Zeitstempel für den Fehler an.

Feld	Beschreibung
Grund für letzten Fehler	Zeigt den Grund für den zuletzt gemeldeten Fehler an. Diese Informationen werden nicht gelöscht, selbst wenn die Fehlerbedingung behoben ist. Diese Informationen ändern sich nur, wenn ein Failover auftritt. Mögliche Fehlerursachen: • Schnittstellenfehler - Die Anzahl der fehlerhaften Schnittstellen erfüllte die Failover-Kriterien und verursachte ein Failover. • Kommunikationsfehler - Die Failover-Verbindung ist fehlgeschlagen oder der Peer ist ausgefallen. • Fehler bei Rückwandplatine
Status	Zeigt den Status Primär/Sekundär und Aktiv/Standby für das Gerät an.
Dieser Host/andere Hosts	Dieser Host gibt Informationen zu dem Gerät an, auf dem der Befehl ausgeführt wurde. Ein anderer Host gibt Informationen für das andere Gerät im Failover-Paar an.

<#root>

>

show failover descriptor

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

Fehlerbehebung

Fehlerbehebung

<#root>

>

debug fover ?

```
cable         Failover LAN status
cmd-exec      Failover EXEC command execution
fail          Failover internal exception
fmsg          Failover message
ifc           Network interface status trace
open          Failover device open
```

```
rx            Failover Message receive
rxdmp         Failover recv message dump (serial console only)
rxip          IP network failover packet recv
snort         Failover NGFW mode snort processing
switch        Failover Switching status
sync          Failover config/command replication
tx            Failover Message xmit
txdmp         Failover xmit message dump (serial console only)
txip          IP network failover packet xmit
verify        Failover message verify
```

Aufnahmen:

Failover-Schnittstellenerfassung:

Anhand dieser Erfassung können Sie bestimmen, ob die Failover-Hello-Pakete mit der Geschwindigkeit, mit der sie gesendet werden, über die Failover-Verbindung gesendet werden.

<#root>

>

show capture

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
>
```

show capture capfail

```
15 packets captured

1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

ARP-Erfassung auf der Failover-Verbindung:

Sie können diese Aufzeichnung verwenden, um zu sehen, ob die Peers Mac-Einträge in der ARP-Tabelle haben.

```
<#root>

>

show capture


capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
>

show capture caparp



22 packets captured

1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

Szenarien

Wenn die Peer-Einheit der HA-Gruppe nicht beitritt oder während der Bereitstellung von Änderungen an der aktiven Einheit fehlschlägt, melden Sie sich bei der fehlerhaften Einheit an, navigieren Sie zur Seite für hohe Verfügbarkeit, und klicken Sie auf den Link Failover History.

APP-SYNC-Fehler

Wenn die Ausgabe von show failover history einen Fehler bei der App-Synchronisierung anzeigt, gab es zum Zeitpunkt der HA-Validierungsphase ein Problem, bei dem das System überprüft, ob die Geräte als Hochverfügbarkeitsgruppe richtig funktionieren.

Die Meldung "Alle Validierungen bestanden" wird angezeigt, wenn der Absenderstatus "App Sync" lautet und der Knoten in den Status "Standby Ready" wechselt.

Bei einem Validierungsfehler wird der Peer in den Status "Deaktiviert" (Fehler) versetzt. Beheben Sie die Probleme, damit die Peers wieder als Hochverfügbarkeitsgruppe fungieren.

Beachten Sie, dass Sie, wenn Sie einen App-Synchronisierungsfehler beheben und Änderungen an der aktiven Einheit vornehmen, diese bereitstellen und anschließend die hohe Verfügbarkeit wieder herstellen müssen, damit der Peer-Knoten beitreten kann.

Die Meldungen zeigen Fehler an und erläutern, wie Sie die Probleme beheben können. Diese Fehler können beim Beitritt zu einem Knoten und bei jeder nachfolgenden Bereitstellung auftreten.

Beim Knotenbeitritt führt das System eine Prüfung mit der zuletzt bereitgestellten Konfiguration auf der aktiven Einheit durch.

Standby-Knoten kann nicht in HA integriert werden: "CD-App-Synchronisierungsfehler: Anwendung der App-Konfiguration fehlgeschlagen"

In der Standby-FTD-Befehlszeile muss **/ngfw/var/log/action_queue.log** den Grund für einen Konfigurationsfehler haben.
Behebung: Nach Erkennen des Konfigurationsfehlers und Vornehmen erforderlicher Änderungen kann die hohe Verfügbarkeit wieder hergestellt werden.
Siehe Cisco Bug IDCSCvu15611.

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
15:10:16 CDT Sep 28 2021
Not Detected                Disabled                    No Error
15:10:18 CDT Sep 28 2021
Disabled                    Negotiation                 Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation                 Cold Standby                Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby                App Sync                    Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync                    Disabled
```

