

Nexus 7000 スーパーバイザ 2/2E コンパクト フラッシュ障害リカバリ

内容

[概要](#)

[背景](#)

[症状](#)

[診断](#)

[シナリオ](#)

[各シナリオの回復手順](#)

[シングル スーパーバイザの障害シナリオ](#)

[シナリオ A \(アクティブで1つの障害\)](#)

[シナリオ B \(アクティブで2つの障害\)](#)

[デュアル スーパーバイザの障害シナリオ](#)

[シナリオ C \(アクティブの障害なし、スタンバイで1つの障害\)](#)

[シナリオ D \(アクティブで1つの障害、スタンバイの障害なし\)](#)

[シナリオ E \(アクティブで1つの障害、スタンバイで1つの障害\)](#)

[シナリオ F \(アクティブで2つの障害、スタンバイの障害なし\)](#)

[シナリオ G \(アクティブの障害なし、スタンバイで2つの障害\)](#)

[シナリオ H \(アクティブで2つの障害、スタンバイで1つの障害\)](#)

[シナリオ I \(アクティブで1つの障害、スタンバイで2つの障害\)](#)

[シナリオ J \(アクティブで2つの障害、スタンバイで2つの障害\)](#)

[要約](#)

[FAQ](#)

[この問題に対する恒久的な解決策はありますか。](#)

[スタンバイのスーパーバイザをリロードしてフェールオーバーすることにより、アクティブとスタンバイでデュアル フェールオーバーを回復できないのはなぜですか。](#)

[フラッシュ回復ツールで Compact Flash をマウントし直すことができない場合どうなりますか。](#)

[このバグは Nexus 7700 Sup2E にも影響しますか。](#)

[回復ツールは NPE イメージに対して機能しますか。](#)

[コードの解決済みバージョンへの ISSU によってこの問題は解決されますか。](#)

[影響を受けるボードをリセットします。RAID の状態は 0xF0 を示しますが、GOLD テストは失敗しますか。](#)

[フラッシュの障害は動作に影響しますか。](#)

[監視と回復に関してユーザの観点から健全な実行システムを実現するにはどのような推奨事項がありますか。](#)

[GOLD コンパクト テストの状態障害がないか確認し、最初のフラッシュ パーツで障害が発生するとすぐに回復を行います。影響のあるコードから修正済みリリースへの ISSU を実行して eUSB フラッシュの障害を修正できますか。](#)

[プラグインまたはリロードを使用してフラッシュの障害を修正した場合、問題が再発するまでのくらの時間がかかりますか。](#)

[長期にわたる解決策](#)

概要

このドキュメントでは、ソフトウェアの問題 [CSCus22805](#) に記載されている Nexus 7000 スーパーバイザ 2/2E Compact Flash の障害に関する問題、起こりうるすべての障害シナリオ、および回復手順について説明します。

回避策を実行する前に、物理的な抜き差しが必要な場合に備えてデバイスに物理的にアクセスできるようにすることを強くお勧めします。一部のリロード アップグレードでは、コンソール アクセスが必要になる場合があります。常にスーパーバイザへのコンソール アクセスでこれらの回避策を実行してブート プロセスを確認することを強くお勧めします。

回避策のどの手順も失敗する場合は、実行可能な他の回復オプションについて Cisco TAC にお問い合わせください。

背景

各 N7K Ssupervisor 2/2E には 2 つの eUSB フラッシュ デバイス (プライマリとミラー) が RAID1 構成で搭載されています。これらのデバイスにより、ブート イメージ、スタートアップ コンフィギュレーション、永続アプリケーション データのための不揮発性リポジトリが提供されます。

数か月または数年にわたって使用するうちに、いずれかのデバイスと USB バスの接続が切断され、これが原因で RAID ソフトウェアが設定からそのデバイスを削除します。2 つのデバイスのうち 1 つのデバイスだけでも引き続き正常に機能できます。ただし、2 つ目のデバイスがアレイからドロップされると、ブートフラッシュは読み取り専用として再マウントされます。つまり、設定やファイルをブートフラッシュに保存できず、またリロード時にスタンバイがアクティブと同期できなくなります。

デュアル フラッシュ障害状態で稼働するシステムでは、その動作には影響はありませんが、この状態から回復するには、影響を受けるスーパーバイザをリロードする必要があります。また、実行コンフィギュレーションの変更は起動時には反映されず、停電発生時にはこの変更が失われます。

症状

次の症状が確認されています。

- Compact Flash 診断の失敗

```
switch# show diagnostic result module 5
```

```
Current bootup diagnostic level: complete
```

```
Module 5: Supervisor module-2 (Standby)
```

```
Test results: (. = Pass, F = Fail, I = Incomplete,  
U = Untested, A = Abort, E = Error disabled)
```

```
1) ASICRegisterCheck-----> .  
2) USB-----> .  
3) NVRAM-----> .
```

```

4) RealTimeClock-----> .
5) PrimaryBootROM-----> .
6) SecondaryBootROM-----> .
7) CompactFlash-----> F <=====
8) ExternalCompactFlash-----> .
9) PwrMgmtBus-----> U
10) SpineControlBus-----> .
11) SystemMgmtBus-----> U
12) StatusBus-----> U
13) StandbyFabricLoopback-----> .
14) ManagementPortLoopback-----> .
15) EOBCPortLoopback-----> .
16) OBFL-----> .

```

- 「copy run start」を実行できない

```

dcd02.ptfrnyfs# copy running-config startup-config
[#####] 100%
Configuration update aborted: request was aborted

```

- eUSB が読み取り専用になる、または応答しない

```

switch %MODULE-4-MOD_WARNING: Module 2 (Serial number: JAF1645AHQT) reported warning
due to The compact flash power test failed in device DEV_UNDEF (device error 0x0)

```

```

switch %DEVICE_TEST-2-COMPACT_FLASH_FAIL: Module 1 has failed test CompactFlash 20
times on device Compact Flash due to error The compact flash power test failed

```

- 通常スタンバイ スーパバイザにフェールオーバーを実行するときに発生する ISSU の失敗

診断

Compact Flash カードの現在の状態を診断するには、以下の内部コマンドを使用する必要があります。コマンドでは解析は実行されません。またコマンドは以下のように完全に入力する必要があります。

```
switch# show system internal raid | grep -A 1 "Current RAID status info"
```

```
switch# show system internal file /proc/mdstat
```

シャーシに 2 台のスーパバイザがある場合、発生している障害シナリオを判別するためにはスタンバイ スーパバイザの状態をチェックする必要があります。これを確認するには、コマンドの前に「slot x」キーワードを追加します。「x」はスタンバイ スーパバイザのロット番号です。これにより、スタンバイでコマンドをリモート実行することができます。

```
switch# slot 2 show system internal raid | grep -A 1 "Current RAID status info"
```

```
switch# slot 2 show system internal file /proc/mdstat
```

これらのコマンドでは、多くの RAID 統計情報とイベントが示されますが、関心があるのは現在の RAID 情報のみです。

「RAID data from CMOS」の行で、0xa5 の後の 16 進数値を確認します。これにより、現在問題が発生しているフラッシュの数がわかります。

以下に、いくつかの例を示します。

```
switch# show system internal raid | grep -A 1 "Current RAID status info"
Current RAID status info:
RAID data from CMOS = 0xa5 0xc3
```

