# Solucionar problemas de recarregamento inesperado nas plataformas Cisco IOS®/Cisco IOS® XE com TAC

## Contents



## Introduction

Este documento descreve os arquivos necessários para determinar a causa de uma recarga inesperada no Cisco IOS®/Cisco IOS XE e carregá-los em um caso TAC. As implantações de SDWAN não são discutidas.

## Prerequisites

### Requirements

- Este documento se aplica aos roteadores e switches Cisco que executam o software Cisco IOS/Cisco IOS XE.
- Para coletar os arquivos descritos neste documento, o dispositivo deve estar ativo e estável.
- Para extrair os arquivos por meio do protocolo de transferência, é necessário um servidor (com aplicativo/serviço de transferência de arquivos instalado) com acessibilidade de L3.

- Énecessário um console ou conexão remota via SSH/Telnet para o dispositivo.

  **Note**: Em um evento de recarregamento inesperado, é possível que alguns arquivos não sejam gerados com base na natureza do recarregamento e na plataforma.

# Mostrar arquivos de suporte técnico

A saída do comando **show tech-support** inclui informações gerais sobre o status atual do dispositivo (utilização de memória e CPU, logs, configuração, etc.) e informações sobre os arquivos criados relacionados a quando o evento de recarregamento inesperado ocorreu.

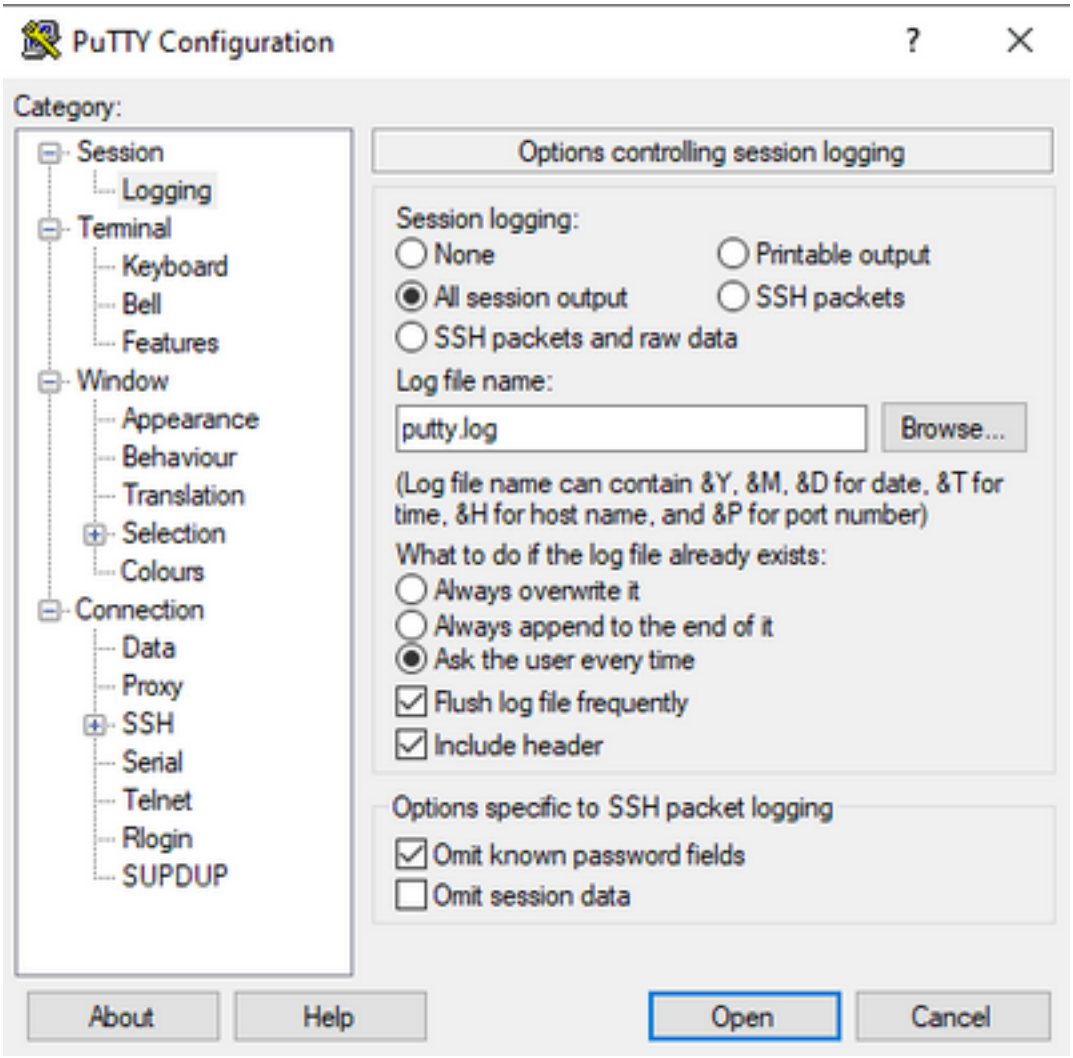
No caso de uma situação de reinicialização inesperada, os pontos principais a serem analisados são:

