Fehlerbehebung bei Split-Brain-Problemen mit ASA-Failover

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Was ist Split-Brain?](#)
[Proaktive Vorbereitung auf Failover-Probleme](#)
[Mögliche Gründe für Split-Brain](#)
[Verfahren zur Fehlerbehebung - Flussdiagramm](#)
[Notfallwiederherstellung von Split-Brain](#)
[Daten für das TAC freigeben](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie häufige Probleme im Split-Brain-Bereich beheben können, die bei Cisco Adaptive Security Appliance (ASA) Failover oder FirePOWER Threat Defense (FTD) High Availability (HA) Pairs auftreten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie wissen, wie ASA/FTD High Availability Pair (Failover) funktioniert - Informationen zum Failover.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen beschränkt und gilt für alle unterstützten ASA/FTD-Bereitstellungen in Failover.

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 potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Was ist Split-Brain?

Split-Brain ist ein Szenario, in dem die Einheiten einer ASA/FTD HA einander im Netzwerk nicht erkennen können und daher beide die aktive Rolle übernehmen. Dies führt dazu, dass beide Einheiten dieselbe IP-Adresse und MAC-Adresse für die Schnittstelle haben, und kann zu schwerwiegenden Inkonsistenzen im Netzwerk führen, die zu Service-Verlusten führen.

Um festzustellen, ob sich Ihr HA im Split-Hirn befindet, führen Sie den Befehl **show failover state** auf beiden Geräten aus, und überprüfen Sie, ob beide Kästchen aktiv sind.

Ein Beispiel für ein Split-Gehirn:

Primäre Einheit:

```
ciscoasa1/act/pri# show failover state

State Last Failure Reason Date/Time
This host - Primary
 Active None
Other host - Secondary
Failed Comm Failure 02:39:43 UTC Jan 10 2022

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

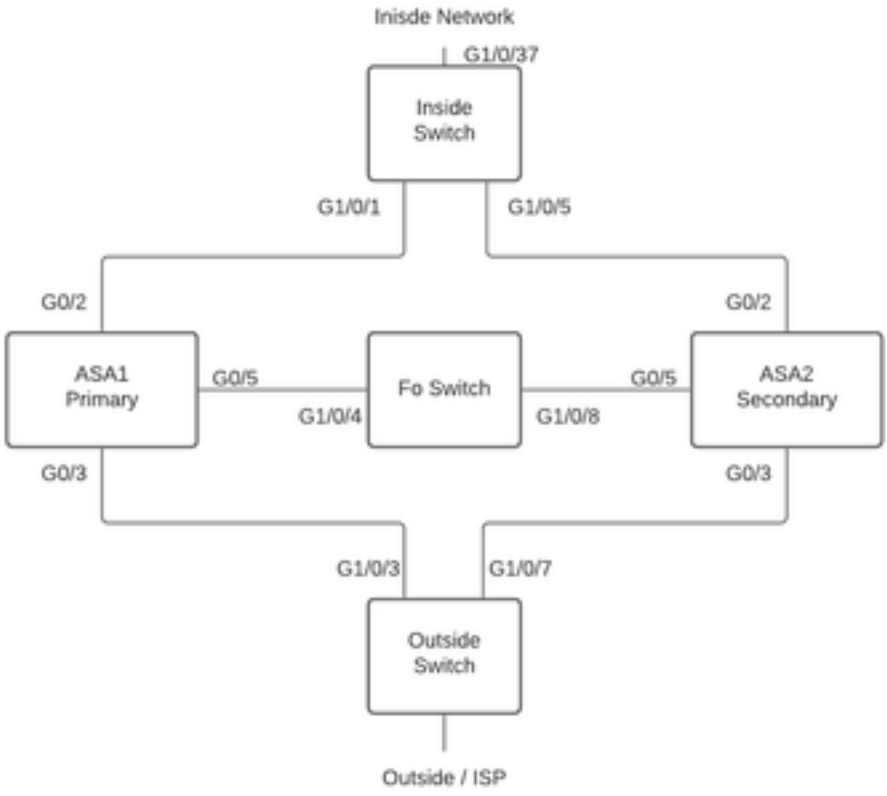
Sekundäreinheit:

```
ciscoasa2/act/sec# show failover state

State Last Failure Reason Date/Time
This host - Secondary
 Active None
Other host - Primary
Failed Comm Failure 02:39:40 UTC Jan 10 2022

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

Split-Hirn kann einen Ausfall verursachen, wenn die MAC-Adresse, die für die aktiven IP-Adressen auf den angeschlossenen Geräten empfangen wurde, nicht alle derselben Einheiten sind. Betrachten Sie beispielsweise die Netzwerktopologie:



Labortopologie

VMACs wurden der Schnittstelle wie folgt zugewiesen, um die **MAC-Adresstabelle** leicht verständlich zu machen:

```
Inside (G0/2)    : Active MAC    - 00c1.1000.aaaa
                         Standby MAC - 00c1.1000.bbbb

Outside (G0/4) : Active MAC    - 00c1.2000.aaaa

                         Standby MAC - 00c1.2000.bbbb
```

> **Hinweis:** Wenn VMACs nicht konfiguriert sind, muss das aktive Gerät stets die MAC-Adresse für die Schnittstelle der primären Einheit verwenden, und der Standby-Modus übernimmt die sekundäre MAC-Adresse.

MAC-Adresstabelle auf dem Switch bei guter HA-Einstellung:

```
Switch#show mac address-table

Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
100 00c1.1000.aaaa DYNAMIC Gi1/0/5
100 00c1.1000.bbbb DYNAMIC Gi1/0/1
300 00c1.64bc.c508 DYNAMIC Gi1/0/4
300 00d7.8f38.8424 DYNAMIC Gi1/0/8
200 00c1.2000.aaaa DYNAMIC Gi1/0/7
200 00c1.2000.bbbb DYNAMIC Gi1/0/3
```

Wenn die Failover-Verbindung ausfällt, bleibt die aktive Einheit aktiv, und der Standby-Modus bleibt erhalten. Wenn eine Einheit nicht drei aufeinander folgende HELLO-Meldungen auf der Failover-Verbindung empfängt, sendet die Einheit LANTEST-Nachrichten auf jeder Datenschnittstelle, einschließlich der Failover-Verbindung, um zu überprüfen, ob der Peer reagiert oder nicht. Die von der ASA ergriffenen Maßnahmen hängen von der Reaktion der anderen Einheit ab.

Mögliche Maßnahmen sind:

- Wenn die ASA eine Antwort auf die Failover-Verbindung erhält, erfolgt kein Failover.
- Wenn die ASA keine Antwort auf die Failover-Verbindung erhält, aber eine Antwort auf eine Datenschnittstelle erhält, führt das Gerät keinen Failover aus. Die Failover-Verbindung ist als ausgefallen gekennzeichnet. Sie sollten die Failover-Verbindung so bald wie möglich wiederherstellen, da das Gerät bei Ausfall der Failover-Verbindung nicht auf den Standby-Modus umschalten kann.
- Wenn die ASA auf keiner Schnittstelle eine Antwort erhält, wechselt die Standby-Einheit in den aktiven Modus und klassifiziert die andere Einheit als ausgefallen. Dies führt zu einem Split-Hirn-Szenario.

In dieser Phase werden alle Datenschnittstellen auf beiden Firewalls so funktionieren, als wären sie die aktive Einheit. Daher verwenden die Schnittstellen der aktiven und Standby-Firewall dieselbe IP- und MAC-Adresse. Dies führt zu einer inkonsistenten MAC-Adresstabelle aufgrund von Gift-Arp-Einträgen und führt somit zu einem Ausfall.

> **Anmerkung:** Failover Link ist für die Kommunikation dieser Daten zwischen dem Failover-Paar (Einheitenstatus (aktiv/Standby), Hello-Nachrichten, Network Link Status, MAC Address Exchange, Config Replication und Sync verantwortlich.