この出力から、0xa5 の横にある番号 0xc3 を確認します。これらのキーを使用して、障害が発生しているのはプライマリまたはセカンダリどちらの Compact Flash が、あるいは両方であるかを確認できます。上記の出力には 0xc3 と示されているので、プライマリとセカンダリ両方の Compact Flash で障害が発生していることがわかります。

```
0xf0          障害は報告されていない
0xe1   プライマリ フラッシュで障害が発生している
0xd2  代替 ( ミラー ) フラッシュで障害が発生している
0xC3   プライマリと代替の両方で障害が発生している
```

「/proc/mdstat」出力を見ると、すべてのディスクが「U」として表示されています。これは、「U」P (起動) を表します。

```
switch# slot 2 show system internal file /proc/mdstat
Personalities : [raid1]
md6 : active raid1 sdc6[0] sdb6[1]
      77888 blocks [2/1] [_U]

md5 : active raid1 sdc5[0] sdb5[1]
      78400 blocks [2/1] [_U]

md4 : active raid1 sdc4[0] sdb4[1]
      39424 blocks [2/1] [_U]

md3 : active raid1 sdc3[0] sdb3[1]
      1802240 blocks [2/1] [_U]
```

このシナリオでは、プライマリ Compact Flash が起動していない ([_U]) ことがわかります。正常な出力ではすべてのブロックが [UU] として表示されます。

注：スーパーバイザが正常として診断されるためにはどちらの出力も正常 (0xf0 および [UU]) として示される必要があります。そのため、0xf0 出力が CMOS データに表示されていても、/proc/mdstat に [_U] が表示されている場合、ボックスは異常です。

シナリオ

発生しているシナリオを確認するには、「診断」セクションの上記コマンドを使用して、以下のシナリオ文字に関連付ける必要があります。カラムを使用して、各スーパーバイザで障害が発生している Compact Flash の数と照合します。

たとえば、アクティブスーパーバイザのコードが 0xe1 で、スタンバイが 0xd2 の場合は、アクティブで「1つの障害」、スタンバイで「1つの障害」となり、シナリオ文字は「D」となります。

シングルスーパーバイザ：

シナリオ文字	アクティブスーパーバイザ	アクティブスーパーバイザのコード
A	1つの障害	0xe1 または 0xd2
B	2つの障害	0xC3

デュアルスーパーバイザ：

シナリオ文字	アクティブ スーパーバイザ	スタンバイ スーパーバイザ	アクティブ スーパーバイザのコード	スタンバイ スーパーバイザのコード
C	障害なし	1つの障害	0xf0	0xe1 または 0xf0
D	1つの障害	障害なし	0xe1 または 0xd2	0xf0
E	1つの障害	1つの障害	0xe1 または 0xd2	0xe1 または 0xf0
F	2つの障害	障害なし	0xC3	0xf0
G	障害なし	2つの障害	0xf0	0xC3
H	2つの障害	1つの障害	0xC3	0xe1 または 0xf0
I	1つの障害	2つの障害	0xe1 または 0xd2	0xC3
J	2つの障害	2つの障害	0xC3	0xC3

各シナリオの回復手順

シングル スーパーバイザの障害シナリオ

シナリオ A (アクティブで1つの障害)

回復シナリオ：

アクティブで1つの障害

解決の手順：

シングル スーパーバイザ シャーシの成功および失敗シナリオでは、影響を与えない回復を実行できます。最も影響が小さい回復から最も影響が大きい回復の順に示されている以下の手順に従います。

1. ブートフラッシュを修復するためのフラッシュ回復ツールをロードします。CCO の N7000 プラットフォーム用ユーティリティから回復ツールをダウンロードするか、以下のリンクを使用できます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

これは、tar の gz 圧縮ファイルで提供されます。このファイルを解凍して .gbin 回復ツールと .pdf の readme を見つけてください。readme ファイルに目を通し、.gbin ツールを N7K のブートフラッシュにロードします。この回復ツールは影響を与えない設計になっており、ライブで実行できますが、TAC では、予期しない問題が発生した場合に備えてメンテナンス期間での実行をお勧めしています。ファイルをブートフラッシュ上に置いた後に、次のコマンドで回復ツールを実行できます。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
  77888 blocks [2/1] [U_] <-- "U_" represents the broken state  
    resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
  78400 blocks [2/1] [U_]   
    resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
  39424 blocks [2/1] [U_]   
    resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
 1802240 blocks [2/1] [U_]   
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
  77888 blocks [2/2] [UU] <-- "UU" represents the fixed state  
  
md5 :active raid1 sdd5[1] sdc5[0]  
  78400 blocks [2/2] [UU]  
  
md4 :active raid1 sdd4[1] sdc4[0]  
  39424 blocks [2/2] [UU]  
  
md3 :active raid1 sdd3[1] sdc3[0]  
 1802240 blocks [2/2] [UU]  
unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

2.ステップ1でフラッシュ回復ツールが成功しなかった場合、次のステップとしてログを収集し、TACにデバッグプラグインを使用したディスクの手動回復を依頼します。回復ツールが成功しなかった場合、この作業は成功しない可能性があります。

収集：

```
show version  
show module  
show accounting log  
show logging logfile  
show system internal raid (非表示のコマンド)  
show system internal kernel messages  
show logging onboard
```

3.手動リカバリが機能せず、スーパーバイザが1つしかない場合は、復旧のためにシャーシのリロードが必要になる可能性があります。

ただし、ラボ デバイスに予備のスーパーバイザがある場合は、これをスタンバイ スロットに (メンテナンス ウィンドウに) ロードし、アクティブと完全に同期して HA (ハイ アベイラビリティ) 状態になるかどうか確認できます。

RAID が唯一の障害ディスクであるため、アクティブに対するスタンバイの同期は可能です。これがオプションの場合は、「show module」および「show system redundancy status」を使用し

てスタンバイをアクティブと完全に同期し、スタンバイが「ha-standby」状態になるか確認します。これは、ステートフル スイッチオーバー (SSO) が「system switchover」コマンドを使用して実行可能であることを示します。スタンバイが起動したら、コンフィギュレーションを「copy run ftp:vdc-all」で外部に保存し、「copy run start vdc-all」でスタートアップに完全に保存します。この後に、「system switchover」を試すことができます。このコマンドで現在のアクティブがリロードされ、現在のスタンバイが強制的にアクティブになります。アクティブがスタンバイにリロードされた後、その RAID アレイは自動的に回復します。リロードしたスーパーバイザが「ha-standby」状態に戻った後に RAID アレイが回復しているか確認し、「slot x show system internal raid」を実行してすべてのディスクが [UU] になっているか確認できます。それでもディスクが完全にバックアップされないときは、回復ツールをもう一度実行して解決されない問題をクリアしてください。それでも成功しない場合は、影響のあるモジュールで「out-of-service module x」を試した後に、「no poweroff module x」を試すことができます。それも成功しない場合は、影響のあるモジュールの物理的な抜き差しを試してみてください。それでも回復しない場合は、正当な HW 障害である可能性があり、RMA が必要になりますが、パスワード回復手順を使用してスイッチ ブート モードにリロードし、回復の最後の手段である「init system」を実行することができます。

