Probleemoplossing voor onverwachte herladingen met TAC in Cisco IOS®/Cisco IOS® XE-platforms

Inhoud

Inleiding

Dit document beschrijft de bestanden die nodig zijn om de oorzaak van een onverwacht opnieuw laden in Cisco IOS®/Cisco IOS XE te bepalen en ze naar een TAC-case te uploaden. SDWAN-implementaties worden niet besproken.

Voorwaarden

Vereisten

- Dit document is van toepassing op Cisco-routers en -switches waarop Cisco IOS/Cisco IOS XE-software wordt uitgevoerd.
- Om de bestanden te verzamelen die in dit document worden beschreven, moet het apparaat omhoog en stabiel zijn.
- Om de bestanden via het overdrachtsprotocol te extraheren, is een server (met applicatie voor

bestandsoverdracht/service geïnstalleerd) met L3 bereikbaarheid vereist.
- Console of externe verbinding via SSH/Telnet naar het apparaat is nodig.

Opmerking: Bij een onverwachte herladegebeurtenis, is het mogelijk dat sommige bestanden niet worden gegenereerd op basis van de aard van de herlading en het platform.

Bestanden voor technische ondersteuning tonen

De opdrachtoutput voor **show tech-support** bevat algemene informatie over de huidige status van het apparaat (geheugen- en CPU-gebruik, logbestanden, configuratie, enzovoort) en informatie over de gemaakte bestanden die betrekking hebben op het moment dat de onverwachte herladegebeurtenis plaatsvond.

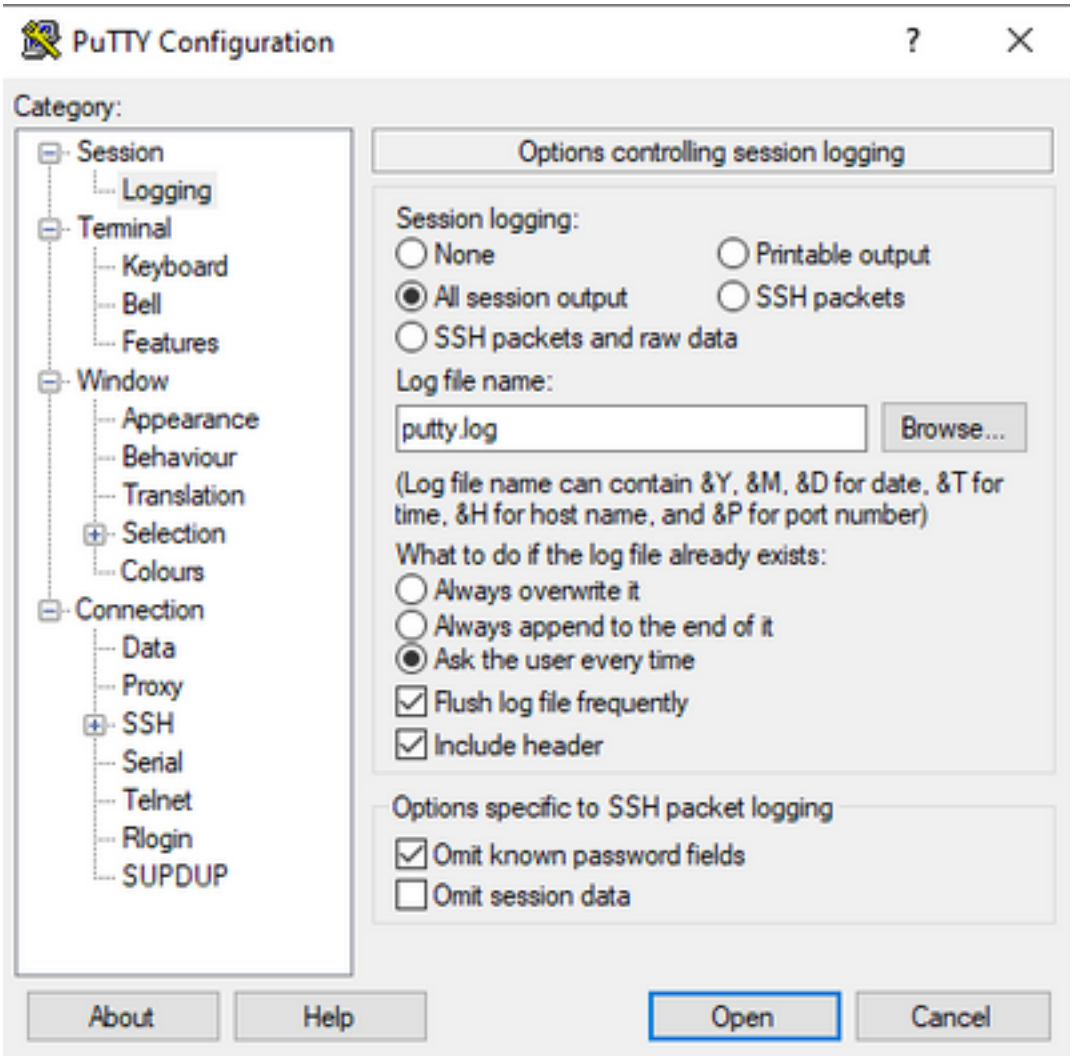
In het geval van een onverwachte reboot situatie, zijn de belangrijkste punten om te herzien:

- De huidige versie van Cisco IOS/Cisco IOS XE die op het apparaat is geïnstalleerd.
- Systeemconfiguratie met poorten, kaarten en modules details.
- Aanwezigheid van extra bestanden om een analyse van de basisoorzaak in de bestandssystemen.

De output van de show tech-support kan op twee verschillende manieren worden opgenomen: **log een terminalsessie in** of **maak een bestand in opslag en breng het van het apparaat over**:

Een terminalsessie registreren

Ga in Putty naar **Session > Logging** en selecteer in het tabblad **Session logging** de optie **All Session output**, zoals in deze afbeelding wordt getoond.



Het bestand wordt standaard met de naam putty.log opgeslagen in de map Putty. De map en de naam van het bestand kunnen worden gewijzigd met de knop **Bladeren**.

Wanneer de configuratie is voltooid, moet de **Putty-**sessie worden aangesloten op het apparaat via **console**, **Telnet** of **SSH**.

In de apparaatsessie is het raadzaam om de opdracht **terminal length 0** in te stellen in de voorkeursmodus en vervolgens de opdracht **show tech-support** te gebruiken.

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

> **Opmerking:** De uitvoering van de opdracht kan een paar seconden duren. Onderbreek de executie niet.

Een bestand in opslag maken

Een **show tech-support** bestand kan worden gemaakt op het apparaat en opgeslagen in een van de bestandssysteem opslag (intern of extern). De opdrachtsyntaxis blijft hetzelfde in alle apparaten, maar het gebruikte bestandssysteem kan worden gewijzigd. Het bestand kan ook direct op een externe server worden gemaakt, deze sectie toont de syntaxis voor een lokaal bestandssysteem.

Om het bestand in de flitser te maken, moet u de opdracht **show tech-support** gebruiken **| flitser omleiden:Showtech.txt** in privilege-modus:

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

De terminal kan een paar seconden niet worden gebruikt terwijl het tekstbestand wordt gegenereerd. Nadat het is voltooid, kunt u controleren of het maken van het bestand correct is met de **show [file system]:** commando; aangezien het bestand een onbewerkte tekstbestand is, kan de inhoud met **meer** opdracht op het apparaat worden weergegeven.

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

Zodra het bestand is gemaakt, kan het worden geëxtraheerd naar een externe opslag met een overdrachtprotocol naar keuze (FTP/TFTP/SCP) en worden gedeeld voor analyse.

