アップグレード前のチェックリスト

ファブリックの基本情報の確認

ファブリックの基本情報を確認して、スムーズなアップグレードに必要なものがすべて揃っていることを確認します。具体的には、すべての障害をクリアすることが重要です。いくつかの障害は アップグレードの失敗を引き起こす可能性のある設定と条件の確認 （2 ページ） で特定の問題として説明されていますが、ステージングフェーズでの設定が原因で予想される障害を除き、アップグレードを実行する前に必ず障害をクリアする必要があります。

- すべての障害をクリアする
- AES 暗号化を使用して設定のエクスポートを実行する
- すべての ACI ノード（すべての APIC ノードとスイッチ ノード）のアウトオブバンド IP アドレスへのアクセスを確認します。
- すべての APIC の CIMC アクセスを確認します。
- すべてのスイッチのコンソール アクセスを確認する
- ターゲットと現在のバージョン間のバージョンの **APIC** および ACI スイッチのリリース ノートの動作の変更を理解する
- ターゲット バージョンの **APIC** スイッチと **ACI** スイッチの両方のリリース ノートで未解決の問題と既知の問題を理解する

アップグレードの失敗を引き起こす可能性のある設定と条件の確認

次の表に、アップグレードの失敗またはアップグレードに関連する既知の問題を回避するために確認する必要がある設定と条件を示します。

テーブル内の項目は、APIC に組み込まれたアップグレード前の検証ツールによって自動的に検出されます。ただし、現時点では一部の項目が APIC に含まれていないか、APIC がまだチェックを実装していないバージョンを実行している可能性があります。このような場合は、dcappcenter.cisco.com からアップグレード前検証アプリを実行するか、以下に示すスタンドアロン スクリプトを使用します。

- **アップグレード前検証ツール（APIC）**：APIC アップグレード設定に組み込まれている検証ツール。これは、APIC またはスイッチの更新グループを設定するときに自動的に実行されます。
- アップグレード前検証ツール（App Center アプリケーション）：**dcappcenter.cisco.com** からダウンロードできるアプリケーションとして APIC にインストールできる検証ツール。これはオンデマンドで実行でき、リリース 3.2 以降でサポートされています。
- **スクリプト**：アップグレード前検証ツールに現在実装されていない機能の場合、スタンドアロン スクリプトを APIC で直接実行して、アップグレード前に既存の問題を検証できます。スクリプトは、ソフトウェアのすべてのバージョンをサポートします。スクリプトの詳細については、https：//github.com/datacenter/ACI-Pre-Upgrade-Validation-Script を参照してください。

各項目の詳細については、アップグレード前の検証の設定と条件の詳細 （5 ページ） を参照してください。

品目	障害、不具合、またはバージョン （ある場合またはバージョン固有）	アップグレード前の検証ツール によって制御されるようになっています。	アップグレード前の検証ツール (App)	Script
すべての APIC が完全に適合する状態 （5 ページ）		4.2(6)	☑	☑
すべての ACI スイッチがアクティブ状態になっています （6 ページ）				☑
互換性（ターゲット ACI バージョン） （6 ページ）		4.2(4)	☑	☑
互換性（CIMC バージョン） （6 ページ）		4.2(4)	☑	☑

品目	障害、不具合、またはバージョン （ある場合またはバージョン固有）	アップグレード前の検証ツール によって制御されるようになっています。	アップグレード前の検証ツール **(App)**	**Script**
互換性（APIC、スイッチ ハードウェア） （6 ページ）		4.2(4)	☑	☑
互換性（リモート リーフ スイッチ）（6 ページ）	5.0（1）以降へ			☑
NTP（クロックがファブリック全体で同期される） （7 ページ）		4.2(5)	☑	☑
リリース 4.0(1) からの APIC のファームウェア更新グループの実装の変更（7 ページ）			☑	☑
アップグレード前に無効にする必要がある設定 （8 ページ）		AppCenter アプリ: 5.2(c)		☑
ルール 1：リーフ スイッチとスパイン スイッチを少なくとも 2 つのグループに分割する				☑
ルール 2：スパイン スイッチのグループ化方法を決定する		4.2（4） [1]	☑	☑
ルール 3：リーフ スイッチをグループ化する方法を決定します				☑
スイッチのグレースフルアップグレードのガイドライン			☑	☑
vPC 内のすべてのスイッチ ノード （8 ページ）		4.2(4)	☑	☑
APIC ディスク領域の使用状況（F1527、F1528、F1529） （9 ページ）	F1527: 80% - 85% F1528: 85% - 90% F1529：90% 以上	4.2(1)	☑	☑
ACI スイッチのブート フラッシュの使用 （10 ページ）	F1821：90% 以上	4.2(4)	☑	☑
APIC およびスイッチ ファームウェアの MD5sum チェック （12 ページ）		5.2(3e)		☑
APIC 間の APIC ファームウェア同期（13 ページ）		5.1(1)		☑

品目	障害、不具合、またはバージョン （ある場合またはバージョン固有）	アップグレード前の検証ツール によって制御されるようになっています。	アップグレード前の検証ツール **(App)**	**Script**
スタンバイ APIC のファイル システム（13 ページ）		5.2(3a)		☑
APIC に接続されたポートの EPG 設定（F0467：port-configured-for-apic）（14 ページ）	F0467： port-configured-for-apic	6.0(1g)		☑
インターフェイス L2 / L3 モード（F0467：port-configured-as-l2、port-configured-as-l3）の競合 （15 ページ）	F0467： port-configured-as-l2 F0467： port-configured-as-l3	5.2(4d)		☑
コントラクト向け L3Out サブネットの競合（F0467： prefix-entry-already-in-use） （16 ページ）	F0467： prefix-entry-already-in-use	6.0(1g)		☑
同じ VRF 内の BD サブネットの重複（F0469：重複、F1425：サブネット重複） （17 ページ）	F0469： duplicate-subnets-within-ctx F1425：subnet-overlap	5.2(4d)		☑
APIC の SSD ヘルス ステータス（F0101、F2730、F2731、F2732） （19 ページ）	F0101：not available F2730：残り 10% 未満 F2731：残り 5% 未満 F2732：残り 1% 未満	4.2(1)	☑	☑
ACI スイッチの SSD ヘルス ステータス（F3074、F3073） （20 ページ）	F3074：80% のライフタイムに達しました F3073：90% のライフタイムに達しました	4.2(1)	☑	☑
VMM コントローラの接続（F0130）（21 ページ）	F0130	4.2(1)	☑	☑
リーフ ノードと VMM ハイパーバイザ間の LLDP/CDP 隣接関係がない（F606391） （22 ページ）	F606391	4.2(1)	☑	☑
LLDP を介して注入される異なるインフラ VLAN（F0454： infra-vlan-mismatch） （23 ページ）	F0454： infra-vlan-mismatch			☑

品目	障害、不具合、またはバージョン （ある場合またはバージョン固有）	アップグレード前の検証ツール によって制御されるようになっています。	アップグレード前の検証ツール (App)	Script
コントラクト向けポリシー CAM プログラミング（F3545） （24 ページ）	F3545	5.1(1)	☑	☑
コントラクト向け L3Out サブネット プログラミング（F3544） （25 ページ）	F3544	5.1(1)	☑	☑
一般的なスケーラビリティの制限値（26 ページ）				☑
重複する VLAN プール （26 ページ）				☑
L3Out MTU の不一致 （27 ページ）				☑
ループバックのないノードプロファイル下の L3Out BGP ピア接続プロファイル （28 ページ）	CSCvm28482 – 4.1(2) 以降			☑
L3Out の誤ったルート マップ方向（CSCvm75395） （29 ページ）	CSCvm75395 – 4.1(1) 以降			☑
互換性（リモート リーフ スイッチ）（6 ページ）	CSCvs16767 – 14.2(2)			☑
EP Announce バージョンの不一致（CSCvi76161） （29 ページ）	CSCvi76161 – 13.2(2) 以降			☑
Intersight Device Connector をアップグレード中です。 （30 ページ）		4.2(5)	☑	☑

[1] IPN 接続がアップグレード前の検証でチェックされない

（注） 列の各項目の横にチェックボックスがない場合は、対応する検証項目がその自動化されたオプションの対象になっていないことを意味します。

アップグレード前の検証の設定と条件の詳細

すべての APIC が完全に適合する状態

[システム（System）]>**[ダッシュボード（Dashboard）]**>**[コントローラ（Controller]** でステータスを確認し、すべての APIC のクラスタステータスが**完全に適合**する状態であることを確認

します。1 つ以上の APIC が **Data Layer Partially Diverged** などの他の状態にある場合は、最初に APIC クラスタのステータスを解決する必要があります。

APIC が現在リリース 4.2(1) 以降である場合、各 APIC CLI のコマンド `acidiag cluster` は、APIC クラスタリングに関連する基本的な項目を確認します。そうでない場合は、『ACI トラブルシューティング ガイド第 2 版』の「初期ファブリック セットアップ」（http://cs.co/9003ybZ1d）に従ってください。

すべての ACI スイッチがアクティブ状態になっています

APIC GUI で **[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）]** を確認し、すべての ACI スイッチが**アクティブ**状態であることを確認します。1 つ以上の ACI スイッチが**非アクティブ、メンテナンス**などの他の状態にある場合は、まずこれらの問題を解決する必要があります。

- **非アクティブ**：スイッチに、ACI インフラ ネットワークを介した APIC からの IP 到達可能性などのファブリック検出の問題があることを意味します。スイッチが現在リリース 14.2(1) 以降である場合、スイッチの CLI で `show discoveryissues` コマンドを実行すると、スイッチ ファブリックの検出に関連する基本的な項目がチェックされます。
- **メンテナンス**：これは、スイッチが GIR（正常な挿入と取り外し）操作によって**メンテナンス モード**であることを意味します。これは、スイッチがファブリックから分離され、アップグレード関連の通信を含むほとんどの APIC 通信を処理しないことを意味します。アップグレードを実行する前に、スイッチを**アクティブ**状態に戻す必要があります。最初にスイッチをネットワークから分離してグレースフルにアップグレードを行う場合は、代わりに**グレースフル アップグレード**を検討してください。詳細については、ACI スイッチのグレースフル アップグレードを参照してください。

互換性（ターゲット ACI バージョン）

現在のバージョンからサポートされているアップグレード パスについては、『APIC アップグレード/ダウングレード サポート マトリクス』を参照してください。

互換性（CIMC バージョン）

ターゲット APIC バージョンでサポートされている UCS HUU バージョンの APIC アップグレード/ダウングレード サポートマトリックスを確認して、すべてのサーバーコンポーネントがサポートされている HUU バンドルのバージョンを実行していることを確認します。

互換性（APIC、スイッチ ハードウェア）

ターゲット バージョンの APIC スイッチと ACI スイッチの両方のリリース ノートを参照して、ハードウェアがサポートされていることを確認します。

互換性（リモート リーフ スイッチ）

このリリース以降、APIC リリース 5.0(1) にアップグレードする前に、リモート リーフスイッチの**ダイレクト トラフィック転送**を有効にすることが重要です。

ダイレクト トラフィック転送は、APIC リリース 4.1(2) 以降で有効にできます。このオプションを有効にするには、ルーティング可能なサブネットや外部 TEP などの TEP IP アドレスの追加設定が必要になる場合があることに注意してください。つまり、4.1(2) よりも前のバージョンを実行していて、リモート リーフ スイッチが設定されている場合、リリース 5.0 に直接アップグレードすることはできません。この場合は、4.2 リリースにアップグレードし、ダイレクト トラフィック転送を有効にしてから、目的の 5.0 バージョンにアップグレードすることをお勧めします。

