Cisco APIC インストールおよび ACI アップグレード、ダウングレード ガイド

初版：2016 年 7 月 1 日

最終更新：2021 年 8 月 20 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

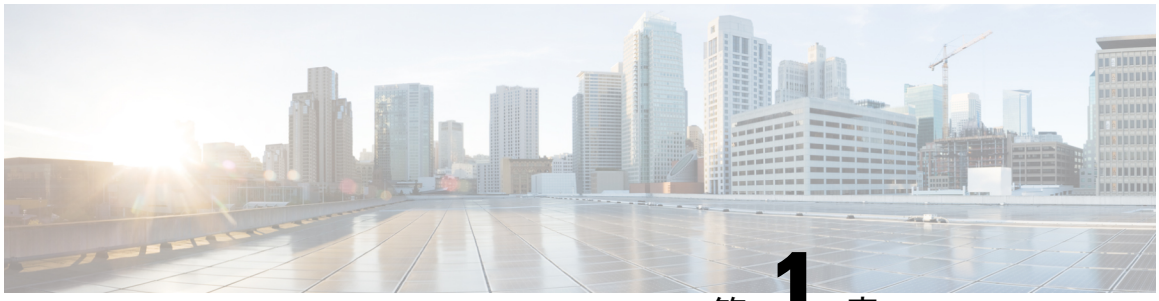
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新機能と更新情報

新規および変更情報

（注） 最初に操作するリリースの「*Cisco Application Policy Infrastructure Controller Release Notes*」を常に確認してください。

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能の中には、一部、この表に記載されていないものもあります。

表 *1*: 新機能および変更された機能に関する情報

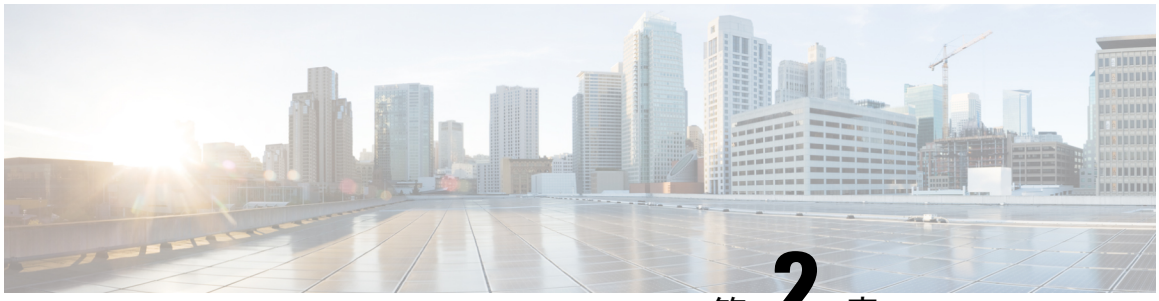
Cisco APIC のリリースバージョン	特長	説明	参照先
5.2(4)	デフォルトのインターフェイスポリシーの作成	5.2(4) 以降のリリースにアップグレードすると、Cisco APIC はデフォルトのインターフェイスポリシーを自動的に作成することがあります。	5.2(4) リリース以降のデフォルトインターフェイスポリシー （60 ページ）

Cisco APIC のリリースバージョン	特長	説明	参照先
該当なし	ユーザビリティを向上させるためのドキュメントの再編成。	2021 年 7 月 30 日、ユーザビリティを向上させるために、このドキュメントの内容が完全に再編成され、書き直されました。このドキュメントのタイトルは、この再編成作業の一部を反映するため、『*Cisco APIC* インストールおよび *ACI* アップグレードおよびダウングレードガイド』に名前が変更されました。	
5.2(1)	スイッチは、特定のコンポーネントの通常のブートアップ シーケンス中に、起動中の ACI スイッチ イメージに基づいて、APIC を介して実行されるアップグレード操作ではない場合でも、FPGA / EPLD / BIOS を自動的にアップグレードします。	リリース 5.2(1) および ACI スイッチ リリース 15.2(1) 以降、ACI スイッチは、特定のコンポーネントの通常のブートアップ シーケンス中に、起動中の ACI スイッチ イメージに基づいて、APIC を介して実行されるアップグレード操作ではない場合でも、FPGA / EPLD / BIOS を自動的にアップグレードします。	FPGA/EPLD/BIOS ファームウェアの管理 （171 ページ）
5.2(1)	ソフトウェア メンテナンス アップグレード パッチ	特定の不具合に対する修正を含むソフトウェア メンテナンス アップグレード（SMU）パッチをインストールできます。SMU パッチは、従来のパッチ リリースよりもはるかに迅速にリリースできるため、特定の問題をタイムリーに解決できます。SMU パッチは、Cisco APIC および Cisco ACI モード スイッチで使用できます。	ソフトウェア メンテナンス アップグレード パッチ （181 ページ）
5.1(1)	APIC またはスイッチ ソフトウェアのアップグレード時の GUI によるアップグレード プロセスの拡張。	リリース 5.1(1) から、GUI を使用した APIC およびスイッチ ソフトウェアのアップグレード プロセスが強化されました。	GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ）