- A versão atual do Cisco IOS/Cisco IOS XE instalada no dispositivo.
- Configuração do sistema com detalhes de portas, placas e módulos.
- Presença de arquivos adicionais para fornecer uma análise da causa raiz nos sistemas de arquivos.

A saída show tech-support pode ser capturada de duas maneiras diferentes: **registre uma sessão de terminal** ou **crie um arquivo no armazenamento e transfira-o para fora do dispositivo**:

## Registrar uma sessão de terminal

Em Putty, navegue para **Session > Logging** e selecione dentro da guia **Session logging**, selecione a opção **All session output**, como mostrado nesta imagem.




O arquivo é armazenado na pasta Putty por padrão com o nome putty.log. A pasta e o nome do arquivo podem ser alterados com o botão **Browse**.

Uma vez concluída a configuração, a sessão **Putty** precisa ser conectada ao dispositivo através do **Console**, **Telnet** ou **SSH**.

Na sessão do dispositivo, é aconselhável definir o comando **terminal length 0** no modo privilegiado e usar o comando **show tech-support** .

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

**Note**: A execução do comando pode levar alguns segundos. Não interrompa a execução.

## Criar um arquivo no armazenamento

Um arquivo **show tech-support** pode ser criado no dispositivo e armazenado em um dos armazenamentos do sistema de arquivos (interno ou externo). A sintaxe do comando permanece a mesma em todos os dispositivos, mas o sistema de arquivos usado pode ser alterado. O arquivo também pode ser criado diretamente em um servidor externo. Esta seção mostra a sintaxe de um sistema de arquivos local.

Para criar o arquivo dentro da flash, é necessário usar o comando **show tech-support | redirect**

**flash:Showtech.txt** no modo privilegiado:

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

O terminal não pode ser usado por alguns segundos enquanto o arquivo de texto é gerado. Após a conclusão, você pode verificar se a criação do arquivo está correta com o comando **show** [file system]: comando; como o arquivo é de texto simples, o conteúdo pode ser exibido no dispositivo com o comando **more**.

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

Uma vez criado, o arquivo pode ser extraído para um armazenamento externo com um protocolo de transferência de sua escolha (FTP/TFTP/SCP) e compartilhado para análise.

# Arquivo Crashinfo

O arquivo **crashinfo** é um arquivo de texto, que inclui detalhes de depuração que ajudariam a identificar o motivo do travamento. O conteúdo pode variar de acordo com a plataforma. Em geral, ele tem o **buffer de registro** antes do travamento e as funções que eram executadas pelo processador, antes do travamento em um modo codificado. Nas plataformas Cisco IOS, esse é o arquivo mais comum que pode ser encontrado nos sistemas de arquivos após o travamento. Nas plataformas Cisco IOS XE, esse arquivo é gerado quando o travamento acontece apenas no processo IOSd; se qualquer outro processo falhar, o dispositivo não criará um arquivo crashinfo.

Arquivos de informação de travamento podem ser encontrados em flash, bootflash, disco rígido ou armazenamento de informação de travamento na base na plataforma. No caso de plataformas de plano de controle redundantes, os arquivos de travamento podem ser encontrados no supervisor ativo e/ou em espera.

O conteúdo deste arquivo é limitado, pois ele apenas utiliza um instantâneo da memória DRAM antes da reinicialização inesperada e da região da memória dos processos. Arquivos/saídas adicionais podem ser necessários para identificar a causa raiz da reinicialização em alguns casos.

# Arquivos principais

Nas plataformas Cisco IOS XE, quando um processo ou serviço termina sua execução devido a um erro de tempo de execução (e causa uma reinicialização inesperada), um arquivo de núcleo é criado. Este arquivo contém informações de contexto sobre o evento de recarregamento.

Nas plataformas Cisco IOS XE, ele é gerado por padrão quando a reinicialização inesperada é orientada por software. Os arquivos principais podem ser criados em qualquer processo Linux (processos IOSd incluídos).

