

3650/3850スタックマネージャリロードのトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[システムレポートとスイッチレポート](#)

[システムレポートおよびスイッチレポートの収集場所](#)

[システムレポートの重要なセクション](#)

[障害のタイプ](#)

[関連バグ](#)

[スタックケーブルまたはポートに潜在的な問題を診断する](#)

[その他のヒント](#)

[1. Crashinfoディレクトリのアーカイブ](#)

[2. 不安定なスタックの回復](#)

[3. システムレポートの手動生成](#)

[関連情報](#)

はじめに

このドキュメントでは、システムレポートを活用してスタックの問題を診断する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、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。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

システムレポートを使用してクラッシュがないにもかかわらずスタックのリロードをトラブルシューティングする場合、通常はNGWCスイッチングプラットフォームで行われるのは、stackwiseテクノロジーを使用する方法です。現在のドキュメントでは、システムレポートの使用に制限があります。このガイドでは、これらのレポートを利用して、スタック構成の問題で一般的に見られる問題を診断する方法について説明します。このガイドは、スタック機能をサポートするCisco IOS® XEを実行するCatalyst 3650/3850スイッチアーキテクチャに特に焦点を当てています。

Stackwiseテクノロジーに関する問題の大部分は、スタック内のメンバ間の通信の問題に起因します。メンバ間の情報の不整合や接続の切断が発生すると、スタック全体に問題が浸透し、最終的にはスタックマネージャによるリセットが発生する可能性があります。このドキュメントでは、スタックマネージャのリロード、システムレポートの使用、および診断に使用できる関連CLIやさまざまな種類の問題で発生する一般的な障害の種類に焦点を当てます。

システムレポートとスイッチレポート

システムレポートは、スタックの状態を認識する方法に基づくメンバの包括的なレポートです。これはcrashinfo（今後のデバッグのためにメモリをダンプする可能性がある）ではなく、Cisco IOS XEで実行されるさまざまなサービスのログおよびデバッグ情報を含むレポートであり、そのサービスの状態を追跡するために開発を行う際に役立ちます。システムレポートは、スタックマネージャによってスイッチがリロードされた場合、プロセスのクラッシュが発生した場合、または実稼働中にユーザが手動で生成した場合に生成できます。

多くの場合、スタック内の1つのスイッチに障害が発生しても、残りのメンバはそのまま残ります。特定の時点でのスタックの状態に関する情報として収集するために、switch_reportsが導入されました。この機能により、メンバのダウンを検出したときに現在のメンバによって生成されます。switch_reportは、メンバがスタックの現在の状態をどのように認識しているかを示すローカルレポートです。

 注：これらのレポートは書き込みと圧縮が行われるため、moreを指定して端末に出力することはできません。ログを表示するには、スイッチから転送して圧縮解除する必要があります。

システムレポートおよびスイッチレポートの収集場所

システムレポートは通常、そのスタックのメンバのcrashinfo：ディレクトリに書き込むことができます。たとえば、xメンバスイッチスタックが存在する場合、各スイッチには独自のcrashinfoディレクトリを作成し、dir crashinfo-xを使用してアクセスできます。ここでxはスタック内のそのメンバに対応します。

```
3850#dir crashinfo-1:
```

```
crashinfo:/のディレクトリ
```