Cisco APIC のリリースバージョン	特長	説明	参照先
5.1(1)	アップグレードまたはダウングレード操作がトリガーされる前に、追加の検証が実行されます。	ソフトウェアをアップグレードまたはダウングレードすると、追加の検証が実行され、検証中に問題が見つかった場合は 5.1(1) リリースの一部として警告が表示されます。	GUI を使用した APIC リリース 5.1 以降でのアップグレード（127ページ）
4.2(5)	アップグレードまたはダウングレード操作がトリガーされる前に、追加の検証が実行されます。	リリース 4.2(5) 以降、アップグレードまたはダウングレード操作をトリガーしようとすると、操作がトリガーされる前に追加の検証が実行され、検証中に問題が見つかった場合は警告が表示されます。	• 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（115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）
4.2(5)	コントローラのアップグレード時に提供される追加情報。	リリース 4.2(5) 以降では、コントローラのアップグレード プロセスのステータスに関する追加情報が提供される場合があります。	• 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（115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）
4.2(5)	ファームウェア アップグレード グループのスイッチ ノードをアップグレードするときに提供される追加情報。	リリース 4.2(5) 以降では、ファームウェア アップグレード グループのノードをアップグレードするときに、ファームウェアのダウンロードの進行中にステータスが表示されます。	• 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（115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）
4.2(5)	システムが一度にアップグレードできるスイッチの数が変更されました。	リリース 4.2(5) 以降、デフォルトでは、システムが一度にアップグレードできるスイッチの数が 20 から無制限に変更されました。	• 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（115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）

Cisco APIC のリリースバージョン	特長	説明	参照先
4.2(1)	検証は、アップグレードまたはダウングレード操作がトリガーされる前に実行されます。	リリース 4.2(1) 以降では、アップグレードまたはダウングレード操作をトリガーしようとすると、操作がトリガーされる前に、いくつかの検証が実行され、検証中に障害が見つかった場合は警告が表示されます。	• 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（115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）
	APIC アップグレードパスおよびダウングレード パスをドキュメントから削除	APIC アップグレードパスおよびダウングレード パスをドキュメントから削除しました。APIC アップグレード パスおよびダウングレード パスについては、「*Cisco APIC* アップグレードまたはダウングレード サポート一覧表」を参照してください。 https://www.cisco.com/c/dam/en/us/td/docs/Website/datacenter/apicmatrix/index.html	
4.1(2x)	サイレント ロール パッケージのアップグレード	サイレント ロール パッケージのアップグレードでは、ACI スイッチ ソフトウェア OS 全体をアップグレードすることなく、ACI スイッチハードウェア SDK、ドライバなどの内部パッケージのアップグレードを手動で実行できます。	サイレント ロール パッケージのアップグレード（175 ページ）
	「*Cisco APIC* リリース *4.0(1)* インストール、アップグレード、ダウングレード ガイド」はもうご利用いただけません。	『*Cisco APIC* リリース *4.0(1)* インストール、アップグレード、ダウングレード ガイド』はもうご利用いただけません。掲載されていた情報は、アップグレード パスおよびダウングレード パス以外はすべて本ドキュメントでご覧いただけます。	

