Dépannage des rechargements inattendus sur les plates-formes IOS avec TAC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
- Afficher les fichiers d'assistance technique
  - Consigner une session de terminal
  - Créer un fichier dans le stockage
- Fichier Crashinfo
- Fichiers principaux
- Tracelogs
- Rapports système
- Noyaux du noyau
- Comment extraire des fichiers
  - TFTP
  - FTP
  - SCP
  - USB
- Dépannage
  - Confirmer les ports ouverts
  - Format USB
  - Interruptions de transfert
  - Serveur TFTP intermédiaire

Introduction

Ce document décrit les fichiers requis pour déterminer la cause d'un rechargement inattendu dans Cisco IOS®/ XE et les télécharger dans un dossier TAC.

Conditions préalables

Exigences

- Ce document s'applique aux routeurs et commutateurs Cisco qui exécutent le logiciel Cisco IOS®/Cisco IOS® XE.
- Afin de collecter les fichiers décrits dans ce document, le périphérique doit être opérationnel et stable.
- Afin d'extraire les fichiers via le protocole de transfert, un serveur (avec application/service

de transfert de fichiers installé) avec l'accessibilité de couche 3 est nécessaire.
- Une connexion console ou à distance via SSH/Telnet au périphérique est nécessaire.
- Les déploiements SD-WAN ne sont pas abordés.

Remarque : Dans un événement de rechargement inattendu, il est possible que certains fichiers ne soient pas générés en fonction de la nature du rechargement et de la plate-forme.

Afficher les fichiers d'assistance technique

La sortie de la commande show tech-support inclut des informations générales sur l'état actuel du périphérique (utilisation de la mémoire et du CPU, journaux, configuration, etc.), et des informations sur les fichiers créés liés au moment où l'événement de rechargement inattendu a eu lieu.

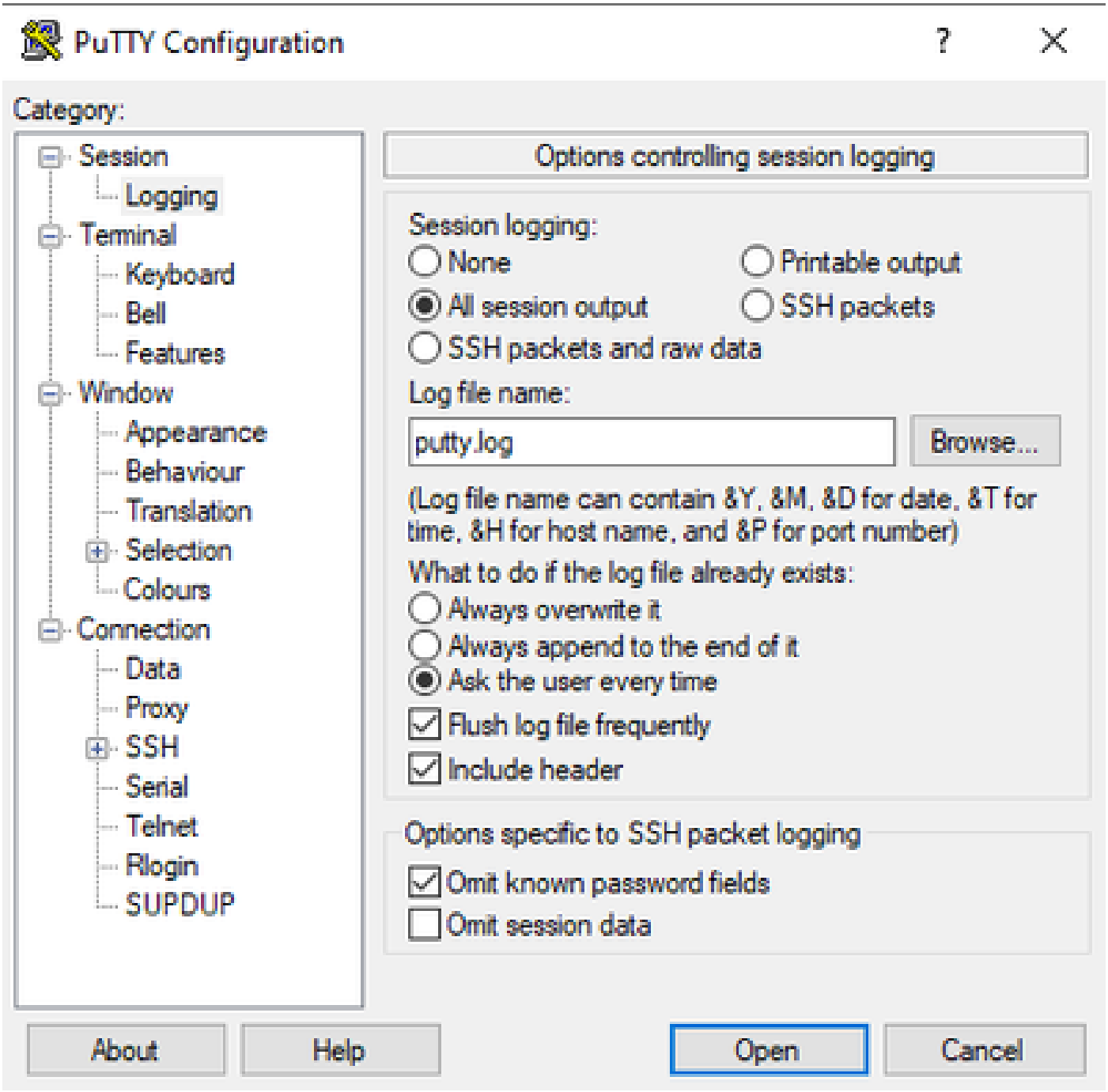
En cas de redémarrage inattendu, les points clés à examiner sont les suivants :