11 -rwx 355 2015年8月14日07:48:17 -04:00 last_systemreport_log

12 -rwx 724015 2014年10月15日07:14:32 -04:00システムレポート_1_20141015-111342-UTC.gz

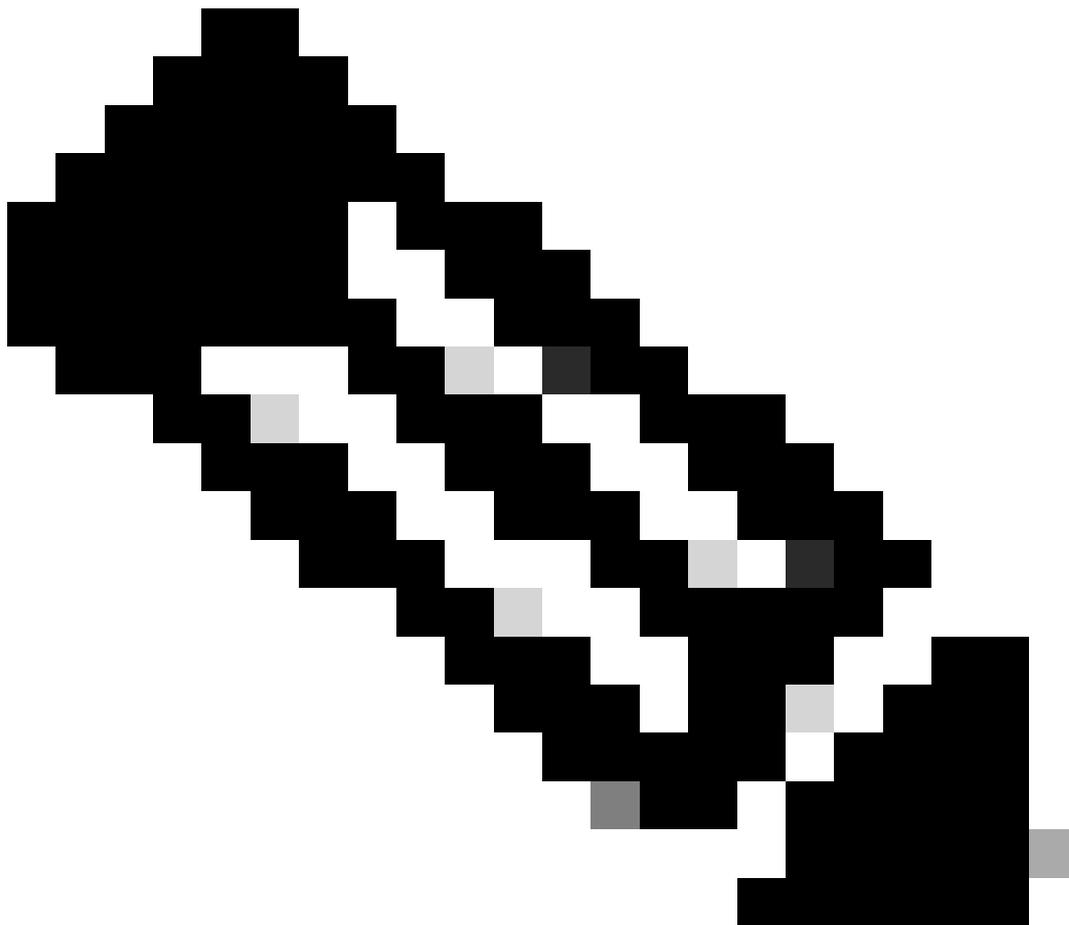
3850#dir crashinfo-2:

crashinfo-2:/のディレクトリ

11 -rwx 357 2015年8月14日07:50:49 -04:00 last_systemreport_log

12 -rwx 751340 2014年10月15日06:41:12 -04:00システムレポート_1_20141015-104022-UTC.gz

 注：スタック内のすべてのスイッチについて、dir crashinfo-xの出力を必ず収集してください。これは、show techでは使用可能なファイルシステムやcrashinfoファイルをリストできないためです。そのスタック内のすべてのメンバーの全体像を把握することが重要です。更新：新しいCisco IOS XEリリース> 3.6Eでは、show techでdir crashinfo: + show file systemsの出力を反映できます。Cisco Bug ID [CSCun50428](#)を参照してください。



注：シスコのバグ情報およびツールへのアクセスは、登録ユーザのみ可能です。

システムレポートの重要なセクション

TACの観点から見ると、特定の問題のイベントの診断に役立つ、システムレポート内で最も一般的に表示されるエントリの一部を次に示します。ここに含まれている他のサービスのログもあり、開発担当者はこのログを確認できます。

