基本操作（Basic Operations）

- APIC クラッシュ シナリオのトラブルシューティング （1 ページ）
- Cisco APIC トラブルシューティング オペレーション （13 ページ）
- スイッチ操作 （16 ページ）
- ファブリックの再構築の実行 （20 ページ）
- ループバック障害のトラブルシューティング （22 ページ）
- 不要な _ui_ オブジェクトの削除 （24 ページ）
- Cisco APIC SSD の交換 （25 ページ）
- CRC エラー カウンターの表示 （27 ページ）

APIC クラッシュ シナリオのトラブルシューティング

クラスタのトラブルシューティング シナリオ

次の表は、Cisco APIC に共通するクラスタのトラブルシューティングのシナリオを示します。

問題	ソリューション
APIC ノードはクラスタ内でエラーが発生します。たとえば、5 つの APIC のクラスタのノード 2 がエラーを起こすとします。	2 つの解決策があります。 • 目標サイズはそのままにし、APIC を交換します。 • クラスタ サイズを 4 に減らし、コントローラ 5 をデコミッションし、APIC 2 として再コミッションします。ターゲット サイズは 4 のままで、再構成された APIC がアクティブになったときの運用サイズは 4 です。 （注） クラスタに交換する APIC を追加し、目標サイズと動作サイズを増大することができます。新しい APIC を追加する方法については、『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』を参照してください。

問題	ソリューション
新しい APIC はファブリックに接続し、リーフ スイッチへの接続は失われます。	インフラ（インフラストラクチャ）VLAN の不一致があるかを確認するには、次のコマンドを使用します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：リーフ スイッチ上で構成された VLAN を表示します。 • cat /mit/sys/lldp/inst/if-\[eth1--1\]/ctrlradj/summary：接続された APIC によってアドバタイズされるインフラ（インフラストラクチャ）VLAN を表示します。 これらのコマンドの出力が異なる VLAN を表示する場合、新しい APIC は正しいインフラ（インフラストラクチャ）VLAN で設定されていません。この問題を解決するには、次の手順に従います。 • レスキューユーザーを使用して APIC にログインします。 （注） APIC はファブリックの一部ではないため、管理者のログイン情報は機能しません。 • 構成を消去し、 **acidiag touch setup** コマンドを使用して APIC を再起動します。 • APIC を再構成します。ファブリック名、TEP アドレス、およびクラスタの APIC にマッチするインフラ（インフラストラクチャ）VLAN を確認します。 • リーフ ノードをリロードします。25-03-2015 22:13
2 つの APIC は、再起動後に通信できません。	この問題は次の一連のイベントの後に発生することがあります。 • APIC1 と APIC2 が相互に検出します。 • APIC1 がリブートし、新しいシャーシ ID （APIC1a）でアクティブになる。 • 2 つの APIC が通信しなくなる。 このシナリオでは、APIC1a が APIC2 を検出しますが、APIC2 はオフラインと見なされる APIC1 があるクラスタ内に存在するので使用できません。その結果、APIC1a は APIC2 からのメッセージを受け入れません。 この問題を解決するには、APIC2 上の APIC1 をデコミッションし、再度 APIC1 を稼働させます。

問題	ソリューション
デコミッションされた APIC がクラスタに参加します。	この問題は次の一連のイベントの後に発生することがあります。 • クラスタのメンバーが使用できなくなるか、クラスタが分割されます。 • APIC はデコミッションされます。 • クラスターが回復すると、デコミッションされた APIC が自動的に試運転されます。 この問題を解決するには、クラスタの回復後に APIC をデコミッションします。
再起動後の ChassisID が一致しません。	この問題は、APICがクラスタで登録されたシャーシIDと異なるシャーシIDで起動したときに起こります。その結果、このAPICからのメッセージが廃棄されます。 この問題を解決するには、リブートの前に APIC が解放されていることを確認してください。
APIC はクラスタ サイズの変更時のエラーを表示します。	さまざまな条件が、AdminstrativeClusterSize に合わせたクラスタによる OperationalClusterSize の拡張の妨げになる可能性があります。詳細については、障害を調べて、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「クラスタ障害」セクションを確認してください。
APIC がクラスタに参加できない	この問題は、クラスタを拡大するときに 2 つの APIC が同じクラスタ ID で設定されると起こります。その結果、2 つのうち 1 つの APIC がクラスタに参加できず、拡張競合シャーシ ID 不一致のエラーが表示されます。 この問題を解決するには、新しいクラスタ ID でクラスタの外側に APIC を設定します。

問題	ソリューション
APIC がクラスタで到達不能です。	この問題を診断するには、次の設定を確認してください。 • ファブリック検出が完了していることを確認します。 • ファブリックから欠落しているスイッチを特定します。 • スイッチが APIC からの IP アドレスを要求し、受信したかどうかを確認します。 • スイッチがソフトウェア イメージをロードしたことを確認します。 • スイッチがアクティブになっている時間を確認します。 • すべてのプロセスがスイッチ上で動作していることを確認します。詳細については、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「acidiag コマンド」セクションを参照してください。 • 欠落しているスイッチに正しい日付と時刻が設定されていることを確認します。 • スイッチが他の APIC と通信できることを確認します。
クラスタは拡張しません。	この問題は、次の状況で発生します。 • OperationalClusterSize が APIC の数より少ない。 • 拡張候補はありません (たとえば、管理サイズが 5 であり、clusterID が 4 の APIC がありません。 • クラスタと新しい APIC の間に接続がない • 新しい APIC によってハートビート メッセージが拒否される • システムが正常ではありません。 • 使用できないアプライアンスは、再配置に関連するデータ サブセットを保持しています。 • 再配置に関連するデータ サブセットを持つアプライアンスでサービスがダウンしています。 • 再配置に関する不健全なデータ サブネット

問題	ソリューション
APIC がダウンしています。	次の点を確認します。 • 接続の問題：ping を使用して接続を確認します。 • インターフェイス タイプの不一致：すべての APIC がインバンド通信になっていることを確認します。 • ファブリック接続：ファブリック接続が正常であること、およびファブリック検出が完了していることを確認します。 • 拒否されたハートビート：fltInfraIICIMsgSrcOutsider エラーを確認します。一般的なエラーには、動作クラスタ サイズ、シャーシ ID の不一致、動作クラスタ サイズの外の送信元 ID 、承認されていない送信元、およびファブリック ドメインの不一致が含まれます。

クラスタの障害

APIC は、クラスタの問題の診断に役立つさまざまなエラーをサポートします。ここでは、2 つの主要なクラスタのエラーの種類について説明します。

エラーの破棄

APIC は現在のクラスタのピアまたはクラスタ拡大候補以外からのクラスタ メッセージを破棄します。APIC によりメッセージを破棄した場合、発信元の APIC のシリアル番号、クラスタ ID、タイムスタンプを含むエラーが発生します。次の表で、破棄されるメッセージのエラーを要約します。

