Fehlerbehebung bei unerwarteten Ladevorgängen auf Cisco IOS®/Cisco IOS® XE-Plattformen mit dem TAC

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Dateien beschrieben, um die Ursache für ein unerwartetes Neuladen in Cisco IOS®/Cisco IOS XE zu ermitteln und diese in ein TAC-Ticket hochzuladen. SDWAN-Bereitstellungen werden nicht behandelt.

Voraussetzungen

Anforderungen

- Dieses Dokument gilt für Cisco Router und Switches, auf denen die Cisco IOS/Cisco IOS XE Software ausgeführt wird.
- Um die in diesem Dokument beschriebenen Dateien zu sammeln, muss das Gerät betriebsbereit und stabil sein.
- Um die Dateien per Übertragungsprotokoll zu extrahieren, wird ein Server (mit installierter

Dateiübertragungsanwendung/installiertem Dienst) mit L3-Erreichbarkeit benötigt.
- Konsole oder Remote-Verbindung über SSH/Telnet zum Gerät ist erforderlich.

Anmerkung: Bei einem unerwarteten Neuladeereignis ist es möglich, dass einige Dateien aufgrund der Art des Neuladevorgangs und der Plattform nicht generiert werden.

Dateien für den technischen Support anzeigen

Die Ausgabe des Befehls **show tech-support** enthält allgemeine Informationen zum aktuellen Status des Geräts (Arbeitsspeicher- und CPU-Nutzung, Protokolle, Konfiguration usw.) sowie Informationen zu den erstellten Dateien zum Zeitpunkt des unerwarteten erneuten Ladens.

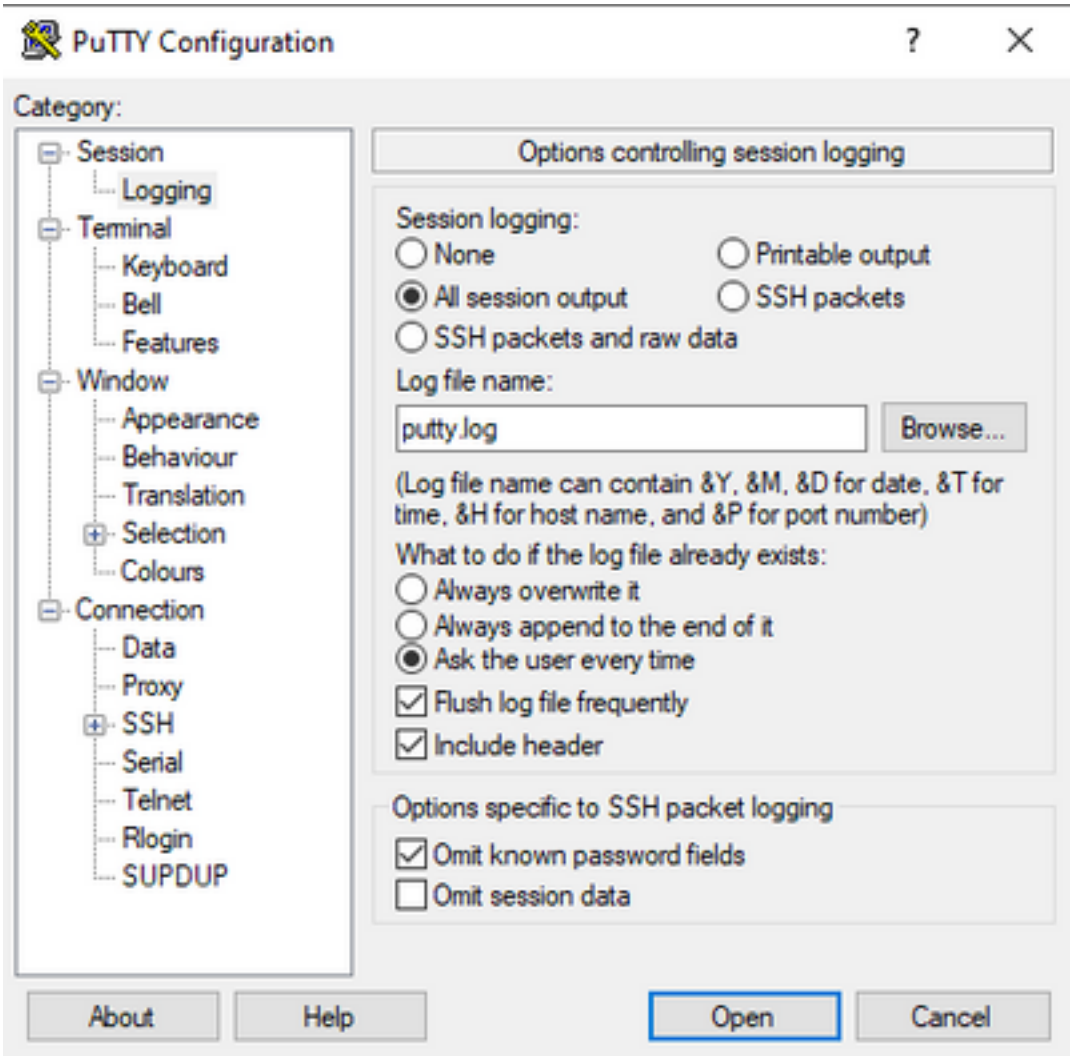
Im Fall eines unerwarteten Neustarts sollten folgende Hauptpunkte überprüft werden:

- Die aktuelle Cisco IOS-/Cisco IOS XE-Version, die auf dem Gerät installiert ist.
- Systemkonfiguration mit Details zu Ports, Karten und Modulen
- Vorhandensein zusätzlicher Dateien, um eine Ursachenanalyse in den Dateisystemen zu ermöglichen

Die Ergebnisse des technischen Supports können auf zwei verschiedene Arten erfasst werden: **eine Terminalsitzung protokollieren** oder **eine Datei im Speicher erstellen und vom Gerät übertragen**:

Protokollieren einer Terminalsitzung

Navigieren Sie in Putty zu **Session > Logging**, und wählen Sie auf der Registerkarte **Session logging** die Option **All session output aus, wie in diesem Bild dargestellt.**



Die Datei wird standardmäßig mit dem Namen putty.log im Ordner Putty gespeichert. Der Ordner und der Name der Datei können mit der Schaltfläche **Durchsuchen** geändert werden.

Nach Abschluss der Konfiguration muss die **Putty-**Sitzung über die **Konsole, Telnet** oder **SSH** mit dem Gerät verbunden werden.

In der Gerätesitzung wird empfohlen, den Befehl **terminal length 0** im privilegierten Modus festzulegen und dann den Befehl **show tech-support** zu verwenden.

```
# terminal length 0
# show tech-support
```

> **Anmerkung:** Die Ausführung des Befehls kann einige Sekunden dauern. Unterbrechen Sie die Ausführung nicht.

Erstellen einer Datei im Speicher

Eine **Show-Tech-Support**-Datei kann auf dem Gerät erstellt und in einem der Dateisystemspeicher (intern oder extern) gespeichert werden. Die Befehlssyntax bleibt auf allen Geräten gleich, das verwendete Dateisystem kann jedoch geändert werden. Die Datei kann auch direkt auf einem externen Server erstellt werden. Dieser Abschnitt zeigt die Syntax für ein lokales Dateisystem.

Um die Datei im Flash zu erstellen, muss der Befehl **show tech-support** verwendet werden. |

flash:Showtech.txt im privilegierten Modus umleiten:

```
# show tech-support | redirect flash:Showtech.txt
```

Das Terminal kann während der Generierung der Textdatei einige Sekunden lang nicht verwendet werden. Wenn die Erstellung abgeschlossen ist, können Sie überprüfen, ob die Datei mit dem Befehl **show [Dateisystem] ordnungsgemäß erstellt wurde:** command; Da die Datei eine reine Textdatei ist, kann der Inhalt mit **mehr** Befehlen auf dem Gerät angezeigt werden.

```
# show flash:
# more flash:Showtech.txt
```

Nachdem die Datei erstellt wurde, kann sie mithilfe eines bevorzugten Übertragungsprotokolls (FTP/TFTP/SCP) in einen externen Speicher extrahiert und zur Analyse freigegeben werden.