ログファイル：/mnt/pss/sup_sysmgr_reset.log

これは、リセットが発生した理由を非常に一般的に理解するための短い出力です。これらの原因がどのように変化するかの意味とコンテキストを調べるには、「次のタイプの障害」セクションを参照してください。

ログファイル：Cisco IOS

これは、Cisco IOSd内から維持されるログバッファです。ユーザが発行したコマンドやCisco IOSd内で生成されたsyslogはこのセクションで確認できます。最新のログは、この出力の最後の方にあります。

トレースバッファ：stack-mgr-events

スタックマネージャから見たイベントを追跡します。このイベントには、他のメンバがスタックに参加またはスタックから削除されたときや、メッセージがどのスタックポートを経由して入ってくるかなどがあります。

トレースバッファ：redundancy-timer-ha_mgr

スタック内のスイッチ間のキープアライブイベントを表示します。タイムスタンプは、通信の中断がいつ始まったかを判断するのに役立ちます。

障害のタイプ

このセクションでは、通常スタックマネージャプロセスによって起動されるシステムレポートからよく見られるリセットを取り上げます。スタックマネージャは、スタック内のメンバを管理し、スタック内のスイッチ間のロールの変更を監視できるLinuxプロセスです。スタックマネージャは、初期化またはロールの選択中に問題を検出すると、スタックをリセットするために個々のスイッチにリロード信号を送信できます。次のリストには、それぞれの障害タイプに関連する既知の不具合を示すこともできます。



注：すべてのスタックマネージャリロードがソフトウェアの問題に起因するわけではありません。実際、これらの問題は、コアハードウェアの問題に対する二次的な問題として現れるのが一般的です。

リセット理由： [スタックマネージャ]によって要求されたりセット/リロード。 [ISSU非互換性]

このタイプのリセットは、スタック内のすべてのメンバ間でアクティブの設定を同期しようとしたときに一括同期エラーが発生した場合に表示されます。ログファイルを確認します。Cisco IOSまたはアクティブスイッチのログで、このリセットの原因となった設定を強調表示できます。

リセット理由： サービス[iosd] pid:[xyz]が異常終了しました[11]。

これは、Cisco IOSdプロセスでスイッチがクラッシュしたときに表示されます。crashinfoディレクトリを調べてcrashinfoファイルを見つけます。さらに、コアダンプを使用してこの障害をさらにデバッグできます。

hap_sup_reset : リセット理由 : [stack-manager]によってリセット/リロードが要求されました。
[スタックのマージ]

スタックのマージは、スタックのアクティブスイッチであると認識されているスイッチが2つ以上ある場合に表示されます。この現象は、スタックのリングが破断した場合（つまり、スタックから2本のケーブルが取り外された場合）に、アクティブ側とスタンバイ側の両方が他のメンバとの通信を失った場合に発生します。すでに給電されているスイッチを現在のスタックに追加すると、スタック内にアクティブなスイッチが2つ存在する可能性があるため、スタックのマージが発生する可能性があります。

[Cisco Bug ID CSCuh58098](#) : スタックのケーブル接続に問題があると3850スタックがリロードする

[Cisco Bug ID CSCui56058](#) : スタックケーブルのデバウンスロジックを有効にします

[Cisco Bug ID CSCup53338](#):3850 IOSDのクラッシュ | Signal=SIGSEGV(11) @
pm_port_data_from_swidb

hap_sup_reset : 理由コード : [4]リセット理由 : [スタックマネージャ]によってリセット/リロードが要求されました。[非互換性によるスタックのマージ]

これは、スタック内にアクティブスイッチとスタンバイスイッチが存在する状況で発生します。アクティブスイッチとスタンバイスイッチとの通信が失われると、アクティブスイッチがアップ状態であっても、スタンバイスイッチがアクティブの引き継ぎを試みることができます。