- La version actuelle de Cisco IOS/Cisco IOS XE installée sur le périphérique.
- Configuration du système avec des détails sur les ports, les cartes et les modules.
- Présence de fichiers supplémentaires pour fournir une analyse de la cause première dans les systèmes de fichiers.

Le résultat de la commande show tech-support peut être capturé de deux manières différentes : consignez une session de terminal ou créez un fichier dans le stockage et transférez-le hors du périphérique.

Consigner une session de terminal

Dans Putty, accédez à Session > Logging et sélectionnez dans l'onglet Session logging, sélectionnez l'option All session output, comme illustré dans cette image.



Le fichier est stocké dans le dossier Putty par défaut avec le nom putty.log. Le dossier et le nom du fichier peuvent être modifiés avec le bouton Browse.

Une fois la configuration terminée, la session Putty doit être connectée au périphérique via Console, Telnet ou SSH.

Dans la session de périphérique, il est conseillé de définir la commande terminal length 0 en mode privilégié, puis d'utiliser la commande show tech-support.

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

Remarque : L'exécution de la commande peut prendre quelques secondes. N'interrompez pas l'exécution.

Créer un fichier dans le stockage

Un fichier show tech-support peut être créé sur le périphérique et stocké dans l'un des systèmes de fichiers de stockage (interne ou externe). La syntaxe de la commande reste la même sur tous les périphériques, mais le système de fichiers utilisé peut être modifié. Le fichier peut également être créé directement sur un serveur externe. Cette section présente la syntaxe d'un système de fichiers local.

Afin de créer le fichier dans la mémoire flash, il est nécessaire d'utiliser la commande show tech-support | redirect flash:Showtech.txt en mode privilégié :

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

Le terminal ne peut pas être utilisé pendant quelques secondes pendant la génération du fichier texte. Une fois qu'il est terminé, vous pouvez vérifier si la création du fichier est correcte avec la commande show [file system] : commande ; étant donné que le fichier est un fichier texte brut, le contenu peut être affiché sur le périphérique à l'aide de la commande more.