Cisco APIC のリリースバージョン	特長	説明	参照先
4.0(1)	アップグレード方式としてサポートされなくなった bash	リリース 4.0(1) 以降、bash を使用して Cisco APIC およびスイッチ ソフトウェアをアップグレードすることはできません。代わりに NX-OS スタイル CLI を使用して Cisco APIC およびスイッチ ソフトウェアをアップグレードしてください。	• 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 （115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ）
4.0(1)	GUI を使用したアップグレード手順の変更	Cisco APIC リース 4.0(1) から、GUI を使用したソフトウェアのアップグレード手順が変更されました。	• 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 （115 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ）
3.2(1m)	Cisco APIC 長寿命リリース		Cisco ACI 長期および短期リリース （7 ページ）
2.3(1e)	ネットワーク設定機能と混合OS動作中の変更	追加機能のサポートが追加されました。	Cisco ACI スイッチの混合バージョンで許可される操作 （65 ページ）
2.2（2e）	ネットワーク設定機能と混合OS動作中の変更	この機能が導入されました。	Cisco ACI スイッチの混合バージョンで許可される操作 （65 ページ）
2.2（2e）	--	このガイドの内容が再編成されました。このガイドの以前のリリースでは Cisco APIC クラスタ コンテンツのハイアベイラビリティは「*Cisco APIC Getting* 開始ガイド、リリース *2.x*」に以降されています。	--
2.2(1n)	APIC クラスタのハイアベイラビリティ	APIC クラスタのハイアベイラビリティ機能では、Active/Standby モードのクラスタで APIC を操作できます。	このコンテンツは「*Cisco APIC* 開始、*2.x* のリリース」で確認できます。
1.3(1g)	このドキュメントのタイトルは変更されています。	以前の名前は、Cisco APIC ファームウェア管理ガイドでした。	



第 2 章

Cisco ACI 長期および短期リリース

長期リリースについて

Cisco ACI長命リリースでは、ながら、品質や安定性を保証する頻繁なメンテナンス ドロップ(約 18 か月)、最大長期的な単位で所定のリリースを維持するのに役立ちますソフトウェア リリースです。Cisco では、時間の任意の時点の 2 つの長命リリースをサポート可能性があります。ただし、アクティブなメンテナンスがプライマリは長命最新のリリースに置かれています。これらのリリースは、他のリリースよりも長い期間に維持されます。長命リリースは、頻繁にアップグレードされませんネットワークのまたは広く採用されている機能を展開するために推奨されます。

次回または前回の長期リリースへのすべての長期リリース サポートへのアップグレードまたはダウン グレード確認済みのサポートについては、『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。

（注） リリース ブランチは、長期リリースとしてサポートされている場合もあれば、サポートされていない場合もあります。たとえば、2.*x* には 2.1、2.2、2.3 の 3 つのリリース ブランチが存在する可能性があります。しかし、2.*x* の 3 つのリリース ブランチのうち、1 つは長期リリース（2.2）としてサポートされている可能性がありますが、他の 2 つのリリース ブランチ（2.1 と 2.3）は長期リリースとしてサポートされていない可能性があります。

短期リリースについて

Cisco ACI 短期間リリースは、新機能の機能のために提供される安定した高品質のリリースです。これらのリリースでは、最初のリリース後 6 ヵ月間はメンテナンス サポートが限定され、

その後はアクティブなメンテナンスは行われません。また、これらのリリースには EOS アナウンスはありません。

すべての Cisco ACI リリースと同様に、以前の 2 つのリリースから短期間リリースへのアップグレードがサポートされている場合があります。確実なサポートに関しては、『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』を参照してください。

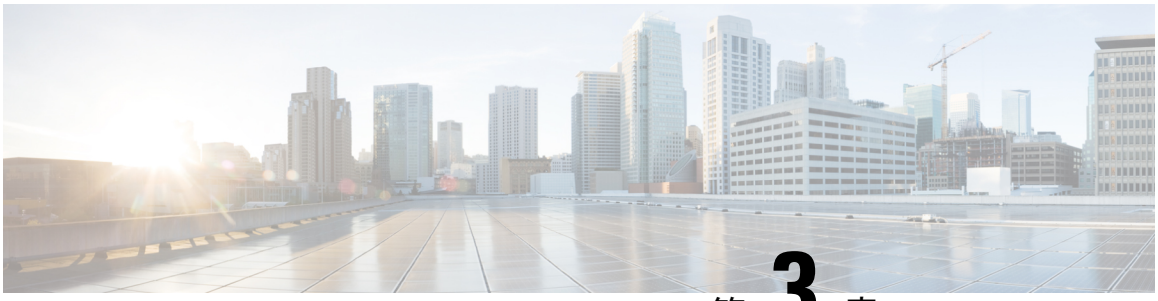
長期リリースのライフ サイクル

- 長命のメジャー リリースのライフ サイクルは、マイナーの最初のリリースの first customer shipment（FCS) から始まります。
- メジャーリリースはその後、メンテナンスリリース導入フェーズに入り、製品の不具合に対応するため、いくつかのリリースが提供されます。
- その後、メジャーリリースは成熟メンテナンスフェーズに移行します。このフェーズでは、顧客によって発見された重要度 1 および重要度 2 の欠陥に対してのみ、修復が行われます。内部で発見された不具合には個別に対処します。内部で発見された不具合で個別に対処します。
- すべての長期リリースは、次の長期リリースまたは前の長期リリースの最終メンテナンス バージョンへのアップグレード、またはダウングレードをサポートしています。