予備のスーパーバイザを利用できなければ、「reload」コマンドによる完全なリロードが必要です。この場合は、物理的な抜き差しが必要になる場合に備えてデバイスに物理的にアクセスできるようにすることをお勧めします。すべての実行コンフィギュレーションを外部にバックアップします。また安全のため USB ディスクにそれらのコンフィギュレーションをシステムやキックスタート イメージとともに保存することをお勧めします。リロードが実行され、デバイスが起動したら、RAID 状態が [UU] になっているか確認し、完全に修復されていないような場合は回復ツールを実行します。システムが起動していない場合、または回復ツールが機能しない場合は、スーパーバイザ モジュールの物理的な抜き差しを行い、コンソールを使ってブート プロセスを確認します。物理的な抜き差しでも回復しない場合は、パスワード回復手順を使用してローダーに入り、キックスタート イメージをブートしてスイッチ ブート モードを有効にした後、「init system」を実行してブートフラッシュを再初期化します。これによって、ブートフラッシュ上のファイルが消去されるため、これらの手順を実行する前に必要なすべてのファイルとコンフィギュレーションをバックアップしておくことが重要です。

他のすべての方法が失敗する場合は、まれにハードウェアが故障している可能性があり、スーパーバイザを RMA 処理し、場合によっては EFA が必要になります。回復手順の前に、すべてのコンフィギュレーションを外部にバックアップするのはこのためです。緊急の RMA が必要な場合、システムを迅速に元に戻すために必要なすべてのコンフィギュレーションを用意しておきます。

シナリオ B (アクティブで 2 つの障害)

回復シナリオ：

アクティブで 2 つの障害

解決の手順：

デュアル フラッシュ障害が発生しているシングル スーパーバイザのシナリオでは、回復するために強制的なリロードを実行する必要があります。

1. 「copy run ftp:vdc-all」を使用して外部にバックアップします。デュアル フラッシュ障害が発生している場合、読み取り専用で再マウントされたシステムがスタートアップ コンフィギュレーションに存在しないため、コンフィギュレーションが変更されています。「show run diff | i\+」を使用して、デュアルフラッシュ障害後に行われた変更を確認します。これにより、リロード時にスタートアップコンフィギュレーションが実行コンフィギュレーションと異なる場合に追加する内容がわかります。

デュアル フラッシュ障害が発生している 1 台のスーパーバイザをリロードするとスタートアップ コンフィギュレーションが消去される可能性があるため、コンフィギュレーションを外部にバックアップする必要があります。

2.デバイスをリロードします。コンソールアクセスを使用することを強く推奨します。物理的なアクセスが必要になる場合があります。スーパーバイザがリロードされ、そのブートフラッシュが修復されます。システムが起動した後に、両方のディスクが起動し、[UU]の状態で作動していることを「`how system internal file /proc/mdstat`」と「`show system internal raid`」で確認します。両方のディスクが起動し、動作している場合、回復は完了しており、以前のすべてのコンフィギュレーションを復元することができます。回復が失敗した場合や部分的に成功した場合は、手順3に進んでください。

注：一般的に、デュアルフラッシュ障害の場合、ソフトウェアのリロードでRAIDは完全に回復せず、回復するには回復ツールまたは何度かリロードを実行する必要がある場合があります。ほとんどの場合、この問題はスーパーバイザモジュールを物理的に抜き差しすることで解決しています。したがって、デバイスへの物理アクセスが可能な場合は、コンフィギュレーションを外部にバックアップした後、デバイスのリロードの準備ができたならスーパーバイザを物理的に抜き差しすることで成功する可能性が最も高い迅速な回復方法を試すことができます。これで、スーパーバイザから電源が完全に外されて、RAIDの両方のディスクの回復が可能になります。物理的な抜き差しによる回復が部分的に成功する場合は手順3に進み、まったく成功せずシステムが完全に起動しない場合は手順4に進みます。

3.部分的な回復の場合、つまりリロード後に1つのディスクが起動し、もう1つのディスクがまだ[U_]状態でダウンしている場合は、次の推奨手順として、フラッシュ回復ツールを実行して他のディスクを再同期します。回復ツールが成功しない場合は、TACに手動による回復手順を依頼します。スーパーバイザの物理的な抜き差しも試すことができます。

リロードしてもスーパーバイザが完全に起動しない場合は、スーパーバイザモジュールの物理的な抜き差しを行ってください。一般的に、デュアルフラッシュ障害の場合、ソフトウェアの「リロード」では、電源がモジュールから完全に外されないため、両方のディスクは完全に回復されませんが、物理的な抜き差しを行うとモジュールから電源を完全に外すことができます。物理的な抜き差しが成功しない場合は、手順4に進みます。

4.物理的な抜き差しが成功しない場合、次のステップは、パスワード回復手順を使用してローダープロンプトに入り、キックスタートをスイッチブートモードにロードし、「`init system`」を実行します。これにより、ブートフラッシュが消去され、アレイの修復が試みられます。`init system`が完了するか失敗して、問題が解決されない場合は、もう一度物理的な抜き差しを試してください。

他のすべての方法が失敗する場合は、まれにハードウェアが故障している可能性があり、スーパーバイザをRMA処理し、場合によってはEFAが必要になります。回復手順の前に、すべてのコンフィギュレーションを外部にバックアップするのはこのためです。緊急のRMAが必要な場合、システムを迅速に元に戻すために必要なすべてのコンフィギュレーションを用意しておきます。

デュアルスーパーバイザの障害シナリオ

シナリオC (アクティブの障害なし、スタンバイで1つの障害)

障害シナリオ：

アクティブの障害なし

スタンバイで1つの障害

解決の手順：

デュアルスーパーバイザ設定のシナリオで、アクティブにはフラッシュ障害がなく、スタンバイで1つの障害が発生している場合は、影響を与えない回復を実行できます。

1.アクティブには障害がなく、スタンバイには1つの障害しかないため、フラッシュ回復ツールをアクティブにロードして実行できます。ツールを実行すると、ツールそのものがスタンバイに自動的にコピーされて、アレイの再同期が実行されます。回復ツールは下記からダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、ボックスのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
    77888 blocks [2/1] [U_]    <-- "U_" represents the broken state  
    resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
    78400 blocks [2/1] [U_]    resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
    39424 blocks [2/1] [U_]    resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
    1802240 blocks [2/1] [U_]    
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
    77888 blocks [2/2] [UU]    <-- "UU" represents the correct state
```

```
md5 :active raid1 sdd5[1] sdc5[0]
      78400 blocks [2/2] [UU]

md4 :active raid1 sdd4[1] sdc4[0]
      39424 blocks [2/2] [UU]

md3 :active raid1 sdd3[1] sdc3[0]
      1802240 blocks [2/2] [UU]

unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

2.フラッシュ回復ツールが失敗した場合、アクティブに両方のディスクが起動しているため、スタンバイはリロード時にアクティブに正常に同期できます。

したがって、スケジュールされた期間に、スタンバイ スーパーバイザに対して「**out-of-service module x**」を実行します。予期しない問題が生じた場合のためにブート プロセスを確認できるようにスタンバイにコンソールからアクセスできるようにしてください。スーパーバイザがダウンした後、数秒間待機してから、スタンバイで「**no poweroff module x**」を実行します。スタンバイが「**ha-standby**」の状態ですべて完全に起動するまで待機します。

スタンバイをバックアップしたら、「**slot x show system internal raid**」と「**slot x show system internal file /proc/mdstat**」で RAID をチェックします。

リロード後に両方のディスクが完全にバックアップされなければ、回復ツールを再度実行します。

3.リロードと回復ツールが失敗した場合は、ウィンドウ内のスタンバイモジュールを物理的に再装着して、状態をクリアすることを試みることをお勧めします。物理的な抜き差しが失敗した場合は、パスワード回復手順に従ってブート時にスイッチ ブート モードに入り、このモードで「**init system**」を実行してみてください。それでも成功しない場合は、TAC に手動リカバリを依頼してください。