Crashinfo-Datei

Die **crashinfo**-Datei ist eine Textdatei. Sie enthält Details zum Debuggen, anhand derer der Absturzgrund identifiziert werden kann. Die Inhalte können von Plattform zu Plattform variieren. Im Allgemeinen verfügt es über den **Protokollierungspuffer** vor dem Absturz und die Funktionen, die vom Prozessor vor dem Absturz im codierten Modus ausgeführt wurden. Bei Cisco IOS-Plattformen ist dies die häufigste Datei, die sich nach dem Absturz in den Dateisystemen befindet. Bei Cisco IOS XE-Plattformen wird diese Datei nur dann generiert, wenn der Absturz im IOSd-Prozess stattfindet. Wenn ein anderer Prozess fehlschlägt, erstellt das Gerät keine Crashfo-Datei.

Crashinfo-Dateien finden Sie unter Flash, Bootflash, Festplatte oder Crashfo-Speicher in Basis auf der Plattform. Bei redundanten Kontrollebenen-Plattformen befinden sich die Crash-Dateien im aktiven und/oder Standby-Supervisor.

Der Inhalt dieser Datei ist begrenzt, da sie nur einen Schnappschuss des DRAM-Speichers vor dem unerwarteten Neustart und dem Speicherbereich der Prozesse benötigt. In einigen Fällen können zusätzliche Dateien/Ausgaben erforderlich sein, um die Ursache des Neustarts zu identifizieren.

Kerndateien

Auf Cisco IOS XE-Plattformen wird eine Core-Datei erstellt, wenn ein Prozess oder ein Dienst seine Ausführung aufgrund eines Laufzeitfehlers beendet (und einen unerwarteten Neustart verursacht). Diese Datei enthält Kontextinformationen über das Ereignis zum erneuten Laden.

Bei Cisco IOS XE-Plattformen wird er standardmäßig generiert, wenn der unerwartete Neustart softwarebasiert ist. Die Core-Dateien können unter jedem Linux-Prozess erstellt werden (einschließlich IOSd-Prozessen).

Kerndateien sind komprimierte Dateien, die die Informationen des gesamten ausgeführten Speichers enthalten, der von dem bestimmten Prozess verwendet wird, der den Absturz ausgelöst hat. Diese Datei erfordert spezielle Tools zu dekodieren, daher, um seine Konsistenz zu erhalten, ist es erforderlich, die Datei ohne Änderungen zu extrahieren. Dekomprimieren Sie die Datei, oder extrahieren Sie die Informationen als Text (wie mit **mehr** Befehl), nicht die Möglichkeit, den Inhalt durch das Support-Team zu dekodieren.

Core-Dateien werden normalerweise im **Core-**Ordner, im **Bootflash** oder auf der **Festplatte** gespeichert.

Das folgende Beispiel zeigt, wie die Kerndatei im Kernordner des Bootflash-Dateisystems angezeigt wird:

```
------------------ show bootflash: all ------------------

 9   10628763 Jul 14 2021 09:58:49 +00:00
/bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_3129_1626256707.core.gz
10   10626597 Jul 23 2021 13:35:26 +00:00
/bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_2671_1627047304.core.gz
```

> **Anmerkung:** Damit das TAC Corefile erfolgreich analysieren kann, müssen die Dateien ohne Änderungen extrahiert werden.

Um zu überprüfen, wie diese Datei vom Gerät extrahiert werden kann, navigieren Sie zum Abschnitt Dateien extrahieren.