CD App Sync error is App Config Apply Failed

```
================================================================================
```

Standby-Knoten kann HA nicht beitreten mit "HA-Statusfortschritt aufgrund APP SYNC-Timeout fehlgeschlagen"

In der Standby FTD-Befehlszeile muss **/ngfw/var/log/ngfwmanager.log** den Grund für die App-Sync-Zeitüberschreitung haben.
In dieser Phase schlagen auch die Richtlinienbereitstellungen fehl, da die aktive Einheit glaubt, dass die App-Synchronisierung noch läuft.
Die Richtlinienbereitstellung gibt den Fehler aus: "Da der Prozess newNode join/AppSync ausgeführt wird, sind Konfigurationsänderungen nicht zulässig, und die Bereitstellungsanforderung wird daher zurückgewiesen. Versuchen Sie die Bereitstellung später erneut."

Problembehebung: Wenn Sie die hohe Verfügbarkeit auf dem Standby-Knoten wiederherstellen, kann das Problem in manchen Fällen behoben werden.
Siehe Cisco Bug-ID CSCvt48941
Siehe Cisco Bug-ID CSCvx11636

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
19:07:01 EST MAY 31 2021
Not Detected               Disabled                    No Error
19:07:04 EST MAY 31 2021
Disabled                   Negotiation                 Set by the config command
19:07:06 EST MAY 31 2021
Negotiation                Cold Standby                Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby               App Sync                    Detected an Active mate
21:11:18 EST Jun 30 2021
App Sync                   Disabled

HA state progression failed due to APP SYNC timeout

================================================================================
```

Der Standby-Knoten kann nicht zur HA-Sitzung hinzugefügt werden: Fehler bei der Synchronisierung der CD-Anwendung beim Anwenden der SSP-Konfiguration auf den Standby-Modus.

In der Standby FTD-Befehlszeile muss **/ngfw/var/log/ngfwmanager.log** den genauen Grund für den Fehler angeben.

Problembehebung: Wenn Sie die hohe Verfügbarkeit auf dem Standby-Knoten wiederherstellen, kann das Problem in manchen Fällen behoben werden.

Siehe Cisco Bug-ID CSCvy04965

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
04:15:15 UTC Apr 17 2021
Not Detected               Disabled                    No Error
04:15:24 UTC Apr 17 2021
Disabled                   Negotiation                 Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation                Cold Standby                Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby               App Sync                    Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync                   Disabled

CD App Sync error is Failed to apply SSP config on standby
```

```
==========================================================================
```

Integritätsprüfung fehlgeschlagen

"HELLO not heard from mate" (HELLO wird nicht von MATE empfangen) bedeutet, dass der MATE offline ist oder dass die Failover-Verbindung die HELLO-Keepalive-Nachrichten nicht übermittelt.

Versuchen Sie, sich beim anderen Gerät anzumelden. Wenn SSH nicht funktioniert, rufen Sie den Konsolenzugriff auf, und überprüfen Sie, ob das Gerät betriebsbereit oder offline ist.