シナリオ D (アクティブで1つの障害、スタンバイの障害なし)

回復シナリオ:

アクティブで1つの障害

スタンバイの障害なし

解決の手順:

デュアル スーパーバイザ設定のシナリオで、アクティブで1つのフラッシュ障害が発生し、スタンバイでは障害が発生していない場合は、フラッシュ回復ツールを使用して影響を与えない回復を実行できます。

1.スタンバイには障害がなく、アクティブには1つの障害しかないため、フラッシュ回復ツールを

アクティブにロードして実行できます。ツールを実行すると、ツールそのものがスタンバイに自動的にコピーされて、アレイの再同期が実行されます。回復ツールは下記からダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&relind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、アクティブのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
  77888 blocks [2/1] [U_]    <-- "U_" represents the broken state  
    resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
  78400 blocks [2/1] [U_]      
    resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
  39424 blocks [2/1] [U_]      
    resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
 1802240 blocks [2/1] [U_]      
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
  77888 blocks [2/2] [UU]    <-- "UU" represents the correct state  
  
md5 :active raid1 sdd5[1] sdc5[0]  
  78400 blocks [2/2] [UU]  
  
md4 :active raid1 sdd4[1] sdc4[0]  
  39424 blocks [2/2] [UU]
```

```
md3 :active raid1 sdd3[1] sdc3[0]
      1802240 blocks [2/2] [UU]
unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

2.フラッシュ回復ツールが失敗した場合は、次のステップとして「システムスイッチオーバー」を実行し、メンテナンス時間帯にスーパーバイザモジュールをフェールオーバーします。

したがって、スケジュールされた期間に、「system switchover」を実行します。予期しない問題が生じたときのためにブートプロセスを確認できるようコンソールアクセスできるようにしてください。スタンバイが「ha-standby」の状態ですべて完全に起動するまで待機します。

スタンバイをバックアップしたら、「slot x show system internal raid」と「slot x show system internal file /proc/mdstat」で RAID をチェックします。

リロード後に両方のディスクが完全にバックアップされなければ、回復ツールを再度実行します。

3.リロードと回復ツールが失敗した場合は、ウィンドウ内のスタンバイモジュールを物理的に再装着して、状態をクリアすることを試みることをお勧めします。物理的な抜き差しが失敗した場合は、パスワード回復手順に従ってブート時にスイッチブートモードに入り、このモードで「init system」を実行してみてください。それでも成功しない場合は、TAC に手動リカバリを依頼してください。

シナリオ E (アクティブで 1 つの障害、スタンバイで 1 つの障害)

回復シナリオ :

アクティブで 1 つの障害

スタンバイで 1 つの障害

解決の手順 :

アクティブとスタンバイの両方で 1 つのフラッシュ障害が発生した場合も、影響を与えない回避策を実行できます。

1.スーパーバイザが読み取り専用状態ではないため、最初のステップはフラッシュ回復ツールを使用することです。

回復ツールは下記からダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、アクティブのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

これによって、アクティブで切断されているディスクが自動的に検出されて、修復が行われます。またツールそのものが自動的にスタンバイにコピーされ、障害の検出と修正が行われます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
  77888 blocks [2/1] [U_]    <-- "U_" represents the broken state  
    resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
  78400 blocks [2/1] [U_]    resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
  39424 blocks [2/1] [U_]    resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
 1802240 blocks [2/1] [U_]      
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
  77888 blocks [2/2] [UU]    <-- "UU" represents the correct state  
  
md5 :active raid1 sdd5[1] sdc5[0]  
  78400 blocks [2/2] [UU]  
  
md4 :active raid1 sdd4[1] sdc4[0]  
  39424 blocks [2/2] [UU]  
  
md3 :active raid1 sdd3[1] sdc3[0]  
 1802240 blocks [2/2] [UU]  
unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完

全にバックアップされます。

両方のスーパーバイザが [UU] 状態で回復した場合、回復は完了です。回復が部分的に成功した場合や、失敗した場合は、手順 2 に進みます。

2.回復ツールが成功しなかった場合は、モジュールのRAIDの現在の状態を特定します。両方で1つのフラッシュ障害がまだ発生する場合は、「system switchover」を実行して現在のアクティブをリロードし、スタンバイを強制的にアクティブ ロールにします。

前のアクティブがリロードされて「ha-standby」状態に戻ったら、リロード中に回復している必要のある RAID の状態を確認します。
スーパーバイザがスイッチオーバー後に正常に回復した場合は、フラッシュ回復ツールを再実行して現在のアクティブスーパーバイザの1つのディスク障害を修復するか、もう一度「system switchover」を実行して現在のアクティブをリロードし、前のアクティブと修復された現在のスタンバイを強制的にアクティブ ロールにすることができます。リロードされたスーパーバイザで両方のディスクが再度修復されているか確認し、必要に応じて回復ツールを再実行します。

3.このプロセスの間にスイッチオーバーでRAIDが修正されない場合は、スタンバイに対して「out-of-service module x」を実行し、次に「no poweroff module x」を実行して電源を完全に切断し、モジュールに再供給します。

out of service が失敗した場合は、スタンバイの物理的な抜き差しを試してみてください。

回復ツールの実行後に1台のスーパーバイザのRAIDが回復し、もう1台に障害が残る場合は、1つの障害があるスーパーバイザを必要に応じて「system switchover」で強制的にスタンバイにします。1つの障害があるスーパーバイザがすでにスタンバイになっている場合は、スタンバイに対して「out-of-service module x」を実行し、「no poweroff module x」を実行して電源を完全に切断し、モジュールに電力を再供給します。それでも回復しない場合は、モジュールの物理的な抜き差しを試します。抜き差しで修正されない場合は、パスワード回復手順を使用してスイッチ ブート プロンプトに入り、「init system」を実行してブートフラッシュを再初期化します。それでも失敗する場合は、TAC に手動回復を依頼してください。

注：いずれかの時点でスタンバイが「powered-up」状態でスタックし、「ha-standby」にならず、上記の手順でスタンバイが完全に起動できない場合、シャーシのリロードが必要です。

シナリオ F (アクティブで2つの障害、スタンバイで0つの障害)

回復シナリオ：

アクティブで2つの障害

スタンバイの障害なし

解決の手順：

アクティブに2つの障害があり、スタンバイのスーパーバイザに障害がない場合、スタンバイが実行コンフィギュレーションをアクティブと同期できなくなってから追加された実行コンフィギュレーションの量によっては、影響を与えない回復が可能です。

回復手順では、アクティブスーパーバイザの現在の実行コンフィギュレーションをコピーして、正常なスタンバイスーパーバイザにフェールオーバーし、不足している実行コンフィギュレーションを新しいアクティブにコピーして、前のアクティブを手動でオンラインにした後に、回復ツールを実行します。

1. すべての実行コンフィギュレーションを「**copy running-config tftp:vdc-all**」を使用して外部にバックアップします。デュアルフラッシュ障害が発生している場合、読み取り専用に変更されたシステムがスタートアップコンフィギュレーションに存在しないため、コンフィギュレーションが変更されています。影響を受けるモジュールの「**show system internal raid**」を参照して、2つ目のディスクで障害が発生してこのシステムが読み取り専用になった時点を確認できます。そこから、各VDCの「**show accounting log**」を参照して、デュアルフラッシュ障害後に実行された変更内容を確認し、リロード時にスタートアップコンフィギュレーションで維持される追加内容を把握できます。