Cisco Nexus 9000 ACI モード スイッチと Application Policy Infrastructure Controller（APIC）を、新規に展開するお客様、またはすでに展開済みのお客様は、次の長期リリースから選択することをお勧めします。

Cisco APIC の長期リリース バージョン	長命の Cisco スイッチのリリース バージョン
5.2(x)	15.2(x)
4.2(x)	14.2(x)

特定の長期リリース バージョンに対応した最新のメンテナンス リリースとパッチにアップグレードすることをお勧めします。最新の Cisco Nexus 9000 ACI モード スイッチと Cisco APIC の展開は、該当する Cisco ソフトウェア ダウンロード ページからダウンロードできます。



第 3 章

インストールまたはCisco APICイメージの回復

設置上の注意事項

- ハードウェアのインストール手順については、「Cisco ACI ファブリック ハードウェア インストール ガイド」を参照してください。
- このリリースをインストールまたはアップグレードする前に、Cisco APIC 設定をバックアップします。実稼働で実行しない単一の Cisco APIC クラスタは、インストールまたはアップグレード中にデータベースの破損が発生すると設定が失われる可能性があります。
- 初めて Cisco APIC にアクセスする方法については、『Cisco APIC 入門ガイド』を参照してください。
- Microsoft System Center Virtual Machine Manager（SCVMM）または Microsoft Windows Azure パックを持つ Cisco ACI は ASCII 文字のみをサポートしています。非 ASCII 文字はサポートしていません。Windows のシステム ロケールの設定に [English] が設定されていることを確認します。それ以外の場合、 SCVMM および Windows Azure Pack を持つ Cisco ACI はインストールされません。また、システム ロケールをインストール後に英語以外のロケールに変更した場合、Cisco APIC や Cisco ACI ファブリックと通信すると統合コンポーネントが失敗する場合があります。
- インストールの指示を含む Cisco APIC Python SDK ドキュメントについては、「APIC Python SDK ドキュメンテーション」を参照してください。

インストールに必要な SDK egg ファイルがパッケージに含まれます。egg ファイル名の形式は次のとおりです。

```
acicobra-A.B_CD-py2.7.egg
```

- *A*：メジャーリリース番号。
- *B*：マイナーリリース番号。
- *C*：メンテナンスリリース番号。
- *D*：リリースレター（パッチレター）。文字は小文字です。

たとえば、5.2(4d) リリースの egg ファイル名は次のとおりです。

```
acicobra-5.2_4d-py2.7.egg
```

- UNIX/Linux および Mac OS X で SSL 対応の SDK をインストールするには、コンパイラが必要です。Windows インストールでは、wheel パッケージを使用して SDK の依存関係用のコンパイル済み共有オブジェクトをインストールできます。
- モデル パッケージは SDK のパッケージによって異なります。SDK のパッケージを先にインストールしてください。

使用上のガイドライン

- Cisco APIC GUI は次の ブラウザをサポートします。
  - Mac および Windows 向け Chrome バージョン 59（最低）
  - Mac、Linux、Windows 向け Firefox バージョン 59 (最低)
  - Internet Explorer バージョン 11（最低）
  - Safari 10（最低）

（注） リリース 1.3(1) にアップグレードした後、ブラウザを再起動します。

- Cisco APIC GUI には、ビデオ デモンストレーションを含むクイックスタート ガイドのオンライン バージョンが含まれます。
- インフラストラクチャの IP アドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ファブリックで使用する他の IP アドレスと重複してはなりません。
- Cisco APIC はテナントの負荷に IPAM サービスを提供しません。