Fault	意味
expansion-contender-chassis-id-mismatch	送信側 APIC のシャーシ ID が拡大のためにクラスタが認識するシャーシ ID と一致しません。
expansion-contender-fabric-domain-mismatch	送信側 APIC のファブリック ID が拡大のためにクラスタが認識するファブリック ID と一致しません。
expansion-contender-id-is-not-next-to-oper-cluster-size	送信側 APIC に拡大に不適切なクラスタ ID があります。値は、現在の OperationalClusterSize よりも 1 大きい必要があります。
expansion-contender-message-is-not-heartbeat	送信側 APIC が継続的ハートビート メッセージを送信しません。
fabric-domain-mismatch	送信側 APIC のファブリック ID がクラスタのファブリック ID と一致しません。
operational-cluster-size-distance-cannot-be-bridged	送信側 APIC に、受信側 APIC のものとは 1 以上違う OperationalClusterSize があります。受信側 APIC は要求を拒否します。

Fault	意味
source-chassis-id-mismatch	送信側 APIC のシャーシ ID がクラスタに登録されたシャーシ ID と一致しません。
source-cluster-id-illegal	送信側 APIC に許可されていないクラスタ ID 値があります。
source-has-mismatched-target-chassis-id	送信側 APIC の目標シャーシ ID が受信側 APIC のシャーシ ID に一致しません。
source-id-is-outside-operational-cluster-size	送信側 APIC に、クラスタの OperationalClusterSize 外のクラスタ ID があります。
source-is-not-commissioned	送信側 APIC にクラスタで現在解放されている ID があります。

クラスタ変更時エラー

次のエラーは、APIC のクラスタ サイズの変更時のエラーがある場合に適用されます。

Fault	意味
cluster-is-stuck-at-size-2	このエラーは、OperationalClusterSize が拡張期間にわたり 2 のままになると発行されます。問題を解決するには、クラスタの目標サイズをリストアします。
most-right-appliance-remains-commissioned	クラスタ内の最後の APIC が稼働中で、クラスタの縮小を妨げています。
no-expansion-contender	クラスタがより大きいクラスタ ID を持つ APIC を検出できず、クラスタの拡張を行えません。
service-down-on-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、障害が起きているサービス上にコピーがあります。APIC に複数のこのような障害があることを示します。
unavailable-appliance-carrying-replica-related-to-relocation	移動するデータのサブセットは、使用できない APIC 上にコピーがあります。このエラーを解決するには、使用できない APIC を復元します。
unhealthy-replica-related-to-relocation	移動するデータのサブセットは、正常でない APIC 上にコピーがあります。このエラーを解決するには、障害の根本原因を特定します。

APIC 使用不可

次のクラスタのエラーは、APIC が使用できない場合に適用できます。

Fault	意味
fltInfraReplicaReplicaState	クラスタがデータのサブセットを起動できません。
fltInfraReplicaDatabaseState	データ ストア サービスの破損を示します。

Fault	意味
fltInfraServiceHealth	データのサブセットが完全には機能していないことを示します。
fltInfraWiNodeHealth	APIC が完全には機能していないことを示します。

ファブリック ノードとプロセス クラッシュのトラブルシューティング

ACI スイッチ ノードには、システムのさまざまな機能面を制御する多数のプロセスがあります。システムの特定のプロセスでソフトウェア障害が発生した場合、コア ファイルが生成され、プロセスがリロードされます。

プロセスが Data Management Engine（DME）プロセスの場合、DME プロセスは自動的に再起動します。プロセスが非 DME プロセスの場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。

このセクションでは、さまざまなプロセスの概要、プロセスがコア化したことを検出する方法、およびこれが発生したときに取るべきアクションについて説明します。

DME プロセス

APIC で実行されている重要なプロセスは、CLI で見つけることができます。APIC とは異なり、 **FABRIC** > **INVENTORY** > **Pod 1** > ***node*** の GUI を介して表示できるプロセスには、リーフで実行されているすべてのプロセスが表示されます。

ps-ef | grep svc_ifc を経由：

```
rtp_leaf1# ps -ef |grep svc_ifc
root 3990 3087 1 Oct13 ? 00:43:36 /isan/bin/svc_ifc_policyelem --x
root 4039 3087 1 Oct13 ? 00:42:00 /isan/bin/svc_ifc_eventmgr --x
root 4261 3087 1 Oct13 ? 00:40:05 /isan/bin/svc_ifc_opflexelem --x -v
dptcp:8000
root 4271 3087 1 Oct13 ? 00:44:21 /isan/bin/svc_ifc_observerelem --x
root 4277 3087 1 Oct13 ? 00:40:42 /isan/bin/svc_ifc_dbgrelem --x
root 4279 3087 1 Oct13 ? 00:41:02 /isan/bin/svc_ifc_confelem --x
rtp_leaf1#
```

スイッチで実行されている各プロセスは、システムのログ ファイルにアクティビティを書き込みます。これらのログ ファイルは、techsupport ファイルの一部として処理されていますが、CLI アクセスを介して /tmp/logs/ ディレクトリにあります。たとえば、ポリシー エレメントのプロセス ログ出力は、/tmp/logs/svc_ifc_policyelem.log に書き込まれます。

以下は、システムで実行されている DME プロセスの簡単な説明です。これは、特定のプロセスのトラブルシューティング時にどのログ ファイルを参照するかを理解したり、プロセスがクラッシュした場合のシステムへの影響を理解したりするのに役立ちます。

プロセス	機能
ポリシー要素	ポリシー要素: APIC からの論理 MO を処理し、具体的なモデルをスイッチにプッシュします

プロセス	機能
eventmgr	イベント マネージャ：ローカルの障害、イベント、ヘルス スコアを処理します
opflexelem	Opflex 要素: スイッチ上の Opflex サーバ
observerelem	オブザーバ要素: APIC に送信されたローカル統計を処理します
dbgrelem	デバッガー要素：コア ハンドラ
nginx	スイッチと APIC 間のトラフィックを処理する Web サーバ

プロセスがいつクラッシュしたかを特定する

プロセスがクラッシュしてコア ファイルが生成されると、イベントだけでなく障害も生成されます。APIC からの次の syslog 出力に示されているように、特定のプロセスの障害は「プロセス クラッシュ」として表示されます。

```
Oct 16 03:54:35 apic3 %LOG_LOCAL7-3-SYSTEM_MSG [E4208395][process-crash][major]
[subj-[dbgs/cores/node-102-card-1-svc-policyelem-ts-2014-10-16T03:54:55.000+00:00]/
rec-12884905092]Process policyelem cored
```

スイッチのプロセスがクラッシュすると、コア ファイルが圧縮され、APIC にコピーされます。syslog メッセージ通知は APIC から送信されます。

プロセスがクラッシュしたときに生成される障害は、プロセスが再起動された Cisco Application Centric Infrastructure 275 のトラブルシューティングでクリアされます。障害は、**[ファブリック（FABRIC）] > [インベントリ（INVENTORY）] > [ポッド 1 （Pod 1）]** でファブリック履歴タブの GUI を介して表示できます。