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

Une fois le fichier créé, il peut être extrait vers un stockage externe avec un protocole de transfert de choix (FTP/TFTP/SCP) et partagé pour analyse.

Fichier Crashinfo

Le fichier crashinfo est un fichier texte, qui inclut des détails de débogage qui permettent d'identifier la raison de l'incident. Le contenu peut varier d'une plate-forme à l'autre. En général, il dispose de la mémoire tampon de journalisation avant la panne et des fonctions qui étaient exécutées par le processeur, avant la panne dans un mode codé. Sur les plates-formes Cisco IOS, il s'agit du fichier le plus courant qui se trouve dans les systèmes de fichiers après la panne. Sur les plates-formes Cisco IOS XE, ce fichier est généré lorsque la panne se produit uniquement dans le processus IOSd ; si un autre processus échoue, le périphérique ne crée pas de fichier crashinfo.

Les fichiers Crashinfo se trouvent sous flash, bootflash, disque dur ou stockage crashinfo dans base sur la plate-forme. Dans le cas de plates-formes de plan de contrôle redondantes, les fichiers de panne se trouvent dans le superviseur actif et/ou en veille.

Le contenu de ce fichier est limité, car il ne prend qu'un instantané de la mémoire DRAM avant le redémarrage inattendu et la zone mémoire des processus. Des fichiers/sorties supplémentaires peuvent être nécessaires pour identifier la cause première du redémarrage dans certains cas.

Fichiers principaux

Sur les plates-formes Cisco IOS XE, lorsqu'un processus ou un service termine son exécution en raison d'une erreur d'exécution (et provoque un redémarrage inattendu), un fichier principal est créé. Ce fichier contient des informations contextuelles sur l'événement de rechargement.

Sur les plates-formes Cisco IOS XE, il est généré par défaut lorsque le redémarrage inattendu est piloté par le logiciel. Les fichiers de base peuvent être créés sous n'importe quel processus Linux (processus IOSd inclus).

Les fichiers Core sont des fichiers compressés qui contiennent les informations de toute la mémoire en cours d'exécution utilisée par le processus spécifique qui a déclenché le plantage. Ce fichier nécessite des outils spéciaux pour le décodage, par conséquent, pour maintenir sa cohérence, il est nécessaire d'extraire le fichier sans aucune modification. La décompression du fichier ou l'extraction des informations sous forme de texte (par exemple avec la commande more) ne permet pas à l'équipe de support de décoder le contenu.

Les fichiers principaux sont généralement stockés dans le dossier principal, à l'intérieur du bootflash ou du disque dur.

Voici un exemple qui montre comment le fichier core apparaît dans le dossier core du système de fichiers 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
```



Remarque : Pour que le centre d'assistance technique puisse analyser correctement le fichier de base, il est nécessaire d'extraire les fichiers sans aucune modification.

Afin de vérifier la façon d'extraire ce fichier du périphérique, naviguez jusqu'à la section Extract Files.

Tracelogs

Les journaux de suivi sont des journaux internes de chaque processus dans Cisco IOS XE. Le répertoire tracelogs est créé par défaut et son contenu est régulièrement remplacé. Ce dossier se trouve dans le bootflash ou sur le disque dur.

Le dossier peut être supprimé en toute sécurité, bien qu'il ne soit pas recommandé car il peut fournir des informations supplémentaires en cas d'événement de rechargement inattendu.

En fonction de l'état du dépannage, il serait nécessaire d'écraser les fichiers tracelogs les plus anciens avec les plus récents ou de collecter les plus anciens. Si les derniers journaux de suivi sont nécessaires, la commande suivante est utilisée :