Arquivos de núcleo são arquivos compactados que contêm as informações de toda a memória em execução usada pelo processo específico que disparou o travamento. Este arquivo requer ferramentas especiais para decodificar, portanto, para manter sua consistência, é necessário extrair o arquivo sem qualquer alteração. Descompactar o arquivo ou extrair as informações como texto (como com o comando **more**) não permite a capacidade de decodificar o conteúdo pela equipe de suporte.

Os arquivos principais geralmente são armazenados na pasta **core**, dentro do **bootflash** ou do **disco rígido**.

A seguir está um exemplo que mostra como o arquivo corefile aparece dentro da pasta core no sistema de arquivos 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
```

> **Note**: Para que o TAC analise com êxito o Corefile, é necessário extrair os arquivos sem qualquer modificação ou alteração.

Para verificar a maneira de extrair este arquivo do dispositivo, navegue para a seção Extrair arquivos.

# Tracelogs

Os registros de rastreamento são registros internos de cada processo no Cisco IOS XE. O diretório tracelogs é criado por padrão e seu conteúdo é substituído periodicamente. Esta pasta pode ser encontrada no **bootflash** ou no **disco rígido**.

A pasta pode ser removida com segurança, embora não seja recomendável, pois ela pode fornecer informações adicionais no caso de um evento de recarregamento inesperado.

Para extrair o conteúdo da pasta, a abordagem mais fácil é criar um arquivo compactado que inclua todos os arquivos tracelogs. Na base na plataforma, você pode usar estes comandos:

Para roteadores Cisco IOS XE:

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

Para switches e controladores sem fio Cisco IOS XE:

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

Tracelogs são arquivos codificados que exigem ferramentas adicionais para decodificar, portanto, é necessário extrair o arquivo compactado quando ele é criado.

Para verificar a maneira de extrair este arquivo do dispositivo, navegue para a seção Extrair arquivos.

# Relatórios do sistema

Um relatório do sistema é um arquivo compactado que coleta a maioria das informações disponíveis na execução do software quando ocorre um recarregamento inesperado. O relatório do sistema contém logs de rastreamento, informações de travamento e arquivos principais. Esse arquivo é criado no caso de uma recarga inesperada em switches Cisco IOS XE e controladores

sem fio.

O arquivo pode ser encontrado no diretório principal do flash de inicialização ou disco rígido.

Ele sempre contém os logs de rastreamento gerados logo antes da reinicialização. No caso de uma recarga inesperada, ele tem arquivos de travamento e arquivos principais do evento.

Este arquivo é compactado, a pasta pode ser descompactada, mas requer ferramentas adicionais para decodificar as informações.

Para verificar a maneira de extrair este arquivo do dispositivo, navegue para a seção Extrair arquivos.

## Núcleos do kernel

Os núcleos do kernel são criados pelo Linux Kernel e não pelos processos do Cisco IOS XE. Quando um dispositivo é recarregado devido a uma falha do kernel, geralmente um núcleo do kernel completo (arquivo compactado) e um resumo dos arquivos do núcleo do kernel (texto simples) são criados.

Os processos que levaram à reinicialização inesperada podem ser revisados, mas é sempre recomendável fornecer o arquivo ao TAC da Cisco para fornecer uma análise completa do motivo do recarregamento.

Os arquivos núcleo do kernel podem ser encontrados no diretório principal do **bootflash** ou do disco rígido.

## Como extrair arquivos

Esta seção descreve a configuração básica necessária para transferir os arquivos necessários da plataforma Cisco IOS/Cisco IOS XE para um cliente de armazenamento externo.

Espera-se que a acessibilidade do dispositivo para o servidor esteja disponível. Se necessário, confirme se não há firewall ou configuração que bloqueie o tráfego do dispositivo para o servidor.

Nenhum aplicativo de servidor específico é recomendado nesta seção.

### TFTP

Para transferir um arquivo sobre **TFTP**, é necessário definir a acessibilidade para o aplicativo de servidor **TFTP**. Nenhuma configuração adicional é necessária.

Por padrão, alguns dispositivos têm a configuração **ip tftp source interface** ativa através da interface de gerenciamento. Se o servidor não estiver acessível através da interface de gerenciamento, execute o comando para remover esta configuração:

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

Depois que a configuração para acessar o servidor estiver concluída, para transferir o arquivo você poderá executar estes comandos:

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

## FTP

Para transferir um arquivo via **FTP**, é necessário definir a acessibilidade para o aplicativo de servidor **FTP**. É necessário configurar o nome de usuário e a senha do **FTP** a partir do dispositivo e do aplicativo do servidor **FTP**. Para definir as credenciais no dispositivo, execute estes comandos:

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

Opcionalmente, você pode configurar uma interface de origem FTP no dispositivo com estes comandos:

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

Quando a configuração para acessar o servidor estiver concluída, para transferir o arquivo você pode executar estes comandos:

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

## SCP

Para transferir um arquivo sobre **SCP**, é necessário definir a acessibilidade para o aplicativo de servidor **SCP**. É necessário configurar o nome de usuário e a senha locais no dispositivo (as credenciais são necessárias para iniciar a transferência) e no aplicativo de servidor **SCP**. Também é necessário ter o **SSH** configurado no dispositivo. Para confirmar se o serviço **SSH** está configurado, execute o 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 definir as credenciais no dispositivo, execute o comando:

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

> **Note**: Caso **TACACS** ou outro serviço seja usado para autenticação de usuário SSH, essas credenciais podem ser usadas se o servidor SCP também tiver as informações do usuário.

Uma vez concluída a configuração, para transferir o arquivo você pode executar estes comandos:

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

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

### USB

A transferência de arquivos através da flash USB não exige acessibilidade a qualquer servidor externo na rede, mas exige acesso físico ao dispositivo.

Todos os dispositivos físicos com Cisco IOS/Cisco IOS XE têm portas USB que podem ser usadas como armazenamento externo.

Para confirmar se a unidade flash USB é reconhecida, execute o 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:
```