コア ファイルの収集

APIC GUI は、ファブリック ノードのコア ファイルを収集するための中心的な場所を提供します。

エクスポート ポリシーは、**ADMIN** > **IMPORT/EXPORT** > **Export Policies** > **Core** から作成されます。ただし、ファイルを直接ダウンロードできるデフォルトのコア ポリシーがあります。

コア ファイルには、コア ファイルが配置されている APIC の /data/techsupport にある APIC を介して SSH/SCP 経由でアクセスできます。コア ファイルは、クラスタ内の 1 つの APIC の /data/techsupport で入手できることに注意してください。コア ファイルが存在する正確な APIC は、GUI に表示されるエクスポート ロケーション パスで見つけることができます。たとえば、エクスポート先が「files/3/」で始まる場合、ファイルはノード 3（APIC3）にあります。

APIC プロセスのクラッシュの検証と再起動

症状 1

スイッチファブリックのプロセスがクラッシュします。プロセスが自動的に再起動するか、スイッチがリロードして復元します。

- **検証**：

  概要セクションに示されているように、DME プロセスがクラッシュした場合、スイッチを再起動せずに自動的に再起動する必要があります。非 DME プロセスがクラッシュした場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。

  どのプロセスがクラッシュするかによって、プロセス コアの影響は異なります。

  非DMEプロセスがクラッシュすると、通常コンソールに表示されるようにHAPリセットが発生します。

```
[ 1130.593388] nvram_klm wrote rr=16 rr_str=ntp hap reset to nvram
[ 1130.599990] obfl_klm writing reset reason 16, ntp hap reset
[ 1130.612558] Collected 8 ext4 filesystems
```

- **プロセス ログの確認**：

  クラッシュするプロセスには、クラッシュ前に何らかのレベルのログ出力が必要です。スイッチのログの出力は、/tmp/logsディレクトリに書き込まれます。プロセス名はファイル名の一部になります。たとえば、ポリシー エレメント プロセスの場合、ファイルは svc_ifc_policyelem.log です。

```
rtp_leaf2# ls -l |grep policyelem
-rw-r--r-- 2 root root 13767569 Oct 16 00:37 svc_ifc_policyelem.log
-rw-r--r-- 1 root root 1413246 Oct 14 22:10 svc_ifc_policyelem.log.1.gz
-rw-r--r-- 1 root root 1276434 Oct 14 22:15 svc_ifc_policyelem.log.2.gz
-rw-r--r-- 1 root root 1588816 Oct 14 23:12 svc_ifc_policyelem.log.3.gz
-rw-r--r-- 1 root root 2124876 Oct 15 14:34 svc_ifc_policyelem.log.4.gz
-rw-r--r-- 1 root root 1354160 Oct 15 22:30 svc_ifc_policyelem.log.5.gz
-rw-r--r-- 2 root root 13767569 Oct 16 00:37 svc_ifc_policyelem.log.6
-rw-rw-rw- 1 root root 2 Oct 14 22:06 svc_ifc_policyelem.log.PRESERVED
-rw-rw-rw- 1 root root 209 Oct 14 22:06 svc_ifc_policyelem.log.stderr
rtp_leaf2#
```

  /tmp/logsにあるプロセスごとにいくつかのファイルがあります。ログ ファイルのサイズが大きくなるにつれて、ログ ファイルは圧縮され、古いログ ファイルはローテーションされなくなります。コア ファイルの作成時刻（GUI とコア ファイル名に表示される）を確認して、ファイルのどこを確認すればよいかを理解します。また、プロセスが最初に起動しようとすると、ログファイルに「クラッシュ後にプロセスが再起動しています」というエントリが記録されます。このエントリを使用して、クラッシュの前に何が起こったかを遡って検索できます。

- **アクティビティをチェック**：

  実行中のプロセスに変更が加えられたため、クラッシュが発生しました。多くの場合、変更はシステムの構成アクティビティによるものである可能性があります。システムで発生したアクティビティは、システムの監査ログ履歴で確認できます。

- **TAC に連絡する**：

  通常、プロセスのクラッシュは発生しません。上記の手順を超える理由をよりよく理解するには、コア ファイルをデコードする必要があります。この時点で、ファイルを収集して、さらに処理するために TAC に提供する必要があります。

  上記の方法でコア ファイルを収集し、TAC でケースをオープンします。

症状 2

ファブリック スイッチが継続的にリロードするか、BIOS ローダー プロンプトでスタックします。

- **検証**：

  DME プロセスがクラッシュした場合、スイッチの再起動をせずに自動的に再起動する必要があります。非DMEプロセスがクラッシュした場合、プロセスは自動的に再起動せず、スイッチが再起動して回復します。ただし、いずれの場合でもプロセスが継続的にクラッシュすると、スイッチは継続的なリロードループに入るか、BIOS ローダー プロンプトで終了する可能性があります。

```
[ 1130.593388] nvram_klm wrote rr=16 rr_str=policyelem hap reset to nvram
[ 1130.599990] obfl_klm writing reset reason 16, policyelem hap reset
[ 1130.612558] Collected 8 ext4 filesystems
```

- **HAP リセット ループを破る**：

  最初のステップは、スイッチをさらに情報を収集できる状態に戻すことです。

  スイッチが継続的に再起動している場合、スイッチの起動時に、スイッチが起動サイクルの最初の部分である場合 CTRL C を入力して、コンソールから BIOS ローダー プロンプトに侵入します。

  スイッチがローダー プロンプトに表示されたら、次のコマンドを入力します。

  - cmdline no_hap_reset
  - ブート

  cmdline コマンドは、hap リセットが呼び出されたときにスイッチがリロードするのを防ぎます。2番目のコマンドでは、システムを起動します。リロードによって入力されたcmdlineオプションが削除されるため、ローダーでのリロードの代わりに boot コマンドが必要であることに注意してください。

  これで、システムはデータを収集するためのより適切なアクセスを許可するようになったはずですが、プロセスがクラッシュするとスイッチの機能に影響を与えます。

前の表のように、プロセス ログ、アクティビティを確認し、TACの手順に連絡してください。

APIC プロセス クラッシュのトラブルシューティング

APIC には、システムのさまざまな機能的側面を制御する一連のデータ管理エンジン（DME）プロセスがあります。システムの特定のプロセスでソフトウェア障害が発生すると、コア ファイルが生成され、プロセスが再ロードされます。

次のセクションでは、システム プロセスのクラッシュやソフトウェアの障害に関連する潜在的な問題について説明します。まず、さまざまなシステム プロセスの概要、プロセスがコア化されたことを検出する方法、およびこれが発生したときに取るべきアクションについて説明します。正常に動作しているシステムの表示は、突然終了した可能性のあるプロセスを特定するために使用できます。

DME プロセス

APIC で実行されている重要なプロセスは、GUI または CLI のいずれかで見つけることができます。GUI を使用すると、実行中のプロセスとプロセス ID が **[システム（System）] > [コントローラ（Controllers）] > [プロセス（Processes）]** に表示されます。