Crashinfo-bestand

Het **crashinfo** bestand is een tekstbestand, het bevat debug details die helpen om de reden voor de crash te identificeren. De inhoud kan van platform tot platform variëren. Over het algemeen heeft het de **logboekbuffer** voorafgaand aan de crash en de functies die werden uitgevoerd door de processor, voorafgaand aan de crash in een gecodeerde modus. Op Cisco IOS-platforms is dit het meest voorkomende bestand dat na de crash in de bestandssystemen kan worden gevonden. In Cisco IOS XE-platforms wordt dit bestand gegenereerd wanneer de crash alleen in het IOS D-proces plaatsvindt; als een ander proces mislukt, dan maakt het apparaat geen crashinfo-bestand.

Crashinfo-bestanden zijn te vinden onder flash, bootflash, harddisk of crashinfo opslag op basis van het platform. In het geval van redundante besturingsplatformen kunnen de crashbestanden worden gevonden in de actieve en/of stand-by supervisor.

De inhoud van dit bestand is beperkt, omdat het alleen een momentopname van het DRAM-geheugen neemt voorafgaand aan de onverwachte herstart en het geheugengebied van de processen. In sommige gevallen kunnen extra bestanden/uitgangen nodig zijn om de basisoorzaak van de herstart te identificeren.

Core-bestanden

In Cisco IOS XE-platforms wordt een kernbestand gemaakt als een proces of een service de uitvoering beëindigt vanwege een runtime-fout (en een onverwachte herstart veroorzaakt). Dit bestand bevat contextinformatie over de herlaadgebeurtenis.

In Cisco IOS XE-platforms wordt het standaard gegenereerd wanneer de onverwachte reboot softwaredrift is. De kernbestanden kunnen worden gemaakt onder elk Linux-proces (IOSd-processen inbegrepen).

Kernbestanden zijn gecomprimeerde bestanden die de informatie bevatten van al het geheugen in uitvoering gebruikt door het specifieke proces dat de crash heeft veroorzaakt. Dit bestand vereist speciale tools om te decoderen, daarom, om zijn consistentie te behouden, is het nodig om het bestand te extraheren zonder enige wijziging. Decomprimeer het bestand of haal de informatie als tekst (zoals met **meer** opdracht), laat de mogelijkheid om de inhoud te decoderen door het ondersteuningsteam niet toe.

Kernbestanden worden meestal opgeslagen in de **kern** map, binnen de **bootflash** of **harddisk**.

Volgende is een voorbeeld dat toont hoe het corefile verschijnt binnen de kernmap in het bootflash bestandssysteem:

```
------------------ 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
```

> **Opmerking:** Om TAC met succes te kunnen analyseren Corefile, is het nodig om de bestanden te extraheren zonder enige wijziging of wijziging.

Om te controleren hoe u dit bestand uit het apparaat kunt halen, navigeer dan naar het gedeelte Bestanden uitnemen.

Tracelogs

De sporen zijn interne logboeken van elk proces binnen Cisco IOS XE. De tracelogs directory wordt standaard aangemaakt en de inhoud ervan wordt periodiek overschreven. Deze map kan worden gevonden in de **bootflash** of de **harddisk**.

De map kan veilig worden verwijderd, hoewel het niet wordt aanbevolen, omdat het extra informatie kan geven in het geval van een onverwachte herladingsgebeurtenis.

Om de inhoud van de map te extraheren, is de eenvoudigste benadering om een gecomprimeerd bestand te maken dat alle tracelogbestanden bevat. Op basis van het platform kunt u deze opdrachten gebruiken:

Voor Cisco IOS XE-routers:

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

Voor Cisco IOS XE-switches en draadloze controllers:

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

Tracelogs zijn gecodeerde bestanden die aanvullende tools vereisen om te decoderen, dus het is vereist om het gecomprimeerde bestand te extraheren zoals het is gemaakt.

Om te controleren hoe u dit bestand uit het apparaat kunt halen, navigeer dan naar het gedeelte Bestanden uitpakken.