Proaktive Vorbereitung auf Failover-Probleme

Proaktive Vorbereitung auf einen Split-Hirn-Zustand:

- Nehmen Sie an der empfohlenen Version von Cisco Golden Release teil. Unter bestimmten Umständen kann auch Split-Brain-Aktivität aufgrund von Problemen wie Speicherlecks verursacht werden. Durch die Nutzung der von Cisco empfohlenen Versionen können Sie das Risiko solcher Situationen erheblich reduzieren.
- Netzwerktopologie - Es wird empfohlen, dass die Datenschnittstellen und die Failover-Links unterschiedliche Pfade haben, um das Risiko eines gleichzeitigen Ausfalls aller Schnittstellen zu verringern.
- Verwenden Sie eine Port-Channel-Schnittstelle für die Failover-Schnittstelle. Wenn Sie über ungenutzte Schnittstellen auf Ihrer Firewall verfügen, paaren Sie diese, um einen Port-Channel zu bilden und diesen als Failover Link zu verwenden, wird dadurch die Zuverlässigkeit der Verbindungen erhöht und ein Single Point of Failure (SPOF) entfernt.
- Vergewissern Sie sich, dass die Failover-Schnittstelle nicht zu viel Latenz aufweist. (Laut ASA-Konfigurationsleitfaden "Die Latenz für die Zustandsverbindung sollte bei Verwendung von Failover über große Entfernungen weniger als 10 Millisekunden und nicht mehr als 250 Millisekunden betragen.) Beträgt die Latenz mehr als 10 Millisekunden, kann die Leistung aufgrund der erneuten Übertragung von Failover-Nachrichten teilweise beeinträchtigt werden."

- Passen Sie die Werte für den Umfragezeitgeber/Hold Timer entsprechend Ihrer Bereitstellung an. Für Failover Timer gibt es keine Einheitsgröße. Im Allgemeinen kann ein niedriger Timer zu unnötigen Failovers führen (besonders bei einer Latenz) und zu hohe Werte können zu einer längeren Zeitspanne für ein Failover führen. Dies führt zu merklichen Failovers. Der Wert für den Hold-Timer muss der 5-fache Wert für den Abfragezeitgeber sein.
- Konfigurieren einer virtuellen MAC-Adresse für Schnittstellen - Wenn "die Sekundäreinheit startet, ohne die Primäreinheit zu erkennen, wird die Sekundäreinheit zur aktiven Einheit und verwendet ihre eigenen MAC-Adressen, da sie die MAC-Adressen der Primäreinheit nicht kennt. Sobald die Primäreinheit verfügbar ist, ändert die sekundäre (aktive) Einheit die MAC-Adressen in die Adressen der Primäreinheit, wodurch der Netzwerkverkehr unterbrochen werden kann. Wenn Sie die Primäreinheit durch neue Hardware ersetzen, wird eine neue MAC-Adresse verwendet." Virtuelle MAC-Adressen schützen vor dieser Unterbrechung, da die aktiven MAC-Adressen der Sekundäreinheit beim Start bekannt sind und im Falle der Hardware der neuen Primäreinheit unverändert bleiben. Wenn Sie keine virtuellen MAC-Adressen konfigurieren, müssen Sie möglicherweise die ARP-Tabellen der angeschlossenen Router löschen, um den Datenverkehrsfluss wiederherzustellen." Weitere Informationen finden Sie unter MAC-Adressen und IP-Adressen in Failover.
- Senden Sie ASA-/FTD-Protokolle für beide Einheiten an einen externen Syslog-Server - Dieser Schritt dient eher der Benutzerfreundlichkeit von Problemen.