詳細については、『*Cisco APIC レイヤ 3 ネットワーキング設定ガイド*』の「リモート リーフ スイッチのアップグレードとダイレクト トラフィック転送の有効化」を参照してください。

関連する問題は、「ダイレクト トラフィック転送が有効なリモート リーフ スイッチ」（CSCvs16767）で対処されています。リモート リーフ ノードで**ダイレクト トラフィック転送**が有効になっている状態でリリース 14.2(2) リリースにアップグレードすると、マルチキャスト FIB ディストリビューション マネージャ（MFDM）プロセスが原因でリモート リーフ ノードがクラッシュする可能性のある障害（CSCvs16767）が発生する可能性があります。この問題は、**ダイレクト トラフィック転送**を使用するリモート リーフ ノードがまだリリース 14.1(2) のとき、スパイン ノードを最初にリリース 14.2(2) にアップグレードした場合にのみ発生します。**ダイレクト トラフィック転送**は、リリース 14.1(2) で導入されたことに注意してください。

この問題を回避するには、**ダイレクト トラフィック転送**が有効になっている場合、リリース 14.2(2) ではなく、リリース 14.2(3) 以降にアップグレードすることが重要です。

何らかの理由でリリース 14.2(2) にアップグレードする必要がある場合は、まずこの問題を回避するためにリモート リーフ ノードをアップグレードする必要があります。

NTP（クロックがファブリック全体で同期される）

NTP が APIC とスイッチの両方で設定されていること、および各ノードからアウトオブバンド（OOB）またはインバンド（INB）を介して NTP サーバに必要な IP 到達可能性が設定されていることを確認します。

『Cisco ACI のトラブルシューティング – 第 2 版』の次の項を確認してください。

- インバンドおよびアウトオブバンド管理
- ポッドポリシー — BGP RR / 日付と時刻 / SNMP

リリース 4.0(1) からの APIC のファームウェア更新グループの実装の変更

APIC リリース 4.0(1) 以降では、以前のリリース（ファームウェア グループとメンテナンス グループ）で使用されていた 2 つのスイッチ更新グループの代わりに、1 つのタイプのスイッチ更新グループしかありません。2 つのグループを 1 つに統合することで、アップグレード設定が簡素化されます。ただし、4.0 より前のリリースからリリース 4.0(1) 以降に Cisco APIC をアップグレードする場合は、アップグレードの前にすべてのファームウェア グループおよびメンテナンス グループ ポリシーを削除する必要があります。

- ファームウェア グループ ポリシーを削除するには、**[管理（Admin）] > [ファームウェア（Firmware）] > [ファブリック ノード ファームウェア（Fabric Node Firmware）] > [ファームウェア グループ（Firmware Groups）]** に移動し、ファームウェア グループの名前を右

クリックして**[[ファームウェア グループの削除（Delete the Firmware Group）]** を選択します。

- メンテナンス グループ ポリシーを削除するには、**[管理（Admin）]** > **[ファームウェア（Firmware）]** > **[ファブリック ノード メンテナンス（Fabric Node Maintenance）]** > **[メンテナンス グループ（Maintenance Groups）]** に移動し、メンテナンス グループの名前を右クリックして**[メンテナンスグループの削除（Delete the Maintenance Group）]** を選択します。

APIC が 4.0(1) 以降にアップグレードされたら、新しいスイッチ更新グループを作成し、14.0 より前のリリースから 14.0(1) 以降にアップグレードできます。

これは、APIC を 4.0 より前から 4.0(1) 以降にアップグレードする場合にのみ適用されます。APIC が 4.0(1) 以降になったら、以降のアップグレードでこのことを心配する必要はありません。

（注） 内部的には、4.0(1) 以降のリリースを実行している APIC は、古いメンテナンス グループ ポリシー（`maintMaintP` など）と同じオブジェクトを使用して、追加の属性を持つスイッチ更新グループを処理します。API を使用してアップグレード ポリシーを設定する場合は、以前の 4.0 より前のリリースとは異なり、APIC リリース 4.0(1) 以降のメンテナンス グループ ポリシーのみを使用し、ファームウェア グループ ポリシーを手動で作成する必要はありません。

アップグレード前に無効にする必要がある設定

アップグレードの前に、次の機能を無効にする必要があります。

- App Center アプリ
- **[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）]** > **[メンテナンス（GIR）（Maintenance (GIR)）]** によるメンテナンスモード
- 設定ゾーン
- 不正エンドポイント（実行中のバージョンが 14.1(x) の場合、または 14.1(x) にアップグレードする場合のみ）

vPC 内のすべてのスイッチ ノード

ハイ アベイラビリティ（HA）は、常にネットワーク設計の鍵となります。これを実現する方法は複数あります。たとえば、NIC チーミングなどのサーバ構成、VMware vMotion などの仮想化テクノロジー、異なるシャーシ間でのリンク アグリゲーションなどのネットワーク デバイステクノロジーなどです。ACI は、シャーシ全体のリンク アグリゲーションとして仮想ポート チャネル（vPC）を使用してハイ アベイラビリティを提供します。

同じ HA ペア内の 1 つのスイッチを一度にアップグレードすることで、アップグレード中もトラフィック フローを維持することが重要です。ACI では、サーバ側または仮想化側に他の HA テクノロジーがない限り、これは vPC ペアになります。

アップグレード前検証ツールは、すべてのスイッチ ノードが vPC ペアにあるかどうかを確認します。ACI ではスイッチの前に APIC が最初にアップグレードされ、新しい vPC ペアの設定にはネットワーク設計の変更が必要になる可能性があり、アップグレードの前に行う必要があるため、このチェックはスイッチの代わりに APIC をアップグレードするときに行われます。他の HA テクノロジーが導入されている場合は、この検証を無視できます。 vPC はアップグレードを完了するための要件ではありませんが、vPC ドメイン内のリーフ スイッチが同時にアップグレードされないようにする組み込みツールは、vPC にない場合は機能しません。vPC を使用しない場合は、アップグレード中のスイッチが同時に停止しても停止しないようにする必要があります。

APIC ディスク領域の使用状況（F1527、F1528、F1529）

何らかの理由で APIC のディスク領域が不足している場合、APIC のアップグレードが失敗する可能性があります。APIC は、残りのディスク領域の量に応じて 3 つの異なる障害を発生させます。これらの障害のいずれかがシステムで発生した場合は、アップグレードを実行する前に問題を解決する必要があります。

- **F1527**：APIC ディスク領域使用率の警告レベルの障害。これは、使用率が 80 ー 85% の場合に発生します。
- **F1528**：APIC ディスク領域使用率の主要レベルの障害。これは、使用率が 85 ー 90% の場合に発生します。
- **F1529**：APIC ディスク領域使用率の重大レベルの障害。これは、使用率が 90% 以上の場合に発生します。

APIC の CLI で次の `moqueries` を実行して、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内にも表示されます。次の例では、`/firmware` に障害があるため、APIC GUI の **[管理（Admin）] > [ファームウェア（Firmware）]** で不要なファームウェア イメージを簡単に削除できます。ファームウェア イメージは APIC 間で同期されるため、Linux コマンド `rm` を実行してイメージを `/firmware` から直接削除しないでください。認識していないディスク領域に対して障害が発生した場合は、アップグレードの前に Cisco TAC に連絡して問題を解決してください。

障害の例（F1528：APIC ディスク領域使用率の重大な障害）

次に、APIC 1（ノード 1）の `/ firmware` のディスク領域が不足している状況の例を示します。

```
admin@apic1:~> moquery -c faultInst -f 'fault.Inst.code=="F1528"'
Total Objects shown: 1

# fault.Inst
code             : F1528
ack              : no
annotation       :
cause            : equipment-full
changeSet        : available (Old: 5646352, New: 6036744), capUtilized (Old: 86, New:
85), used (Old: 33393968, New: 33003576)
childAction      :
```

```
created          : 2021-05-27T11:58:19.061-04:00
delegated        : no
descr            : Storage unit /firmware on Node 1 with hostname apic1 mounted at
/firmware is 85% full
dn               :
topology/pod-1/node-1/sys/ch/p-[/firmware]-f-[/dev/mapper/vg_ifc0-firmware]/fault-F1528
domain           : infra
extMngdBy        : undefined
highestSeverity  : major
lastTransition   : 2021-05-27T12:01:37.128-04:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : major
prevSeverity     : major
rn               : fault-F1528
rule             : eqpt-storage-full-major
severity         : major
status           :
subject          : equipment-full
type             : operational
uid              :
```

使用率と障害の重大度を除き、3 つの障害はすべて同じように見えます。

ACI スイッチのブート フラッシュの使用

ACI スイッチには、主に各パーティションのファイル システム使用率に関する 2 つの異なる障害があります。

- **F1820**：スイッチ パーティションの使用に関するマイナー レベルの障害。これは、パーティションの使用率がマイナーしきい値を超えると発生します。
- **F1821**：スイッチ パーティションの使用に関するメジャー レベルの障害。これは、パーティションの使用率がメジャーしきい値を超えると発生します。

マイナーおよびメジャーのしきい値は、パーティションによって異なります。アップグレードで重要なのは /bootflash です。ブートフラッシュのしきい値は、マイナーしきい値が 80%、メジャーしきい値が 90% です。

さらに、すべてのスイッチ ノードに組み込みの動作が追加され、/ bootflash ディレクトリが 50% の容量を維持するようにアクションが実行されます。これは特に、アップグレード中にスイッチのアップグレードが正常にスイッチイメージを転送および抽出できるようにするためです。

これを行うために、/bootflash の使用状況を監視する内部スクリプトがあり、使用率が 50% を超えると、ファイルの削除を開始してファイルシステムを解放します。攻撃性が高いため、使用予定のスイッチ イメージに対してこのクリーンアップ スクリプトがトリガーされる可能性のあるいくつかのシナリオがあり、これにより、ブート イメージが / bootflash から削除された場合、スイッチのアップグレードでローダープロンプトでスイッチが起動する可能性があります。

これを防ぐには、アップグレードの前に /bootflash を確認し、そこに記載されている内容と理由を理解するために必要な手順を実行します。理解したら、必要な手順を実行して不要な

/bootflash ファイルを消去し、自動クリーンアップ ケースのシナリオを回避するのに十分な領域があることを確認します。

アップグレード前の検証ツール（APIC と App の両方）は、任意のパーティションの使用率が高い障害F1821をモニタします。この障害が存在する場合は、ブートフラッシュの障害ではない場合でも、アップグレードの前に解決することを推奨します。

この章で前述したACIアップグレード前検証スクリプトでは、各スイッチのブートフラッシュの使用率に重点を置き、使用率が 50% を超えるブートフラッシュに問題があるかどうかを確認します。これにより、内部クリーンアップスクリプトがトリガーされる可能性があります。

この問題を確認するには、アップグレード前検証ツールまたはスクリプトを実行します。次に、50% しきい値のブートフラッシュの内部クリーンアップに関する詳細情報を示します。