Tracelogs

Die Ablaufverfolgungsprotokolle sind interne Protokolle der einzelnen Prozesse in Cisco IOS XE. Das Verzeichnis tracelogs wird standardmäßig erstellt, und sein Inhalt wird regelmäßig überschrieben. Dieser Ordner befindet sich im **Bootflash** oder auf der **Festplatte**.

Der Ordner kann sicher entfernt werden, es wird jedoch nicht empfohlen, da er im Fall eines unerwarteten Ereignisses zum erneuten Laden zusätzliche Informationen bereitstellen kann.

Um den Inhalt des Ordners zu extrahieren, ist es am einfachsten, eine komprimierte Datei zu erstellen, die alle tracelogs-Dateien enthält. Basierend auf der Plattform können Sie die folgenden Befehle verwenden:

Für Cisco IOS XE-Router:

```
# request platform software trace slot rp active archive target bootflash:TAC_tracelogs
```

Für Cisco IOS XE Switches und Wireless Controller:

```
# request platform software trace archive target bootflash:TAC_tracelogs
```

Ablaufverfolgungsprotokolle sind codierte Dateien, die zusätzliche Tools zum Decodieren erfordern. Daher muss die komprimierte Datei beim Erstellen extrahiert werden.

Um zu überprüfen, wie diese Datei vom Gerät extrahiert werden kann, navigieren Sie zum Abschnitt Dateien extrahieren.

Systemberichte

Ein Systembericht ist eine komprimierte Datei, die den Großteil der bei der Softwareausführung verfügbaren Informationen erfasst, wenn ein unerwartetes Neuladen auftritt. Der Systembericht enthält Ablaufverfolgungsprotokolle, Crashfo und Kerndateien. Diese Datei wird bei einem

unerwarteten Neuladen auf Cisco IOS XE-Switches und Wireless-Controllern erstellt.

Die Datei befindet sich im Hauptverzeichnis der bootlfash oder Festplatte.

Es enthält immer die Ablaufverfolgungen, die kurz vor dem Neustart generiert wurden. Im Fall eines unerwarteten erneuten Ladens enthält es Absturzdateien und Kerndateien des Ereignisses.

Diese Datei ist eine komprimierte Datei. Der Ordner kann dekomprimiert werden, es sind jedoch zusätzliche Tools zum Dekodieren der Informationen erforderlich.

Um zu überprüfen, wie diese Datei vom Gerät extrahiert werden kann, navigieren Sie zum Abschnitt Dateien extrahieren.

Kerne

Die Kerne werden vom Linux-Kernel und nicht von Cisco IOS XE-Prozessen erstellt. Wenn ein Gerät aufgrund eines Kernelfehlers neu geladen wird, werden normalerweise ein vollständiger Kernelkern (komprimierte Datei) und eine Zusammenfassung der Kernelkerndateien (Klartext) erstellt.

Die Prozesse, die zu dem unerwarteten Neustart geführt haben, können überprüft werden. Es wird jedoch immer empfohlen, die Datei dem Cisco TAC zur Verfügung zu stellen, um den Grund für das Neuladen vollständig zu analysieren.

Die Kerneldateien befinden sich im Hauptverzeichnis des **Bootflash** oder der Festplatte.

Extrahieren von Dateien

In diesem Abschnitt wird die erforderliche Basiskonfiguration beschrieben, um die erforderlichen Dateien von der Cisco IOS/Cisco IOS XE-Plattform auf einen externen Storage-Client zu übertragen.

Die Erreichbarkeit vom Gerät zum Server ist voraussichtlich verfügbar. Stellen Sie bei Bedarf sicher, dass keine Firewall oder Konfiguration vorhanden ist, die den Datenverkehr vom Gerät zum Server blockiert.

In diesem Abschnitt wird keine spezielle Serveranwendung empfohlen.

TFTP

Um eine Datei über **TFTP** zu übertragen, muss die Erreichbarkeit für die **TFTP-**Serveranwendung festgelegt werden. Es ist keine zusätzliche Konfiguration erforderlich.