Mögliche Gründe für Split-Brain

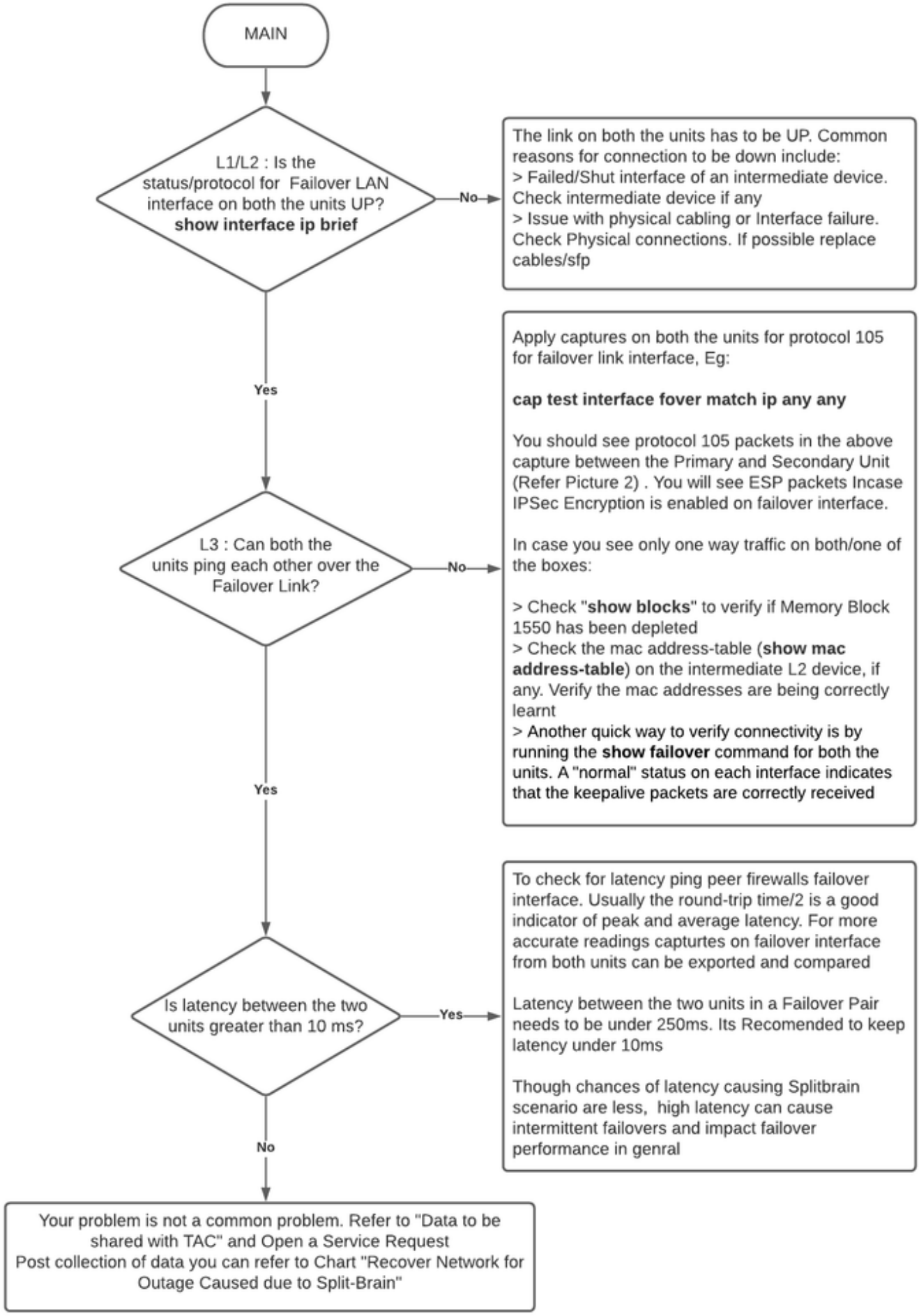
Wie bereits erwähnt, tritt Split-Brain auf, wenn die Kommunikation zwischen den Failover Link-Schnittstellen (unidirektional oder bidirektional) ausgefallen ist. Die häufigsten Gründe sind:

- L1-Probleme - fehlerhaftes Kabel/SFP/Schnittstelle
- Ein Problem mit einem zwischengeschalteten Gerät
- Mangel an Arbeitsspeicher oder CPU-Ressourcen für ASA/FTD **Hinweis:** Die ASA/Lina Engine verwendet 1550-Byte-Speicherblöcke zum Speichern von Paketen zur Verarbeitung. Wenn die Anzahl der freien Blöcke dieser Größe ihre Leistung erschöpft, kann ASA/FTD keine Failover-Pakete mehr verarbeiten. Führen Sie die **Blöcke anzeigen aus**, um die Blockerschöpfung zu überprüfen.