検証

リーフ スイッチの CLI にログインすると、`df -h` を使用して /bootflash の使用状況を確認できます。

```
leaf1# df -h
Filesystem             Size    Used   Avail   Use%   Mounted on
rootfs                 2.5G    935M   1.6G    38%    /bin
/dev/sda4               12G    5.7G   4.9G    54%    /bootflash
/dev/sda2              4.7G    9.6M   4.4G     1%    /recovery
/dev/mapper/map-sda9    11G    5.7G   4.2G    58%    /isan/lib
none                   3.0G    602M   2.5G    20%    /dev/shm
none                    50M    3.4M    47M     7%    /etc
/dev/sda6               56M    1.3M    50M     3%    /mnt/cfg/1
/dev/sda5               56M    1.3M    50M     3%    /mnt/cfg/0
/dev/sda8               15G    140M    15G     1%    /mnt/ifc/log
/dev/sda3              115M     52M    54M    50%    /mnt/pss
none                   1.5G    2.3M   1.5G     1%    /tmp
none                    50M    240K    50M     1%    /var/log
/dev/sda7               12G    1.4G   9.3G    13%    /logflash
none                   350M     54M   297M    16%    /var/log/dme/log/dme_logs
none                   512M     24M   489M     5%    /var/sysmgr/mem_logs
none                    40M    4.0K    40M     1%    /var/sysmgr/startup-cfg
none                   500M      0    500M     0%    /volatile
```

/bootflash 自動削除の確認

自動クリーンアップによって /bootflash 内の一部のファイルが削除された疑いがある場合は、ログを確認してこれを検証できます。

```
leaf1# egrep "higher|removed" /mnt/pss/core_control.log
[2020-07-22 16:52:08.928318] Bootflash Usage is higher than 50%!!
[2020-07-22 16:52:08.931990] File: MemoryLog.65%_usage removed !!
[2020-07-22 16:52:08.943914] File: mem_log.txt.old.gz removed !!
[2020-07-22 16:52:08.955376] File: libmon.logs removed !!
[2020-07-22 16:52:08.966686] File: urib_api_log.txt removed !!
[2020-07-22 16:52:08.977832] File: disk_log.txt removed !!
[2020-07-22 16:52:08.989102] File: mem_log.txt removed !!
[2020-07-22 16:52:09.414572] File: aci-n9000-dk9.13.2.1m.bin removed !!
```

APIC の CLI で次の moquery を実行して、各スイッチ ノードのブートフラッシュの使用状況を確認できます。

```
f2-apic1# moquery -c eqptcapacityFSPartition -f
'eqptcapacity.FSPartition.path=="/bootflash"'
Total Objects shown: 6
```

```
# eqptcapacity.FSPartition
name             : bootflash
avail            : 7214920
childAction      :
dn               : topology/pod-1/node-101/sys/eqptcapacity/fspartition-bootflash
memAlert         : normal
modTs            : never
monPolDn         : uni/fabric/monfab-default
path             : /bootflash
rn               : fspartition-bootflash
status           :
used             : 4320184
```

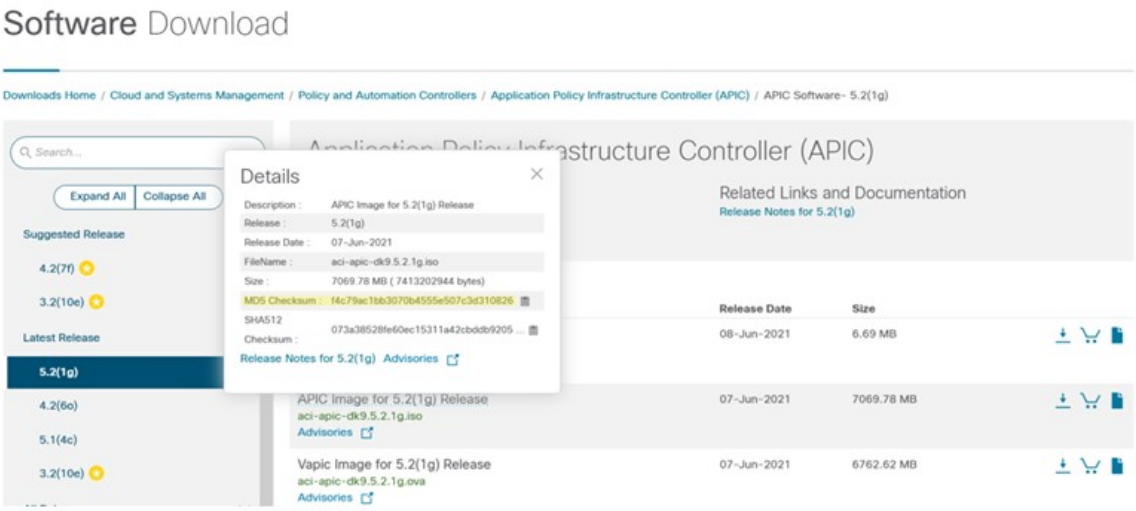
APIC およびスイッチ ファームウェアの MD5sum チェック

ACI ファブリックでアップグレードを実行する場合、すべてのノードのアップグレードを準備するために複数のイメージ転送が必要です。これらの転送のほとんどは、第1レベルのイメージ検証を実行します。ただし、障害が発生した場合、それぞれのノードでイメージを再確認する価値があります。

イメージ転送タッチポイントのアップグレード：

1. cisco.com からデスクトップ/ファイル サーバにイメージを転送します。

   このイメージに対してMD5を手動で実行します。cisco.com からイメージの予想される MD5 を検証できます。



2. デスクトップまたは FTP サーバからいずれかの APIC にイメージをアップロードします。
   - APIC でこの操作を実行する手順については、該当する章の『*APIC* での *APIC* およびスイッチ イメージのダウンロード』の項を参照してください。
     - GUI を使用した 4.x より前の APIC リリースでのアップグレード
     - GUI を使用した APIC リリース 4.x または 5.0 でのアップグレード
     - GUI を使用した APIC リリース 5.1 以降でのアップグレード

- 転送が完了すると、イメージが破損または不完全に見える場合、APIC は自動的にイメージ検証を実行し、障害 F0058 を発生させます。

3. イメージがファームウェア リポジトリに追加されると、最初にアップロードされた APIC は、そのイメージをクラスタ内の残りの APIC にコピーします。

   各 APIC のイメージ コピーに対して `md5sum` コマンドを実行することで、各 APIC のアップグレード イメージで MD5 を手動で確認できます。

   次に例を示します。

   ```
   APIC1# md5sum /firmware/fwrepos/fwrepo/aci-apic-dk9.5.2.1g.bin
   f4c79ac1bb3070b4555e507c3d310826 /firmware/fwrepos/fwrepo/aci-apic-dk9.5.2.1g.bin
   ```

4. スイッチは、アップグレードの準備中に、最終的にそれぞれが switch.bin イメージのコピーを取得します。

   /bootflash 内の個々のスイッチ イメージで MD5 を実行できます。

   次に例を示します。

   ```
   leaf1# md5sum /bootflash/aci-n9000-dk9.15.2.1g.bin
   02e3b3fb45a51e36db28e7ff917a0c96 /bootflash/aci-n9000-dk9.15.2.1g.bin
   ```

APIC 間の APIC ファームウェア同期

イメージが APIC の 1 つにダウンロードされると、イメージはクラスタ内のすべての APIC に同期されます。これは、各 APIC がイメージをローカルでアップグレードする必要があるため、特に APIC イメージにとって重要です。

これを行うには、各 APIC にログインし、ターゲット イメージの `/firmare/fwrepos/fwrepo` を確認します。

1 つ以上の APIC でイメージが欠落している場合は、ダウンロード後すぐに約 5 分間待機します。イメージがまだ見つからない場合は、APIC クラスタリング ステータスがすべての APIC で正常であることを確認し、GUI または API からイメージを削除します（Linux コマンド `rm` を使用しない）。その後、イメージを再ダウンロードしてファイル同期を再度トリガーします。それでもイメージが表示されない場合は、Cisco TAC にお問い合わせください。

スタンバイ APIC のファイル システム

スタンバイ APIC はコールド スタンバイであり、クラスタの一部ではないため、障害状態についてアクティブにモニタされません。ファイル システムの完全なチェックはこのカテゴリに該当するため、これらの状態を示すスタンバイ APIC は障害にフラグを立てず、代わりに手動で確認する必要があります。

これを行うには、`rescue-user` としてスタンバイ APIC にログインし、`df -h` を実行してファイル システムの使用状況を手動で確認します。

いずれかのファイル システムが 75% 以上であることが判明した場合は、TAC に連絡して状態を特定し、解決してください。

APIC に接続されたポートの EPG 設定（F0467：port-configured-for-apic）

正常な ACI 展開では、APIC コントローラが接続されているインターフェイスにプッシュされるEPGまたはポリシーはありません。APICがリーフスイッチに接続されている場合は、APICとリーフ スイッチの間でLLDP検証が行われ、ユーザが設定することなくファブリックに許可されます。APICに接続されているリーフ スイッチ インターフェイスにポリシーがプッシュされると、その設定は拒否され、障害が発生します。ただし、APIC へのリンクが何らかの理由でフラップした場合、主に APIC のリブート時のアップグレード中に、そのリーフ スイッチ インターフェイスにポリシーを展開できます。これにより、APIC がリロード後にファブリックへの再参加がブロックされます。

問題を回避するために、アップグレードの前にこれらの問題を解決することが重要です。APICのCLIで以下のmoqueryを実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F0467：port-configured-for-apic）：

次の障害は、いくつかの EPG 設定を持つ APIC に接続されているノード 101 eth1/1 の例を示しています。

```
admin@apic1:~> moquery -c faultInst -x
'query-target-filter=wcard(faultInst.descr,"port-configured-for-apic")'
Total Objects shown: 1

# fault.Inst
code             : F0467
ack              : no
annotation       :
cause            : configuration-failed
changeSet        : configQual:port-configured-for-apic, configSt:failed-to-apply,
debugMessage:port-configured-for-apic: Port is connected to the APIC;, temporaryError:no
childAction      :
created          : 2021-06-03T07:51:42.263-04:00
delegated        : yes
descr            : Configuration failed for uni/tn-jr/ap-ap1/epg-epg1 node 101 eth1/1
due to Port Connected to Controller, debug message: port-configured-for-apic: Port is
connected to the APIC;
dn               :
topology/pod-1/node-101/local/svc-policyelem-id-0/uni/epp/fv-[uni/tn-jr/ap-ap1/epg-epg1]
/node-101/stpathatt-[eth1/1]/nwissues/fault-F0467
domain           : tenant
extMngdBy        : undefined
highestSeverity  : minor
lastTransition   : 2021-06-03T07:53:52.021-04:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : minor
prevSeverity     : minor
rn               : fault-F0467
rule             : fv-nw-issues-config-failed
severity         : minor
status           :
subject          : management
type             : config
uid              :
```

インターフェイス L2 / L3 モード（F0467：port-configured-as-l2、port-configured-as-l3）の競合

これは、アップグレード前に確認する必要がある F0467 障害コード ファミリのもう 1 つのタイプです。この障害は、ポリシーが展開されているポートが反対のモードで動作しているため、レイヤ 3 アウト（L3Out）で設定されたインターフェイスに障害が発生したことを警告します。たとえば、L3Out の下にルーテッド サブインターフェイスを設定し、ポートを L3 ポートにする場合があります。ただし、そのポートにはすでに L2 ポリシーがあります。ACI のポートは、「**switchport**」（L2）または「**no switchport**」（L3）のいずれかである可能性があるレイヤ 3 スイッチ上のポートと同様に、L2 または L3 のいずれかです。ポートがすでに L3 ポートである場合、同じルールが適用されますが、そのポートに L2 設定を展開します。アップグレード後、スイッチのリロード後にこの障害のあるポリシーが最初に展開されると、以前に動作していた設定が破損する可能性があります。

