TACを使用したCisco IOS®/Cisco IOS® XEプラットフォームでの予期しないリロードのトラブルシューティング

内容

概要

このドキュメントでは、Cisco IOS®/Cisco IOS XEでの予期しないリロードの原因を特定し、TACケースにアップロードするために必要なファイルについて説明します。SDWANの導入については説明しません。

前提条件

要件

- このドキュメントは、Cisco IOS/Cisco IOS XEソフトウェアが稼働するCiscoルータおよびスイッチに適用されます。
- このドキュメントで説明されているファイルを収集するには、デバイスが稼働していて安定している必要があります。
- 転送プロトコルを介してファイルを抽出するには、L3到達可能性のあるサーバ（ファイル転

送アプリケーション/サービスがインストールされているサーバ）が必要です。
- デバイスへのSSH/Telnet経由のコンソールまたはリモート接続が必要です。

注：予期しないリロードイベントでは、リロードの性質とプラットフォームに基づいて一部のファイルが生成されない可能性があります。

Show Tech-Support Files

show tech-supportコマンドの出力には、デバイスの現在のステータス（メモリおよびCPU使用率、ログ、設定など）に関する一般情報、および予期しないリロードイベントが発生した時期に関連する作成されたファイルに関する情報が含まれます。

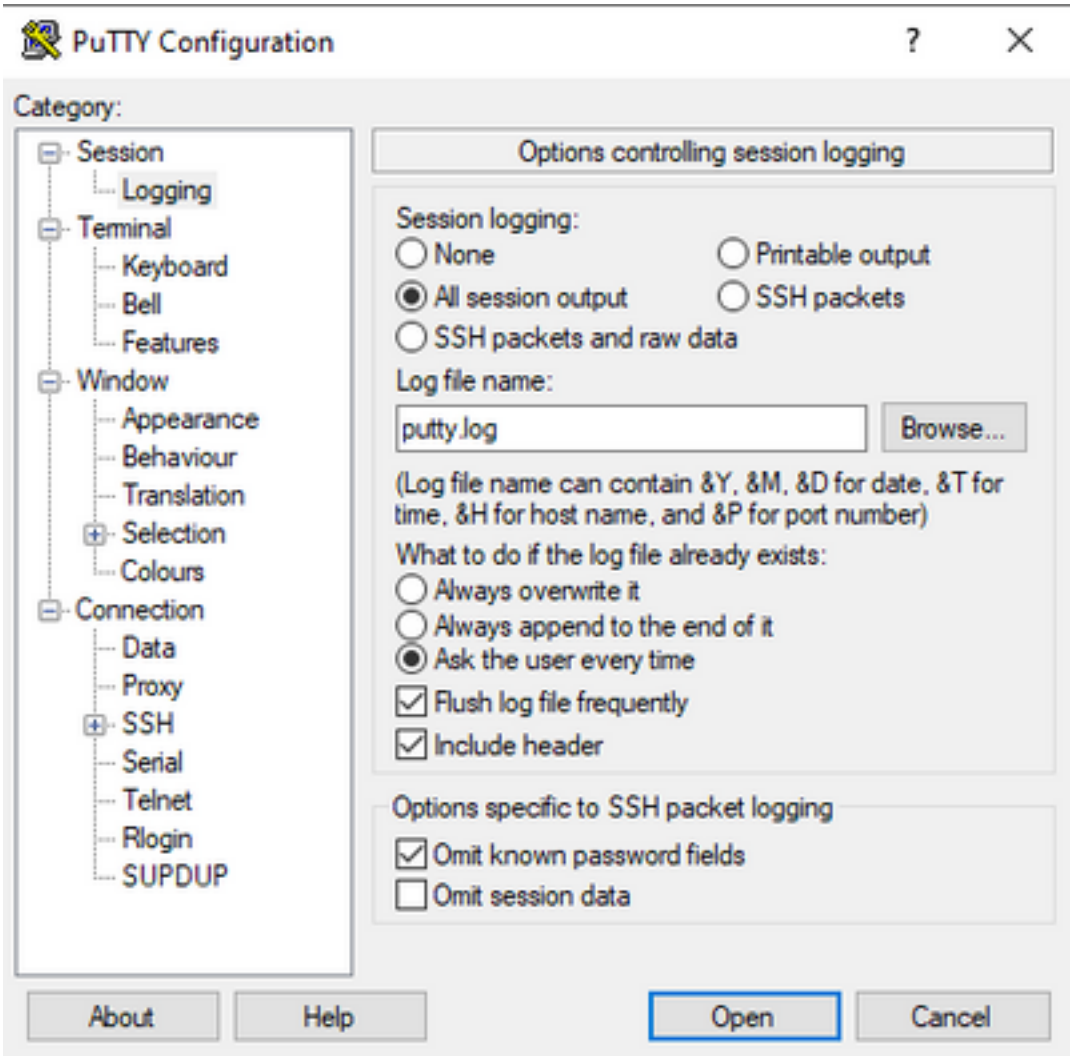
予期しないリブート状況が発生した場合は、次の点を確認してください。

- デバイスにインストールされている現在のCisco IOS/Cisco IOS XEバージョン。
- ポート、カード、およびモジュールを含むシステム設定の詳細。
- ファイルシステム内の根本原因分析を提供する追加ファイルの存在。

show tech-supportの出力は、2つの異なる方法でキャプチャできます。**ターミナルセッションをログに記録するか、ストレージにファイルを作成してデバイスから転送します**。

ターミナルセッションの記録

Puttyで、[Session] > [Logging] に移動し、[Session logging] タブ内を選択して、次の図に示すように[All session output] オプションを選択します。



このファイルは、デフォルトではputty.logという名前でPuttyフォルダに保存されます。ファイルのフォルダと名前は、**Browse**ボタンで変更できます。

設定が完了したら、**Putty**セッションを**コンソール**、**Telnet**、または**SSH**経由でデバイスに接続する必要があります。

デバイスセッションでは、特権モードで**terminal length 0**コマンドを設定してから、**show tech-support**コマンドを使用することをお勧めします（この例では、show tech-supportコマンドを使用します）。

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

