Risoluzione dei problemi di ricarica imprevista nelle piattaforme Cisco IOS®/Cisco IOS® XE con TAC

Sommario

Introduzione

Questo documento descrive i file richiesti per determinare la causa di un ricaricamento imprevisto in Cisco IOS®/Cisco IOS XE e caricarli in una richiesta TAC. Le distribuzioni SDWAN non vengono discusse.

Prerequisiti

Requisiti

- Questo documento è relativo ai router e agli switch Cisco con software Cisco IOS/Cisco IOS XE.
- Per raccogliere i file descritti in questo documento, il dispositivo deve essere attivo e stabile.
- Per estrarre i file tramite il protocollo di trasferimento, è necessario un server (con applicazione/servizio di trasferimento file installato) con raggiungibilità L3.

- Ènecessario disporre di una console o di una connessione remota al dispositivo tramite SSH/Telnet.

  Nota: In un evento di ricaricamento imprevisto, è possibile che alcuni file non vengano generati in base alla natura del ricaricamento e della piattaforma.

Mostra file di supporto tecnico

L'output del comando **show tech-support** include informazioni generali sullo stato corrente del dispositivo (utilizzo di memoria e CPU, registri, configurazione, ecc.) e informazioni sui file creati relativi al momento in cui si è verificato l'evento di ricaricamento imprevisto.

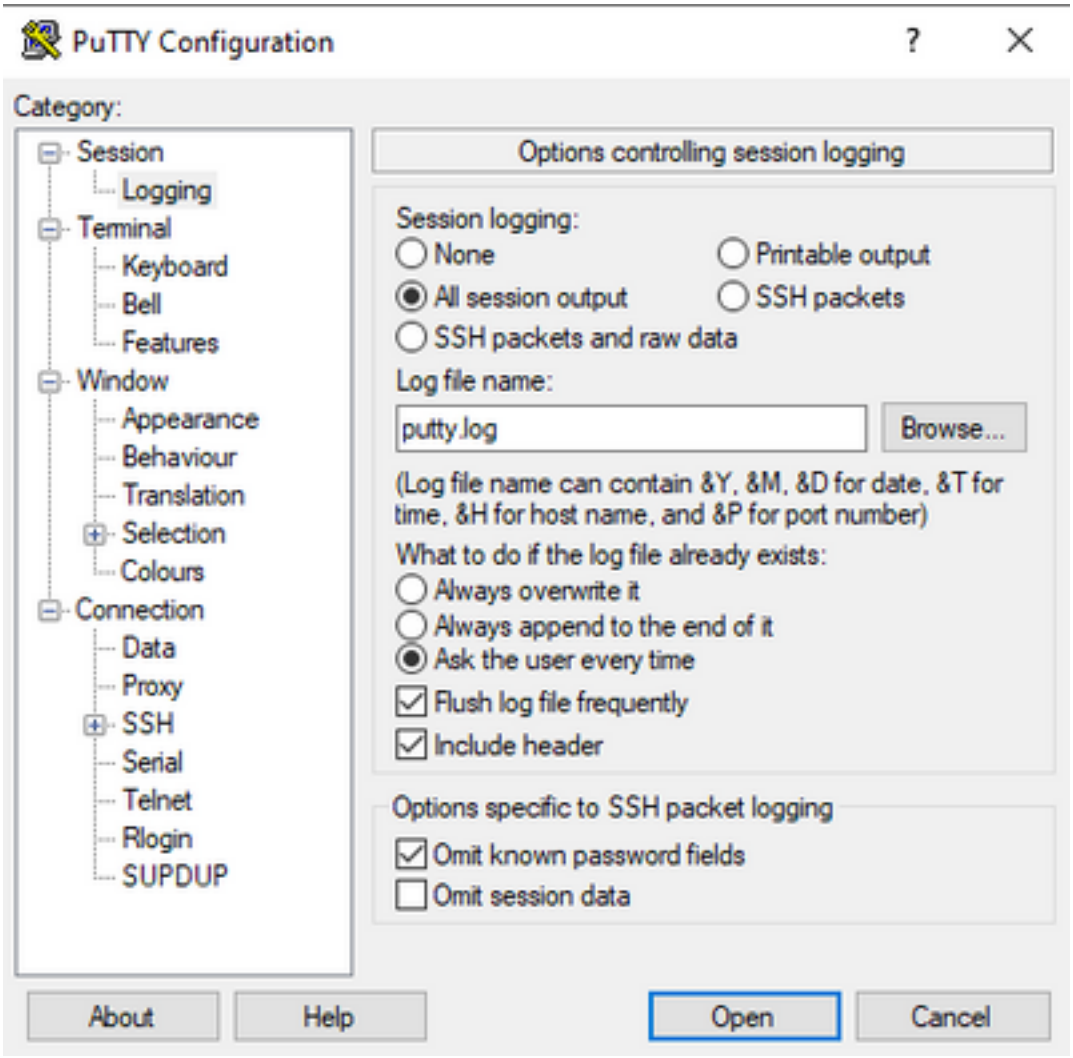
In caso di riavvio imprevisto, i punti chiave da esaminare sono:

- La versione corrente di Cisco IOS/Cisco IOS XE installata sul dispositivo.
- Configurazione del sistema con dettagli su porte, schede e moduli.
- Presenza di file aggiuntivi per fornire una root cause analysis nei file system.

L'uscita show tech-support può essere acquisita in due modi: **registrare una sessione terminale** o **creare un file in archiviazione e trasferirlo dal dispositivo**:

Registra sessione terminale

In Putty, spostatevi su **Session > Logging** e selezionate nella scheda **Session logging**, quindi selezionate l'opzione **All session output**, come mostrato nell'immagine.



Per impostazione predefinita, il file viene memorizzato nella cartella Putty con il nome putty.log. La cartella e il nome del file possono essere modificati con il pulsante **Sfoglia**.

Al termine della configurazione, la sessione **Putty** deve essere connessa al dispositivo tramite **Console**, **Telnet** o **SSH**.

Nella sessione del dispositivo, si consiglia di impostare il comando **terminal length 0** in modalità privilegiata e quindi di utilizzare il comando **show tech-support**.

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

> **Nota:** L'esecuzione del comando può richiedere alcuni secondi. Non interrompere l'esecuzione.

Crea un file nell'archivio

Èpossibile creare un file **show tech-support** sul dispositivo e archiviarlo in uno dei file system di storage (interno o esterno). La sintassi del comando rimane la stessa in tutti i dispositivi, ma è possibile modificare il file system utilizzato. Il file può anche essere creato direttamente su un server esterno. In questa sezione viene illustrata la sintassi di un file system locale.

Per creare il file nella memoria flash, è necessario usare il comando **show tech-support |**

reindirizzare flash:Showtech.txt in modalità privilegiata:

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

Durante la creazione del file di testo, il terminale non può essere utilizzato per alcuni secondi. Al termine, è possibile verificare se la creazione del file è corretta tramite il comando **show [file system]:** comando; poiché il file è un file di testo normale, il contenuto può essere visualizzato sul dispositivo con il comando **more**.

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

Una volta creato, il file può essere estratto su una memoria esterna con un protocollo di trasferimento a scelta (FTP/TFTP/SCP) e condiviso per l'analisi.

File Crashinfo

Il file **crashinfo** è un file di testo e include i dettagli di debug che consentono di identificare la causa dell'arresto anomalo. Il contenuto può variare da piattaforma a piattaforma. In generale, dispone del **buffer di registrazione** prima dell'arresto anomalo e delle funzioni eseguite dal processore prima dell'arresto anomalo in modalità codificata. Nelle piattaforme Cisco IOS, è il file più comune che si può trovare nei file system dopo l'arresto anomalo. Nelle piattaforme Cisco IOS XE, questo file viene generato quando il crash si verifica solo nel processo IOSd; se si verifica un errore in un altro processo, il dispositivo non crea un file crashinfo.

I file Crashinfo si trovano sotto memoria flash, bootflash, hard disk o crashinfo in base alla piattaforma. Nel caso di piattaforme di control plane ridondanti, i file di arresto anomalo possono essere trovati nel supervisore attivo e/o in standby.

Il contenuto di questo file è limitato, in quanto è sufficiente una copia istantanea della memoria DRAM prima del riavvio imprevisto e della regione di memoria dei processi. In alcuni casi, è possibile che siano necessari file/output aggiuntivi per identificare la causa principale del riavvio.

File principali

Nelle piattaforme Cisco IOS XE, quando un processo o un servizio termina la sua esecuzione a causa di un errore di runtime (e causa un riavvio imprevisto), viene creato un file di base. Questo file contiene informazioni di contesto sull'evento reload.

Nelle piattaforme Cisco IOS XE, viene generato per impostazione predefinita quando il riavvio imprevisto è basato su software. I file di base possono essere creati in qualsiasi processo Linux (inclusi i processi IOSd).