[Cisco Bug ID CSCuo49555](#)

[Cisco Bug ID CSCup58016 \(登録ユーザ専用\)](#):管理ポートでのユニキャストフラッドが原因で3850/3650がクラッシュする

Cisco Bug ID [CSCur07909](#) : [アクティブとスタンバイの接続が失われたことが原因のスタックマージ](#)

リセット理由 : [スタックマネージャ]によって要求されたリセット/リロード。[ASIC投票の後で間違ったネイバーが検出されました]

スイッチはブートアップ中にASICの割り当てに参加し、スタック内の隣接スイッチを決定します。このリセットは、ネイバーが自身を宣言するためにタイマーが時間切れになった場合、またはnbcastカンバセーション中に論理エラーが発生した場合に表示されます。この問題は、スタックケーブルの障害が発生し、交換によって解決された場合に発生します。

[Cisco Bug ID CSCun60777](#):ASICの割り当て後に、誤ったネイバーが原因でスイッチがリロードされる

[Cisco Bug ID CSCud93761](#):ASICの割り当て後にネイバーの誤りが原因でスイッチがリロードされる

[Cisco Bug ID CSCun17506](#) - Amur:ng3k : 同じネイバーが3メンバースタックの両方のスタックポートで見られる

hap_sup_reset : 理由コード : [4] Reset Reason:[stack-manager]によってリセット/リロードが要求されました。[アクティブとスタンバイの両方の喪失]

これは通常、アクティブロールまたはスタンバイロールではないスタックのメンバから見られます。アクティブに障害が発生し、スタックのアクティブロールを引き継ぐスタンバイスイッチがない場合、スタック全体をリセットできます。スタックが不安定な状態であるか、冗長性ポリシーがまだ同期されていない場合は、この状態が発生する可能性があります。これは、アクティブ/スタンバイスイッチがダウンした原因の犠牲者か、冗長性が正しく同期されないことを示している可能性があります。これは、ハーフリング設定でスタックが設定されている場合にも見られません。

[Cisco Bug ID CSCup53882](#):3850スタックのリポート時のメンバスイッチ-[アクティブとスタンバイの両方が失われる]

hap_sup_reset : 理由コード : [1] Reset Reason:[stack-manager]によってリセット/リロードが要求されました。[Keepalive_Timeout]

スタック内のスイッチからキープアライブメッセージが受信されない場合に表示されます。Trace Buffer: redundancy-timer-ha_mgrを調べると、キープアライブメッセージの交換が表示され、通信の中断が始まった時間のパースペクティブが提供されます。スタックの残りの部分からスイッチレポートを収集し、時間枠を通してログを確認すると役立ちます。

hap_sup_reset : リセット理由 : [stack-manager]によってリセット/リロードが要求されました。[リロードコマンド]

これは、非常に直観的なリセットの理由です。スタックマネージャが、CLIまたは管理デバイス(SNMP)を介して外部から起動できるリロード要求を受信した場合に見られます。Cisco Bug ID [CSCuj17317](#)の場合は、reloadコマンドが発行された場合にも表示されます。ログファイルCisco IOSでは、次の情報を確認できます。

```
CMD: 'reload'  
%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload command.  
%STACKMGR-1-RELOAD_REQUEST: 1 stack-mgr: Received reload request for all switches, reason Reload command  
%STACKMGR-1-RELOAD: 1 stack-mgr: Reloading due to reason Reload command
```

関連バグ

[Cisco Bug ID CSCur76872](#) : システムがSDPバッファを使い果たした場合にスタックマネージャがダウンする。

[Cisco Bug ID CSCup49704](#):3850 FEDクラッシュ - SPIチャネルFED_SPI_FLCD、FED_SPI_FASTを待機...