問題を回避するために、アップグレードの前にこれらの問題を解決することが重要です。障害が発生したインターフェイスは、障害をクリアするために修正または削除する必要があります。APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F0467：port-configured-as-l2）：

次の障害は、同じポートがすでに SVI と同じポートを使用する EPG や他の L3Out などの他のコンポーネントによって L2 として設定されているため、テナント jr がノード 101 eth1/7 で失敗した L3Out ***OSPF*** からの設定の例を示しています。この場合、L3Out ***OSPF*** はノード 101 eth1/7 を SVI（L2）ではなくルーテッドポートまたはルーテッドサブインターフェイス（L3）として使用しようとしています。

```
admin@apic1:~> moquery -c faultDelegate -x
'query-target-filter=wcard(faultInst.changeSet,"port-configured-as-l2")'
Total Objects shown: 1

# fault.Delegate
affected         :
resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-OSPF]/node-101/stpathatt-[eth1/7]/nwissues
code             : F0467
ack              : no
cause            : configuration-failed
changeSet        : configQual:port-configured-as-l2, configSt:failed-to-apply,
temporaryError:no
childAction      :
created          : 2021-06-23T12:17:54.775-04:00
descr            : Fault delegate: Configuration failed for uni/tn-jr/out-OSPF node 101
 eth1/7 due to Interface Configured as L2, debug message:
dn               :
uni/tn-jr/out-OSPF/fd-[resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-OSPF]/node-101/
stpathatt-[eth1/7]/nwissues]-fault-F0467
domain           : tenant
highestSeverity  : minor
lastTransition   :2021-06-23T12:20:09.780-04:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : minor
prevSeverity     : minor
rn               :
fd-[resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-OSPF]/node-101/stpathatt-[eth1/7]/nwissues]-fault-F0467
rule             : fv-nw-issues-config-failed
severity         : minor
```

```
status           :
subject          : management
type             : config
```

障害の例（F0467：port-configured-as-l3）：

次の障害は、上記の状況の逆の例を示しています。この例では、L3Out ***IPV6*** は L2 ポートとしてノード 101 eth1/7 を使用しようとしますが、他の L3Out がすでに同じポートを L3 ポートとして使用しているため、失敗しました。

```
admin@apic1:~> moquery -c faultDelegate -x
'query-target-filter=wcard(faultInst.changeSet,"port-configured-as-l3")'
Total Objects shown: 1

# fault.Delegate
affected         :
resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-IPV6]/node-101/stpathatt-[eth1/7]/nwissues
code             : F0467
ack              : no
cause            : configuration-failed
changeSet        : configQual:port-configured-as-l3, configSt:failed-to-apply,
debugMessage:port-configured-as-l3: Port has one or more layer3 sub-interfaces;,
temporaryError:no
childAction      :
created          : 2021-06-23T12:31:41.949-04:00
descr            : Fault delegate: Configuration failed for uni/tn-jr/out-IPV6 node 101
 eth1/7 due to Interface Configured as L3, debug message: port-configured-as-l3: Port
has one or more layer3 sub-interfaces;
dn               :
uni/tn-jr/out-IPV6/fd-[resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-IPV6]/node-101/
stpathatt-[eth1/7]/nwissues]-fault-F0467
domain           : tenant
highestSeverity  : minor
lastTransition   : 2021-06-23T12:31:41.949-04:00
lc               : soaking
modTs            : never
occur            : 1
origSeverity     : minor
prevSeverity     : minor
rn               :
fd-[resPolCont/rtdOutCont/rtdOutDef-[uni/tn-jr/out-IPV6]/node-101/stpathatt-[eth1/7]/nwissues]-fault-F0467
rule             : fv-nw-issues-config-failed
severity         : minor
status           :
subject          : management
type             : config
```

コントラクト向け L3Out サブネットの競合（F0467：prefix-entry-already-in-use）

アップグレードの前に確認する必要がある別のタイプの F0467 障害コード ファミリがあります。この障害は、Layer3 Out（L3Out）で定義された外部 EPG に、同じ VRF 内の別の L3Out 外部 EPG と重複する「**外部 EPG の外部サブネット**」範囲が設定されたサブネットがあることを警告します。アップグレード後、スイッチのリロード後にこの障害のあるポリシーが最初に展開されると、以前の動作中の設定が破損する可能性があります。

スイッチのアップグレード時に予期しない停止を防ぐために、アップグレードの前にこれらの問題を解決することが重要です。障害が発生したサブネットは、障害をクリアするために修正または削除する必要があります。APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F0467：prefix-entry-already-in-use）：

次に、***all***という外部EPGを使用したL3Out***OSPF***の例を示します。この外部EPGでは、L3Outサブネット112.112.112.112/32が「**外部EPGの外部サブネット**」で設定され、パケットの送信元または宛先IPアドレスをこの外部EPGにコントラクトアプリケーションに分類します。ただし、同じサブネットが同じVRF内の別の外部EPGによってすでに使用されているため、失敗しました。

```
admin@apic1:~> moquery -c faultInst
-x'query-target-filter=wcard(faultInst.descr,"prefix-entry-already-in-use")'
Total Objects shown: 1

# fault.Inst
code              : F0467
ack               : no
annotation        :
cause             : configuration-failed
changeSet         : configQual:prefix-entry-already-in-use, configSt:failed-to-apply,
debugMessage:prefix-entry-already-in-use: Prefix entry sys/ctx-[vxlan-2621440]/pfx-[112.
112.112.112/32] is in use;, temporaryError:no
childAction       :
created           : 2021-06-22T09:02:36.630-04:00
delegated         : yes
descr             : Configuration failed for uni/tn-jr/out-OSPF/instP-all due to Prefix
Entry Already Used in Another EPG, debug message: prefix-entry-already-in-use: Prefix
entry sys/ctx-[vxlan-2621440]/pfx-[112.112.112.112/32] is in use;
dn                :
topology/pod-1/node-101/local/svc-policyelem-id-0/uni/epp/rtd-[uni/tn-jr/out-OSPF/instP-all]/nwissues/fault-F0467
domain            : tenant
extMngdBy         : undefined
highestSeverity   : minor
lastTransition    : 2021-06-22T09:04:51.985-04:00
lc                : raised
modTs             : never
occur             : 1
origSeverity      : minor
prevSeverity      : minor
rn                : fault-F0467
rule              : fv-nw-issues-config-failed
severity          : minor
status            :
subject           : management
type              : config
uid               :
```

同じVRF内のBDサブネットの重複（F0469：重複、F1425：サブネット重複）

重複するIPアドレスまたはサブネットがVRF内に展開されると、そのポリシーは失敗し、ノードレベルで障害が発生します。ただし、アップグレード時に、以前に失敗した設定が以前に動作していた設定の前にリーフスイッチにプッシュされる可能性があります。これにより、アップグレード前の既知の動作状態がアップグレード後に破損し、以前に動作していたサブネットの接続の問題が発生する可能性があります。

この状況には2つの障害があります。

- F0469（duplicate-subnets-within-ctx）は、複数のBDサブネットが同じVRFのまったく同じサブネットで設定されている場合に発生します。

- F1425（subnet-overlap）は、BD サブネットが同じではなく重複している場合に発生します。

問題を回避するために、アップグレードの前にこれらの問題を解決することが重要です。障害が発生したサブネットは、障害をクリアするために修正または削除する必要があります。APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F0469：duplicate-subnets-within-ctx）：

```
admin@f1-apic1:~> moquery -c faultInst -f 'fault.Inst.code=="F0469"'
Total Objects shown: 4

# fault.Inst
code             : F0469
ack              : no
annotation       :
cause            : configuration-failed
changeSet        : configQual (New: duplicate-subnets-within-ctx), configSt (New:
failed-to-apply), debugMessage (New: uni/tn-TK/BD-BD2,uni/tn-TK/BD-BD1)
childAction      :
created          : 2021-07-08T17:40:37.630-07:00
delegated        : yes
descr            : BD Configuration failed for uni/tn-TK/BD-BD2  due to
duplicate-subnets-within-ctx: uni/tn-TK/BD-BD2 ,uni/tn-TK/BD-BD1
dn               :
topology/pod-1/node-101/local/svc-policyelem-id-0/uni/bd-[uni/tn-TK/BD-BD2]-isSvc-no/bdcfgissues/fault-F0469
domain           : tenant
extMngdBy        : undefined
highestSeverity  : minor
lastTransition   : 2021-07-08T17:40:37.630-07:00
lc               : soaking
modTs            : never
occur            : 1
origSeverity     : minor
prevSeverity     : minor
rn               : fault-F0469
rule             : fv-bdconfig-issues-config-failed
severity         : minor
status           :
subject          : management
type             : config
uid              :
```

障害の例（F1425：subnet-overlap）：

```
admin@apic1:~> moquery -c faultInst -f 'fault.Inst.code=="F1425"'
Total Objects shown: 1

# fault.Inst
code             : F1425
ack              : no
annotation       :
cause            : ip-provisioning-failed
changeSet        : ipv4CfgFailedBmp (New:
ipv4:Addraddr_failed_flag,ipv4:Addrctrl_failed_flag,ipv4:AddrlcOwn_failed_flag,
ipv4:AddrmodTs_failed_flag,ipv4:AddrmonPolDn_failed_flag,ipv4:Addrpref_failed_flag,ipv4:Addrtag_failed_flag,
ipv4:Addrtype_failed_flag,ipv4:AddrvpcPeer_failed_flag), ipv4CfgState (New: 1), operStQual
 (New: subnet-overlap)
childAction      :
created          : 2020-02-27T01:50:45.656+01:00
delegated        : no
```

```
descr            : IPv4 address(10.10.10.1/24) is operationally down, reason:Subnet
overlap on node 101 fabric hostname leaf-101
dn               :
topology/pod-1/node-101/sys/ipv4/inst/dom-jr:v1/if-[vlan10]/addr-[10.10.10.1/24]/fault-F1425
domain           : access
extMngdBy        : undefined
highestSeverity  : major
lastTransition   : 2020-02-27T01:52:49.812+01:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : major
prevSeverity     : major
rn               : fault-F1425
rule             : ipv4-addr-oper-st-down
severity         : major
status           :
subject          : oper-state-err
type             : operational
uid              :
```

APIC の SSD ヘルス ステータス（F0101、F2730、F2731、F2732）

APIC リリース 2.3(1) から、SSD メディアの消耗インジケータ（残りの寿命）が APIC ノードで特定のパーセンテージ未満になると、障害が発生します。ライフタイムが短い SSD を使用すると、アップグレードやダウングレード操作など、内部データベースの更新が必要な操作が失敗する可能性があります。APIC は、残りの SSD の寿命に応じて 3 つの異なる障害を発生させます。システムで最も重大な障害（F2732）が発生した場合は、アップグレードを実行する前に Cisco TAC に連絡して SSD を交換する必要があります。

- **F2730**：APIC SSD の寿命に関する警告レベルの障害。これは、残りの寿命が 10% 未満の場合に発生します。
- **F2731**：APIC SSD の寿命に関するメジャー レベルの障害。これは、残りの寿命が 5% 未満の場合に発生します。
- **F2732**：APIC SSD の寿命に関する重大レベルの障害。これは、残りの寿命がが 1% 未満の場合に発生します。

また、ごくまれに、SSDの寿命以外の動作上の問題が発生する場合があります。このような場合は、障害 F0101 を探します。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