- GUI から Cisco APIC CLI に到達するには、[システム (System)] > [コントローラ (Controllers)] を選択し、コントローラをハイライトしてから、[SSH の起動 (launch SSH)] を右クリックして選択します。コマンドのリストを取得するには、esc キーを 2 回押します。
- 5 分間の統計データの一部では 10 秒のサンプルの数は 30 ではなく 29 です。
- 次のサービスでは、アウトオブバンド管理接続を持つ DNS ベースのホスト名を使用します。IP アドレスは、インバンドおよびアウトオブバンド管理接続両方で使用できます。
  - Syslog サーバ
  - Call Home SMTP サーバ
  - テクニカル サポート エクスポート サーバ
  - 設定エクスポート サーバ
  - 統計情報エクスポート サーバ
- リーフおよびスパイン スイッチは、IP 接続を持つホストからファブリックへ管理できます。
- 2 個のエンドポイント間でアトミック カウンタを設定する場合、IP は 2 個のエンドポイントのどちらかで学習され、エンドポイントベース ポリシーではなく IP ベース ポリシーを使用することをお勧めします。
- 同じノードで 2 つのレイヤ 3 の外部ネットワークを設定するときに、ループバックはレイヤ 3 ネットワークに別々に設定されます。
- アプリケーション EPG およびレイヤ 3 外部 EPG を含むすべてのエンドポイント グループ（EPG）にはドメインが必要です。インターフェイス ポリシー グループは、接続エンティティ プロファイル（AEP）に関連付けられ、AEP はドメインに関連付けられている必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。これは、ブリッジ型のレイヤ 2 アウトサイドおよびルーテッド レイヤ 3 アウトサイド EPG を含むすべての EPG に適用されます。詳細については、『Cisco Fundamentals GuideCisco』、および KB の記事、「Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port」を参照してください。

（注） 1.0(4X) 以前のリリースでは、アプリケーション EPG またはレイヤ 2/レイヤ 3 アウトサイド EPG のスタティック パスを作成するとき、物理ドメインは必要ありませんでした。このリリースでは必須です。物理ドメインを使用しないアップグレードは、EPG で「無効なパス設定」という 障害が発生します。

- EPG は、それ自体のテナント内でのみコントラクト インターフェイスに関連付けられます。

- ユーザ パスワードは、次の基準を満たす必要があります。
  - 最少文字数は 8 文字
  - 最大文字数は 64 文字
  - 連続して繰り返される文字は 3 文字未満
  - 次の文字タイプのうち 3 個を含む：小文字、大文字、数字、記号
  - 簡単に推測することができない
  - ユーザ名やユーザ名を逆にしたものは使用できません
  - cisco、isco、またはこれらの文字列の並べ替えを変化させたものや、それらの文字の大文字化の変更により取得される変形語であってはなりません
- 電力消費の統計情報がリーフ スイッチ ノード スロット 1 では表示されません。
- API またはアドバンスト GUI で作成され CLI を通して更新されたレイヤ 3 外部ネットワークについては、プロトコルは API またはアドバンスト GUI を通して外部ネットワークでグローバルに有効にする必要があり、CLI を介してさらに更新を行う前に、すべての参加ノードのノード プロファイルは API またはアドバンスト GUI を通して追加される必要があります。
- CLI から作成されたレイヤ 3 外部ネットワークについては、API を使用して更新しないようにする必要があります。これらの外部ネットワークは、「__ui_」で始まる名前で識別されます。
- NX OS スタイル CLI で発行された「show」コマンドの出力は、今後のソフトウェア リリースで変更されます。Cisco は、自動化に show コマンドの出力の使用を推奨していません。
- このソフトウェアのバージョンで、CLI は管理ログイン権限を持つユーザに対してのみサポートされています。
- 仮想プライベート クラウド（vPC）メンバ ノードを異なる設定ゾーンんに分離しないでください。ノードが異なる設定ゾーンにあるとき、インターフェイス ポリシーが変更され vPC メンバ ノードの 1 つのみに展開されている場合、vPC のモードが不一致になります。
- 複数のログイン ドメインを定義する場合は、Cisco APIC にログインするときに使用するログイン ドメインを選択できます。デフォルトでは、ドメイン ドロップダウンリストは空であり、ドメインを選択しない場合 DefaultAuth ドメインが認証に使用されます。この場合、DefaultAuth のログイン ドメインにユーザ名がないとログインに失敗する可能性があります。その結果、選択したログイン ドメインに基づくクレデンシャルを入力する必要があります。
- ファームウェア メンテナンス グループに含められるのは、最大 80 ノードです。
- コントラクトがエンドポイント グループに関連付けられていない場合、DSCP マーキングは vzAny コントラクトを持つ VRF ではサポートされていません。DSCP は actrl ルールとともにリーフ スイッチに送信されますが、vzAny コントラクトに actrl ルールはありません。したがって、DSCP 値が送信されることはありません。