スタックケーブルまたはポートに潜在的な問題を診断する

症状1)スタックケーブルに問題がある兆候は、リセット前のスタックポートのフラッピングによ

って明らかになります。通常は、リセット前のログファイル：Cisco IOSレポートから作業を始めることを推奨します。ここでは、現在のSW2とスタンバイSW1の両方に登録されているスタックポートのフラッピングが表示される例を示します。この同じスタックポートがリセットの各インスタンスでそれぞれフラッピングし、スタックケーブルを交換したときに解決されました。

```
===== log file: Cisco IOS =====
```

```
.
```

```
Aug 8 21:40:14.532 UTC: %STACKMGR-1-STACK_LINK_CHANGE: STANDBY:1 stack-mgr: Stack port 1 on switch 1
Aug 8 21:40:17.242 UTC: %STACKMGR-1-STACK_LINK_CHANGE: STANDBY:1 stack-mgr: Stack port 1 on switch 1
Aug 8 21:46:11.194 UTC: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr: Stack port 2 on switch 2 is down
Aug 8 21:46:12.937 UTC: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr: Stack port 2 on switch 2 is up
Aug 8 21:48:23.063 UTC: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr: Stack port 2 on switch 2 is down
Aug 8 21:48:24.558 UTC: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr: Stack port 2 on switch 2 is up
Aug 8 21:50:40.666 UTC: %STACKMGR-6-SWITCH_REMOVED: 2 stack-mgr: Switch 1 has been removed from the s
Aug 8 21:50:40.671 UTC: Starting SWITCH-DELETE sequence, switch 1
```

症状2)使用されているstackwise設定 (180、480、およびプラス) に基づいて、ポートASICごとの送信リングの数は異なります。これらのコマンドは、送信リングごとに読み取りエラーが発生する数だけ増加する合計を維持するグローバルレジスタをポーリングします。port-asic 0はスタックポート1に対応し、port-asic 1はスタックポート2に対応します。これは、すべてのスイッチに対して発行する必要があります。カウントが増加する兆候があると、ポートまたはスタックケーブルに問題があるかどうか特定されます。

これらを数分で数回収集して、カウントの差分を比較できます。

```
show platform port-asic <0-1> read register SifRacDataCrcErrorCnt switch <switch#>
```

- データCRCエラーのあるセグメント。

```
show platform port-asic <0-1> read register SifRacRwCrcErrorCnt switch <switch#>
```

- CRCチェックが失敗すると増加する。

```
show platform port-asic <0-1> read register SifRacPcsCodeWordErrorCnt switch <switch#>
```

- 検出された視差エラーを実行する無効なPCSコード (不明なPCSコードワード) に対して増分されます。

```
show platform port-asic <0-1> read register SifRacInvalidRingWordCnt switch <switch#>
```

- スタック上のビットエラーが原因で、リングワードCRCエラーが発生しました。

Polaris (16.Xコード) の場合、次のコマンドがあります。

```
show plat hardware fed sw <#/active/standby> fwd-asic register read register-name SifRacDataCrcErrorCnt ASIC <0-1>
```

```
show plat hardware fed sw <#/active/standby> fwd-asic register read register-name
```

SifRacRwCrcErrorCnt asic<0-1>

```
show plat hardware fed sw <#/active/standby> fwd-asic register read register-name  
SifRacPcsCodeWordErrorCnt asic <0-1>
```

```
show plat hardware fed sw <#/active/standby> fwd-asic register read register-name  
SifRacInvalidRingWordCnt asic <0-1>
```

この例では、スタックのマージイベントで、2メンバのスタックの両方のメンバが、スタックポートのフラッピングを示す兆候なしに検出された場所を示します。スイッチ1のスタックポート1でリング[0]がCRCとともに増加していることがわかります。この問題を解決するには、スタックケーブルを交換します。

```
3850#show platform port-asic 0 read register SifRacRwCrcErrorCnt switch 1  
Load for five secs: 11%/4%; one minute: 11%; five minutes: 12%  
Time source is NTP, 14:02:49.119 EDT Thu Aug 20 2015
```