Standardmäßig ist bei einigen Geräten die **IP-TFTP-Quellschnittstellenkonfiguration** über die Verwaltungsschnittstelle aktiv. Wenn der Server nicht über die Verwaltungsoberfläche erreichbar ist, führen Sie den Befehl aus, um die folgende Konfiguration zu entfernen:

```
(config)# no ip tftp source interface
```

Wenn die Konfiguration abgeschlossen ist, um den Server zu erreichen, können Sie zum

Übertragen der Datei folgende Befehle ausführen:

```
#copy :<file> tftp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

FTP

Um eine Datei über **FTP** zu übertragen, muss die Erreichbarkeit für die **FTP-**Serveranwendung festgelegt werden. Sie müssen den **FTP-**Benutzernamen und das -Kennwort auf dem Gerät und der **FTP-**Serveranwendung konfigurieren. Führen Sie die folgenden Befehle aus, um die Anmeldeinformationen auf dem Gerät festzulegen:

```
(config)#ip ftp username username
(config)#ip ftp password password
```

Optional können Sie mit den folgenden Befehlen eine FTP-Quellschnittstelle auf dem Gerät konfigurieren:

```
(config)# ip ftp source interface interface
```

Sobald die Konfiguration zum Erreichen des Servers abgeschlossen ist, können Sie zum Übertragen der Datei den folgenden Befehl ausführen:

```
#copy :<file> ftp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

SCP

Um eine Datei über **SCP** zu übertragen, muss die Erreichbarkeit für die **SCP-**Serveranwendung festgelegt werden. Auf dem Gerät (für den Start der Übertragung sind Anmeldeinformationen erforderlich) und der **SCP-**Serveranwendung müssen Benutzername und Kennwort lokal konfiguriert werden. Außerdem muss **SSH** auf dem Gerät konfiguriert sein. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass der **SSH**-Dienst konfiguriert ist:

```
#show running-config | section ssh
ip ssh version 2
ip ssh server algorithm encryption 3des-cbc aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption 3des-cbc aes128-ctr aes192-ctr aes256-ctr
transport input ssh
transport input ssh
```

Führen Sie den folgenden Befehl aus, um die Anmeldeinformationen auf dem Gerät festzulegen:

```
(config)#username USER password PASSWORD
```

> **Anmerkung:** Falls **TACACS** oder ein anderer Dienst für die SSH-Benutzerauthentifizierung verwendet wird, können diese Anmeldeinformationen verwendet werden, wenn der SCP-Server auch über die Benutzerinformationen verfügt.

Nach Abschluss der Konfiguration können Sie zum Übertragen der Datei die folgenden Befehle ausführen:

```
#copy :<file> scp:
Address or name of remote host []? X.X.X.X
Destination filename [<file>]?
```

USB

Für die Übertragung von Dateien über den USB-Flash-Speicher ist keine Erreichbarkeit mit einem externen Server im Netzwerk erforderlich. Es ist jedoch physischer Zugriff auf das Gerät erforderlich.

Alle physischen Geräte mit Cisco IOS/Cisco IOS XE verfügen über USB-Ports, die als externer Speicher verwendet werden können.

Führen Sie den Befehl **show file systems** aus, um zu überprüfen, ob das USB-Flash-Laufwerk erkannt wurde:

```
#show file systems
File Systems:

Size(b) Free(b) Type Flags Prefixes - - opaque rw system: - - opaque rw tmpsys: * 11575476224
10111098880 disk rw bootflash: flash: 2006351872 1896345600 disk ro webui: - - opaque rw null: -
- opaque ro tar: - - network rw tftp: 33554432 33527716 nvram rw nvram: - - opaque wo syslog: -
- network rw rcp: - - network rw pram: - - network rw http: - - network rw ftp: - - network rw
scp: - - network rw sftp - - network rw https: - - network ro cns: 2006351872 1896345600 disk rw
usbflash0:
```

> **Hinweis:** Cisco IOS-/Cisco IOS XE-Geräte unterstützen offizielle Cisco USB-Flash-Laufwerke. USB-Flash-Laufwerke von Drittanbietern werden nur begrenzt unterstützt.