- Cisco ACI ファブリックの NTP サーバとしては、リーフ スイッチを使用することをお勧めします。

Cisco APIC ソフトウェア イメージの回復またはインストールの条件

（注） Cisco Technical Assistance Center（TAC）のサポートのみで、このセクションで手順を使用します。

このクラスタは Cisco APIC をインストールまたは回復する方法を説明します。既存のサーバが完全に応答していない Cisco APIC イメージを所有し、新しい Cisco APIC イメージをインストールする場合、Cisco APIC イメージを回復します。

（注） 既存の UCSサーバが存在する場合、Cisco APIC ソフトウェア セクションのインストールをスキップします。

Cisco APIC イメージをインストールすることで、次のタスクを完了します。

- ディスク上にある既存のデータが消去されます。
- ディスクが再フォーマットされます。
- 新しいソフトウェア イメージがインストールされます。

次のいずれかの方法を使用して、サーバに Cisco APIC ソフトウェアをインストールすることができます。

- PXE サーバの使用
- 仮想メディアの使用

（注） 他の仮想メディアのインストールを実行するときと同じように、Cisco APIC ISO イメージファイルを使用してインストールを行うことができます。手順の詳細については、このマニュアルでは説明していません。

PXE サーバを使用した Cisco APIC ソフトウェアのインストール

Preboot Execution Environment（PXE）サーバを使用して Cisco APIC ソフトウェアをインストールするには、以下の手順に従ってください。

手順

ステップ 1 Linux の標準構成で PXE サーバを設定します。

ステップ 2 リリース 4.0 以降のCisco APICソフトウェア イメージをインストールするために、PXE 設定ファイルに次のようなエントリがあることを確認します。

```
label 25
   kernel vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2
noprobe=ata3 noprobe=ata4
   append initrd=initrd root=live:squashfs.img_URL rd.live.img rd.live.debug=1
rd.live.ram=1 rd.debug atomix.isourl=iso_URL
```

例：

```
label 25
   kernel ifcimages/vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1
noprobe=ata2 noprobe=ata3 noprobe=ata4
   append initrd=ifcimages/initrd.img
root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

ステップ 3 Cisco.com から Cisco APIC.iso イメージをダウンロードします。

ステップ 4 マウント フォルダを作成し、Cisco APIC.iso イメージをマウントします。

```
$ mkdir -p mount_folder
$ mount -t iso9660 -o loop iso_image mount_folder
```

例：

```
$ cd /home/user
$ mkdir -p myisomount
$ mount -t iso9660 -o loop /local/aci-apic-dk9.4.0.0.iso myisomount
```

ステップ 5 Initrd. imgおよびvmlinuzファイルがマウントフォルダの場所にあることを確認します。

例：

```
$ ls /home/user/myisomount/images/pxeboot/
initrd.img  vmlinuz
```

ステップ 6 マウントされた Cisco APIC.iso イメージから、vmlinuz および intird を tftpboot パスにコピーします。

例：

```
$ mkdir -p /var/lib/tftpboot/ifcimages
$ cp -f /home/user/myisomount/images/pxeboot/vmlinuz /var/lib/tftpboot/ifcimages/
$ cp -f /home/user/myisomount/images/pxeboot/initrd.img /var/lib/tftpboot/ifcimages/
```

ステップ 7 Cisco APIC.iso イメージとマウントフォルダを HTTP ルートディレクトリにコピーします。

例：

```
$ cp -R /local/aci-apic-dk9.4.0.0.iso /var/www/html
$ cp -R /home/user/myisomount /var/www/html
```

ステップ 8 PXE の構成(/var/lib/tftpboot/pxelinux.cfg/default)にエントリを追加して、Cisco APIC.iso イメージのためのキックスタート ファイルを参照するようにします。

例：

```
[root@pxeserver ~]# cat /var/lib/tftpboot/pxelinux.cfg/default
label 25
   kernel ifcimages/vmlinuz dd blacklist=isci blacklist=ahci nodmraid noprobe=ata1
noprobe=ata2 noprobe=ata3 noprobe=ata4
   append initrd=ifcimages/initrd.img
root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