APIC が 2.3(1) リリースよりも古いリリースで実行されている場合は、Cisco TAC に連絡して SSD の残りの寿命を確認してください。

詳細については、『APIC SSD の交換に関する技術情報』を参照してください。

障害の例（F2731：APIC SSD 寿命の重大な障害）：

次に、SSD の残り寿命が 1% の APIC 3（ノード 3）の例を示します（主な障害 F2731）。この場合、寿命 1% 未満の重大な障害 F2732 は発生しませんが、F2732 のしきい値に十分近いため、SSD を交換することをお勧めします。

```
APIC1# moquery -c faultInfo -f 'fault.Inst.code=="F2731"'
Total Objects shown: 1

# fault.Inst
code              : F2731
ack               : no
annotation        :
cause             : equipment-wearout
changeSet         : mediaWearout (Old: 2, New: 1)
childAction       :
created           : 2019-10-22T11:47:40.791+01:00
delegated         : no
descr             : Storage unit /dev/sdb on Node 3 mounted at /dev/sdb has 1% life
remaining
dn                : topology/pod-2/node-3/sys/ch/p-[/dev/sdb]-f-[/dev/sdb]/fault-F2731
domain            : infra
extMngdBy         : undefined
highestSeverity   : major
lastTransition    : 2019-10-22T11:49:48.788+01:00
lc                : raised
modTs             : never
occur             : 1
origSeverity      : major
prevSeverity      : major
rn                : fault-F2731
rule              : eqpt-storage-wearout-major
severity          : major
status            :
subject           : equipment-wearout
type              : operational
uid               :
```

ACI スイッチの SSD ヘルス ステータス（F3074、F3073）

リリース2.1（4）、2.2（4）、2.3（1o）、および3.1（2m）から、フラッシュSSDのライフタイムの使用率がリーフまたはスパインスイッチで特定の耐久性の上限に達した場合に障害が発生します。ライフタイムが短いフラッシュ SSD では、APIC 通信などの内部データベースの更新が必要な操作が失敗する、またはスイッチが起動しない可能性があります。ACI スイッチは、消費する SSD の寿命に応じて 2 つの異なる障害を発生させます。システムで最も重大な障害（F3073）が発生した場合は、アップグレードを実行する前に Cisco TAC に連絡して SSD を交換する必要があります。

- **F3074**：スイッチ SSD ライフタイムの警告レベルの障害。これは、寿命が制限の 80% に達したときに発生します。
- **F3073**：スイッチ SSD ライフタイムの警告レベルの障害。これは、寿命が制限の 90% に達したときに発生します。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

APIC が古いリリースを実行している場合は、Cisco TAC に連絡して SSD のライフ ステータスを確認してください。

詳細については、『ACI スイッチ ノード SSD 寿命の説明』テクニカル ノートを参照してください。

障害の例（F3074：スイッチ SSDの寿命に関する警告）：

次に、SSD 寿命の 85% に達したノード 101 の例を示します。

```
APIC1# moquery -c faultInst -f 'fault.Inst.code=="F3074"'

Total Objects shown: 4

# fault.Inst
code             : F3074
ack              : no
annotation       :
cause            : equipment-flash-warning
changeSet        : acc:read-write, cap:61057, deltape:23, descr:flash, gbb:0, id:1,
lba:0, lifetime:85, majorAlarm:no, mfgTm:2020-09-22T02:21:45.675+00:00, minorAlarm:yes,
 model:Micron_M600_MTFDDAT064MBF, operSt:ok, peCycles:4290, readErr:0, rev:MC04,
ser:MSA20400892, tbw:21.279228, type:flash, vendor:Micron, warning:yes, wlc:0
childAction      :
created          : 2020-09-21T21:21:45.721-05:00
delegated        : no
descr            : SSD has reached 80% lifetime and is nearing its endurance limit.
Please plan for Switch/Supervisor replacement soon
dn               : topology/pod-1/node-101/sys/ch/supslot-1/sup/flash/fault-F3074
domain           : infra
extMngdBy        : undefined
highestSeverity  : minor
lastTransition   : 2020-09-21T21:24:03.132-05:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : minor
prevSeverity     : minor
rn               : fault-F3074
rule             : eqpt-flash-flash-minor-alarm
severity         : minor
status           :
subject          : flash-minor-alarm
type             : operational
```

VMM コントローラの接続（F0130）

APIC と VMM コントローラ間の通信に問題がある場合、VMM コントローラのステータスはオフラインとしてマークされ、障害 F0130 が発生します。アップグレード後に APIC が必要な情報を取得できないためにVMMコントローラとの通信に基づいてスイッチに現在展開されているリソースが変更または失われないように、アップグレード前にそれらの間の接続が復元されていることを確認します。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F0130：VMM コントローラの接続障害）：

次に、APIC が VMM ドメイン `LAB_VMM` の IP 192.168.100.100 で VMM コントローラ `MyVMMControler` と通信できない例を示します。

```
apic1# moquery -c faultInst -f 'fault.Inst.code=="F0130"'
Total Objects shown: 1

# fault.Inst
code             : F0130
ack              : no
```

```
cause            : connect-failed
changeSet        : operSt (Old: unknown, New: offline)
childAction      :
created          : 2016-05-23T16:07:50.205-05:00
delegated        : yes
descr          : Connection to VMM controller: 192.168.100.100 with name MyVMMController
 in datacenter LAB1 in domain: LAB_VMM is failing repeatedly with error: [Failed to
retrieve ServiceContent from the vCenter server 192.168.100.100]. Please verify network
 connectivity of VMM controller 192.168.100.100 and check VMM controller user credentials
 are valid.
dn               : comp/prov-VMware/ctrlr-[LAB_VMM]-MyVMMController/fault-F0130
domain           : external
highestSeverity  : major
lastTransition   : 2016-05-23T16:10:04.219-05:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : major
prevSeverity     : major
rn               : fault-F0130
rule             : comp-ctrlr-connect-failed
severity         : major
status           :
subject          : controller
type             : communications
uid              :
```

リーフ ノードと VMM ハイパーバイザ間の LLDP/CDP 隣接関係がない（F606391）

VMM ドメインを EPG に接続する際の**事前プロビジョニング**ではなく、**オンデマンド**または**即時**解決の即時性により、VMware DVS 統合などの一部の VMM 統合では、APIC はハイパーバイザに接続されたリーフ スイッチから、そしてハイパーバイザを管理する VMM コントローラからの LLDP または CDP 情報をチェックします。この情報は、Cisco UCS ファブリック インターコネクトなどの間に中間スイッチがある場合でも、リーフ スイッチとハイパーバイザの両方から、ハイパーバイザに接続するリーフ インターフェイスを動的に検出するために必要です。インターフェイスが検出されると、APIC は、ハイパーバイザが接続されているリーフ スイッチの必要なインターフェイスにのみ VLAN を動的に展開します。

APIC リリース 3.0(1) より前では、APIC がハイパーバイザの観点から LLDP または CDP 情報を比較できないため、APIC が VMM コントローラへの接続を失った場合、VLAN はリーフ インターフェイスから削除されていました。APIC リリース 3.0(1) 以降では、一時的な管理プレーンの問題がデータプレーン トラフィックに影響を与えないようにするために、APIC が VMM コントローラへの接続を失っても、VLAN はリーフ インターフェイスから削除されません。ただし、LLDP / CDP 情報を繰り返し取得しようとすると、APIC プロセスでチャーンが発生する可能性があります。LLDP / CDP 情報が欠落している場合、障害 F606391 が発生します。

これらの理由により、APIC のリリースに関係なく、アップグレードの前にこの障害を解決することが重要です。Cisco Application Virtual Edge（AVE）用に設定された VMM ドメインで障害が発生した場合、LLDP / CDP ではなく opflex プロトコルに基づいてスイッチをプログラムするために構築された制御プレーンが使用されるため、LLDP および CDP は完全に無効にできます。LLDP および CDP が無効の場合、障害はクリアされます。VMM ドメインの LLDP/CDP 状態を変更するための設定は、VMM ドメインの vSwitch ポリシーで設定されます。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F606391：ハイパーバイザの LLDP/CDP 隣接関係がない）：

```
apic1# moquery -c faultInst -f 'fault.Inst.code=="F606391"'
Total Objects shown: 5

# fault.Inst
code                     : F606391
ack                      : no
annotation               :
cause                    : fsm-failed
changeSet                :
childAction              :
created                  : 2019-07-18T01:17:39.435+08:00
delegated                : yes
descr                    : [FSM:FAILED]: Get LLDP/CDP adjacency information for the
physical adapters on the host: hypervisor1.cisco.com(TASK:ifc:vmmmgr:CompHvGetHpNicAdj)
dn                       :
comp/prov-VMware/ctrlr-[LAB_VMM]-MyVMMController/hv-host-29039/fault-F606391
domain                   : infra
extMngdBy                : undefined
highestSeverity          : major
lastTransition           : 2019-07-18T01:17:39.435+08:00
lc                       : raised
modTs                    : never
occur                    : 1
origSeverity             : major
prevSeverity             : major
rn                       : fault-F606391
rule                     : fsm-get-hp-nic-adj-fsm-fail
severity                 : major
status                   :
subject                  : task-ifc-vmmmgr-comp-hv-get-hp-nic-adj
type                     : config
uid                      :
```

LLDP を介して注入される異なるインフラ VLAN（F0454：infra-vlan-mismatch）

2 つの異なる ACI ファブリック間でバックツーバック接続されたインターフェイスがある場合は、アップグレードの前にこれらのインターフェイスで LLDP を無効にする必要があります。これは、アップグレード後にスイッチが復帰すると、別のインフラ VLAN を使用している可能性がある他のファブリックから LLDP パケットを受信して処理する可能性があるためです。その場合、スイッチは誤って他のファブリックのインフラ VLAN を介して検出され、正しいファブリックでは検出されません。

ACI スイッチが現在、他のファブリックからインフラ VLAN の不一致を含む LLDP パケットを受信しているかどうかを検出する場合に障害があります。

任意の APIC の CLI で次の moquery を実行して、システムに障害が存在するかどうかを確認できます。

障害の例（F0454：不一致のパラメータを持つ LLDP）：

```
apic1# moquery -c faultInst -f 'fault.Inst.code=="F0454"'
Total Objects shown: 2

# fault.Inst
code             : F0454
ack              : no
alert            : no
annotation       :
```

```
cause            : wiring-check-failed
changeSet        : wiringIssues (New:
ctrlr-uuid-mismatch,fabric-domain-mismatch,infra-ip-mismatch,infra-vlan-mismatch)
childAction      :
created          : 2021-06-30T10:44:25.576-07:00
delegated        : no
descr            : Port eth1/48 is out of service due to Controller UUID mismatch,Fabric
 domain name mismatch,Infra subnet mismatch,Infra vlan mismatch
dn               : topology/pod-1/node-104/sys/lldp/inst/if-[eth1/48]/fault-F0454
--- snip ---
```

コントラクト向けポリシー CAM プログラミング（F3545）

この障害F3545は、ハードウェアまたはソフトウェアのプログラミングの失敗のいずれかが原因で、スイッチがコントロール ルール（ゾーニング ルール）をアクティベートすることができないときに発生します。これが表示されるのは、ポリシー CAM がいっぱいで、スイッチにこれ以上コントラクトを展開できず、リブートまたはアップグレード後に別のコントラクトセットが展開される可能性があるためです。これにより、アップグレード前に動作していたサービスが、アップグレード後に失敗する可能性があります。ポリシー CAM の使用ではなく、コントラクトでサポートされていないタイプのフィルタなど、他の理由で同じ障害が発生する可能性があることに注意してください。たとえば、第 1 世代の ACI スイッチは EtherType IP をサポートしますが、コントラクト フィルタでは IPv4 または IPv6 はサポートしません。この障害が存在する場合は、APIC GUI の **[操作（Operations）]** > **[キャパシティ ダッシュボード（Capacity Dashboard）]** > **[リーフ キャパシティ（Leaf Capacity）]** でポリシー CAM の使用状況を確認します。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F3545：ゾーン分割ルールのプログラミングの失敗）：