> **Observação: os** dispositivos Cisco IOS/Cisco IOS XE suportam as unidades flash USB oficiais da Cisco. Para qualquer flash USB de terceiros, o suporte é limitado.

Quando o flash USB for reconhecido pelo dispositivo no slot apropriado (usbflash0 ou usbflash1) e houver espaço livre suficiente disponível, use estes comandos para transferir o arquivo:

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

## Troubleshoot

Esta seção descreve alguns dos erros e soluções comuns que podem ser encontrados e usados durante a transferência de arquivos (de um dispositivo Cisco IOS ou Cisco IOS XE) para um método externo.

### Confirmar portas abertas

Se o dispositivo mostrar um erro de conexão recusada quando a acessibilidade ao servidor tiver sido confirmada, pode ser útil verificar se as portas no lado do dispositivo estão disponíveis (nenhuma entrada ACL que bloqueie o tráfego) e se as portas no lado do servidor também estão disponíveis (para a última parte, o comando telnet com a porta necessária pode ser usado).

Com base no protocolo usado, execute estes comandos:

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

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

**SCP**

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

> **Note**: As portas anteriores são as portas padrão para cada protocolo; é possível que essas portas sejam alteradas.

Se o comando não fornecer uma porta aberta com êxito, é útil confirmar qualquer erro de configuração (do lado do servidor ou de qualquer firewall no caminho) que possa descartar o tráfego.

## Formato USB

A USB de terceiros não pode ser reconhecida para a maioria dos dispositivos Cisco IOS e Cisco IOS XE.

USB maiores que 4 GB não podem ser reconhecidos pelos roteadores e switches Cisco IOS. USB com tamanho superior a 4 GB podem ser reconhecidos pelas plataformas Cisco IOS XE.

No caso de uma USB de terceiros, ela pode ser testada com a formatação FAT32 ou FAT16. Nenhum outro formato pode ser reconhecido, mesmo para uma unidade de memória USB compatível.

## Interrupções de transferência

Épossível que a transferência de arquivos possa ser interrompida e necessária para iniciar a transferência novamente para servidores com muitos saltos.

Neste cenário, pode ser útil usar esta configuração nas linhas vty:

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

A configuração anterior garante que a sessão de transferência não seja descartada, mesmo se o pacote de controle for descartado no caminho ou se o pacote demorar muito para ser confirmado.

Após a conclusão da transferência, é recomendável remover essa configuração das linhas vty.

Ésempre recomendável colocar o servidor de arquivos o mais próximo possível do dispositivo.

## Intermediate TFTP Server (Servidor TFTP intermediário).

Os dispositivos Cisco podem ser usados como um servidor TFTP temporal para transferências que não podem ser feitas diretamente a um servidor de arquivos local.

No dispositivo (com o arquivo que requer extração) você pode executar o comando:

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

A partir do dispositivo configurado como um cliente, você pode executar os comandos que aparecem na seção TFTP.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.