Systeemrapporten

Een systeemrapport is een gecomprimeerd bestand dat de meeste informatie verzamelt die beschikbaar is in de softwareuitvoering wanneer er een onverwachte herlading optreedt. Het systeemrapport bevat overtrekken, crashinformatie en kernbestanden. Dit bestand wordt gemaakt in het geval van een onverwacht herladen van Cisco IOS XE-switches en draadloze controllers.

Het bestand is te vinden in de hoofdmap van de bootflash of harddisk.

Het bevat altijd de tracelogs die vlak voor de reboot worden gegenereerd. In het geval van een onverwacht herladen heeft het crashbestanden en kernbestanden van de gebeurtenis.

Dit bestand is een gecomprimeerd bestand. De map kan gedecompresseerd worden maar er zijn extra gereedschappen nodig om de informatie te decoderen.

Om te controleren hoe u dit bestand uit het apparaat kunt halen, navigeer dan naar het gedeelte Bestanden uitnemen.

Kernel Cores

De kernel kernen worden gemaakt door de Linux Kernel en niet door Cisco IOS XE processen. Wanneer een apparaat herlaadt vanwege een kernel-fout, worden meestal een volledige kernel kern (gecomprimeerd bestand) en een samenvatting van de kernel kern (platte tekst) bestanden gemaakt.

De processen die tot de onverwachte herstart hebben geleid, kunnen worden bekeken, maar het wordt altijd aanbevolen het bestand aan Cisco TAC te leveren om een volledige analyse van de reden voor het opnieuw laden te leveren.

De kernel core bestanden kunnen worden gevonden in de hoofdmap van de **bootflash** of harddisk.

Bestanden uitpakken

In deze sectie wordt de basisconfiguratie beschreven die vereist is om de benodigde bestanden van het Cisco IOS/Cisco IOS XE-platform naar een externe opslagclient over te dragen.

De bereikbaarheid van het apparaat naar de server is naar verwachting beschikbaar. Indien nodig, bevestig dat er geen firewall of configuratie is die het verkeer van het apparaat naar de server blokkeert.

In deze sectie wordt geen specifieke servertoepassing aanbevolen.

TFTP

Om een bestand via **TFTP** te kunnen verzenden, moet bereikbaarheid worden ingesteld op de **TFTP**-servertoepassing. Er is geen extra configuratie vereist.

Standaard is bij sommige apparaten de configuratie van de **ip tftp-broninterface** actief via de beheerinterface. Als de server niet bereikbaar is via de beheerinterface, voert u de opdracht uit om deze configuratie te verwijderen:

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

Nadat de configuratie om de server te bereiken is voltooid, kunt u deze opdrachten uitvoeren om het bestand over te brengen:

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

FTP

Om een bestand via **FTP** te kunnen verzenden, moet bereikbaarheid worden ingesteld op de **FTP-**servertoepassing. De gebruikersnaam en het wachtwoord voor **FTP** moeten worden geconfigureerd vanuit het apparaat en de **FTP**-servertoepassing. Als u de referenties op het apparaat wilt instellen, voert u deze opdrachten uit:

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

U kunt desgewenst een FTP-broninterface op het apparaat configureren met deze opdrachten:

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

Als de configuratie om de server te bereiken is voltooid, kunt u deze opdracht uitvoeren om het bestand over te brengen:

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

SCP

Om een bestand via **SCP** te kunnen overdragen, moet bereikbaarheid ingesteld worden op de **SCP** server applicatie. Het is noodzakelijk om lokale gebruikersnaam en wachtwoord op het apparaat (referenties zijn vereist om de overdracht te starten) en de **SCP** server applicatie te configureren. Het is ook nodig om **SSH** op het apparaat te hebben geconfigureerd. Om te bevestigen dat de **SSH-**service is geconfigureerd, voert u de opdracht uit:

```
#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
```

Om de referenties op het apparaat in te stellen, voert u de opdracht uit:

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

> **Opmerking:** Als **TACACS** of een andere service wordt gebruikt voor SSH-gebruikersverificatie, kunnen die referenties worden gebruikt als de SCP-server ook de gebruikersinformatie heeft.