次に、266 のコントラクト ルールに対して、プログラミング エラー（zoneRuleFailed）があるノード 101 の例を示します。また、changeSet の L3Out サブネットのプログラミング障害（pfxRuleFailed）も表示されますが、そのために別の障害 F3544 が発生します。

```
apic1# moquery -c faultInst -f 'fault.Inst.code=="F3545"'
Total Objects shown: 1

# fault.Inst
code             : F3545
ack              : no
annotation       :
cause            : actrl-resource-unavailable
changeSet        : pfxRuleFailed (New: 80), zoneRuleFailed (New: 266)
childAction      :
created          : 2020-02-26T01:01:49.256-05:00
delegated        : no
descr            : 266 number of Rules failed on leaf1
dn               : topology/pod-1/node-101/sys/actrl/dbgStatsReport/fault-F3545
domain           : infra
extMngdBy        : undefined
highestSeverity  : major
lastTransition   : 2020-02-26T01:03:59.849-05:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : major
```

```
prevSeverity     : major
rn               : fault-F3545
rule             : actrl-stats-report-zone-rule-prog-failed
severity         : major
status           :
subject          : hwprog-failed
type             : operational
uid              :
```

コントラクト向け L3Out サブネット プログラミング（F3544）

この障害F3544は、ハードウェアまたはソフトウェアのプログラミングの失敗のいずれかが原因で、**pcTag** へのプレフィックスをマッピングするために、スイッチがエントリをアクティベートすることができないときに発生します。これらのエントリは、L3Outの外部EPGの下の『**External Subnets for the External EPG**』範囲を持つL3Outサブネット用に設定され、L3Outサブネットを L3Out EPG にマッピングするために使用されます。スイッチの LPM またはホスト ルート キャパシティが原因でこれが表示される場合、そのようなスイッチは、リブートまたはアップグレード後に異なるエントリ セットをアクティブにする可能性があります。これにより、アップグレード前に動作していたサービスが、アップグレード後に失敗する可能性があります。この障害が発生している場合は、APIC GUI の **[操作（Operations）] > [キャパシティ ダッシュボード（Capacity Dashboard）] > [リーフ キャパシティ（Leaf Capacity）]** で LPM および /32 または /128 ルートの使用状況を確認します。

APIC の CLI で以下の moquery を実行し、これらの障害がシステムに存在するかどうかを確認できます。障害は GUI 内でも確認できます。

障害の例（F3544：L3Out サブネット プログラミング障害）：

次に、「外部 EPG 向け外部サブネット」（pfxRuleFailed）で 80 L3Out サブネットのプログラミングに失敗したノード 101 の例を示します。また、changeSet のコントラクト自体のプログラミング障害（zoneRuleFailed）も表示されますが、そのために別の障害F3545が発生します。

```
apic1# moquery -c faultInst -f 'fault.Inst.code=="F3544"'
Total Objects shown: 1

# fault.Inst
code             : F3544
ack              : no
annotation       :
cause            : actrl-resource-unavailable
changeSet        : pfxRuleFailed (New: 80), zoneRuleFailed (New: 266)
childAction      :
created          : 2020-02-26T01:01:49.246-05:00
delegated        : no
descr            : 80 number of Prefix failed on leaf1
dn               : topology/pod-1/node-101/sys/actrl/dbgStatsReport/fault-F3544
domain           : infra
extMngdBy        : undefined
highestSeverity  : major
lastTransition   : 2020-02-26T01:03:59.849-05:00
lc               : raised
modTs            : never
occur            : 1
origSeverity     : major
prevSeverity     : major
rn               : fault-F3544
rule             : actrl-stats-report-pre-fix-prog-failed
severity         : major
```

```
status          :
subject         : hwprog-failed
type            : operational
uid             :
```

一般的なスケーラビリティの制限値

APIC GUI の **[操作（Operations）] > [キャパシティ ダッシュボード（Capacity Dashboard）]** から [キャパシティ ダッシュボード（Capacity Dashboard）] を確認し、容量が制限を超えていないことを確認します。制限を超えると、コントラクト向けポリシー CAM プログラミング（F3545）（24 ページ）およびコントラクト向け L3Out サブネット プログラミング（F3544）（25 ページ）の警告と同様に、アップグレードの前後に展開されたリソースに不整合が生じる可能性があります。

これらは通常、ソフトウェアの制限値ではなくハードウェアの制限値のため、各スイッチの [キャパシティ ダッシュボード（Capacity Dashboard）] は、**[操作（Operations）] > [キャパシティ ダッシュボード（Capacity Dashboard）] > [リーフ キャパシティ（Leaf Capacity）]** で確認することをお勧めします。たとえば、MAC（学習済み）、IPv4（学習済み）、ポリシー CAM、LPM、ホスト ルートなどのエンドポイントの数。

重複する VLAN プール

異なる VLAN プール間で VLAN ブロックが重複すると、次のような転送の問題が発生する可能性があります。

- エンドポイントの学習の問題によるパケット損失
- BPDU 転送ドメインによるスパニング ツリー ループ

スイッチはアップグレード後にポリシーを最初から取得し、アップグレード前に使用されていたものとは異なるプールから同じ VLAN ID を適用する可能性があるため、**スイッチのアップグレード後にこれらの問題が突然発生することがあります**。その結果、VLAN ID は他のスイッチ ノードとは異なる VXLAN VNID にマッピングされます。これにより、上記の 2 つの問題が発生します。

VLAN ID と VXLAN ID マッピングをバックグラウンドで適切に理解している場合を除き、ファブリック内に重複する VLAN プールがないことを確認することが重要です。よくわからない場合は、APIC GUI（リリース 3.2(6) 以降で使用可能）の **[システム（System）] > [システム設定（System Settings）] > [ファブリック全体の設定（Fabric Wide Setting）]** で **[EPG VLAN検証を適用する（Enforce EPG VLAN Validation）]** を検討してください。これにより、もっとも問題が発生する設定を防ぎます（同じ EPG に関連付けられている重複 VLAN プールを含む 2 つのドメイン）。

重複 VLAN プールがどのように問題になるか、およびこのシナリオがいつ発生するかを理解するには、次のドキュメントを参照してください。

- 重複 VLAN プールによる VPC エンドポイントへの断続的なパケット ドロップとスパニング ツリー ループ
- ACI：一般的な移行の問題/ VLAN プールの重複

- 『Cisco APIC レイヤ 2 ネットワーキング設定ガイド、リリース 4.2(x)』の「重複する *VLAN* の検証」

L3Out MTU の不一致

ACI L3Out インターフェイスとそれらに接続するルータの MTU 値が一致していることを確認することが重要です。そうしないと、アップグレード後に ACI スイッチが起動したときに、ルーティング プロトコルのネイバーシップの確立中またはピア間のルート情報の交換中に問題が発生する可能性があります。

各プロトコルの詳細については、以下を参照してください。

BGP は、MTU を考慮せずにセッションを確立するプロトコルです。BGP の「オープンおよび確立」メッセージは小さいですが、ルートを交換するためのメッセージは非常に大きくなる可能性があります。

リンクの両端からの MTU が一致しない場合、OSPF はネイバーシップを形成できません。ただし、これは強く推奨されませんが、MTU が大きい側が MTU を無視して OSPF ネイバーシップを起動するように設定されている場合は、OSPF ネイバーシップが形成されます。

境界リーフ スイッチのアップグレード中は、ルーティング セッションが切断されます。境界リーフ スイッチが新しいバージョンでオンラインになると、ルーティング ピアが起動します。その後、ルーティング プレフィックスに関する情報の交換を開始すると、より大きなペイロードを持つフレームが生成されます。テーブルのサイズに基づいて、更新にはより大きなフレーム サイズが必要になる場合があります。このペイロードのサイズは、ローカル MTU によって異なります。反対側の MTU が一致しない場合（ローカル MTU サイズよりも小さい場合）、これらの交換は失敗し、ルーティングの問題が発生します。

[テナント（Tenant）] > [ネットワーキング（Networking）] > [L3Out] > [論理ノード プロファイル（Logical Node Profile）] > [論理インターフェイス プロファイル（Logical Interface Profile）] > [インターフェイス タイプの選択（Select interface type）] で L3Out インターフェイスの MTU も確認して設定できます。

任意の APIC の CLI で次の moquery を実行して、すべての L3Out インターフェイスの設定済み MTU を確認できます。次の例のように、必要に応じて簡潔な出力に `grep` を使用します。

```
egrep "dn|encap|mtu"
```

この例では、VLAN 2054 を持つ L3Out インターフェイスは、テナント *[TK]*、[L3Out] *[OSPF]*、[論理ノード プロファイル（Logical Node Profile）] *[OSPF_nodeProfile]*、および [論理インターフェイス プロファイル（Logical Interface Profile）] *[OSPF_interfaceProfile]* で MTU 9000 で設定されます。

```
apic1# moquery -c l3extRsPathL3OutAtt
Total Objects shown: 1

# l3ext.RsPathL3OutAtt
addr      : 20.54.0.1/24
        --- snip ---
dn        : uni/tn-TK/out-OSPF/lnodep-OSPF_nodeProfile/lifp-OSPF_interfaceProfile/
rspathL3OutAtt-[topology/pod-1/paths-101/pathep-[eth1/12]]
encap     : vlan-2054
        --- snip ---
```

```
mtu       : 9000
        --- snip ---
```

または、境界リーフ ノードでも `fabric <node_id> show interface` を実行できます。

MTU が `[継承（inherit）]` と表示される場合、値は **[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[ポリシー（Policies）]** > **[グローバル（Global）]** > **[ファブリック L2 MTU（Fabric L2 MTU）]** > **[デフォルト（default）]** から継承されます。

この章で提供されるスクリプトは、すべての L3Out インターフェイスの MTU を確認します。ただし、APIC でスクリプトを実行する必要があり、APIC は接続されたデバイスで設定された MTU 値の可視性を持ちません。したがって、接続されたデバイスの MTU を手動で確認する必要があります。

ループバックのないノード プロファイル下の L3Out BGP ピア接続プロファイル

リリース 4.1(2) 以降にアップグレードする前に、次の 2 つの要件のいずれかが満たされていることを確認する必要があります。

- BGP ピア接続プロファイルを持つノード プロファイルに、プロファイル内のすべてのスイッチにループバックが設定されている。
- BGP ピア接続プロファイルは、インターフェイスごとに設定されます。

BGP ピア接続プロファイルは、ノード プロファイルまたはインターフェイスごとに設定できます。前者はループバックから BGP セッションを送信し、後者は各インターフェイスから BGP セッションを送信します。