注：コマンドの実行には、数秒かかることがあります。実行を中断しないでください。

ストレージにファイルを作成する

show tech-supportファイルをデバイス上に作成し、ファイルシステムストレージ（内部または外部）のいずれかに保存できます。 コマンド構文はすべてのデバイスで同じですが、使用するファイルシステムは変更できます。このファイルは、外部サーバ上に直接作成することもできます。このセクションでは、ローカルファイルシステムの構文を示します。

フラッシュ内にファイルを作成するには、**show tech-support**コマンドを使用する必要があります

|特権モードのredirect flash:Showtech.txt:

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

テキストファイルの生成中は、端末を数秒間使用できません。完了したら、**show** [file system]を使用して、ファイルの作成が正しいかどうかを確認できます。コマンド;ファイルはプレーンテキストファイルであるため、**more**コマンドを使用してデバイスにコンテンツを表示できます。

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

ファイルが作成されると、選択した転送プロトコル(FTP/TFTP/SCP)を使用して外部ストレージに抽出し、分析のために共有できます。

crashinfo ファイル

crashinfoファイルはテキストファイルで、クラッシュの原因を特定するのに役立つデバッグの詳細が含まれています。コンテンツはプラットフォームによって異なります。一般に、クラッシュ前の**ロギングバッファ**と、符号化モードでのクラッシュ前にプロセッサによって実行された機能があります。Cisco IOSプラットフォームでは、これはクラッシュ後にファイルシステムで見つかる最も一般的なファイルです。Cisco IOS XEプラットフォームでは、このファイルはIOSdプロセスでのみクラッシュが発生したときに生成されます。他のプロセスが失敗した場合、デバイスはcrashinfoファイルを作成しません。

Crashinfoファイルは、プラットフォームのフラッシュ、ブートフラッシュ、ハードディスク、またはcrashinfoストレージにあります。冗長コントロールプレーンプラットフォームの場合、クラッシュファイルはアクティブまたはスタンバイのスーパーバイザにあります。

予期しないリブートが発生する前のDRAMメモリとプロセスのメモリ領域のスナップだけを取得するため、このファイルの内容は制限されています。場合によっては、リブートの根本原因を特定するために、追加のファイルや出力が必要になることがあります。

コア ファイル

Cisco IOS XEプラットフォームでは、ランタイムエラーが原因でプロセスまたはサービスの実行が終了し、予期しないリブートが発生すると、コアファイルが作成されます。このファイルには、リロードイベントに関するコンテキスト情報が含まれています。