I file di base sono file compressi che contengono le informazioni di tutta la memoria in esecuzione utilizzata dal processo specifico che ha attivato l'arresto anomalo. Questo file richiede strumenti speciali per decodificare, quindi, per mantenere la sua coerenza, è necessario estrarre il file senza alcuna modifica. La decompressione del file o l'estrazione delle informazioni come testo (ad esempio con il comando **more**) non consente al team di supporto di decodificare il contenuto.

I file core sono in genere memorizzati nella cartella **core**, all'interno del **bootflash** o del **disco rigido**.

Di seguito è riportato un esempio che mostra come il file corefile appare nella cartella principale nel file system 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_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
```

> **Nota:** Affinché TAC riesca ad analizzare Corefile, è necessario estrarre i file senza alcuna modifica.

Per verificare il modo in cui estrarre il file dal dispositivo, passare alla sezione Estrai file.

Log

I registri di traccia sono registri interni di ciascun processo in Cisco IOS XE. La directory tracelogs viene creata per impostazione predefinita e il relativo contenuto viene sovrascritto periodicamente. Questa cartella si trova in **bootflash** o sul **disco rigido**.

La cartella può essere rimossa senza problemi, sebbene non sia consigliata in quanto può fornire informazioni aggiuntive in caso di evento di ricaricamento imprevisto.

Per estrarre il contenuto della cartella, l'approccio più semplice consiste nel creare un file compresso che includa tutti i file di log di traccia. In base alla piattaforma, è possibile utilizzare i seguenti comandi:

Per i router Cisco IOS XE:

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

Per switch e controller wireless Cisco IOS XE:

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

I registri di traccia sono file codificati che richiedono strumenti aggiuntivi per la decodifica, pertanto è necessario estrarre il file compresso al momento della creazione.

Per verificare come estrarre il file dal dispositivo, passare alla sezione Estrai file.

Report di sistema

Un report di sistema è un file compresso che raccoglie la maggior parte delle informazioni disponibili nell'esecuzione del software quando si verifica un ricaricamento imprevisto. Il report di sistema contiene i registri di traccia, le informazioni di arresto anomalo e i file di base. Questo file viene creato in caso di un ricaricamento imprevisto sugli switch Cisco IOS XE e sui controller wireless.

Il file si trova nella directory principale del bootflash o del disco rigido.

Contiene sempre i registri di traccia generati immediatamente prima del riavvio. In caso di un ricaricamento imprevisto, contiene i file di arresto anomalo e i file principali dell'evento.

Il file è compresso. La cartella può essere decompressa, ma sono necessari strumenti aggiuntivi per decodificare le informazioni.

Per verificare il modo in cui estrarre il file dal dispositivo, passare alla sezione Estrai file.

Core del kernel

I core del kernel vengono creati dal kernel Linux e non dai processi Cisco IOS XE. Quando un dispositivo viene ricaricato a causa di un errore del kernel, vengono in genere creati un core del kernel completo (file compresso) e un riepilogo dei file core del kernel (testo normale).

I processi che hanno causato il riavvio imprevisto possono essere rivisti, ma si consiglia sempre di inviare il file a Cisco TAC per fornire un'analisi completa del motivo del riavvio.

I file di base del kernel si trovano nella directory principale di **bootflash** o hard disk.

Come estrarre i file

In questa sezione viene descritta la configurazione di base necessaria per trasferire i file richiesti dalla piattaforma Cisco IOS/Cisco IOS XE a un client di storage esterno.

Èprevista la possibilità di raggiungere il server dal dispositivo. Se necessario, verificare che non vi sia alcun firewall o configurazione che blocchi il traffico tra il dispositivo e il server.

In questa sezione non è consigliata alcuna applicazione server specifica.

TFTP

Per trasferire un file sul protocollo **TFTP**, è necessario impostare la raggiungibilità dell'applicazione server **TFTP**. Non sono necessarie configurazioni aggiuntive.

per impostazione predefinita, alcuni dispositivi hanno la configurazione dell'**interfaccia sorgente ip tftp** attiva tramite l'interfaccia di gestione. Se il server non è raggiungibile tramite l'interfaccia di gestione, eseguire il comando per rimuovere questa configurazione:

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

Al termine della configurazione per raggiungere il server, per trasferire il file è possibile eseguire i seguenti comandi:

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

FTP

Per trasferire un file su **FTP**, è necessario impostare la raggiungibilità dell'applicazione server

FTP. È necessario configurare il nome utente e la password FTP dal dispositivo e dall'applicazione server FTP. Per impostare le credenziali sul dispositivo, eseguire i seguenti comandi:

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

Facoltativamente, è possibile configurare un'interfaccia FTP sul dispositivo con questi comandi:

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

Una volta completata la configurazione per raggiungere il server, per trasferire il file è possibile eseguire questi comandi:

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

SCP

Per trasferire un file su SCP, è necessario impostare la raggiungibilità dell'applicazione server SCP. È necessario configurare il nome utente e la password locali sul dispositivo (per avviare il trasferimento sono necessarie le credenziali) e sull'applicazione server SCP. Inoltre, è necessario avere configurato il protocollo SSH sul dispositivo. Per verificare che il servizio SSH sia configurato, eseguire il 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
```