リリース 4.1(2) 以前では、BGP ピア接続プロファイルがループバックを設定せずにノード プロファイルで設定されている場合、APIC は別の L3Out からのループバック IP アドレスや、各インターフェイスに設定されている IP アドレスなど BGP 送信元と同じ VRF 内の同じ境界リーフ スイッチで使用可能な別の IP アドレスを使用します。これにより、リブートまたはアップグレード中に意図せずに BGP 送信元 IP アドレスが変更されるリスクがあります。この動作は CSCvm28482 に基づいて変更され、ループバックがノードプロファイルで設定されていない場合、ACI はノードプロファイルで BGP ピア接続プロファイルを介して BGP セッションを確立しなくなりました。代わりに、障害 F3488 がこれらの状況で発生します。この障害は、アップグレード後にのみ発生するため、アップグレード前のチェックとして使用することはできません。

この変更により、古いバージョンからリリース 4.1(2) 以降にアップグレードする場合、BGP ピア接続プロファイルを介してセッションがノード プロファイルで生成され、ループバックがノード プロファイルで設定されていない場合、BGP セッションは確立されなくなります。

同じノードプロファイル内の複数のインターフェイスが同じピア IP を使用して BGP ピアを確立する必要がある場合、同じ BGP ピア設定がループバックがないため、同じノード プロファイル内の各インターフェイスに対してフォールバックとして適用されるように、ループバックを使用せずノード プロファイルで BGP ピア接続プロファイルを設定する場合があります。これは、同じピア IP アドレスを持つ BGP ピア接続プロファイルが、同じノード プロファイル内の複数のインターフェイス プロファイルで設定できないためです。この制限は、4.2(7f) の CSCvw88636 に基づいて緩和されました。それまでは、この特定の要件について、インター

フェイス プロファイルごとにノードインターフェイスを設定し、異なるノード プロファイルの各インターフェイスプロファイルでBGP ピア接続プロファイルを設定する必要があります。

L3Out の誤ったルート マップ方向（CSCvm75395）

リリース 4.1(1) 以降にアップグレードする前に、ルート マップ（ルート プロファイル）の設定が正しいことを確認する必要があります。

CSCvm75395 の不具合により、誤った設定（方向の不一致）にもかかわらず、次の設定がリリース 4.1(1) より前に機能していた可能性があります。

- **インポート ルート制御サブネット**を持つ L3Out サブネットに接続された**エクスポート**方向のルートマップ
- **エクスポート ルート制御サブネット**を持つ L3Out サブネットに接続された**インポート**方向のルートマップ

ここで、L3Out サブネットは、L3Out の外部 EPG で設定されたサブネットを意味します。

ただし、ファブリックをリリース 4.1(1) 以降にアップグレードした後は、これらの誤った設定は機能しなくなります。これは予想される動作です。

この方法は、ACI L3Outs によってアドバタイズまたは学習されるルートを制御するための最も一般的な方法または推奨される方法ではありませんが、この方法での正しい設定は次のとおりです。

- **エクスポート ルート制御サブネット**を持つ L3Out サブネットに接続された**エクスポート**方向のルートマップ
- **インポート ルート制御サブネット**でL3Outサブネットに接続された**インポート**方向のルートマップ

または、以下の推奨設定に従って、代わりに L3Outs のルート交換を制御できます。

- IP プレフィックス リストを持つ **default-export** ルート マップ
- IP プレフィックスリストを持つ **default-import** ルート マップ

この設定では、外部 EPG に **[エクスポート ルート制御サブネット（Export Route Control Subnet）]** または **[インポート ルート制御サブネット（Import Route Control Subnet）]** は必要ありません。また、通常のルータと同様に、ルート マップを通じてルーティング プロトコルを完全に制御しながら、コントラクトまたはルート リーク専用の外部 EPG を使用できます。

また、インポート方向のルートマップは、**[テナント（Tenant）]** > **[ネットワーキング（Networking）]** > **[L3Out]** > **[メイン プロファイル（Main profile）]**でインポートに対してルート制御の適用が有効になっている場合にのみ有効になることに注意してください。それ以外の場合は、すべてがデフォルトでインポート（学習）されます。

EP Announce バージョンの不一致（CSCvi76161）

現在の ACI スイッチのバージョンが 12.2(4p) よりも前または 12.3(1) で、リリース 13.2(2) 以降にアップグレードする場合、Cisco ACI リーフ スイッチ間のバージョン不一致により、リーフ

スイッチの EPM プロセスが予期しない EP アナウンス メッセージを受信し、EPM がクラッシュしてスイッチがリロードされる場合があり、障害 CSCvi76161 を検出しやすくなります。

この問題を回避するには、リリース 13.2(2) 以降にアップグレードする前に、修正バージョンの CSCvi76161 にアップグレードすることが重要です。

- 12.2(4p) 以前の ACI スイッチ リリースを実行しているファブリックの場合、12.2(4r) にアップグレードしてから目的のリリースにアップグレードします。
- 12.3(1) ACI スイッチ リリースを実行しているファブリックの場合、13.1(2v) にアップグレードしてから目的のリリースにアップグレードします。

Intersight Device Connector をアップグレード中です。

intersight Device Connector（DC）アップグレードが進行中に APIC アップグレードが開始する場合、DC アップグレードが失敗する場合があります。

Intersight DC のステータスは、**[システム（System）]** > **[システム設定（System Settings）]** > **[intersight]** から確認できます。DC のアップグレードが進行中の場合は、しばらく待ってから APIC のアップグレードを再試行します。Intersight Device Connector のアップグレードは、通常 1 分未満で完了します。

ダウングレードのチェックリスト

一般に、アップグレードと同じチェックリストをダウングレードに適用する必要があります。さらに、古いバージョンではまだサポートされていない可能性がある新機能に注意する必要があります。このような機能を使用している場合は、ダウングレードの前に設定を無効にするか、変更する必要があります。そうしないと、ダウングレード後に一部の機能が停止します。

次に、ダウングレードの前に注意する必要がある機能の例を示します。ただし、次のリストは完全ではないため、使用している機能が古いリリースでもサポートされていることを確認するために、リリース ノートまたは設定ガイドを確認することを強く推奨します。

- Cisco APIC にログインする際の認証方式として DUO アプリケーションを使用する機能が、Cisco APIC リリース 5.0 (1) で導入されました。リリース 5.0(1) を実行していて、デフォルトの認証方式として [DUO] が設定されていて、リリース 5.0 (1) から以前のリリースに DUO がサポートされていない場合は、その後で、リリース 5.0 (1) より前のリリース (ローカル、LDAP、RADIUS など) にデフォルトの認証方式を変更することを推奨します。この状況でダウングレードする前にデフォルトの認証方式を変更しない場合は、ダウングレード後にフォールバック オプションを使用してログインする必要があります。その後、認証方式をリリース5.0(1) より前に使用可能なオプションに変更する必要があります。

  [管理 (Admin)] > **[AAA]** > **[認証 (Authentication)]** に移動し、ページの **)[デフォルト認証 (default authentication)]** エリアの **[Realm (領域)]** フィールドの設定を変更して、システムをダウングレードする前にデフォルトの認証方式を変更します。また、ダウングレード後に、手動で DUO ログイン ドメインを削除する必要があります。

- 4.2(6) リリース以降、SNMPv3 は Secure Hash Algorithm-2（SHA-2）認証タイプをサポートします。Cisco APIC リリース 4.2(6) 以降を実行していて、SHA-2 認証タイプを使用している場合、Cisco APIC リリース 4.2 (6) から前のリリースにダウングレードすると、ダウングレードがブロックされ、次のエラーメッセージが表示されます。

  ```
  SHA-2 認証タイプはサポートされていません。
  ```

  認証タイプを MD5 に変更するか、対応する SNMPv3 ユーザを削除して続行するかを選択できます。

- APIC のコンテナ ブリッジ IP アドレスの変更は、APIC リリース 4.2(1) 以降でのみサポートされます。AppCenter の APIC のコンテナ ブリッジ IP アドレスがデフォルト以外の IP アドレスで設定されている場合は、4.2(1) よりも古いバージョンにダウングレードする前に、デフォルトの172.17.0.1/16 に戻します。

- [テナント（Tenants）]**[管理（mgmt）]** > **[ノード管理 EPG（Node Management EPGs）]** のインバンドおよび/またはアウトオブバンド EPG のスタティック ルート（MO：**mgmtStaticRoute**）は、APIC リリース 5.1 以降でのみサポートされます。この設定を削除し、必要なサービスがダウングレード前に他の手段で到達可能であることを確認します。

- 新しく追加されたマイクロセグメンテーション EPG 設定は、サポートしていないソフトウェア リリースにダウングレードする前に削除する必要があります。

- リーフ スイッチから始まるファブリックをダウングレードすると、障害コード F 1371 の policy-deployment-failed のような障害が発生します。

- FIPS をサポートしているリリースから FIPS をサポートしていないリリースにファームウェアをダウングレードする必要がある場合、最初に Cisco ACI ファブリックで FIPS を無効にして、FIPS 設定の変更のためファブリック内のすべてのスイッチをリロードする必要があります。

- エニーキャストサービスを Cisco ACI ファブリックで設定している場合は、Cisco APIC 3.2(x) から前のリリースにダウングレードする前に、外部デバイスでエニーキャストゲートウェイ機能を無効にしてエニーキャストサービスを停止する必要があります。

- Cisco APIC 3.0(1) より前のリリースにダウングレードする前に、CiscoN9K-C9508-FM-E2 ファブリックモジュールを物理的に削除する必要があります。同じことが、サポートされているバージョンの新しいモジュールにも適用されます。

- リモートリーフスイッチを展開している場合、Cisco APIC ソフトウェアをリリース 3.1(1) またはそれ以降からリモートリーフスイッチ機能をサポートしていない前のリリースにダウングレードする場合は、ダウングレードする前にノードの使用を停止する必要があります。リモートリーフ スイッチのダウングレードの前提条件に関する詳細は、「*Cisco APIC レイヤ 3 ネットワーキング設定ガイド*」の「リモート リーフ スイッチ」の章を参照してください。

- 次の条件が満たされている場合、

  - 5.2(4) リリースを実行中で、Cisco APIC で 1 つまたは複数のシステム生成ポリシーが作成されている場合。

- Cisco APIC を 5.2(4) リリースからダウングレードし、次に 5.2(4) リリースにアップグレード直した場合。

この場合、次のいずれかの動作が発生します。

- Cisco APIC が作成しようとしているシステム生成ポリシーと同じ名前とパラメータを持つポリシーが見つかった場合、Cisco APIC ではそのポリシーの所有権を取得するため、ポリシーは変更できません。これは、5.2(4) リリースからダウングレードした後で、ポリシーを変更しなかった場合に発生します。
- Cisco APIC で Cisco APIC が作成しようとしているシステム生成ポリシーと同じ名前のポリシーが見つかったがパラメータが異なる場合、 Cisco APIC ではそのポリシーをカスタムポリシーと見なし、ポリシーを変更できます。これは、5.2(4) リリースからダウングレードした後で、ポリシーを変更した場合に発生します。