Verfahren zur Fehlerbehebung - Flussdiagramm

Verwenden Sie dieses Flussdiagramm, um eine Fehlerbehebung und Lösung für ein Split-Hirn-Szenario durchzuführen. Beginnen Sie mit dem Feld **Main** (**Main)**. Es gibt einige Probleme, die hier möglicherweise nicht gelöst werden können. In diesen Fällen werden Links zum technischen Support von Cisco bereitgestellt. Um eine Serviceanfrage zu öffnen, benötigen Sie einen gültigen Servicevertrag.

> **Hinweis:** In FTD-Bereitstellungen müssen die Schritte in diesem Diagramm aus der "**System Support Diagnostics-CLI**" abgeleitet werden.



Flussdiagramm zur Fehlerbehebung

Notfallwiederherstellung von Split-Brain

Um Ihr Netzwerk von einem Split-Hirn zu erholen, müssen Sie sicherstellen, dass der Datenverkehr nur auf eine der beiden Firewalls trifft, d. h. die für die aktiven IPs erhaltenen MAC-Adressen sollten alle auf eine Einheit zeigen. Dazu können Sie das Failover auf der Einheit deaktivieren oder das Netzwerk vollständig ausschalten.

1. Deaktivierung der Failover-Funktion für das Gerät, das keinen Datenverkehr weiterleitet: Navigieren Sie auf der ASA-Plattform über die CLI zum Konfigurationsterminal, und geben Sie **keinen Failover-**Befehl ein.Geben Sie auf der FTD-Plattform über den Clish-Modus den Befehl **configure high-Availability Suspend** (Hochverfügbarkeits-Suspendiermodus konfigurieren) ein.
2. Für ASA schließen Sie die Datenschnittstellen. Für FTD die Schnittstellen am angeschlossenen Gerät schließen. Alternativ können Sie die Schnittstellen auch physisch trennen. Sie können das Gerät auch ausschalten, was jedoch die Verwaltung des Geräts einschränkt. Weitere Schritte hierzu finden Sie in der Anleitung zur Gerätekonfiguration.

   Hinweis: Wenn Sie Verbindungsprobleme bemerken, auch nachdem Sie die genannten Schritte ausgeführt haben, ist es wahrscheinlich, dass die angeschlossenen Geräte veraltete ARP-Einträge enthalten. Überprüfen Sie die ARP-Einträge auf Upstream- und Downstream-Geräten. Um das Problem zu beheben, können Sie diese entweder leeren oder die funktionierende ASA/FTD dazu zwingen, ein Paket mit einer garp-Schnittstelle für die IP-Schnittstelle zu senden, bei der das Problem vorliegt. Führen Sie hierzu den Befehl in enable mode (für FTD im System unterstützt diagnostics-cli) aus - **debug menu ipaddrutl 6 <interface ip address>**.

   Vorsicht: Falls Sie ein Support-Ticket mit dem TAC für Split-Brain-bezogene Probleme eröffnen, teilen Sie uns bitte die Informationen unter Abschnitt **Daten, die für TAC Service Request** in diesem Dokument **zu sammeln sind**.

Daten für das TAC freigeben

Bitte teilen Sie uns Ihre Daten mit, falls Sie eine TAC Service Anfrage erstellen müssen.

1. Topologiediagramm, das ASA/FTD-HA und seine physischen Verbindungen zu benachbarten Geräten (einschließlich Failover-Schnittstellen) zeigt.
2. Ausgabe für **show tech-support** auf ASA oder Troubleshooting File auf Plattformen mit FTD.
3. Syslogs zusammen mit Zeitstempeln für +/- 5 Minuten, wenn das Problem auftrat.
4. FXOS-Dateien zur Fehlerbehebung, wenn es sich bei der Hardware um eine FPR-Appliance handelt.

Informationen zum Generieren von Fehlerbehebungsdateien für FTD oder FXOS finden Sie unter Verfahren zur Dateierstellung für Firepower-Fehlerbehebung. Öffnen Sie einen TAC-Serviceticket.