デュアルフラッシュ障害が発生している1台のスーパーバイザをリロードすると、スタートアップコンフィギュレーションが消去される可能性があるため、コンフィギュレーションを外部にバックアップする必要があります。

2. 実行コンフィギュレーションをアクティブスーパーバイザからコピーしたら、スタートアップコンフィギュレーションと比較して、最後の保存以降の変更内容を確認することをお勧めします。これは、「**show startup-configuration**」で確認できます。当然、違いは環境によってまったく異なりますが、スタンバイがアクティブとしてオンラインになるときに失われている内容を把握しておく役に立ちます。また、違いをメモ帳にコピーして、スイッチオーバー後に新しいアクティブスーパーバイザにすぐに追加できるようにすることをお勧めします。

を選択します。違いを評価した後に、スーパーバイザのスイッチオーバーを実行する必要があります。TACでは、予測しない問題が生じる可能性があるため、スイッチオーバーはメンテナンス期間に実行することをお勧めします。スタンバイへのフェールオーバーを実行するコマンドは、「**system switchover**」です。

4. スwitchオーバーは非常に迅速に実行され、新しいスタンバイがリブートを開始します。この際に、失われたコンフィギュレーションを新しいアクティブに追加します。これはTFTPサーバ（または以前にコンフィギュレーションを保存した場所）からコンフィギュレーションをコピーするか、単純にCLIでコンフィギュレーションを手動で追加することで可能になります。ほとんどの場合、失われたコンフィギュレーションは非常に短く、CLIオプションで対応できます。

5. しばらくすると、新しいスタンバイスーパーバイザが「**ha-standby**」状態でオンラインに復帰する場合がありますが、通常は「**powered-up**」状態でスタックします。この状態は、「**show module**」コマンドを使用して、モジュールの横にある「**Status**」列を参照することで確認できます。

新しいスタンバイが「**powered-up**」状態で起動する場合は、手動でオンラインに戻す必要があります。これは、次のコマンドを実行して行います。「**x**」は「**powered-up**」状態でスタックしているスタンバイモジュールです。

```
(config)# out-of-service module x
```

```
(config)# no poweroff module x
```

6. スタンバイが「ha-standby」状態でオンラインに戻ったら、回復ツールを実行して回復が完了したか確認する必要があります。 ツールは次のリンクからダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、ボックスのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
          77888 blocks [2/1] [U_]    <-- "U_" represents the broken state  
          resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
          78400 blocks [2/1] [U_]      
          resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
          39424 blocks [2/1] [U_]      
          resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
          1802240 blocks [2/1] [U_]    
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat  
  
Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
      77888 blocks [2/2] [UU]    <-- "UU" represents the correct state
```



```
md5 :active raid1 sdd5[1] sdc5[0]
      78400 blocks [2/2] [UU]

md4 :active raid1 sdd4[1] sdc4[0]
      39424 blocks [2/2] [UU]

md3 :active raid1 sdd3[1] sdc3[0]
      1802240 blocks [2/2] [UU]

unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

シナリオ G (アクティブの障害なし、スタンバイで2つの障害)

アクティブの障害なし、スタンバイで2つの障害

回復シナリオ:

アクティブの障害なし

スタンバイで2つの障害

解決の手順:

アクティブに障害がなく、スタンバイ スーパーバイザに2つの障害がある場合は、影響を与えない回復を実行できます。

回復手順では、スタンバイのリロードを実行します。

1.通常、デュアルフラッシュ障害のあるスーパーバイザでは、ソフトウェアの「**reload module x**」によってRAIDが部分的にしか修復されないか、またはリブート時に電源投入状態のままになる可能性があります。

そのため、デュアルフラッシュ障害が発生しているスーパーバイザの物理的な抜き差しを行い、電源を外してからモジュールに電力を再供給するか、以下のコマンドを実行できます (x はスタンバイ スロット番号)。

```
# out-of-service module x
# no poweroff module x
```

スタンバイが powered-up 状態でスタックし、上記の手順を実行した後、最終的に電源サイクルが続くのは、スタンバイをリロードしているアクティブが時間内に起動しないことが原因である可能性があります。

これは、ブートフラッシュや RAID の再初期化を試行するスタンバイを起動していることが原因です。この処理には最大 10 分かかる可能性があります。その処理が完了する前にアクティブによってリセットが行われます。

この問題を解決するには、powered-up 状態でスタックしているスタンバイ スロット番号を表す「x」を使用して、次を設定します。

```
(config)# system standby manual-boot
(config)# reload module x force-dnld
```

上記のコマンドを実行すると、アクティブがスタンバイを自動的にリセットすることはなくなり、スタンバイをリロードしてそのイメージをアクティブから強制的に同期します。

10 ~ 15 分待つと、スタンバイは最終的に ha-standby 状態になります。ha-standby 状態になった後、次のコマンドでスタンバイの自動リブートを再度有効にします。

```
(config)# system no standby manual-boot
```

6. スタンバイが「ha-standby」状態でオンラインに戻ったら、回復ツールを実行して回復が完了したか確認する必要があります。ツールは次のリンクからダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、ボックスのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat
Personalities : [raid1]
md6      : active raid1 sdd6[2] sdc6[0]
          77888 blocks [2/1] [U_]    <-- "U_" represents the broken state
          resync=DELAYED

md5      : active raid1 sdd5[2] sdc5[0]
          78400 blocks [2/1] [U_]
          resync=DELAYED

md4      : active raid1 sdd4[2] sdc4[0]
          39424 blocks [2/1] [U_]
          resync=DELAYED

md3      : active raid1 sdd3[2] sdc3[0]
          1802240 blocks [2/1] [U_]
          resync=DELAYED
```

```
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
    77888 blocks [2/2] [UU]    <-- "UU" represents the correct state  
  
md5 :active raid1 sdd5[1] sdc5[0]  
    78400 blocks [2/2] [UU]  
  
md4 :active raid1 sdd4[1] sdc4[0]  
    39424 blocks [2/2] [UU]  
  
md3 :active raid1 sdd3[1] sdc3[0]  
    1802240 blocks [2/2] [UU]  
unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

シナリオ H (アクティブで 2 つの障害、スタンバイで 1 つの障害)

アクティブで 2 つの障害、スタンバイで 1 つの障害

回復シナリオ :

アクティブで 2 つの障害

スタンバイで 1 つの障害

解決の手順 :

アクティブで 2 つの障害が発生し、スタンバイ スーパーバイザで 1 つの障害が発生している場合、スタンバイがアクティブと実行コンフィギュレーションを同期できなくなってから追加された実行コンフィギュレーションの量によっては、影響を与えない回復が可能です。

回復手順では、アクティブ スーパーバイザの現在の実行コンフィギュレーションをバックアップして、正常なスタンバイ スーパーバイザにフェールオーバーし、不足している実行コンフィギュレーションを新しいアクティブにコピーして、前のアクティブを手動でオンラインにした後に、回復ツールを実行します。

