Solucionar problemas de recargas inesperadas en plataformas Cisco IOS® con TAC

Contenido

Introducción

Este documento describe los archivos necesarios para determinar la causa de una recarga inesperada en Cisco IOS®/Cisco IOS XE y cargarlos en un caso TAC.

Prerequisites

Requirements

- Este documento se aplica a los routers y switches Cisco que ejecutan el software Cisco IOS/Cisco IOS XE.
- Para recopilar los archivos descritos en este documento, el dispositivo debe estar activo y estable.
- Para extraer los archivos a través del protocolo de transferencia, se requiere un servidor

(con aplicación/servicio de transferencia de archivos instalado) con alcance L3.
- Se necesita una conexión remota o de consola a través de SSH/Telnet al dispositivo.
- Las implementaciones de SDWAN no se analizan.

Nota: En un evento de recarga inesperado, es posible que algunos archivos no se generen en función de la naturaleza de la recarga y la plataforma.

Mostrar archivos de soporte técnico

El resultado del comando show tech-support incluye información general sobre el estado actual del dispositivo (utilización de la memoria y la CPU, registros, configuración, etc.) e información sobre los archivos creados relacionados con cuándo tuvo lugar el evento de recarga inesperado.

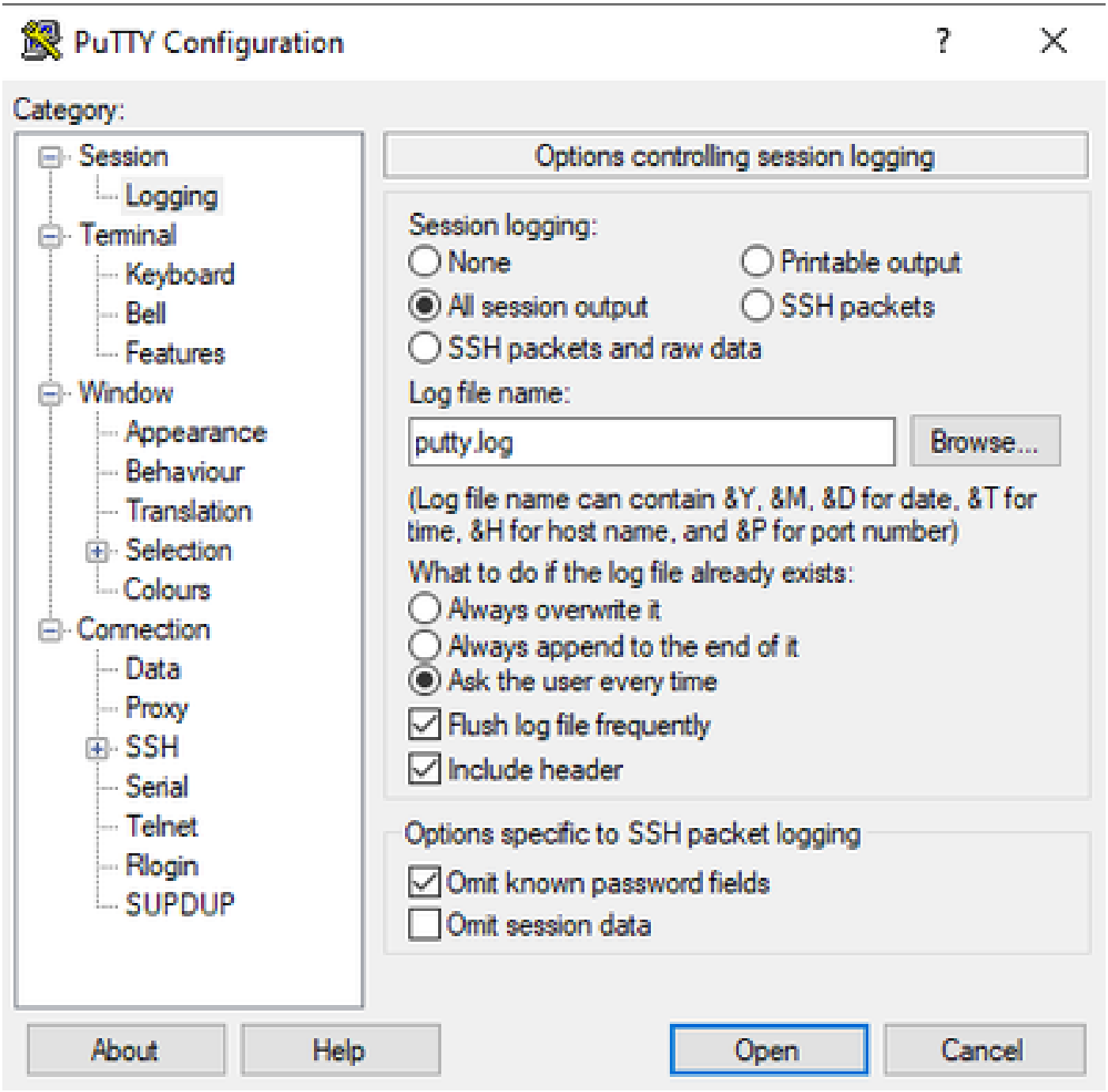
En caso de que se produzca un reinicio inesperado, los puntos clave que se deben revisar son:

- La versión actual de Cisco IOS/Cisco IOS XE instalada en el dispositivo.
- Configuración del sistema con detalles de puertos, tarjetas y módulos.
- Presencia de archivos adicionales para proporcionar un análisis de la causa raíz en los sistemas de archivos.

El resultado de show tech-support se puede capturar de dos maneras diferentes: registrar una sesión de terminal o crear un archivo en almacenamiento y transferirlo fuera del dispositivo:

Registrar una sesión de Terminal

En Putty, navegue hasta Session > Logging y seleccione dentro de la pestaña Session logging, seleccione la opción All session output, como se muestra en esta imagen.



El archivo se almacena en la carpeta de masilla de forma predeterminada con el nombre putty.log. La carpeta y el nombre del archivo se pueden cambiar con el botón Browse.

Una vez completada la configuración, la sesión Putty debe ser conectada al dispositivo a través de la Consola, Telnet o SSH.

En la sesión del dispositivo se recomienda establecer el comando terminal length 0 en el modo de privilegio y luego utilizar el comando show tech-support .

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

Nota: La ejecución del comando puede tardar un par de segundos. No interrumpa la ejecución.

Crear un archivo en almacenamiento

Se puede crear un archivo show tech-support en el dispositivo y almacenarlo en uno de los sistemas de almacenamiento (interno o externo). La sintaxis de los comandos sigue siendo la misma en todos los dispositivos, pero el sistema de archivos utilizado se puede cambiar. El archivo también se puede crear directamente en un servidor externo. En esta sección se muestra la sintaxis de un sistema de archivos local.

Para crear el archivo dentro de la memoria flash, es necesario utilizar el comando show tech-support | redirect flash:Showtech.txt en modo de privilegio:

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

El terminal no se puede utilizar durante un par de segundos mientras se genera el archivo de texto. Una vez completado, puede verificar si la creación del archivo es correcta con el comando show [sistema de archivos]:; dado que el archivo es un archivo de texto sin formato, el contenido se puede mostrar en el dispositivo con el comando more.

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

Una vez creado el archivo, se puede extraer a un almacenamiento externo con un protocolo de transferencia elegido (FTP/TFTP/SCP) y compartirse para su análisis.

Archivo Crashinfo

El archivo crashinfo es un archivo de texto, incluye detalles de depuración que ayudarían a identificar la razón del desperfecto. El contenido puede variar de una plataforma a otra. En general, tiene el buffer de registro antes del desperfecto y las funciones que ejecutó el procesador, antes del desperfecto en un modo codificado. En las plataformas Cisco IOS, este es el archivo más común que se puede encontrar en los sistemas de archivos después del desperfecto. En las plataformas Cisco IOS XE, este archivo se genera cuando el desperfecto ocurre solamente en el proceso IOSd; si cualquier otro proceso falla, el dispositivo no crea un archivo crashinfo.

Los archivos Crashinfo se pueden encontrar en flash, bootflash, harddisk o crashinfo storage en base a la plataforma. En el caso de las plataformas de plano de control redundantes, los archivos crashfile se pueden encontrar en el supervisor activo y/o en espera.

El contenido de este archivo es limitado, ya que solo toma un instante de la memoria DRAM antes del reinicio inesperado y la región de memoria de los procesos. En algunos casos, pueden ser necesarios archivos/salidas adicionales para identificar la causa raíz del reinicio.

Archivos de núcleo

En las plataformas Cisco IOS XE, cuando un proceso o un servicio finaliza su ejecución debido a un error de tiempo de ejecución (y provoca un reinicio inesperado), se crea un archivo de núcleo. Este archivo contiene información de contexto sobre el evento reload.

En las plataformas Cisco IOS XE, se genera de forma predeterminada cuando el reinicio inesperado se basa en software. Los archivos de núcleo se pueden crear bajo cualquier proceso de Linux (procesos IOSd incluidos).