Wenn der Befehl betriebsbereit ist, ermitteln Sie mit dem Befehl die Ursache des Fehlers, und **zeigen Sie den Failover-Status an.**

Wenn das Gerät nicht funktioniert, starten Sie es neu und überprüfen Sie, ob auf der Konsole Bootprotokolle angezeigt werden. Andernfalls kann das Gerät als Hardware fehlerhaft angesehen werden.

<#root>

```
==========================================================================
From State                To State                  Reason
==========================================================================
04:53:36 UTC Feb 6 2021
Failed                    Standby Ready
```

Interface check

```
02:12:46 UTC Jul 11 2021
Standby Ready             Just Active               HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied     Active                    HELLO not heard from mate
==========================================================================
```

Snort-Down oder Datenträgerfehler

Wenn die FTD diesen Fehler "Detect Inspection Engine Failure due to disk Failure" (Erkennt einen Ausfall der Inspektionsmaschine aufgrund eines Festplattenausfalls) meldet, gibt es zwei Möglichkeiten.

Die Erkennungs-Engine (SNORT-Instanz) ist ausgefallen.

Dies kann mithilfe des Linux-Befehls **pmtool status** validiert werden. **| grep -i de,**

Problembehebung: Wenn eine der Instanzen ausgefallen ist, suchen Sie nach /ngfw/**var/log/messages,** und identifizieren Sie die Ursache.

Das Gerät weist eine hohe Festplattenauslastung auf.

Dies kann mit dem Linux-Befehl **df -Th** validiert werden.

Problembehebung: Identifizieren Sie das Verzeichnis, das den Großteil der Festplatte beansprucht, und wenden Sie sich an das TAC, um die unerwünschten Dateien zu löschen.

<#root>

```
================================================================================
From State                 To State                   Reason
================================================================================
Active Config Applied      Active                     No Active unit found
16:07:18 UTC Dec 5 2020
Active                     Standby Ready              Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready              Failed
```

Detect Inspection engine failure due to disk failure

```
16:07:29 UTC Dec 5 2020
Failed                     Standby Ready              My Inspection engine is as good as peer due to dis
================================================================================
```

Ausfall der Servicekarte

Derartige Probleme werden im Allgemeinen aufgrund eines FirePOWER-Modulausfalls auf ASA 5500-X-Geräten gemeldet. Bitte überprüfen Sie die Plausibilität des Moduls über **show module sfr details**.

Problembehebung: Sammeln Sie ASA Syslog etwa zum Zeitpunkt des Ausfalls, und diese können Details wie einen Ausfall auf Kontroll- oder Datenebene enthalten.

Dies kann auf verschiedene Gründe im SFR-Modul zurückzuführen sein. Es wird empfohlen, das TAC zu öffnen, um die Ursache dieses Problems auf dem IPS zu finden.

<#root>

```
================================================================================
From State                 To State                   Reason
================================================================================
21:48:19 CDT Aug 1 2021
Active                     Standby Ready              Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready              Just Active
```

Service card in other unit has failed

```
21:48:19 CDT Aug 1 2021
Active Config Applied      Active                     Service card in other unit has failed
================================================================================
```

MIO-Heartbeat-Fehler

FirePOWER Threat Defense/ASA meldet einen Fehler aufgrund eines "MIO-Blade-Heartbeat-Fehlers" bei FPR1.000, 2.000, 4.000, 9.000.

Siehe Cisco Bug-ID CSCvy14484
Siehe Cisco Bug-ID CSCvh26447

<#root>

```
================================================================================
From State                 To State                   Reason
================================================================================
20:14:45 EDT Apr 14 2021
Active Config Applied      Active                     No Active unit found
20:15:18 EDT Apr 14 2021
Active                     Failed
```

MIO-blade heartbeat failure

```
20:15:19 EDT Apr 14 2021
Failed                     Negotiation                MIO-blade heartbeat recovered
================================================================================
```

Zugehörige Informationen

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185
- **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.