この情報を使用して、PXE メニュー エントリ イメージが正しく設定されていることを確認します。

ステップ 9 PXE サーバを再起動します。

ステップ 10 Cisco APIC を再起動し、F12 キーを押してネットワーク ブートを開始します。

ステップ 11 PXE サーバで設定されたオプションを選択して、Cisco APIC イメージを起動します。

インストール Cisco APIC 仮想メディアを使用してソフトウェア

仮想メディア（vMedia）を使用した Cisco APIC ソフトウェアのインストールまたはアップグレードは、次の高度なプロセスが必要です。

- 必要に応じて、Cisco Integrated Management Controller（CIMC）ソフトウェアをアップグレードします。
- Cisco.com から関連する Cisco APIC .iso イメージを取得します。

- コントローラの CIMC Web インターフェイスにアクセスします。

（注） CIMC へのアクセスと、仮想メディアを管理の詳細については、CIMC ソフトウェア (1.5 または 2.0) のコントローラのバージョンに対応する「CIMC 設定ガイド」を参照してください。

- CIMC vMedia 機能を使用して、.iso イメージをマウントします。
- コントローラを起動し電源を再投入します。
- 起動プロセス中に **[F6]** を押し、ワンタイム起動デバイスとして **[Cisco vCIMC-Mapped vDVD]** を選択します。BIOS パスワードを入力する必要があります。デフォルト パスワードは **password** です。
- インストールする画面の指示に従って、 Cisco APIC ソフトウェア。

（注） VMedia の速度が遅く転送速度、によりオプションで、ネットワークから主要なイメージをインストールすることができます。プロンプトが表示されたら、キーを押します **Enter** IMC vMedia インストール プロセス中に 30 秒以内です。インストーラは vMedia インストールからネットワーク イメージの場所が切り替わります。該当するホスト IP アドレス、サブネット、ゲートウェイ、および [image path などの構成の詳細情報ネットワー キングを入力して、プロンプトに応答します。

CIMC ソフトウェアのアップグレード

Cisco ACI ファブリック内の Cisco APIC ソフトウェアをアップグレードする場合は、ファブリックで実行されている CIMC のバージョンもアップグレードする必要があります。したがって、各Cisco APICリリースでサポートされている CIMC ソフトウェアバージョンのリストについては、該当するCisco APICリリースノートを確認することをお勧めします。Cisco APIC リリース ノートは、 APIC のドキュメンテーション ページで入手できます。

CIMC ソフトウェアをアップグレードするには、まず、ファブリック内の Cisco APIC について、使用している UCS C シリーズ サーバのタイプを決定する必要があります。

Cisco APICは、次の UCS C シリーズ サーバを使用します。

- Cisco UCS 220 M5 (第 3 世代アプライアンス APIC-SERVER-M3 および APIC-SERVER-L3)
- Cisco UCS 220 M4 (第 2 世代アプライアンス APIC-SERVER-M2 および APIC-SERVER-L2)
- Cisco UCS 220 M3 (第 1 世代アプライアンス APIC-SERVER-M1 および APIC-SERVER-L1)

これら Cisco APIC のサーバのバージョンは、信頼されたプラットフォームモジュール (TPM) 証明書および APIC 製品 ID (PID) を使用してセキュリティ保護されたイメージを使用して製造されている Cisco APIC バージョンの標準バージョンとは異なります。

次の表に、これら Cisco APIC サーバごとの詳細について説明します。

APIC プラットフォーム	対応する UCS プラットフォーム	説明
APIC-SERVER-M1	UCS-C220-M3	中規模の CPU、ハード ドライブ、および最大 1000 個のエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第 1 世代コントローラで構成されるクラスタ。
APIC-SERVER-M2	UCS-C220-M4	中規模の CPU、ハード ドライブ、および最大 1000 個のエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスタ。
APIC-SERVER-M3	UCS-C220-M5	中規模の CPU、ハード ドライブ、および最大 1000 個のエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスタ。
APIC-SERVER-L1	UCS-C220-M3	大規模の CPU、ハード ドライブ、および 1000 個を超えるエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第 1 世代コントローラで構成されるクラスタ。
APIC-SERVER-L2	UCS-C220-M4	大規模の CPU、ハード ドライブ、および 1000 個を超えるエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスタ。
APIC-SERVER-L3	UCS-C220-M5	大規模の CPU、ハード ドライブ、および 1000 個を超えるエッジ ポート用のメモリ構成を備えた 3 台の Cisco APIC 第