Los archivos de núcleo son archivos comprimidos que contienen la información de toda la memoria en ejecución utilizada por el proceso específico que desencadenó el desperfecto. Este archivo requiere herramientas especiales para decodificar, por lo tanto, para mantener su consistencia, se requiere extraer el archivo sin ningún cambio. Descomprima el archivo o extraiga la información como texto (por ejemplo, con el comando more), no permite que el equipo de soporte técnico pueda descodificar el contenido.

Los archivos de núcleo generalmente se almacenan en la carpeta core, dentro de la bootflash o el disco duro.

A continuación se muestra un ejemplo que muestra cómo aparece el archivo corefile dentro de la carpeta core en el sistema de archivos bootflash:

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

 9   10628763 Jul 14 2021 09:58:49 +00:00 /bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_3129_16
10   10626597 Jul 23 2021 13:35:26 +00:00 /bootflash/core/Router_216_Router_RP_0_ucode_pkt_PPE0_2671_16
```

Nota: Para que el TAC analice con éxito el archivo Corefile, es necesario extraer los archivos sin ninguna modificación o cambio.

Para verificar la manera de extraer este archivo del dispositivo, navegue hasta la sección Extraer archivos.

Tracelogs

Los tracelogs son registros internos de cada proceso dentro de Cisco IOS XE. El directorio tracelogs se crea de forma predeterminada y su contenido se sobrescribe periódicamente. Esta carpeta se puede encontrar en el bootflash o en el disco duro.

La carpeta se puede quitar de forma segura, aunque no se recomienda, ya que puede proporcionar información adicional en caso de que se produzca un evento de recarga inesperado.

Para extraer el contenido de la carpeta, el método más sencillo consiste en crear un archivo comprimido que incluya todos los archivos tracelogs. En base a la plataforma, puede utilizar estos comandos:

Para routers Cisco IOS XE:

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

Para switches y controladores inalámbricos Cisco IOS XE:

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

Los tracelogs son archivos codificados que requieren herramientas adicionales para descodificar, por lo que es necesario extraer el archivo comprimido a medida que se crea.

Para comprobar la forma de extraer este archivo del dispositivo, vaya a la sección Extraer archivos.

Informes del sistema

Un informe del sistema es un archivo comprimido que recopila la mayor parte de la información disponible en la ejecución del software cuando se produce una recarga inesperada. El informe del sistema contiene tracelogs, crashinfo y archivos de núcleo. Este archivo se crea en el caso de una recarga inesperada en los switches Cisco IOS XE y los controladores inalámbricos.

El archivo se puede encontrar en el directorio principal de bootflash o harddisk.

Siempre contiene los tracelogs generados justo antes del reinicio. En el caso de una recarga inesperada tiene archivos crashfile y archivos core del evento.

Este archivo es un archivo comprimido, la carpeta se puede descomprimir pero requiere herramientas adicionales para descodificar la información.

Para verificar la manera de extraer este archivo del dispositivo, navegue hasta la sección Extraer archivos.

Núcleos de núcleo

Los núcleos del kernel son creados por el kernel de Linux y no por los procesos de Cisco IOS XE.

Cuando un dispositivo se recarga debido a una falla del núcleo, generalmente se crea un núcleo del núcleo completo (archivo comprimido) y un resumen de los archivos del núcleo del núcleo (texto sin formato).

Los procesos que llevaron al reinicio inesperado se pueden revisar, pero siempre se recomienda proporcionar el archivo al TAC de Cisco para proporcionar un análisis completo del motivo de la recarga.

Los archivos de núcleo del núcleo se pueden encontrar en el directorio principal del bootflash o disco duro.

Cómo extraer archivos

En esta sección se describe la configuración básica necesaria para transferir los archivos requeridos de la plataforma Cisco IOS/Cisco IOS XE a un cliente de almacenamiento externo.

Se espera que el acceso desde el dispositivo al servidor esté disponible. Si es necesario, confirme que no existe ningún firewall o configuración que bloquee el tráfico desde el dispositivo al servidor.

En esta sección no se recomienda ninguna aplicación de servidor específica.

TFTP

Para transferir un archivo a través de TFTP, es necesario establecer la disponibilidad en la aplicación del servidor TFTP. No se requiere una configuración adicional.

De forma predeterminada, algunos dispositivos tienen la configuración de la interfaz de origen ip tftp activa a través de la interfaz de administración. Si el servidor no es accesible a través de la interfaz de administración, ejecute el comando para quitar esta configuración:

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

Una vez finalizada la configuración para llegar al servidor, para transferir el archivo puede ejecutar estos comandos:

```
#copy

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

FTP

Para transferir un archivo a través de FTP, es necesario establecer la disponibilidad en la aplicación del servidor FTP. Es necesario configurar el nombre de usuario y la contraseña de FTP desde el dispositivo y la aplicación del servidor FTP. Para configurar las credenciales en el dispositivo, ejecute estos comandos:

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

Opcionalmente, puede configurar una interfaz de origen FTP en el dispositivo con estos comandos:

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

Una vez que la configuración para llegar al servidor se haya completado, para transferir el archivo puede ejecutar estos comandos:

```
#copy
```

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

SCP

Para transferir un archivo a través de SCP, es necesario establecer la disponibilidad en la aplicación del servidor SCP. Es necesario configurar el nombre de usuario y la contraseña locales en el dispositivo (se requieren credenciales para iniciar la transferencia) y en la aplicación del servidor SCP. También es necesario tener SSH configurado en el dispositivo. Para confirmar que el servicio SSH está configurado, ejecute el comando:

```
#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
```

Para establecer las credenciales en el dispositivo, ejecute el comando:

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

Nota: En caso de que se utilice TACACS u otro servicio para la autenticación de usuario SSH, esas credenciales se pueden utilizar si el servidor SCP también tiene la información de usuario.

Una vez finalizada la configuración, para transferir el archivo puede ejecutar estos comandos:

```
#copy

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

USB

La transferencia de archivos a través de la memoria flash USB no requiere la disponibilidad de ningún servidor externo de la red, pero sí el acceso físico al dispositivo.

Todos los dispositivos físicos con Cisco IOS/Cisco IOS XE tienen puertos USB que se pueden utilizar como almacenamiento externo.

Para confirmar que se reconoce la unidad flash USB, ejecute el comando show file systems:

```
#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:
```

Nota: Los dispositivos Cisco IOS/Cisco IOS XE admiten unidades flash USB oficiales de Cisco. Para cualquier flash USB de terceros, la compatibilidad es limitada.

Una vez que el dispositivo reconozca la memoria flash USB en la ranura adecuada (usbflash0 o usbflash1) y haya suficiente espacio libre disponible, utilice estos comandos para transferir el archivo:

```
#copy

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

Troubleshoot

En esta sección se describen algunos de los errores y soluciones alternativas más comunes que se pueden encontrar y utilizar para transferir archivos (desde un dispositivo Cisco IOS o Cisco IOS XE) a un método externo.

Confirmar puertos abiertos

Si el dispositivo muestra un error de conexión rechazada cuando se ha confirmado el alcance al servidor, puede ser útil verificar que los puertos en el lado del dispositivo estén disponibles (ninguna entrada ACL que bloquee el tráfico) y que los puertos en el lado del servidor también estén disponibles (para la última parte, se puede utilizar el comando telnet con el puerto requerido).

En función del protocolo utilizado, ejecute estos comandos:

<#root>

TFTP

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

FTP

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

SCP

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

Nota: Los puertos anteriores son los puertos predeterminados para cada protocolo; es posible cambiar estos puertos.

Si el comando no proporciona un puerto abierto exitoso, es útil confirmar cualquier configuración incorrecta (del lado del servidor o de cualquier firewall en la trayectoria) que pueda descartar el tráfico.

Formato USB

La mayoría de los dispositivos Cisco IOS y Cisco IOS XE no admiten USB de terceros.

Los routers y switches Cisco IOS no reconocen USB de más de 4 GB. Las plataformas Cisco IOS XE admiten USB con un tamaño superior a 4 GB.

En el caso de un USB de terceros, se puede probar con el formato FAT32 o FAT16. No se puede reconocer ningún otro formato ni siquiera en una unidad de memoria USB compatible.

Interrupciones de transferencia

Es posible que la transferencia de archivos se pueda interrumpir y se requiera para iniciar la transferencia nuevamente para servidores con muchos saltos.

En este escenario, puede ser útil utilizar esta configuración en las líneas vty:

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

La configuración anterior garantiza que la sesión de transferencia no se descarte, incluso si el paquete de control se descarta en el trayecto o si el paquete tarda demasiado en ser reconocido.

Una vez completada la transferencia, se recomienda quitar esta configuración de las líneas vty.

Siempre se recomienda colocar el servidor de archivos lo más cerca posible del dispositivo.

Servidor TFTP intermedio.

Los dispositivos de Cisco se pueden utilizar como un servidor TFTP temporal para transferencias que no se pueden hacer directamente a un servidor de archivos local.

En el dispositivo (con el archivo que requiere extracción) puede ejecutar el comando:

```
(config)#tftp-server

      :<file>
```

Desde el dispositivo que está configurado como cliente, puede ejecutar los comandos que aparecen en la sección TFTP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).