1. すべての実行コンフィギュレーションを「copy running-config tftp:vdc-all」を使用して外部にバックアップします。デュアル フラッシュ障害が発生している場合、読み取り専用に変更されたシステムがスタートアップ コンフィギュレーションに存在しないため、コンフィギュレーションが変更されています。影響を受けるモジュールの「show system internal raid」を参照して、2 つ目のディスクで障害が発生してこのシステムが読み取り専用になった時点を確認できます。そこから、各 VDC の「show accounting log」を参照して、デュアル フラッシュ障害後に実行

された変更内容を確認し、リロード時にスタートアップ コンフィギュレーションで維持される追加内容を把握できます。

デュアル フラッシュ障害が発生している 1 台のスーパーバイザをリロードすると、スタートアップ コンフィギュレーションが消去される可能性があるため、コンフィギュレーションを外部にバックアップする必要があります。

2. 実行コンフィギュレーションをアクティブ スーパーバイザからコピーしたら、スタートアップ コンフィギュレーションと比較して、最後の保存以降の変更内容を確認することをお勧めします。これは、「show startup-configuration」で確認できます。当然、違いは環境によってまったく異なりますが、スタンバイがアクティブとしてオンラインになるときに失われている内容を把握しておくに役に立ちます。また、違いをメモ帳にコピーして、スイッチオーバー後に新しいアクティブ スーパーバイザにすぐに追加できるようにすることをお勧めします。

を選択します。違いを評価した後に、スーパーバイザのスイッチオーバーを実行する必要があります。TAC では、予測しない問題が生じる可能性があるため、スイッチオーバーはメンテナンス期間に実行することをお勧めします。スタンバイへのフェールオーバーを実行するコマンドは、「system switchover」です。

4. スwitchオーバーは非常に迅速に実行され、新しいスタンバイがリブートを開始します。この際に、失われたコンフィギュレーションを新しいアクティブに追加します。これは TFTP サーバ（または前にコンフィギュレーションが保存された場所）からコンフィギュレーションをコピーするか、単純に CLI でコンフィギュレーションを追加して実行できます。tftp から実行コンフィギュレーションに直接コピーせず、最初にブートフラッシュにコピーしてから実行コンフィギュレーションにコピーします。ほとんどの場合、失われたコンフィギュレーションは非常に短く、CLI オプションで対応できます。

5. しばらくすると、新しいスタンバイ スーパーバイザが「ha-standby」状態でオンラインに復帰する場合がありますが、通常は「powered-up」状態でスタックします。この状態は、「show module」コマンドを使用して、モジュールの横にある「Status」列を参照することで確認できます。

新しいスタンバイが「powered-up」状態で起動する場合は、手動でオンラインに戻す必要があります。これは、次のコマンドを実行して行います。「x」は「powered-up」状態でスタックしているスタンバイ モジュールです。

```
(config)# out-of-service module  
(config)# no poweroff module x
```

スタンバイが powered-up 状態でスタックし、上記の手順を実行した後、最終的に電源サイクルが続くのは、スタンバイをリロードしているアクティブが時間内に起動しないことが原因である可能性があります。

これは、ブートフラッシュや RAID の再初期化を試行するスタンバイを起動していることが原因です。この処理には最大 10 分かかる可能性があります。その処理が完了する前にアクティブによってリセットが行われます。

この問題を解決するには、powered-up 状態でスタックしているスタンバイ スロット番号を表す「x」を使用して、次を設定します。

```
(config)# system standby manual-boot
(config)# reload module x force-dnld
```

上記のコマンドを実行すると、アクティブがスタンバイを自動的にリセットすることはなくなり、スタンバイをリロードしてそのイメージをアクティブから強制的に同期します。

10 ~ 15 分待つと、スタンバイは最終的に ha-standby 状態になります。ha-standby 状態になった後、次のコマンドでスタンバイの自動リブートを再度有効にします。

```
(config)# system no standby manual-boot
```

6. スタンバイが「ha-standby」状態でオンラインに戻ったら、回復ツールを実行して回復が完了したことを確認し、アクティブの 1 つのディスク障害を修復する必要があります。ツールは次のリンクからダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、ボックスのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \
Personalities : [raid1]
md6      : active raid1 sdd6[2] sdc6[0]
          77888 blocks [2/1] [U_]    <-- "U_" represents the broken state
          resync=DELAYED

md5      : active raid1 sdd5[2] sdc5[0]
          78400 blocks [2/1] [U_]
          resync=DELAYED

md4      : active raid1 sdd4[2] sdc4[0]
          39424 blocks [2/1] [U_]
          resync=DELAYED

md3      : active raid1 sdd3[2] sdc3[0]
          1802240 blocks [2/1] [U_]

[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s peed=12613K/sec
```

```
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat Personalities : [raid1]
md6 :active raid1 sdd6[1] sdc6[0]
      77888 blocks [2/2] [UU]      <-- "UU" represents the correct state

md5 :active raid1 sdd5[1] sdc5[0]
      78400 blocks [2/2] [UU]

md4 :active raid1 sdd4[1] sdc4[0]
      39424 blocks [2/2] [UU]

md3 :active raid1 sdd3[1] sdc3[0]
      1802240 blocks [2/2] [UU]
unused devices: <none>
```

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

1 つの障害が発生している現在のアクティブが回復ツールで回復しない場合は、もう一度「system switchover」を試して現在のスタンバイを「ha-standby」の状態にします。それでも成功しない場合は、Cisco TAC にお問い合わせください。

シナリオ I (アクティブで 1 つの障害、スタンバイで 2 つの障害)

回復シナリオ :

アクティブで 1 つの障害

スタンバイで 2 つの障害

解決の手順 :

アクティブに 1 つの障害があり、スタンバイ スーパーバイザに 2 つの障害があるデュアル スーパーバイザのシナリオでは、影響を与えない回復が可能です。多くの場合はリロードが必要です。

このプロセスでは、最初にすべての実行コンフィギュレーションをバックアップした後に、回復ツールを使用して障害のある Compact Flash をアクティブに回復するように試み、成功した場合は、スタンバイを手動でリロードして回復ツールを再実行します。最初の回復でアクティブの障害のあるフラッシュを回復できなかった場合は、TAC にデバッグ プラインを使用した手動回復を依頼する必要があります。

1. すべての実行コンフィギュレーションを「**copy running-config tftp:vdc-all**」を使用して外部にバックアップします。環境に TFTP サーバが設定されていない場合は、実行コンフィギュレーションをローカルの USB スティックにもコピーする場合があります。
2. 現在の実行コンフィギュレーションをバックアップしたら、回復ツールを使用して、アクティブの障害のあるフラッシュの回復を実行する必要があります。ツールは次のリンクからダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

ツールをダウンロードして解凍し、ボックスのブートフラッシュにアップロードした後、次のコマンドを実行して回復を開始する必要があります。

```
# load bootflash:n7000-s2-flash-recovery-tool.10.0.2.gbin
```

ツールの実行が開始され、切断されたディスクが検出されて、それらのディスクが RAID アレイと再同期されます。

回復の状態を次のコマンドで確認できます。

```
# show system internal file /proc/mdstat
```

回復処理が進んでいることを確認します。すべてのディスクが完全に修復されて [UU] の状態になるまで数分かかる場合があります。回復処理例は次のようになります。

```
switch# show system internal file /proc/mdstat \  
Personalities : [raid1]  
md6      : active raid1 sdd6[2] sdc6[0]  
          77888 blocks [2/1] [U_]    <-- "U_" represents the broken state  
          resync=DELAYED  
  
md5      : active raid1 sdd5[2] sdc5[0]  
          78400 blocks [2/1] [U_]      
          resync=DELAYED  
  
md4      : active raid1 sdd4[2] sdc4[0]  
          39424 blocks [2/1] [U_]      
          resync=DELAYED  
  
md3      : active raid1 sdd3[2] sdc3[0]  
          1802240 blocks [2/1] [U_]    
  