```
# request platform software trace rotate all
```

Afin d'extraire le contenu du dossier, l'approche la plus simple est de créer un fichier compressé qui inclut tous les fichiers tracelogs. Dans la base sur la plate-forme, vous pouvez utiliser ces commandes :

Pour les routeurs Cisco IOS XE :

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

Pour les commutateurs Cisco IOS XE et les contrôleurs sans fil :

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

Les journaux de suivi sont des fichiers codés qui nécessitent des outils supplémentaires pour le décodage. Par conséquent, il est nécessaire d'extraire le fichier compressé au fur et à mesure de sa création.

Pour vérifier la façon d'extraire ce fichier du périphérique, accédez à la section Extract Files.

Rapports système

Un rapport système est un fichier compressé qui collecte la plupart des informations disponibles dans l'exécution du logiciel lorsqu'un rechargement inattendu se produit. Le rapport système contient des journaux de suivi, des infos de panne et des fichiers de base. Ce fichier est créé en cas de rechargement inattendu sur les commutateurs Cisco IOS XE et les contrôleurs sans fil.

Le fichier se trouve dans le répertoire principal du bootlfash ou du disque dur.

Il contient toujours les journaux de suivi générés juste avant le redémarrage. Dans le cas d'un rechargement inattendu, il a des fichiers de plantage et des fichiers de base de l'événement.

Ce fichier est un fichier compressé, le dossier peut être décompressé, mais il nécessite des outils

supplémentaires pour décoder les informations.

Afin de vérifier la façon d'extraire ce fichier du périphérique, naviguez jusqu'à la section Extract Files.

Noyaux du noyau

Les coeurs du noyau sont créés par le noyau Linux et non par les processus Cisco IOS XE. Lorsqu'un périphérique se recharge en raison d'une défaillance du noyau, un noyau complet (fichier compressé) et un résumé des fichiers du noyau (texte brut) sont généralement créés.

Les processus qui ont conduit au redémarrage inattendu peuvent être revus, mais il est toujours recommandé de fournir le fichier au TAC Cisco afin de fournir une analyse complète de la raison du redémarrage.

Les fichiers du noyau se trouvent dans le répertoire principal du bootflash ou du disque dur.

Comment extraire des fichiers

Cette section décrit la configuration de base requise pour transférer les fichiers requis de la plate-forme Cisco IOS/Cisco IOS XE vers un client de stockage externe.

L'accessibilité du périphérique au serveur est attendue. Si nécessaire, vérifiez qu'aucun pare-feu ou configuration ne bloque le trafic du périphérique vers le serveur.

Aucune application serveur spécifique n'est recommandée dans cette section.

TFTP

Afin de transférer un fichier sur TFTP, il est nécessaire de définir l'accessibilité à l'application du serveur TFTP. Aucune configuration supplémentaire n'est requise.

Par défaut, certains périphériques ont la configuration d'interface source ip tftp active via l'interface de gestion. Si le serveur n'est pas accessible via l'interface de gestion, exécutez la commande afin de supprimer cette configuration :

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

Une fois la configuration pour atteindre le serveur terminée, afin de transférer le fichier, vous pouvez exécuter ces commandes :

```
#copy
      :<file> tftp:
```

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

FTP

Pour transférer un fichier via FTP, il est nécessaire de définir l'accessibilité à l'application du serveur FTP. Vous devez configurer le nom d'utilisateur et le mot de passe FTP à partir du périphérique et de l'application du serveur FTP. Afin de définir les informations d'identification sur le périphérique, exécutez ces commandes :

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

Vous pouvez éventuellement configurer une interface source FTP sur le périphérique à l'aide des commandes suivantes :

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

Une fois la configuration pour atteindre le serveur terminée, afin de transférer le fichier, vous pouvez exécuter ces commandes :

```
#copy

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

SCP

Afin de transférer un fichier sur SCP, il est nécessaire de définir l'accessibilité à l'application du serveur SCP. Il est nécessaire de configurer le nom d'utilisateur et le mot de passe locaux sur le périphérique (des informations d'identification sont nécessaires pour démarrer le transfert) et sur l'application du serveur SCP. Il est également nécessaire de configurer SSH sur le périphérique. Afin de confirmer que le service SSH est configuré, exécutez la commande suivante :

```
#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
```

Afin de définir les informations d'identification sur le périphérique, exécutez la commande :

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

Remarque : Si TACACS ou un autre service est utilisé pour l'authentification de l'utilisateur SSH, ces informations d'identification peuvent être utilisées si le serveur SCP dispose également des informations de l'utilisateur.