Cisco IOS XEプラットフォームでは、予期しないリブートがソフトウェアによって行われると、デフォルトで生成されます。コアファイルは、任意のLinuxプロセス（IOSdプロセスを含む）で作成できます。

コアファイルは、クラッシュを引き起こした特定のプロセスによって使用される実行中のすべてのメモリの情報を含む圧縮ファイルです。このファイルをデコードするには特別なツールが必要です。したがって、ファイルの一貫性を維持するには、変更を加えずにファイルを抽出する必要があります。ファイルを解凍するか、テキストとして情報を抽出します(**more**コマンドなど)。サポートチームがコンテンツをデコードすることはできません。

コアファイルは通常、**core**フォルダの**bootflash**または**harddisk**内に保存されます。

次に、ブートフラッシュファイルシステムのcoreフォルダ内にcorefileが表示される例を示します

。

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

> **注：**TACがCorefileを正常に分析するには、変更や変更を加えずにファイルを抽出する必要があります。

デバイスからこのファイルを抽出する方法を確認するには、[Extract Files] セクションに移動します。

トレースログ

トレースログは、Cisco IOS XE内の各プロセスの内部ログです。tracelogsディレクトリはデフォルトで作成され、その内容は定期的に上書きされます。このフォルダは、**bootflash**または**harddisk**にあります。

このフォルダは安全に削除できますが、予期しないリロードイベントが発生した場合に追加情報が得られるため、お勧めできません。

フォルダの内容を抽出する最も簡単な方法は、すべてのtracelogsファイルを含む圧縮ファイルを作成することです。プラットフォームに基づいて、次のコマンドを使用できます。

Cisco IOS XEルータの場合：

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

Cisco IOS XEスイッチおよびワイヤレスコントローラの場合：

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

トレースログはエンコードされたファイルで、デコードに追加のツールが必要なため、圧縮ファイルを作成するときに抽出する必要があります。

デバイスからこのファイルを抽出する方法を確認するには、[Extract Files] セクションに移動します。

システムレポート

システムレポートは、予期しないリロードが発生したときにソフトウェアの実行で利用可能な情報のほとんどを収集する圧縮ファイルです。システムレポートには、tracelogs、crashinfo、およびコアファイルが含まれています。このファイルは、Cisco IOS XEスイッチおよびワイヤレスコントローラで予期しないリロードが発生した場合に作成されます。

このファイルはbootflashまたはharddiskのメインディレクトリにあります。

リブート直前に生成されたトレースログが常に含まれています。予期しないリロードの場合は、

イベントのクラッシュファイルとコアファイルがあります。

このファイルは圧縮ファイルなので、フォルダを解凍できますが、情報をデコードするための追加ツールが必要です。

デバイスからこのファイルを抽出する方法を確認するには、[Extract Files] セクションに移動します。

カーネルコア

カーネルコアは、Cisco IOS XEプロセスではなく、Linuxカーネルによって作成されます。カーネルの障害が原因でデバイスがリロードされると、通常、完全なカーネルコア（圧縮ファイル）とカーネルコア（プレーンテキスト）ファイルの要約が作成されます。

予期しないリブートを引き起こしたプロセスは確認できますが、リロードの原因を完全に分析するには、Cisco TACにこのファイルを提供することを常に推奨します。

カーネルコアファイルは、**bootflash**またはハードディスクのメインディレクトリにあります。

ファイルの抽出方法

このセクションでは、必要なファイルをCisco IOS/Cisco IOS XEプラットフォームから外部ストレージクライアントに転送するために必要な基本設定について説明します。

デバイスからサーバへの到達可能性が利用可能であることが期待されます。必要に応じて、デバイスからサーバへのトラフィックをブロックするファイアウォールまたは設定がないことを確認します。

このセクションでは、特定のサーバアプリケーションを推奨しません。

TFTP

TFTP経由でファイルを転送するには、**TFTP**サーバアプリケーションへの到達可能性を設定する必要があります。追加設定は必要ありません。

デフォルトでは、一部のデバイスでは、管理インターフェイス経由で**ip tftp source interface**設定がアクティブになっています。サーバに管理インターフェイスから到達できない場合は、次のコマンドを実行して、この設定を削除します。