Sobald der USB-Flash vom Gerät im richtigen Steckplatz (usbflash0 oder usbflash1) erkannt wurde und genügend freier Speicherplatz zur Verfügung steht, übertragen Sie die Datei mithilfe der folgenden Befehle:

```
#copy :<file> usbflashX:
Destination filename [<file>]?
```

Fehlerbehebung

In diesem Abschnitt werden einige der häufigsten Fehler und Problemumgehungen beschrieben, die beim Übertragen von Dateien (von einem Cisco IOS- oder Cisco IOS XE-Gerät) auf eine externe Methode gefunden und verwendet werden können.

Offene Ports bestätigen

Wenn das Gerät einen Fehler "Verbindung verweigert" anzeigt, wenn die Erreichbarkeit zum Server bestätigt wurde, kann es nützlich sein, zu überprüfen, ob die Ports auf der Geräteseite verfügbar sind (kein ACL-Eintrag, der den Datenverkehr blockiert) und dass die Ports auf der Serverseite ebenfalls verfügbar sind (für den letzten Teil kann der Telnet-Befehl mit dem erforderlichen Port verwendet werden).

Führen Sie je nach verwendetem Protokoll die folgenden Befehle aus:

TFTP
```
#telnet X.X.X.X 69
```

FTP
```
#telnet X.X.X.X 21
```

SCP
```
#telnet X.X.X.X 22
```

> **Anmerkung:** Frühere Ports sind die Standard-Ports für jedes Protokoll. Sie können geändert werden.

Wenn der Befehl keinen erfolgreichen offenen Port bereitstellt, ist es hilfreich, alle Fehlkonfigurationen (von der Serverseite oder einer Firewall im Pfad) zu bestätigen, die den Datenverkehr verwerfen können.

USB-Format

USB-Geräte von Drittanbietern werden bei den meisten Cisco IOS- und Cisco IOS XE-Geräten nicht erkannt.

USB mit einer Größe von mehr als 4 GB wird von Cisco IOS-Routern und -Switches nicht erkannt. USB-Geräte mit einer Größe von mehr als 4 GB sind für Cisco IOS XE-Plattformen geeignet.

Bei USB-Geräten von Drittanbietern kann die Formatierung FAT32 oder FAT16 getestet werden. Jedes andere Format kann nicht erkannt werden, auch nicht für ein kompatibles USB-Speicherlaufwerk.

Übertragungsunterbrechungen

Es ist möglich, dass die Dateiübertragung unterbrochen werden kann und bei Servern mit vielen Hops erneut gestartet werden muss.

In diesem Szenario kann es hilfreich sein, diese Konfiguration für die vty-Leitungen zu verwenden:

```
(config)#line vty 0 4
(config-line)#exec-timeout 0 0
```

Mit der vorherigen Konfiguration wird sichergestellt, dass die Übertragungssitzung nicht verworfen wird, selbst wenn das Steuerungspaket im Pfad verworfen wird oder das Bestätigen des Pakets zu lange dauert.

Nach Abschluss der Übertragung wird empfohlen, diese Konfiguration aus den vty-Zeilen zu entfernen.

Es wird immer empfohlen, den Dateiserver so nahe wie möglich am Gerät zu platzieren.

TFTP-Zwischenserver

Die Cisco Geräte können als temporärer TFTP-Server für Übertragungen verwendet werden, die nicht direkt an einen lokalen Dateiserver übertragen werden können.

Auf dem Gerät (mit der Datei, die extrahiert werden muss) können Sie den folgenden Befehl ausführen:

```
(config)#tftp-server :<file>
```

Auf dem Gerät, das als Client konfiguriert ist, können Sie die Befehle ausführen, die im TFTP- Abschnitt angezeigt werden.

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.