Per impostare le credenziali sul dispositivo, eseguire il comando:

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

> **Nota:** Se per l'autenticazione dell'utente SSH viene usato TACACS o un altro servizio, è possibile usare queste credenziali se anche il server SCP ha le informazioni sull'utente.

Al termine della configurazione, per trasferire il file è possibile eseguire i seguenti comandi:

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

USB

Il trasferimento di file tramite flash USB non richiede la raggiungibilità ad alcun server esterno nella rete, ma richiede l'accesso fisico al dispositivo.

Tutti i dispositivi fisici con Cisco IOS/Cisco IOS XE dispongono di porte USB che possono essere utilizzate come storage esterno.

Per confermare il riconoscimento dell'unità flash USB, eseguire il 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:** i dispositivi Cisco IOS/Cisco IOS XE supportano le unità flash USB ufficiali di Cisco. Il supporto è limitato per qualsiasi flash USB di terze parti.

Una volta che la memoria flash USB viene riconosciuta dal dispositivo nello slot appropriato (usbflash0 o usbflash1) e lo spazio disponibile è sufficiente, utilizzare questi comandi per trasferire il file:

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

Risoluzione dei problemi

In questa sezione vengono descritti alcuni degli errori comuni e le soluzioni possibili che è possibile individuare e utilizzare durante il trasferimento di file (da un dispositivo Cisco IOS o Cisco IOS XE) a un metodo esterno.

Conferma apertura porte

Se il dispositivo mostra un errore di connessione rifiutata quando è stata confermata la raggiungibilità al server, può essere utile verificare che le porte sul lato dispositivo siano disponibili (nessuna voce ACL che blocchi il traffico) e che siano disponibili anche le porte sul lato server (per l'ultima parte, è possibile usare il comando telnet con la porta richiesta).

In base al protocollo utilizzato, eseguire i seguenti comandi:

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

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

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

> **Nota:** Le porte precedenti sono le porte predefinite per ciascun protocollo e possono essere modificate.

Se il comando non restituisce una porta aperta, è utile verificare eventuali configurazioni errate (dal lato server o da un firewall del percorso) che potrebbero causare il blocco del traffico.

Formato USB

Non è possibile riconoscere USB di terze parti per la maggior parte dei dispositivi Cisco IOS e Cisco IOS XE.

I router e gli switch Cisco IOS non sono in grado di riconoscere USB superiori a 4 GB. Le piattaforme Cisco IOS XE sono in grado di riconoscere USB di dimensioni superiori a 4 GB.

Nel caso di un USB di terze parti, può essere testato con la formattazione FAT32 o FAT16. Non è possibile riconoscere altri formati nemmeno per un'unità di memoria USB compatibile.

Interruzioni trasferimento

Èpossibile che il trasferimento di file possa essere interrotto e richiesto per riavviare il trasferimento per i server con più hop.

In questo scenario, può essere utile utilizzare questa configurazione sulle linee vty:

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

La configurazione precedente garantisce che la sessione di trasferimento non venga eliminata, anche se il pacchetto di controllo viene scartato nel percorso o se il pacchetto richiede troppo tempo per essere riconosciuto.

Al termine del trasferimento, si consiglia di rimuovere la configurazione dalle linee vty.

Si consiglia sempre di posizionare il file server il più vicino possibile al dispositivo.

Server TFTP intermedio.

I dispositivi Cisco possono essere utilizzati come server TFTP temporale per trasferimenti che non possono essere eseguiti direttamente su un file server locale.

Sul dispositivo (con il file che richiede l'estrazione) è possibile eseguire il comando:

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

Dal dispositivo configurato come client, è possibile eseguire i comandi visualizzati nella sezione TFTP.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).