この動作のため、5.2(4) リリースからダウングレードした後は、システム生成ポリシーを変更しないでください。

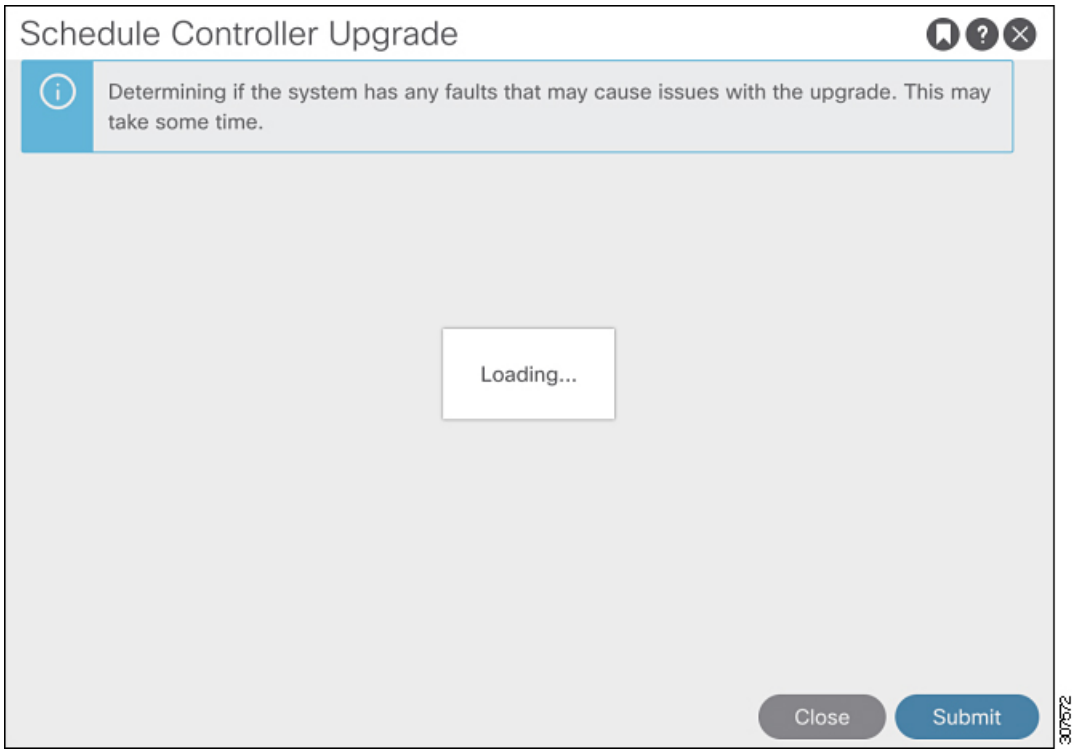
- イメージをダウングレードする前に、Cisco APIC に接続されているサポートされていないリーフ スイッチをデコミッションし、ケーブルをファブリックの一部である他のリーフ スイッチに移動する必要があります。

アップグレード前検証の例（APIC）

APIC リリース 4.2(5) の GUI を使用したエラーメッセージおよびオーバーライドオプションの例

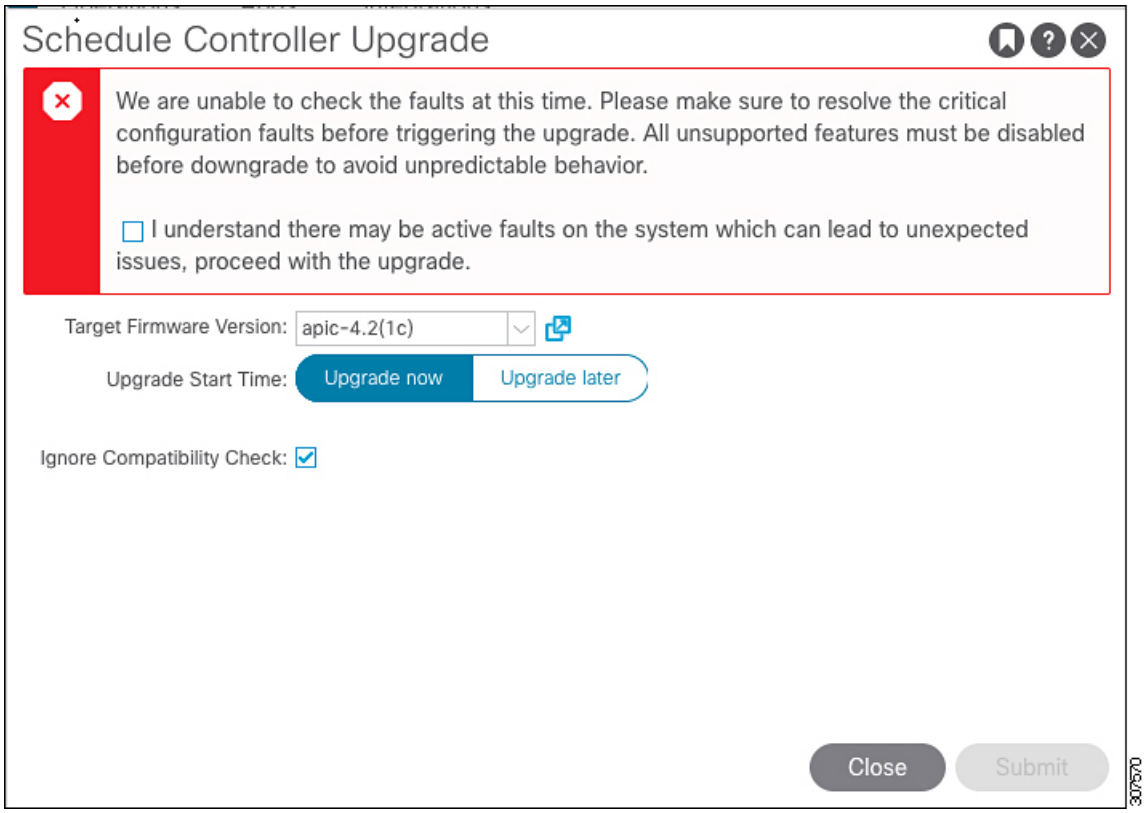
警告メッセージが GUI で表示される場合は、次の 3 つの状況が考えられます。

- クエリのロード中に、次のようなメッセージが表示される場合があります。



これは、クエリからデータをロードするのに少し時間がかかることがあるために発生する可能性があります。この状況では、システムがクエリからのデータのロードを完了するまでしばらく待ちます。

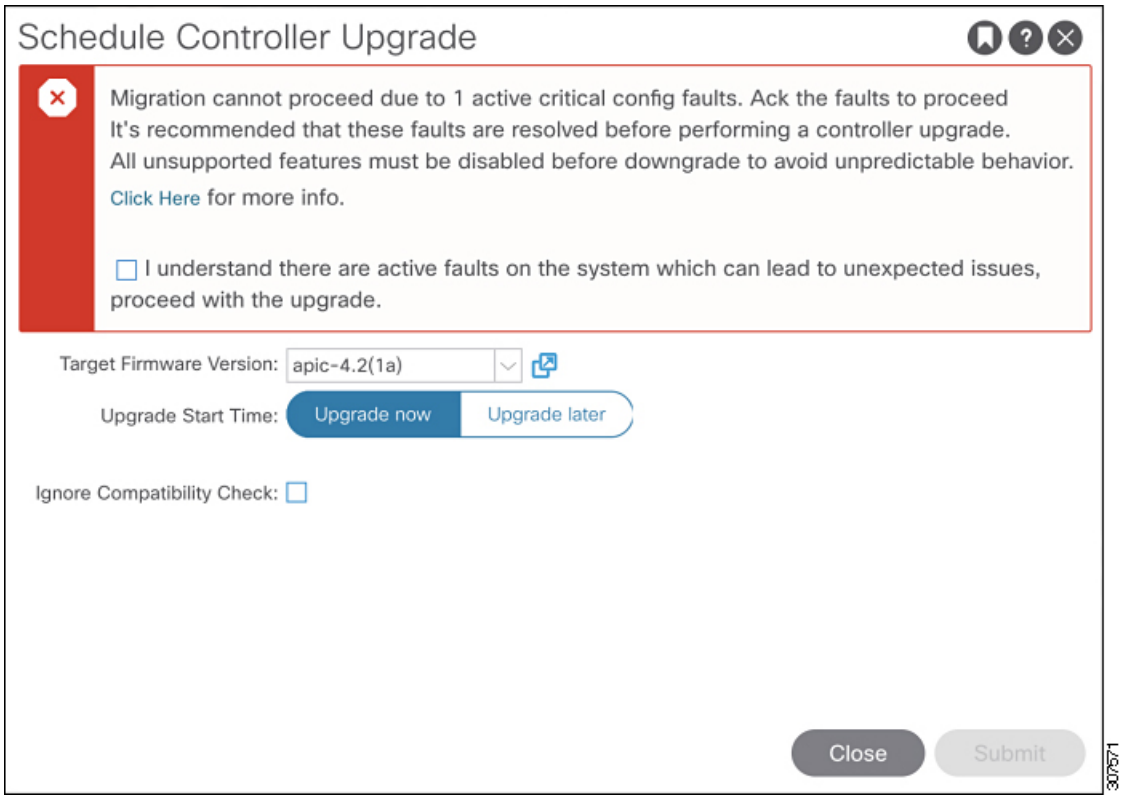
- 何らかの理由でクエリが失敗した場合は、次のようなメッセージが表示されることがあります。



この警告は、何らかの理由でクエリが失敗した場合に表示されます (たとえば、システムで過負荷が発生している可能性があります)。この場合、アップグレードに問題が発生する原因となる障害があるかどうかを確認する必要があります。

ただし、失敗したクエリの問題に対処せずにブロックをオーバーライドし、アップグレードまたはダウングレードを続行する場合は、**[予期していない問題につながることがあるアクティブな障害がシステムに存在している可能性があることを理解しました。アップグレードを続行します (I understand there may be active faults on the system which can lead to unexpected issues, proceed with the upgrade)]** フィールドの横にあるボックスをオンにします。これにより、失敗したクエリに関する問題に対処せずに、アップグレードまたはダウングレード プロセスを続行できます。

- 障害のクエリが完了すると、次のようなメッセージが表示される場合があります。



この警告メッセージは、障害クエリが完了して、システムが1つ以上の障害を検出したときに表示されます。この状況では、**[ここをクリック (Click Here)]** リンクをクリックして、システムが検出した障害の詳細情報を取得してください。

可能な場合は、アップグレードまたはダウングレードプロセスに進む前に、障害で発生した問題を解決することを推奨します。これらの障害と推奨処置の詳細については、CISCO APIC System fault/Events Search Tool および Cisco ACI System Messages Reference Guide を参照してください。

ただし、障害で発生した問題に対処せずにブロックをオーバーライドし、アップグレードまたはダウングレードを続行する場合は、**[予期していない問題につながることがあるアクティブな障害がシステムに存在していることを理解しました。アップグレードを続行します (I understand there are active faults on the system which can lead to unexpected issues, proceed with the upgrade)]** フィールドの横にあるボックスをオンにします。これにより、検出された障害に対処せずに、アップグレードまたはダウングレードプロセスを続行できます。

エラー メッセージの例および NX-OS スタイル CLI を使用したオプションのオーバーライド

NX-OS スタイルの CLI を使用してソフトウェアをアップグレードしようとすると、次のようになる可能性があります。

```
apic# firmware upgrade controller-group
```

ファブリックの障害が検出された場合は、次のようなエラーメッセージが表示されることがあります。

```
Error: Migration cannot proceed due to 23 active critical config faults. Resolve the
faults to proceed
```

可能な場合は、アップグレードまたはダウングレードプロセスに進む前に、障害で発生した問題を解決することを推奨します。これらの障害と推奨処置の詳細については、『CISCO APIC システムの障害/イベント検索ツール』および『Cisco ACI システム メッセージ参照ガイド』を参照してください。

ただし、ブロックをオーバーライドして、障害で発生した問題に対処せずにアップグレードまたはダウングレードを続行する場合は、`ignore-validation` オプションを使用してアップグレードを続行します。

```
apic# firmware upgrade controller-group ignore-validation
```

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。