CLI を使用すると、プロセスとプロセス ID は、/aci/system/controllers/1/processes（APIC1 の場合）のサマリ ファイルにあります。

```
admin@RTP_Apic1:processes> cat summary
processes:
process-id process-name max-memory-allocated state
---------- ---------------- -------------------- -------------------
0 KERNEL 0 interruptible-sleep
331 dhcpd 108920832 interruptible-sleep
336 vmmmgr 334442496 interruptible-sleep
554 neo 398274560 interruptible-sleep
1034 ae 153690112 interruptible-sleep
1214 eventmgr 514793472 interruptible-sleep
2541 bootmgr 292020224 interruptible-sleep
4390 snoopy 28499968 interruptible-sleep
5832 scripthandler 254308352 interruptible-sleep
19204 dbgr 648941568 interruptible-sleep
21863 nginx 4312199168 interruptible-sleep
32192 appliancedirector 136732672 interruptible-sleep
32197 sshd 1228800 interruptible-sleep
32202 perfwatch 19345408 interruptible-sleep
32203 observer 724484096 interruptible-sleep
32205 lldpad 1200128 interruptible-sleep
32209 topomgr 280576000 interruptible-sleep
32210 xinetd 99258368 interruptible-sleep
32213 policymgr 673251328 interruptible-sleep
32215 reader 258940928 interruptible-sleep
32216 logwatch 266596352 interruptible-sleep
32218 idmgr 246824960 interruptible-sleep
32416 keyhole 15233024 interruptible-sleep
admin@apic1:processes>
```

APIC で実行されている各プロセスは、システムのログ ファイルに書き込みます。これらのログ ファイルは、APIC techsupport ファイルの一部としてバンドルできますが、/var/log/dme/log の SSH シェル アクセスを介して確認することもできます。たとえば、Policy Manager プロセス ログ出力は /var/log/dme/log/svc_ifc_policymgr.bin.log に書き込まれます。

以下は、システムで実行されているプロセスの簡単な説明です。これは、特定のプロセスのトラブルシューティング時にどのログ ファイルを参照するかを理解したり、プロセスがクラッシュした場合のシステムへの影響を理解したりするのに役立ちます。

プロセス	機能
カーネル	Linux カーネル
dhcpd	APICがインフラアドレスを割り当てるために実行されている DHCP プロセス
vmmmgr	APICとハイパーバイザ間のプロセスを処理します
neo	Shell CLI インタープリタ
ae	ローカルAPICアプライアンスの状態とインベントリを処理します
eventmgr	システム上のすべてのイベントと障害を処理します
bootmgr	ファブリック ノードでの起動とファームウェアの更新を制御します
snoopy	Shell CLI ヘルプ、タブ コマンド補完
scripthandler	L4-L7 デバイスのスクリプトと通信を処理します
dbgr	プロセスがクラッシュしたときにコア ファイルを生成します
nginx	Web サービス処理 GUI および REST API アクセス
appliancedirector	APIC クラスタの形成と制御を処理します
sshd	APIC への SSH アクセスを有効化
perfwatch	Linux cgroup 技術情報の使用法を監視します
observer	ファブリック システムと状態、統計、正常性のデータ処理を監視します
lldpad	LLDP エージェント
topomgr	ファブリックのトポロジとインベントリを維持します

Cisco APIC トラブルシューティング オペレーション

Cisco APIC システムのシャットダウン

この手順では、Cisco Application Policy Infrastructure Controller（APIC）システムをシャットダウンします。システムをシャットダウンした後、ファブリック全体を再配置してから電源を入れ、それに応じてタイム ゾーンおよび/または NTP サーバーを更新します。

始める前に

クラスタの健全性が完全に適合していることを確認します。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）] > *apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
ステップ 4 Cisco APIC を再配置してから、電源を入れます。
ステップ 5 クラスタが完全に収束したことを確認します。
ステップ 6 次の Cisco APIC についてこの手順を繰り返します。

GUI を使用した Cisco APIC のシャットダウン

この手順では、Cisco Application Policy Infrastructure Controller（APIC）をシャットダウンします。この手順では、Cisco APIC システム全体ではなく、1 つの Cisco APIC システムのみがシャットダウンされます。この手順に従うと、コントローラはすぐにシャットダウンします。コントローラを元に戻すには、実際のマシンから実行するしかないため、シャットダウンの実行には注意が必要です。マシンにアクセスする必要がある場合は、「GUI を使用した LED ロケータの制御 （14 ページ）」を参照してください。

（注） 可能であれば、Cisco APIC を 1 つずつ移動します。クラスタ内にオンラインの Cisco APIC が少なくとも 2 つある限り、読み取り/書き込みアクセスが可能です。一度に複数の Cisco APIC を再配置する必要がある場合、これにより、1 つまたはすべてのコントローラがオンラインになり、ファブリックはシャットダウン時に読み取り専用モードになります。この間、エンドポイントの移動（仮想マシンの移動を含む）を含むポリシーの変更はできません。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
ステップ 4 Cisco APIC を再配置してから、電源を入れます。
ステップ 5 クラスタが完全に収束したことを確認します。

GUI を使用した APIC リロード オプションの使用

この手順では、GUI を使用して、Cisco APIC システム全体ではなく Cisco Application Policy Infrastructure Controller（APIC）をリロードします。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、**[リロード（Reload）]** を選択します。

GUI を使用した LED ロケータの制御

この手順では、GUI を使用して Cisco Application Policy Infrastructure Controller（APIC）の LED ロケータをオンまたはオフにします。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**[コントローラ（Controllers）]** > ***apic_name*** を選択します。
ステップ 3 Cisco APIC を右クリックし、必要に応じて **[ロケータ LED をオンにする（Turn On Locator LED）]** または **[ロケータ LED をオンにする（Turn On Locator LED）]** を選択します。

GUI を使用したファブリックの電源切断

この手順では、電源メンテナンスのため、Cisco Application Policy Infrastructure Controller（APIC）GUI および Cisco 統合管理コントローラ （IMC）GUI を使用してファブリックの電源を切断します。

手順

ステップ 1 Cisco APIC GUI を使用して、最後の 1 台を残し、すべての Cisco APIC をシャットダウンします。

a) Cisco APIC にログインします。
b) メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。
c) Cisco APIC のいずれかのナビゲーションウィンドウで、**[コントローラ（Controllers）]** > ***apic_name***を選択します。
d) Cisco APIC を右クリックし、**[シャットダウン（Shutdown）]** を選択します。
e) 最後の 1 台を除く他のすべての Cisco APIC について、手順 1.c （15 ページ） と 1.d （15 ページ） を繰り返します。

ステップ 2 Cisco IMC GUI を使用して、最後の Cisco APIC をシャットダウンします。

a) 最後の Cisco APIC の Cisco IMC GUI にログインします。
b) [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
c) **[シャーシ（Chassis）]** メニューで **[サマリー（Summary）]** を選択します。
d) 作業ペイン上部のツールバーで、**[ホストの電源（Host Power）]** > **[シャットダウン（Shut Down）]**を選択します。