Une fois la configuration terminée, afin de transférer le fichier, vous pouvez exécuter ces commandes :

```
#copy

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

USB

Le transfert de fichiers via la mémoire flash USB ne nécessite pas l'accessibilité à un serveur externe sur le réseau, mais nécessite un accès physique au périphérique.

Tous les périphériques physiques équipés de Cisco IOS/Cisco IOS XE disposent de ports USB pouvant être utilisés comme stockage externe.

Afin de confirmer que le lecteur flash USB est reconnu, exécutez la commande 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:
```

Remarque : les périphériques Cisco IOS/Cisco IOS XE prennent en charge les lecteurs flash USB Cisco officiels. Pour toute mémoire flash USB tierce, la prise en charge est limitée.

Une fois que la mémoire flash USB est reconnue par le périphérique dans le logement approprié (usbflash0 ou usbflash1) et qu'il y a suffisamment d'espace libre disponible, utilisez ces commandes pour transférer le fichier :

```
#copy

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

Dépannage

Cette section décrit quelques-unes des erreurs courantes et des solutions de contournement qui peuvent être trouvées et utilisées lors du transfert de fichiers (à partir d'un périphérique Cisco IOS ou Cisco IOS XE) vers une méthode externe.

Confirmer les ports ouverts

Si le périphérique affiche une erreur de refus de connexion lorsque l'accessibilité au serveur a été confirmée, il peut être utile de vérifier que les ports côté périphérique sont disponibles (aucune entrée de liste de contrôle d'accès qui bloque le trafic) et que les ports côté serveur sont également disponibles. Pour la dernière partie, la commande telnet avec le port requis peut être utilisée.

En fonction du protocole utilisé, exécutez ces commandes :

<#root>

TFTP

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

FTP

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

SCP

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

Remarque : Les ports précédents sont les ports par défaut de chaque protocole. Il est possible de modifier ces ports.

Si la commande ne fournit pas un port ouvert réussi, il est utile de confirmer toute erreur de configuration du côté du serveur ou de tout pare-feu dans le chemin) qui peut supprimer le trafic.

Format USB

Les périphériques USB tiers ne peuvent pas être reconnus pour la plupart des périphériques Cisco IOS et Cisco IOS XE.

Les routeurs et commutateurs Cisco IOS ne peuvent pas reconnaître un port USB de plus de 4 Go. Les plates-formes Cisco IOS XE peuvent reconnaître les ports USB dont la taille dépasse 4 Go.

Dans le cas d'un USB tiers, il peut être testé avec le formatage FAT32 ou FAT16. Aucun autre format ne peut être reconnu, même pour un lecteur de mémoire USB compatible.

Interruptions de transfert

Il est possible que le transfert de fichiers soit interrompu et qu'il soit nécessaire de redémarrer le transfert pour les serveurs comportant de nombreux sauts.

Dans ce scénario, il peut être utile d'utiliser cette configuration sur les lignes vty :

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

La configuration précédente garantit que la session de transfert n'est pas abandonnée, même si le paquet de contrôle est abandonné sur le chemin ou si l'accusé de réception du paquet prend trop de temps.

Une fois le transfert terminé, il est recommandé de supprimer cette configuration des lignes vty.

Il est toujours recommandé de placer le serveur de fichiers le plus près possible du périphérique.

Serveur TFTP intermédiaire

Les périphériques Cisco peuvent être utilisés comme serveur TFTP temporel pour les transferts qui ne peuvent pas être effectués directement vers un serveur de fichiers local.

Sur le périphérique (avec le fichier qui nécessite l'extraction), vous pouvez exécuter la commande :

```
(config)#tftp-server

      :<file>
```

À partir du périphérique configuré en tant que client, vous pouvez exécuter les commandes qui apparaissent dans la section TFTP.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.