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

サーバに到達するための設定が完了したら、ファイルを転送するために次のコマンドを実行できます。

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

FTP

FTP経由でファイルを転送するには、FTPサーバアプリケーションへの到達可能性を設定する必要があります。デバイスとFTPサーバアプリケーションからFTPユーザ名とパスワードを設定する必要があります。デバイスにクレデンシャルを設定するには、次のコマンドを実行します。

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

必要に応じて、次のコマンドを使用してデバイスにFTP送信元インターフェイスを設定できます。

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

サーバに到達するための設定が完了したら、ファイルを転送するために次のコマンドを実行できます。

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

SCP

SCP経由でファイルを転送するには、SCPサーバアプリケーションへの到達可能性を設定する必要があります。デバイス (転送を開始するにはクレデンシャルが必要) とSCPサーバアプリケーションでローカルユーザ名とパスワードを設定する必要があります。また、デバイスでSSHを設定する必要もあります。SSHサービスが設定されていることを確認するには、次のコマンドを実行します。

```
#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
```

デバイスにクレデンシャルを設定するには、次のコマンドを実行します。

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

> **注：**SSHユーザ認証にTACACSまたは別のサービスを使用する場合、SCPサーバにもユーザ情報があれば、これらのクレデンシャルを使用できます。

設定が完了したら、ファイルを転送するために次のコマンドを実行できます。

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

USB

USBフラッシュを介してファイルを転送する場合、ネットワーク内の外部サーバに到達する必要はありませんが、デバイスに物理的にアクセスする必要があります。

Cisco IOS/Cisco IOS XEを搭載するすべての物理デバイスには、外部ストレージとして使用でき

るUSBポートがあります。

USBフラッシュドライブが認識されていることを確認するには、**show file systems**コマンドを実行します。

```
#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:
```

> **注：**Cisco IOS/Cisco IOS XEデバイスは、公式のCisco USBフラッシュドライブをサポートします。サードパーティ製USBフラッシュのサポートは限られています。

USBフラッシュが適切なスロット（usbflash0またはusbflash1）のデバイスで認識され、使用可能な十分な空き領域が確保されたら、次のコマンドを使用してファイルを転送します。

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

トラブルシュート

このセクションでは、（Cisco IOSデバイスまたはCisco IOS XEデバイスから）ファイルを外部方式に転送する際に検出され、使用される一般的なエラーと回避策について説明します。

開いているポートの確認

サーバへの到達可能性が確認されたときにデバイスでconnection refusedエラーが表示される場合は、デバイス側のポートが使用可能（トラフィックをブロックするACLエントリがない）であること、およびサーバ側のポートも使用可能（最後の部分として、必要なポートを指定したtelnetコマンドを使用できる）であることを確認すると役立ちます。

使用するプロトコルに基づいて、次のコマンドを実行します。

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

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

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

> **注：**以前のポートは各プロトコルのデフォルトポートであり、これらのポートは変更できます。

このコマンドで正常なオープンポートが提供されない場合は、トラフィックをドロップする可能性のある設定ミス（サーバ側またはパス内のファイアウォールから）を確認すると役立ちます。

USBフォーマット

サードパーティ製USBは、ほとんどのCisco IOSデバイスおよびCisco IOS XEデバイスで認識されません。

4 GBを超えるUSBは、Cisco IOSルータおよびスイッチでは認識されません。Cisco IOS XEプラットフォームでは、4 GBを超えるサイズのUSBを認識できます。

サードパーティ製USBの場合は、FAT32またはFAT16フォーマットでテストできます。互換性のあるUSBメモリドライブでも、その他の形式は認識されません。

転送の中断

ホップ数の多いサーバでは、ファイル転送が中断され、転送を再開する必要が生じる可能性があります。

このシナリオでは、vty回線で次の設定を使用すると便利です。

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

前述の設定では、制御パケットがパスで廃棄されたり、パケットの確認応答に時間がかかりすぎたりしても、転送セッションが廃棄されないことが保証されます。

転送が完了したら、vty回線からこの設定を削除することをお勧めします。

ファイルサーバは常にデバイスにできるだけ近い場所に配置することを推奨します。

中間TFTPサーバ。

Ciscoデバイスは、ローカルファイルサーバに直接転送できない転送用の一時的なTFTPサーバとして使用できます。

デバイスで（抽出が必要なファイルを含む）、次のコマンドを実行できます。

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

クライアントとして設定されているデバイスから、「TFTP」セクションに表示されるコマンドを実行できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。