最後の Cisco APIC では、サーバが読み取り専用モードになり、Cisco APIC GUI を使用してシャットダウンリクエストを処理することができなくなるため、Cisco IMC GUI を使用してシャットダウンする必要があります。

ステップ 3 すべての Cisco APIC をシャットダウンした後、各電源装置をオフにしてスイッチの電源をオフにします。

GUI を使用したファブリックの電源投入

この手順では、Cisco 統合管理コントローラ （IMC）GUI を使用してファブリックに電源を入れます。

手順

ステップ 1 Cisco IMC GUI を使用して Cisco APIC の電源をオンにします。

a) Cisco APIC の Cisco IMC GUI にログインします。
b) [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

c) **[シャーシ（Chassis）]** メニューで **[サマリー（Summary）]** を選択します。
d) 作業ペイン上部のツールバーで、**[ホストの電源（Host Power）]** > **[電源オン（Power On）]**を選択します。
e) すべての Cisco APIC に対し、これらのサブステップを繰り返します。

ステップ 2 Cisco APIC に直接接続されているリーフ スイッチの電源をオンにします。

ステップ 3 リーフ スイッチの電源をオンにしてから約 1 分後に、スパイン スイッチの電源をオンにします。

ステップ 4 ファブリックの残りのリーフ スイッチで電源をオンにします。

Cisco APIC は LLDP により、直接接続されているリーフ スイッチを検出し、その後スパイン スイッチと残りのリーフ スイッチを検出します。Cisco APIC はリロードとシャットダウン後も構成とファブリック メンバーシップを保持するので、検出は自動的に行われます。Cisco APIC が接続されているすべてのリーフ スイッチを検出し、スパインスイッチを検出した後、クラスタは完全に適合した状態で起動します。

スイッチ操作

GUI からの無効なインターフェイスおよび廃止されたスイッチの手動での削除

ファブリック ポートがシャットダウンされてから再びアップされるシナリオでは、ポート エントリが GUI で無効のままになる可能性があります。これが発生した場合、ポートで操作を実行できません。これを解決するには、ポートを GUI から手動で削除する必要があります。

手順

ステップ 1 **[ファブリック（Fabric）]** タブで、**[インベントリ（Inventory）]** をクリックします。

ステップ 2 **[ナビゲーション（Navigation）]**ペインで、**[インターフェイスと廃止されたスイッチを無効にする（Disabled Interfaces and Decommissioned Switches）]** をクリックします。
無効になっているインターフェイスと廃止されたスイッチのリストが、**[作業（Work）]**ペインの要約テーブルに表示されます。

ステップ 3 **[作業（Work）]** ペインで、削除するインターフェイスまたはスイッチを右クリックし、**[削除（Delete）]** を選択します。

スイッチのデコミッションおよび再コミッション

ポッドのすべてのノードをデコミッションし、再コミッションするには、この手順を実行します。この使用例の 1 つは、ノード ID をより論理的でスケーラブルな番号付け規則に変更することです。

手順

ステップ 1 ノードごとに次の手順に従って、ポッド内のノードをデコミッションします。

a) **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** に移動し、**Pod** を展開します。

b) スイッチを選択して右クリックし、**[コントローラから削除（Remove from Controller）]** を選択します。

c) アクションを確認し、**[OK]** をクリックします。

プロセスにはおよそ 10 分ほどかかります。ノードは自動的にワイプされ、リロードされます。さらに、ノード構成がコントローラから削除されます。

d) 廃止されたノードにポート プロファイル機能が展開されている場合、一部のポート構成は残りの構成とともに削除されません。ポートをデフォルト状態に戻すには、デコミッション後に手動で構成を削除する必要があります。これを行うにはスイッチにログインし、**setup-clean-config.sh** スクリプトを実行し、実行されるまで待ちます。それから、**リロード** コマンドを入力します。

ステップ 2 すべてのスイッチがポッドから廃止されたら、それらがすべて物理的に接続され、目的の構成で起動されていることを確認します。

ステップ 3 次のアクションを実行して、各ノードを再稼働させます。

（注）
ポート プロファイルが構成されたノードを新しいノードとして再コミッショ二ングさせる前に、**setup-clean-config.sh** スクリプトを実行して、ポート設定をデフォルト構成に復元する必要があります。

a) **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** に移動し、**[クイック スタート（Quick Start）]** を展開し、**[ノードまたはポッドのセットアップ（Node or Pod Setup）** をクリックします。

b) **[セットアップ ノード（Setup Node）]** をクリックします。

c) **[ポッド ID（Pod ID）]** フィールドで、ポッド ID を選択します。

d) [+] をクリックして、**[ノード（Nodes）]** テーブルを開きます。

e) スイッチのノード ID、シリアル番号、スイッチ名、TEP プール ID、およびロール（**リーフ**または**スパイン**）を入力します。

f) [Update] をクリックします。

ステップ 4 **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[ファブリック メンバーシップ（ Fabric Membership）]** に移動して、ノードがすべて設定されていることを確認します。

次のタスク

ポッドがマルチポッド トポロジ内のポッドの 1 つである場合は、このポッドとノード用にマルチポッドを再構成します。詳細については、『*Cisco APIC Layer 3 Networking* 構成ガイド』「マルチポッド」を参照してください。

Cisco ACI モード スイッチのクリーンリロード

この手順では、Cisco ACI モード スイッチのクリーン リロードを実行します。クリーン リロードでは、スイッチのすべての構成が消去されます。スイッチが起動すると、スイッチは Cisco Application Policy Infrastructure Controller（APIC）から構成を取得します。

手順

ステップ 1 クリーン リロードするスイッチにログインします。

ステップ 2 **setup-clean-config.sh** スクリプトに **-k** 引数を指定して実行します。

例：

```
switch1# setup-clean-config.sh -k
```

ステップ 3 スイッチをリロードします。

例：

```
switch1# reload
```

切断されたリーフの復元

リーフにプッシュされた構成が原因で、リーフ上のすべてのファブリック インターフェイス（リーフをスパインに接続するインターフェイス）が無効になっている場合、リーフへの接続は永久に失われ、リーフはファブリック内で非アクティブになります。接続が失われたため、構成をリーフにプッシュしようとしても機能しません。この章では、切断されたリーフを回復する方法について説明します。

NX-OS-Style CLI を使用した切断されたリーフの復元

この手順では、Cisco Application Policy Infrastructure Controller（APIC）NX-OS スタイルの CLI を使用してファブリック インターフェイスを有効にします。REST API コールを実行できる外部ツールがない場合は、この手順を使用します。

（注） この手順では、1/31 がスパイン スイッチに接続するリーフ スイッチ ポートの 1 つであることを前提としています。

手順

ステップ 1 Cisco APIC NX-OS-style CLI を使用して、ブロック リスト ポリシーを削除します。

例：

```
apic1# podId='1'
apic1# nodeId='103'
apic1# interface='eth1/31'
apic1# icurl -sX POST 'http://127.0.0.1:7777/api/mo/.json' -d '{"fabricRsOosPath":{"attributes":

{"dn":"uni/fabric/outofsvc/rsoosPath-[topology/pod-'$podId'/paths-'$nodeId'/pathep-['$interface']]","status":"deleted"}}}'
```

