

ソフトウェア強制クラッシュについて

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[考えられる原因](#)

[トラブルシューティング](#)

[設定手順](#)

[TFTP サーバ ホストの設定手順](#)

[TAC のサービス リクエストをオープンする場合に収集すべき情報](#)

[関連情報](#)

はじめに

このドキュメントでは、ソフトウェア強制クラッシュの原因として最も頻度の高いものについて説明し、さらに、トラブルシューティングのために収集する必要がある情報について説明します。ソフトウェア強制クラッシュの TAC サービス リクエストをオープンする場合は、収集するように要求される情報は、問題のトラブルシューティングに必要です。

前提条件

要件

このドキュメントの読者は次のトピックについて理解している必要があります。

- [ルータのクラッシュのトラブルシューティング](#)方法。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

ルータによって深刻で修復不可能なエラーが検出されると、ソフトウェアによる強制クラッシュ

が発生し、破損したデータの送信を防止するためにリロードが実行されます。ソフトウェア強制クラッシュの大部分は、Cisco IOS®ソフトウェアのバグが原因で発生しますが、一部のプラットフォーム (古いCisco 4000など) ではソフトウェア強制クラッシュとしてハードウェアの問題が報告される場合があります。

ルータの電源のオフ/オンや手動でのリロードを行っていないければ、`show version` コマンドからの出力が次のように表示されます。

```
Router uptime is 2 days, 21 hours, 30 minutes
System restarted by error - Software-forced crash, PC 0x316EF90 at 20:22:37 edt
System image file is "flash:c2500-is-1.112-15a.bin", booted via flash
```

ご使用のシスコデバイスの`show version`コマンドの出力データがあれば、[Cisco CLI Analyzer](#)(登録ユーザ専用)を使用して、潜在的な問題と修正を表示できます。

考えられる原因

次の表に、ソフトウェア強制クラッシュの考えられる原因を示します。

原因

説明

プロセッサは無限ループを避けるためにタイマーを使用していますが、これが原因でルータに失敗した場合、システムのリロードにつながります。ソフトウェア強制クラッシュドッグ タイムアウトについては、ウォッチドッグ タイムアウトのトラブルシューティングは必ずしも関係があるわけではありません。このタイプのソフトウェア強制クラッシュ

[ウォッチドッグ タイムアウト](#)

```
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Exec
```

```
and
```

```
*** System received a Software forced crash ***
signal = 0x17, code = 0x24, context= 0x60ceca60
```

メモリ不足

ルータはメモリが極端に少なくなると、自らリロードしてソフトウェア強制クラッシュメッセージが表示されます。

```
%SYS-2-MALLOCFAIL: Memory allocation of 734 bytes failed from 0x6015EC84,
pool Processor, alignment 0
```

ブートアップの際に、ルータによって Cisco IOS ソフトウェア イメージが破損しているクラッシュとして報告されます。

```
Error : compressed image checksum is incorrect 0x54B2C70A
Expected a checksum of 0x04B2C70A
```

ソフトウェア イメージの破損

```
*** System received a Software forced crash ***
```

```
signal= 0x17, code= 0x5, context= 0x0
```

```
PC = 0x800080d4, Cause = 0x20, Status Reg = 0x3041f003
```

これは、ルータへの転送の際に実際に破損した Cisco IOS ソフトウェア イメージにより行うことができます。[プラットフォームの ROMmon 復旧方法については、Cisco 7200、7300 ルータの ROMmon 復旧手順を参照してください。]また、この現象は、メモリのハードウェアクラッシュの原因になったエラーは、多くの場合、プロセッサ ハードウェアによって検出を識別し、メッセージを出力して、障害に関する情報を保存し、システムを再起動し

その他の障害

出してクラッシュダンプ機能呼び出すクラッシュがあります。これは、本当の「ソフトウェア強制クラッシュ」が `crashdump` 関数が呼び出されたときに出力される再起動理由 (SIGTRAP) ではなく、これらは「SIGTRAP」例外と呼ばれています。その他のすべての点は、SIGTRAP

トラブルシューティング

ソフトウェア強制クラッシュは、通常は Cisco IOS ソフトウェアのバグによって発生します。メモリ割り当てエラーメッセージがログに表示される場合は、「メモリ問題のトラブルシューティング」を参照してください。

メモリ割り当てエラーのエラーメッセージが表示されず、ソフトウェア強制クラッシュ後にルータを手動でリロードまたは電源のオフ/オンを行っていない場合は、[Cisco CLI Analyzer \(登録ユーザ専用\)](#)を使用して既知のバグIDを検索します。このツールには、従来のスタックデコーダツールの機能が組み込まれています。

以下に例を挙げます。

1. ルータから `show stack` の出力を収集します。
2. [Cisco CLI Analyzer\(登録ユーザ専用\)](#) ツールに移動します。
3. プルダウンメニューから `[show stack]` を選択します。
4. 収集した出力を貼り付けます。
5. `[Submit]` をクリックします。 `show stack` コマンドからのデコード出力が既知のソフトウェアバグと一致する場合は、ソフトウェア強制クラッシュの原因である可能性が最も高いソフトウェアバグのバグ ID が送信されます。
6. バグ ID のハイパーリンクをクリックすると、Cisco Bug Toolkit ([登録ユーザ専用](#)) からの [バグ詳細情報が表示されます。この情報は、バグ ID が一致しているかどうかの判別に役立ちます。](#)