Als de configuratie is voltooid, kunt u deze opdrachten uitvoeren om het bestand te verzenden:

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

```
Destination filename [<file>]?
```

USB

De overdracht van bestanden via de USB-flitser vereist geen bereikbaarheid naar een externe server in het netwerk, maar het vereist fysieke toegang tot het apparaat.

Alle fysieke apparaten met Cisco IOS/Cisco IOS XE hebben USB-poorten die als externe opslag kunnen worden gebruikt.

Om te bevestigen dat de USB-flashdrive wordt herkend, voert u de opdracht **Show file systems** uit:

```
#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:
```

> **Opmerking:** Cisco IOS/Cisco IOS XE-apparaten ondersteunen officiële Cisco USB-flashstations. Voor elke USB-flitser van derden is de ondersteuning beperkt.

Zodra de USB-flitser door het apparaat in de juiste sleuf is herkend (usbflash0 of usbflash1) en er voldoende vrije ruimte beschikbaar is, gebruikt u deze opdrachten om het bestand over te brengen:

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

Problemen oplossen

In deze sectie worden enkele veelvoorkomende fouten en tijdelijke oplossingen beschreven die kunnen worden gevonden en gebruikt terwijl u bestanden (van een Cisco IOS- of Cisco IOS XE-apparaat) naar een externe methode overbrengt.

Bevestig open poorten

Als het apparaat een verbinding geweigerde fout toont wanneer de bereikbaarheid aan de server is bevestigd, kan het nuttig zijn om te verifiëren de poorten aan de apparaatkant beschikbaar zijn (geen ACL-ingang die het verkeer blokkeert) en dat de poorten aan de serverzijde ook beschikbaar zijn (voor het laatste deel kan de telnet-opdracht met de vereiste poort worden gebruikt).

Op basis van het gebruikte protocol voert u deze opdrachten uit:

TFTP

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

FTP

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

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

> **Opmerking:** Vorige poorten zijn de standaardpoorten voor elk protocol, het is mogelijk dat deze poorten worden gewijzigd.

Als het commando geen succesvolle open poort biedt, is het handig om eventuele misconfiguraties te bevestigen (vanaf de server-side of een firewall in het pad) die het verkeer kunnen laten vallen.

USB-indeling

USB van derden kan niet worden herkend voor de meeste Cisco IOS- en Cisco IOS XE-apparaten.

USB van meer dan 4 GB kan niet worden herkend door Cisco IOS-routers en -switches. USB met een formaat groter dan 4 GB kan worden herkend door Cisco IOS XE-platforms.

In het geval van een externe USB, kan het worden getest met FAT32 of FAT16 formatting. Een ander formaat kan niet worden herkend, zelfs niet voor een compatibele USB-geheugendrive.

Onderbrekingen van overdrachten

Het is mogelijk dat de bestandsoverdracht onderbroken kan worden en nodig is om de overdracht opnieuw te starten voor servers met veel hop.

In dit scenario kan het handig zijn om deze configuratie op de vty lijnen te gebruiken:

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

De vorige configuratie zorgt ervoor dat de overdrachtsessie niet wordt verbroken, zelfs als het besturingspakket op het pad wordt verbroken of als het pakket te lang duurt om te worden bevestigd.

Nadat de overdracht is voltooid, wordt aanbevolen om deze configuratie uit de vty lijnen te verwijderen.

Het wordt altijd aanbevolen om de bestandsserver zo dicht mogelijk bij het apparaat te plaatsen.

Tussenfase-TFTP-server.

De Cisco-apparaten kunnen worden gebruikt als een tijdelijke TFTP-server voor overdrachten die niet rechtstreeks naar een lokale bestandsserver kunnen worden uitgevoerd.

Op het apparaat (met het bestand dat extractie vereist) kunt u de opdracht uitvoeren:

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

Van het apparaat dat als cliënt wordt gevormd, kunt u de bevelen in werking stellen die in de

sectie van TFTP verschijnen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.