ステップ 2 リーフ スイッチまたはスパイン スイッチの CLI を使用して、サービス中のポートを設定して、リーフ スイッチのポートを起動します。

例：

```
switch1# podId='1'
switch1# nodeId='103'
switch1# interface='eth1/31'
switch1# icurl -X POST
'http://127.0.0.1:7777/api/node/mo/topology/pod-'$podId'/node-'$nodeId'/sys/action.json'
  -d
'{"actionLSubj":{"attributes":{"oDn":"sys/phys-['$interface']"},"children":[{"l1EthIfSetInServiceLTask":

  {"attributes":{"adminSt":"start"}}}]}}'
```

REST API を使用した切断されたリーフの復元

切断されたリーフ スイッチを復元するには、次のプロセスを使用して、ファブリック インターフェイスの少なくとも 1 つを有効にする必要があります。残りのインターフェイスは、GUI、REST API、または CLI を使用して有効にできます。

最初のインターフェイスを有効にするには、REST API を使用してポリシーを投稿し、投稿されたポリシーを削除し、ファブリック ポートをアウト オブ サービスにします。次のように、ポリシーをリーフ スイッチにポストして、アウト オブ サービスのポートをインサービスにすることができます。

（注） この手順では、1/49 がスパイン スイッチに接続するリーフ スイッチ ポートの 1 つであることを前提としています。

手順

ステップ 1 REST API を使用して、Cisco APIC からブロック リスト ポリシーをクリアします。

例：

```
$APIC_Address/api/policymgr/mo/.xml
<polUni>
    <fabricInst>
        <fabricOOServicePol>
            <fabricRsOosPath tDn="topology/pod-1/paths-$LEAF_Id/pathep-[eth1/49]" lc="blacklist"
status ="deleted"/>
        </fabricOOServicePol>
    </fabricInst>
</polUni>
```

ステップ 2 ローカル タスクをノード自体にポストし、**l1EthIfSetInServiceLTask** を使用して必要なインターフェイスを起動します。

例：

```
$LEAF_Address/api/node/mo/topology/pod-1/node-$LEAF_Id/sys/action.xml
<actionLSubj oDn="sys/phys-[eth1/49]">
    <l1EthIfSetInServiceLTask adminSt='start'/>
</actionLSubj>
```

ファブリックの再構築の実行

ファブリックの再構築

⚠

注意 この手順は非常に混乱を招きます。既存のファブリックを取り除き、新しいファブリックを作り直します。

この手順により、ファブリックを再構築（再初期化）できます。これは、次のいずれかの理由で必要になる場合があります。

- TEP IP を変更するには
- インフラ VLAN を変更するには
- ファブリック名を変更するには
- TAC トラブルシューティング タスクを実行するには

APIC を削除すると、それらの構成が消去され、スタートアップ スクリプトでそれらが表示されます。APIC でこれを実行する順序は任意ですが、すべて（ファブリック内のすべてのリーフとスパイン）で手順を実行するようにしてください。

始める前に

以下が所定の場所に準備されていることを確認します。

- 定期的にスケジュールされた構成のバックアップ
- リーフとスパインへのコンソールアクセス

- KVM コンソール アクセスに必要な構成済みの到達可能な CIMC
- Java の問題なし

手順

ステップ 1 現在の構成を保持したい場合は、構成のエクスポートを実行できます。詳細については、『*Cisco ACI Configuration Files：Import and Export*』の文書 https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 2 KVM コンソールに接続し、次のコマンドを入力して、APIC の設定を消去します。

a) **>acidiag touch clean**
b) **>acidiag touch setup**
c) **>acidiag reboot**

各ノードがファブリック検出モードで起動し、以前に構成されたファブリックの一部ではないことを確認します。

（注）
スタートアップ スクリプトで APIC を起動しないため、 **acidiag touch** コマンドだけはこの手順では役に立ちません。

注意
以前のすべてのファブリック構成が削除されていることを確認することが非常に重要です。単一のノードに以前のファブリック構成が存在する場合でも、ファブリックを再構築することはできません。

ステップ 3 以前の構成がすべて削除されたら、すべての APIC のスタートアップ スクリプトを実行します。この時点で、上記の値、TEP、TEP Vlan、および/またはファブリック名のいずれかを変更できます。これらがすべての APIC で一貫していることを確認してください。詳細については、『*Cisco APIC Getting Started Guide*』の https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 4 ファブリック ノードをクリーン リブートするには、各ファブリック ノードにログインし、次を実行します。

a) **>setup-clean-config.sh**
b) **>reload**

ステップ 5 apic1 にログインし、構成のインポートを実行します。詳細については、『*Cisco ACI Configuration Files：Import and Export*』の文書 https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html を参照してください。

ステップ 6 ファブリックが以前のファブリック登録ポリシーを使用してノード上でファブリックを再構築するようになったため、数分間待ちます。（ファブリックのサイズによっては、この作業に時間がかかる場合があります。）

ループバック障害のトラブルシューティング

障害の発生したライン カードの識別

このセクションでは、ループバック障害が発生したときに、障害が発生したラインカードを特定する方法について説明します。

始める前に

ファブリック ノードのオンデマンド TechSupport ポリシーを作成しておく必要があります。オンデマンド TechSupport ポリシーをまだ作成していない場合は、*Cisco APIC* ベーシック コンフィギュレーション ガイド の「GUI を使用したオンデマンド テクニカル サポート ファイルの送信」セクションを参照してください。

手順

ステップ 1 ファブリック ノードのオンデマンド TechSupport ポリシーのログの場所ファイルを収集します。収集を開始するには：

a) メニュー バーで、[Admin] をクリックします。
b) サブメニュー バーで、[Import/Export] をクリックします。
c) **[ナビゲーション（Navigation）]** ペインで、**[ポリシーのエクスポート（Export Policies）]** を展開し、ファブリック ノードのオンデマンド TechSupport ポリシーを右クリックします。
オプションのリストが表示されます。
d) **[Tech サポートの収集（Collect Tech Supports）]** を選択します。
[Tech サポートの収集（Collect Tech Supports）] ダイアログ ボックスが表示されます。
e) **[Tech サポートの収集（Collect Tech Supports）]** ダイアログ ボックスで、**[はい（Yes）]** をクリックして、テクニカル サポート情報の収集を開始します。

ステップ 2 ファブリック ノードのオンデマンド TechSupport ポリシーのログの場所ファイルをダウンロードします。ログの場所ファイルをダウンロードするには：

a) **[作業（Work）]** ペインの [オンデマンド TechSupport ポリシー（On-Demand TechSupport policy）] ウィンドウから、**[操作性（Operational）]** タブをクリックします。
[オンデマンド TechSupport ポリシー（On-Demand TechSupport policy）] ウィンドウに、**[ログの場所（Logs Location）]** 列を含むいくつかの列とともに概要テーブルが表示されます。
b) **[ログの場所（Logs Location）]** 列の URL をクリックします。