[=>.....] recovery = 8.3% (151360/1802240) finish=2.1min s speed=12613K/sec  
unused devices: <none>
```

回復が終了すると、次のようになります。

```
switch# show system internal file /proc/mdstat  
  
Personalities : [raid1]  
md6 :active raid1 sdd6[1] sdc6[0]  
      77888 blocks [2/2] [UU]    <-- "UU" represents the correct state  
  
md5 :active raid1 sdd5[1] sdc5[0]  
      78400 blocks [2/2] [UU]  
  
md4 :active raid1 sdd4[1] sdc4[0]  
      39424 blocks [2/2] [UU]  
  
md3 :active raid1 sdd3[1] sdc3[0]  
      1802240 blocks [2/2] [UU]
```

unused devices: <none>

すべてのディスクが [UU] 状態になった後、RAID アレイは両方のディスクが同期された状態で完全にバックアップされます。

を選択します。手順 2 で回復ツールを実行した後に、アクティブ スーパーバイザの障害のある Compact Flash を回復できない場合は、TAC に linux デバッグ プラグインを使用した手動回復の実行を依頼する必要があります。

4. 両方のフラッシュが「[UU]」としてアクティブに表示されたことを確認した後、スタンバイ スーパーバイザの手動リブートに進みます。これは、次のコマンドを実行して行います。「x」は「powered-up」状態でスタックしているスタンバイ モジュールです。

```
(config)# out-of-service module x
```

```
(config)# no poweroff module x
```

これによりスタンバイ スーパーバイザは「ha-standby」状態になります（「show module」出力の Status カラム表示で確認します）。成功したら、手順 6 に進み、成功しない場合は手順 5 で説明している手順を試します。

5. スタンバイが powered-up 状態でスタックし、上記の手順を実行した後、最終的に電源サイクルが続くのは、スタンバイをリロードしているアクティブが時間内に起動しないことが原因である可能性があります。これは、ブートフラッシュや RAID の再初期化を試行するスタンバイを起動していることが原因です。この処理には最大 10 分かかる可能性があります。その処理が完了する前にアクティブによってリセットが行われます。この問題を解決するには、powered-up 状態でスタックしているスタンバイ スロット番号を表す「x」を使用して、次を設定します。

```
(config)# system standby manual-boot
```

```
(config)# reload module x force-dnld
```

上記のコマンドを実行すると、アクティブがスタンバイを自動的にリセットすることはなくなり、スタンバイをリロードしてそのイメージをアクティブから強制的に同期します。

10 ~ 15 分待つと、スタンバイは最終的に ha-standby 状態になります。ha-standby 状態になった後、次のコマンドでスタンバイの自動リブートを再度有効にします。