エラーと一致するバグ ID が特定されたら、「fixed in」フィールドを参照して、そのバグの修正が入っている最初の Cisco IOS ソフトウェアバージョンを確認します。

バグ ID が不明な場合、または問題の修正が入っている Cisco IOS ソフトウェアバージョンが不明な場合は、Cisco IOS ソフトウェアをリリース群の最新バージョンにアップグレードします。最新バージョンには多数のバグに対する修正プログラムが含まれているため、この方法は有効です。問題が解決しなくても、ソフトウェアが最新バージョンになっていることによって、バグの報告や解決プロセスが簡単かつ迅速になります。

Cisco CLI Analyzerを使用した後、未解決の不具合が疑われる、または明確に特定した場合は、TACサービスリクエストをオープンして、不具合を解決するための追加情報を提供し、不具合が最終的に解決された場合の通知を迅速に行うことをお推奨します。

設定手順

問題が新規のソフトウェアバグであることが確認された場合は、シスコ TAC エンジニアからお客様に、ルータでコアダンプが収集されるように設定することをお願いする場合があります。コアダンプは、ソフトウェアバグの修正方法を突きとめるために必要になることがあります。

コアダンプでできるだけ有用な情報を収集するため、隠しコマンド `debug sanity` を使用することをお勧めします。これにより、システム内で使用されるすべてのバッファについて、それらの割り当て時および解放時に正常性がチェックされます。`debug sanity` コマンドは特権 EXEC モード (イネーブルモード) で発行する必要があるため、多少 CPU を必要としますが、ルータの機能に大きな影響を与えることはありません。サニティチェックを無効にするには、`undebug sanity` 特権 EXEC コマンドを使用します。

ルータのメインメモリが 16 MB 以下の場合は、Trivial File Transfer Protocol (TFTP; トリビアルフファイル転送プロトコル) を使用してコアダンプを収集できます。ルータのメインメモリが 16 MB を超える場合は、File Transfer Protocol (FTP; ファイル転送プロトコル) を使用することをお勧めします。このセクションの設定手順を使用します。または、コアダンプの作成を参照して

ください。

ルータを設定するには、次の手順を実行します。

1. `configure terminal` コマンドを使用してルータを設定します。
2. 「`exception dump n.n.n.n`」と入力します。ここで、`n.n.n.n` はリモート Trivial File Transfer Protocol (TFTP) サーバホストの IP アドレスです。
3. 設定モードを終了します。

TFTP サーバホストの設定手順

次の手順を実行して、TFTP サーバホストを設定します。

1. 任意のエディタを使用して、リモートホストの `/tftpboot` ディレクトリの下にファイルを作成します。ファイル名は Cisco ルータのホスト名-`core` です。
2. UNIX システムでは、「ホスト名-`core`」の権限モードを `666` に変更し、グローバルに互換性のあるものとします。TFTP セットアップを検査するには、そのファイルに `copy running-config tftp` コマンドを使用します。
3. `/tftpboot` の下に `16 MB` を超える空きディスク領域があることを確認します。システムがクラッシュすると、`exception dump` コマンドによって上記のファイルへの出力が作成されます。ルータのメインメモリが `16 MB` を超える場合は、File Transfer Protocol (FTP) または Remote Copy Protocol (RCP) を使用してコアダンプを取得する必要があります。ルータで、次のように設定します。

```
exception protocol ftp
exception dump n.n.n.n
ip ftp username ip ftp password ip ftp source-interface exception core-file
```

コアダンプを収集したら、`ftp://ftp-sj.cisco.com/incoming` にアップロードし (UNIX の場合は `pftp ftp-sj.cisco.com` と入力してから `cd incoming` と入力し)、所有者にこの事例とファイル名を通知します。

TAC のサービスリクエストをオープンする場合に収集すべき情報

上記のトラブルシューティング方法を実行した後も、依然としてサポートが必要で、Cisco TAC でサービスリクエストをオープンする場合は、以下の情報を収集してください。

- `show technical-support` の出力 : `show technical-support` コマンドの出力には、ルータの現在の状態に関する情報が含まれます。
- コンソールログ : 通常は `syslog` サーバに保存されるコンソールログは、クラッシュ前にルータ上で収集可能な最も重要な情報になります。
- [crashinfo ファイル \(存在する場合 \)](#) : [トラブルシューティングを成功させるためには、crashinfo 機能を使用するには、バージョンがネットワークの他のニーズを満たしている必要があります。crashinfo 機能を使用するには、「情報の取得」を参照するか、Software Advisor \(登録ユーザ専用 \) ツールを使用してください。旧バージョンの IOS ソフトウェアリリースに切り替えることによってバグが修正されることもあります。](#)

情報をサービスリクエストに添付するには、[TAC Service Request Tool \(登録ユーザ専用 \)](#) を使用してツールに添付ファイルとして、メッセージの件名にサービスリクエスト番号を付けて attach@cisco.com宛てに送信してください。
注意 : 問題の根本原因を特定するために必要な重要な情報が失われる可能性があるため、上記の情報を収集してください。

関連情報

- [トラブルシューティング : ルータのクラッシュ](#)
- [Crashinfo ファイルからの情報の取得](#)
- [コア ダンプの作成](#)
- [メモリの問題に関するトラブルシューティング](#)
- [テクニカル サポート - Cisco Systems](#)