ステップ 3 ログの場所ファイル内で、/var/sysmgr/tmp_logs/ ディレクトリに移動し、svc_ifc_techsup_nxos.tar ファイルを解凍します。

```
-bash-4.1$ tar xopf svc_ifc_techsup_nxos.tar
```

show_tech_info ディレクトリが作成されます。

ステップ 4 **zgrep "fclc-conn failed" show-tech-sup-output.gz | less** を実行します。

```
-bash-4.1$ zgrep "fclc-conn failed" show-tech-sup-output.gz | less
[103] diag_port_lb_fail_module: Bringing down the module 25 for Loopback test failed. Packets possibly
 lost on the switch SPINE or LC fabric (fclc-conn failed)
[103] diag_port_lb_fail_module: Bringing down the module 24 for Loopback test failed. Packets possibly
 lost on the switch SPINE or LC fabric (fclc-conn failed)
```

（注）
fclc-conn failed メッセージは、ラインカードの障害を示しています。

ステップ 5 現在障害が発生しているファブリック カードの電源を入れ直し、ファブリック カードがオンラインになることを確認します。

ステップ 6 ファブリック カードがオンラインにならない場合、またはファブリック カードが再びオフラインになった後、すぐに diag_port_lb.log ファイルを収集して、そのファイルを TAC チームに送信します。diag_port_lb.log ファイルは、ログの場所ファイルの /var/sysmgr/tmp_logs/ ディレクトリにあります。

不要な _ui_ オブジェクトの削除

注意 APIC の基本 GUI を使用して行われた変更を拡張 GUI で表示することはできますが、変更を加えることはできません。また、拡張 GUI で行われた変更を基本 GUI で表示することはできません。基本 GUI と NX-OS スタイルの CLI は常に同期されるため、NX-OS スタイルの CLI から行った変更は基本 GUI に表示され、基本 GUI で行った変更は NX-OS スタイルの CLI に表示されます。ただし拡張 GUI と NX-OS スタイルの CLI の間ではこのような同期が行われません。次の例を参照してください。

- 基本 GUI モードと拡張 GUI モードを混在させないでください。拡張モードを使用して 2 つのポートにインターフェイス ポリシーを適用し、次に基本モードを使用していずれかのポートの設定を変更すると、変更内容が両方のポートに適用される可能性があります。
- APIC でインターフェイスごとの設定を行う際に、拡張 GUI と CLI を混在させないでください。GUI で行われた設定が、NX-OS CLI では部分的にしか機能しない可能性があります。

  たとえば、GUI の **[Tenants]** > ***[tenant-name]*** > **[Application Profiles]** > ***[application-profile-name]*** > **[Application EPGs]** > ***[EPG-name]*** > **[Static Ports]** > **[Deploy Static EPG on PC, VPC, or Interface]** でスイッチ ポートを設定したと仮定します。

  次に NX-OS スタイルの CLI で show running-config コマンドを使用すると、以下のような出力を受信します。

```
leaf 102
interface ethernet 1/15
switchport trunk allowed vlan 201 tenant t1 application ap1 epg ep1
 exit
 exit
```

  NX-OS スタイルの CLI でこれらのコマンドを使用してスタティック ポートを設定すると、次のエラーが発生します。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/15
apic1(config-leaf-if)# switchport trunk allowed vlan 201 tenant t1 application ap1
epg ep1
No vlan-domain associated to node 102 interface ethernet1/15 encap vlan-201
```

  これは、CLI に APIC GUI では実行されない検証があることが原因です。show running-config コマンドによって出力されたコマンドが NX-OS CLI で機能するためには、VLAN ドメインが事前に設定されている必要があります。設定の順序は GUI に適用されません。

- 拡張 GUI を使用する前に、基本 GUI または NX-OS CLI によって変更を加えないでください。変更を加えてしまうと、名前の先頭に _ui_ が付加されたオブジェクトが意図せず作成される場合があります。このオブジェクトは拡張 GUI で変更または削除できません。

高度な GUI を使用する前に、基本 GUI または NX-OS CLI を変更する場合、これは意図せずにオブジェクトが作成され（名前に_ui_ が付加される）、高度な GUI で変更または削除できなくなる場合があります。

このようなオブジェクトを削除する手順については、REST API を使用した不要な _ui_ オブジェクトの削除 （25 ページ）を参照してください。

REST API を使用した不要な _ui_ オブジェクトの削除

Cisco APIC GUI を使用する前に Cisco NX OS スタイル CLI で変更を行い、名前の先頭に _ui_ が付加されたオブジェクトが表示された場合は、API に対して次を含む REST API 要求を実行することでこれらのオブジェクトを削除できます。

- クラス名（例：**infraAccPortGrp**）
- Dn 属性（例：**dn="uni/infra/funcprof/accportgrp-__ui_l101_eth1--31"**
- **status="deleted"** に設定したステータス属性

次の手順で API に POST を実行します。

手順

ステップ 1 削除するオブジェクトへの書き込みアクセス権を持つユーザ アカウントにログインします。

ステップ 2 API に次の例のような POST を送信します。