```
(config)# system no standby manual-boot
```

6. スタンバイが「ha-standby」状態でオンラインに戻ったら、回復ツールを実行して回復が完了したか確認する必要があります。この手順でアクティブに対して実行したのと同じツールを実行できません。回復ツールはアクティブとスタンバイで実行されるため、追加のダウンロードは不要です。

シナリオ J (アクティブで2つの障害、スタンバイで2つの障害)

回復シナリオ：

アクティブで 2 つの障害

スタンバイで 2 つの障害

解決の手順：

デュアルフラッシュ障害が発生しているデュアルスーパーバイザのシナリオでは、回復するために強制的なリロードを実行する必要があります。解決するには次の手順に従います。

1. バックアップ外部のすべての実行コンフィギュレーション「copy running-config tftp:とvdc-all」を使用して外部にバックアップします。デュアルフラッシュ障害が発生している場合、読み取り専用に再マウントされたシステムがスタートアップコンフィギュレーションに存在しないため、コンフィギュレーションが変更されています。影響を受けるモジュールの「show system internal raid」を参照して、2つ目のディスクで障害が発生してこのシステムが読み取り専用になった時点を確認できます。そこから、各VDCの「show accounting log」を参照して、デュアルフラッシュ障害後に実行された変更内容を確認し、リロード時にスタートアップコンフィギュレーションで維持される追加内容を把握できます。

デュアルフラッシュ障害が発生している1台のスーパーバイザをリロードすると、スタートアップコンフィギュレーションが消去される可能性があるため、コンフィギュレーションを外部にバックアップする必要があります。

2. デバイスをリロードします。コンソールアクセスを使用することを強く推奨します。物理的なアクセスが必要になる場合があります。スーパーバイザがリロードされ、そのブートフラッシュが修復されます。システムが起動した後に、両方のディスクが起動し、[UU]の状態で作動していることを「show system internal file /proc/mdstat」と「show system internal raid」で確認します。両方のディスクが起動し、動作している場合、回復は完了しており、以前のすべてのコンフィギュレーションを復元することができます。回復が失敗した場合や部分的に成功した場合は、手順3に進んでください。

注：一般的に、デュアルフラッシュ障害の場合、ソフトウェアの「リロード」でRAIDは完全に回復せず、回復するには回復ツールまたは何度かリロードを実行する必要がある可能性があります。ほとんどの場合、この問題はスーパーバイザモジュールを物理的に抜き差しすることで解決しています。したがって、デバイスへの物理アクセスが可能な場合は、コンフィギュレーションを外部にバックアップした後、デバイスのリロードの準備ができたならスーパーバイザを物理的に抜き差しすることで成功する可能性が最も高い迅速な回復方法を試すことができます。これで、スーパーバイザから電源が完全に外されて、RAIDの両方のディスクの回復が可能になります。物理的な抜き差しによる回復が部分的に成功する場合は手順3に進み、まったく成功せずシステムが完全に起動しない場合は手順4に進みます。

3. 部分的な回復の場合、つまりリロード後に1つのディスクが起動し、もう1つのディスクがまだ[U_]状態でダウンしている場合は、次の推奨手順として、フラッシュ回復ツールを実行して他のディスクを再同期します。回復ツールが成功しない場合は、TACに手動による回復手順を依頼します。スーパーバイザの物理的な抜き差しも試すことができます。回復ツールは次のリンクからダウンロードできます。

<https://software.cisco.com/download/release.html?mdfid=284472710&flowid=&softwareid=282088132&reind=AVAILABLE&rellifecycle=&reltype=latest>

リロードで両方のスーパーバイザが完全に起動しない場合は、スーパーバイザモジュールの物理的な抜き差しを実行してください。一般的に、デュアルフラッシュ障害の場合、ソフトウェアの「リロード」では、電源がモジュールから完全に外されないため、両方のディスクは完全に回復されませんが、物理的な抜き差しを行うとモジュールから電源を完全に外すことができます。物理的な抜き差しが成功しない場合は、手順4に進みます。

4. 物理的な抜き差しが成功しない場合、次のステップは、パスワード回復手順を使用してローダープロンプトに入り、キックスタートをスイッチブートモードにロードし、「init system」を実行します。これにより、ブートフラッシュが消去され、アレイの修復が試みられます。init systemが完了するか失敗して、問題が解決されない場合は、もう一度物理的な抜き差しを試してください。

上記のすべての手順が完了しても、回復できない場合は、まれなハードウェアの故障が発生している可能性があります。その場合はスーパーバイザをRMAにより交換する必要があります。回復

手順の前に、すべてのコンフィギュレーションを外部にバックアップするのはこのためです。緊急の RMA が必要な場合、システムを迅速に元に戻すために必要なすべてのコンフィギュレーションを用意しておきます。

要約

Modules	Supervisor 1	Supervisor Engine 2/2e (Nexus 7000)	Supervisor Engine 2E (Nexus 7700)
Bootflash types	Legacy Compact Flash for internal bootflash	(2) eUSB flash devices in a RAID mirror	single eUSB flash due to form factor constrains
Bootflash function	software image configuration storage	<ul style="list-style-type: none">internally store software imagesinternal partitions for binary startup configuration	<ul style="list-style-type: none">internally store software imagesinternal partitions for binary startup configurationOBFL and for integrated logflash
Symptoms	This supervisor is not affected by the compact flash bug	<ul style="list-style-type: none">GOLD failures for "Compact Flash" deviceInability to save the running configuration.	<ul style="list-style-type: none">GOLD failures for "Compact Flash" device <CSCuW62106>Inability to save the running configuration.
Root cause	NA	<ul style="list-style-type: none">This is not a hardware failure in most cases.Transient hang of eUSB deviceeUSB firmware, from specific vendor, has a software bug that caused the eUSB Flash to become unresponsive under certain conditionsWhen eUSB flash is unresponsive it causes the device to be removed from USB bus, possibly corrupting files system.Issue seen after months to years of continuous operation in the field and dependent on IO load	<ul style="list-style-type: none">This is not a hardware failure in most cases.Transient hang of eUSB deviceeUSB firmware, from specific vendor, has a software bug that caused the eUSB Flash to become unresponsive under certain conditionsWhen eUSB flash is unresponsive it causes the device to be removed from USB bus, possibly corrupting files system.Issue seen after months to years of continuous operation in the field and dependent on IO load
Workarounds/Fixes	NA	<ul style="list-style-type: none">Manual Repair tool (on CCO)6.2.14 has repair tool integrated into the code that is run on a scheduled basis (CSCus22805)Starting in NxOS 6.2(16) and NxOS 7.2 and later supervisor will update eUSB firmware devices automatically on boot(CSCuV64056)	Starting in NxOS 6.2(16) and NxOS 7.2 and later supervisor will update eUSB firmware devices automatically on boot(CSCuV64056)
Caveats	NA	Dual eUSB failure cannot be repaired via tool or integrated repair function that is available on 6.2(14)	N77 supervisors cannot be repaired using repair tool on CCO as it contains only a single eUSB device for bootflash (No RAID mirrors for bootflash)
Associated Bugs	NA	CSCus22805 CSCuV64056	CSCuV64056
Field Notices	NA	FN - 63975	FN - 64154

FAQ

この問題に対する恒久的な解決策はありますか。

以下の「長期にわたる解決策」を参照してください。

スタンバイのスーパーバイザをリロードしてフェールオーバーすることにより、アクティブとスタンバイでデュアル フェールオーバーを回復できないのはなぜですか

。

回復できない原因は、スタンバイ スーパーバイザを「ha-standby」状態で起動可能にするために、アクティブ スーパーバイザがいくつかのデータ (SNMP 情報など) を Compact Flash に書き込む必要がありますが、それ自体にデュアル フラッシュ障害がある場合、その処理を実行できないためです。

フラッシュ回復ツールで Compact Flash をマウントし直すことができない場合どうなりますか。

このシナリオのオプションについては、Cisco TAC にお問い合わせください。

このバグは Nexus 7700 Sup2E にも影響しますか。

N7700 Sup2E - [CSCuV64056](#) には別の欠陥があります。回復ツールは N7700 では機能しません

。

回復ツールは NPE イメージに対して機能しますか。

回復ツールは NPE イメージでは機能しません。

コードの解決済みバージョンへの ISSU によってこの問題は解決されますか。

いいえ。ISSUはスーパーバイザのスイッチオーバーを利用しますが、コンパクトフラッシュの障害が原因で正常に動作しない場合があります。

影響を受けるボードをリセットします。RAID の状態は 0xF0 を示しますが、GOLD テストは失敗しますか。

RAID の状態ビットは、自動回復の適用後ボードがリセットされるとリセットされます。ただし、すべての障害状態が自動的に回復されるわけではありません。RAID の状態ビットが [2/2] [UU] として示されない場合、回復は不完全です。リストされている回復手順に従ってください。

フラッシュの障害は動作に影響しますか。

いいえ。ただし、システムでは電源障害でバックアップをブートしない場合があります。スタートアップ コンフィギュレーションも失われます。

監視と回復に関してユーザの観点から健全な実行システムを実現するにはどのような推奨事項がありますか。

GOLD コンパクト テストの状態では障害がないか確認し、最初のフラッシュ パーツで障害が発生するとすぐに回復を行います。

影響のあるコードから修正済みリリースへの ISSU を実行して eUSB フラッシュの障害を修正できますか。

ISSU は障害が発生した eUSB を修正しません。最適なオプションは、sup の 1 つの eUSB 障害に対して回復ツールを実行するか、デュアル eUSB 障害の場合は sup をリロードします。問題が修正されたら、アップグレードを実行します。[CSCus22805 の修正では 1 つの eUSB 障害のみを修正できます。これは、システムを定期的にスキャンし、スクリプトを使用してアクセス不可または読み取り専用の eUSB を復旧させることで実行できます。](#)スーパーバイザで両方の eUSB フラッシュ障害が同時に発生することはまれであるため、この回避策は有効です。

プラグインまたはリロードを使用してフラッシュの障害を修正した場合、問題が再発するまでどのくらいの時間がかかりますか。

通常、この問題は稼働時間が長いと発生します。この期間は正確に定量化されていませんが、1年以上にわたる場合があります。結果として、読み書きについて eUSB フラッシュにかかる負荷が多いほど、システムでこのシナリオが生じる可能性が高くなります。

show system internal raid では、フラッシュの状態が異なるセクションに 2 回表示されます。また、これらのセクションは一致していません。

最初のセクションには現在の状態が表示され、2 番目のセクションにはブートアップの状態が表示されます。

現在の状態は重要で、常に UU が示される必要があります。

長期にわたる解決策

この問題の回避策は 6.2(14) にありますが、ファームウェアの修正が 6.2(16) と 7.2(x) 以降に追加されています。

この問題を完全に解決するには、ファームウェアの修正を含むリリースにアップグレードすることをお勧めします。

NXOS の修正済みバージョンにアップグレードできない場合は、2 つの解決策があります。

解決策 1 は、スケジューラを使用してフラッシュ回復ツールを毎週予防的に実行する方法です。ブートフラッシュでフラッシュ回復ツールとともに以下のスケジューラ設定を使用します。

feature scheduler

scheduler job name Flash_Job

```
copy bootflash:/n7000-s2-flash-recovery-tool.10.0.2.gbin bootflash:/flash_recovery_tool_copy
load bootflash:/flash_recovery_tool_copy
```

exit

scheduler schedule name Flash_Recovery

job name Flash_Job

time weekly 7

注：

- フラッシュ回復は同じ名前とし、ブートフラッシュ内に保存する必要があります。
- 「time weekly 7」設定の 7 は曜日を表し、この場合は土曜日です。
- 推奨されるフラッシュ回復ツールの最大実行頻度は週に 1 回です。

解決策 2 は、この[technote リンク](#)で説明されています。

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。