For asic 0

```
SifRacRwCrcErrorCnt on Asic 0  
[0] count 0x00000031 <<  
[1] count 0x00000001  
[2] count 0x00000000  
[3] count 0x00000001  
[4] count 0x00000000  
[5] count 0x00000001
```

```
3850#show platform port-asic 0 read register SifRacRwCrcErrorCnt switch 1  
Load for five secs: 9%/4%; one minute: 11%; five minutes: 12%  
Time source is NTP, 14:02:53.550 EDT Thu Aug 20 2015
```

For asic 0

```
SifRacRwCrcErrorCnt on Asic 0  
[0] count 0x000000c9 <<  
[1] count 0x00000001  
[2] count 0x00000000  
[3] count 0x00000001  
[4] count 0x00000000  
[5] count 0x00000001
```



注：確認したレジスタに基づいて、マスクはケースごとに異なる場合があります。前の例では、マスクは最後の14ビットを囲むことができます。したがって、カウンタが0x00003FFFに達すると、0x00000000にラップバックできます。

その他のヒント

1. Crashinfoディレクトリのアーカイブ

スタック内のスイッチの数が増えると、収集するレポートファイルの数が増えます。生成されるレポートの数に圧倒されがちです。障害を切り分けるために組織は不可欠です。可能であれば、各スイッチが特定のインシデントのレポートファイルを書き込んだ時点のタイムスタンプとの一貫性を確認します。そこから、クライアントが複数のファイルをアップロードしないように、これらの特定のスイッチから非常に具体的なレポートを要求します。crashinfoディレクトリをアーカイブして、シスコユーザが必要なレポートを含む単一のアーカイブを送信できるようにすることもできます。次の例では、フラッシュディレクトリにcrashinfo-archive.tarという名前のアーカイブを作成できます。

```
F340.03.10-3800-1#archive tar /create ?  
WORD Tar filename
```

```
F340.03.10-3800-1#archive tar /create crashinfo-archive.tar ?  
WORD Dir to archive files from
```

```
F340.03.10-3800-1#archive tar /create crashinfo-archive.tar crashinfo ?  
WORD File or Dir  
<cr>
```

```
F340.03.10-3800-1#archive tar /create crashinfo-archive.tar crashinfo:
```

2. 不安定なスタックの回復

スタック選択プロセスが実行された後のブートアップ時に、スタックのリロードで複数のメンバが表示される状況があります。リロードされたスイッチが、自身がアクティブであると認識した場合、多くの場合、スタックのマージイベントが発生し、ブートループ状態に入る可能性があります。このような場合は、Ciscoクライアントに次の項目を確認することをお勧めします。

- スタック全体の電源を切り、すべてのスタックケーブルをしっかりとリセットします。
- スタック内の各メンバスイッチの電源を、すべてのメンバが想定された状態に収束するまで1つずつオンにします。
- メンバがスタックに参加できない場合は、スタックからこのメンバを削除し、スタンドアロンとして起動して、さらにトラブルシューティングを実行します。

3. システムレポートの手動生成

手動で作成されたシステムレポートでは、service internalを有効にする必要があります。これにより、システムレポートがテキストファイルとして書き込まれ、スイッチ単位で実行できます。

```
3800-1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
3800-1(config)#service internal  
3800-1(config)#exit
```

```
3800-1#resource create_system_report ?  
WORD system report filename
```

```
3800-1#resource create_system_report sysreport.txt ?  
switch Switch number  
<cr>
```

```
3800-1#resource create_system_report sysreport.txt switch ?  
<1-1> Switch number
```

```
3800-1#resource create_system_report sysreport.txt switch 1 ?  
<cr>
```

関連情報

- [シスコのテクニカルサポートとダウンロード](#)

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。