```
POST https://192.168.20.123/api/mo/uni.xml
Payload:<infraAccPortGrp dn="uni/infra/funcprof/accportgrp-__ui_l101_eth1--31" status="deleted"/>
```

Cisco APIC SSD の交換

この手順を使用して、Cisco APIC のソリッド ステート ドライブ（SSD）を交換します。

（注） この手順は、クラスタに正常な SSD を備えた APIC が少なくとも 1 つあり、完全に適合している場合にのみ実行する必要があります。クラスタ内のすべての APIC コントローラに障害が発生した SSD がある場合は、Cisco Technical Assistance Center（TAC）でケースをオープンしてください。

Cisco APIC のソリッド ステート ドライブ（SSD）の交換

始める前に

- Cisco IMC リリースが 2.0(9c) より前の場合は、ソリッド ステート ドライブ (SSD) を交換する前に Cisco IMC ソフトウェアをアップグレードする必要があります。対象の Cisco IMC リリースのリリース ノートを参照して、現在のリリースから対象のリリースへの推奨されるアップグレードパスを確認してください。このリンクにある『*Cisco Host Upgrade Utility（HUU）User Guide*』の現在のバージョンの指示に従って、アップグレードを実行します。
- Cisco IMC BIOS で、トラステッドプラットフォーム モジュール（TPM）の状態が「有効」に設定されていることを確認します。KVM コンソールを使用して BIOS 設定にアクセスすると、**[高度（Advanced）] > [トラステッド コンピューティング（Trusted Computing）] > [TPM ステート（TPM State）]** で TPM の状態を表示および構成できます。

（注） TPM ステートが「無効」の場合、APIC は起動に失敗します。

- シスコ ソフトウェア ダウンロード サイトから APIC `.iso` イメージを取得します。

（注） APIC `.iso` イメージのリリース バージョンは、クラスタ内の他の APIC コントローラと同じバージョンである必要があります。

手順

ステップ 1 クラスタ内の別の APIC から、SSD を交換する APIC を廃止します。

a) メニューバーで、 **System** > **Controllers** を選択します。
b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。**apic_controller_name** には、廃止されていない APIC コントローラを指定します。
c) 継続する前に、**Work** ウィンドウで、クラスタの **Health State** (**Active Controllers** サマリ テーブルに示されているもの) が **Fully Fit** になっていることを確認します。
d) 同じ **[作業（Work）]** ペインで、廃止するコントローラを選択し、**[アクション（Actions）] > [廃止（Decommission）]** をクリックします。
e) **Yes** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**[作業（Work）]** ウィンドウには表示されなくなります。

ステップ 2 古い SSD があればそれを物理的に取り外し、新しい SSD を追加します。

ステップ 3 Cisco IMC で、新しく取り付けた SSD を使用して RAID ボリュームを作成します。

Cisco IMC については、『*Cisco UCS C* シリーズ統合管理コントローラ *GUI* 構成ガイド』を参照してください。「ストレージアダプタの管理」の章の「未使用の物理ドライブからの仮想ドライブの作成」の手順に従って、RAID 0 仮想ドライブを作成および初期化します。

ステップ 4 Cisco IMC で、仮想メディアを使用して APIC イメージをインストールします。この手順では、SSD がパーティション分割され、APIC ソフトウェアが HDD にインストールされます。

（注）
Cisco APIC リリース 4.x 以降の新規インストールについては、『*Cisco APIC* のインストール、アップグレード、およびダウングレード ガイド』を参照してください。

a) Cisco IMC vMedia 機能を使用して、APIC `.iso` イメージをマウントします。
b) コントローラを起動し電源を再投入します。
c) 起動プロセス中を押して **F6** を選択、 **Cisco vKVM マッピング vDVD** ワンタイム ブート デバイスとして。BIOS パスワードを入力する必要があります。デフォルトのパスワードは「password」です。
d) 最初の起動時に、構成スクリプトが実行されます。画面の指示に従って、APIC ソフトウェアの初期設定を構成します。
e) インストールが完了したら、仮想メディア マウントのマッピングを解除します。

ステップ 5 クラスタ内の APIC から、廃止された APIC を起動します。

a) クラスタの一部である他の APIC を選択します。メニュー バーで、 **[システム (System)]** > **[コントローラ (Controllers)]** を選択します。
b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。 **apic_controller_name** には、クラスタの一部であるアクティブなコントローラーを指定します。
c) **[作業（Work）]** ウィンドウで、**未登録（Unregistered）** と **稼働状態（Operational State）** 列に表示されている廃止されているコントローラをクリックします。
d) **Work** ウィンドウで、**Actions** > **Commission** をクリックします。
e) **Confirmation** ダイアログボックスで **Yes** をクリックします。

稼働済みコントローラには、正常性状態が**完全適合**と表示され、動作状態が**使用可**能と表示されます。これで、コントローラが **[作業（Work）]** ペインに表示されます。

CRC エラー カウンターの表示

CRC およびストンプ CRC エラー カウンターの表示

Cisco APIC リリース 4.2(3) 以降、CRC エラーは、CRC エラーとストンプ CRC エラーの 2 つのカテゴリに分けられています。CRCエラーはローカルでドロップされた破損フレームであり、ストンプCRCエラーはカットスルー スイッチによる破損フレームです。この区別により、CRC エラーの影響を受ける実際のインターフェイスを識別し、ファブリック内の物理層の問題のトラブルシューティングを行うことが容易になります。

このセクションでは、CRC およびストンプ CRC エラーを表示する方法を示します。

GUI を使用した CRC エラーの表示

このセクションでは、GUI を使用して CRC エラーおよびストンプ CRC エラー カウンターを表示する方法を示します。

手順の概要

1. メニュー バーで **[ファブリック（Fabric）] > [インベントリ（Inventory）]** を選択します。
2. **[ナビゲーション（Navigation）]** ペインで、ポッドをクリックして展開します。
3. **[インターフェイス（Interfaces）]** をクリックして展開します。
4. インターフェイスをクリックして、選択します。
5. **[作業（Work）]** ペインで、**[エラー カウンター（Error Counters）]** タブをクリックします。

手順の詳細

手順

ステップ 1 メニュー バーで **[ファブリック（Fabric）] > [インベントリ（Inventory）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、ポッドをクリックして展開します。

ステップ 3 **[インターフェイス（Interfaces）]** をクリックして展開します。
[ナビゲーション（Navigation）] ペインに、インターフェイスのリストが表示されます。

ステップ 4 インターフェイスをクリックして、選択します。
[作業（Work）] ペインに、ウィンドウの上部にタブのリストが表示されます。

ステップ 5 **[作業（Work）]** ペインで、**[エラー カウンター（Error Counters）]** タブをクリックします。
CRC エラー（FCS エラー）および**ストンプCRC エラー（パケット）**を含む、エラー カテゴリのリストが表示されます。

CLI を使用した CRC エラーの表示

このセクションでは、CLI を使用して CRC エラーおよびストンプ CRC エラー カウンターを表示する方法を示します。

手順

CRC エラーおよびストンプ CRC エラーを表示するには:

例：

```
Switch# show interface ethernet 1/1
Ethernet1/1 is up
admin state is up, Dedicated Interface
```

```
  Belongs to po4
  Hardware: 100/1000/10000/25000/auto Ethernet, address: 00a6.cab6.bda5 (bia 00a6.cab6.bda5)
  MTU 9000 bytes, BW 10000000 Kbit, DLY 1 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  FEC (forward-error-correction) : disable-fec
^[[B  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
  EEE (efficient-ethernet) : n/a
  Last link flapped 3d02h
  Last clearing of "show interface" counters never
  1 interface resets
  30 seconds input rate 0 bits/sec, 0 packets/sec
  30 seconds output rate 4992 bits/sec, 8 packets/sec
  Load-Interval #2: 5 minute (300 seconds)
    input rate 0 bps, 0 pps; output rate 4536 bps, 8 pps
  RX
    0 unicast packets  200563 multicast packets  0 broadcast packets
    200563 input packets  27949761 bytes
    0 jumbo packets  0 storm suppression bytes
    0 runts  0 giants  0 CRC  0 Stomped CRC  0 no buffer
    0 input error  0 short frame  0 overrun   0 underrun  0 ignored
    0 watchdog  0 bad etype drop  0 bad proto drop  0 if down drop
    0 input with dribble  0 input discard
    0 input buffer drop  0 input total drop
    0 Rx pause
  TX
    0 unicast packets  2156812 multicast packets  0 broadcast packets
    2156812 output packets  151413837 bytes
    0 jumbo packets
    0 output error  0 collision  0 deferred  0 late collision
    0 lost carrier  0 no carrier  0 babble  0 output discard
    0 output buffer drops  0 output total drops
    0 Tx pause
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。