APIC プラットフォーム	対応する UCS プラットフォーム	説明
		2 世代コントローラで構成されるクラスタ。

次の手順では、Cisco ホスト アップグレード ユーティリティ (HUU) を使用して Cisco APIC ＣＩＭＣをアップグレードする方法について説明します。HUUを使用してソフトウェアをアップグレードする方法の詳細については、Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU で説明されています。

始める前に

- Cisco APIC リリースノートに記載されている情報を確認し、アップグレードに使用する ＣＩＭＣ ソフトウェアイメージを確認します。Cisco APIC リリースノートは、APIC のドキュメンテーション ページで入手できます。
- ソフトウェア ダウンロードサイトからソフトウェア イメージを取得します。
- イメージの MD5 チェックサムが、Cisco.com で公開されているものと一致することを確認します。
- アップグレードに十分な時間を確保します。

  CIMC バージョンのアップグレード プロセスに必要な時間は、ローカル マシンと UCS-C シャーシ間のリンクの速度と、送信元/ターゲット ソフトウェア イメージ、およびその他の内部コンポーネント バージョンによって異なります。
- CIMC バージョンを変更する場合、vKVM を実行するためにインターネットブラウザと Java ソフトウェアのバージョンの変更が必要になることがあります。

（注） CIMC バージョンをアップグレードしても、Cisco APIC がトラフィックのデータ パスに含まれていないため、実稼働ネットワークには影響しません。また、CIMCソフトウェアをアップグレードするときに Cisco APIC を停止する必要はありません。

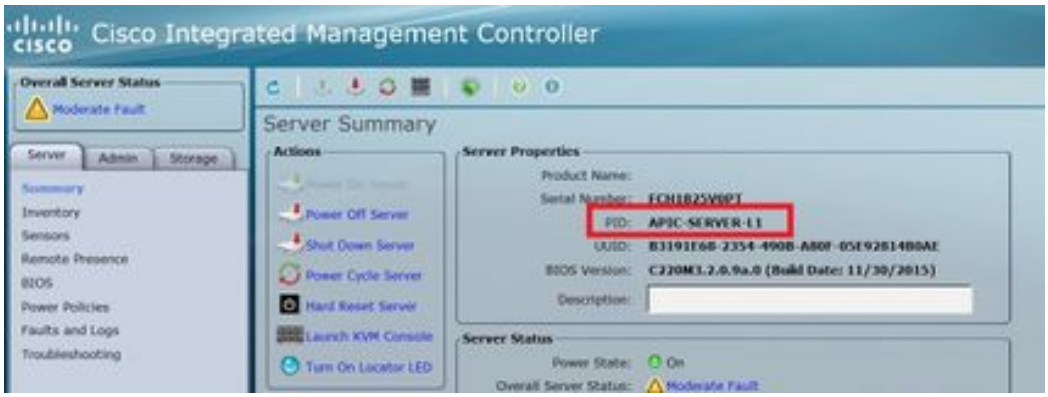
手順

ステップ 1 CIMC クレデンシャルを使用して CIMC にログインします。

CIMC クレデンシャルは、Cisco APIC クレデンシャルとは異なる場合があることに注意してください。

ステップ 2 CIMC GUI を使用して、 Cisco APIC の UCS プラットフォームのモデルを決定します。

a) **[サーバ (Server)]** > **[サマリ (Summary)]** の下に表示される PID エントリを見つけます。



b) この手順の最初に記載されている表を使用して、PID エントリに表示される APIC プラットフォームに対応する UCS プラットフォームを検索します。

たとえば、上記の例に示されている**APIC-SERVER-L1**エントリは、この手順の最初に示されている情報に基づいて、UCS-C220-M3 プラットフォームにマッピングされていることがわかります。

ステップ 3 https://software.cisco.com/download で適切な HUU.iso イメージを見つけます。

a) https://software.cisco.com/download の検索ウィンドウに、前の手順で見つけた Cisco APIC の UCS プラットフォームモデルを、ダッシュを使用せずに入力します。

前の手順の例では、検索ウィンドウに **UCS C220 M3** と入力します。

b) 検索結果のリンクをクリックすると、UCS プラットフォームで使用可能なソフトウェアが表示されます。

c) お使いのサーバで使用可能なソフトウェアのリストで、ファームウェアエントリを見つけます。これは、**Unified Computing System (UCS) Server Firmware** のように表示されています。ファームウェアのリンクをクリックします。

d) **CISCO UCS Host Upgrade Utility**.iso イメージのリンクを見つけて、このイメージのリリース情報をメモしておきます。

ステップ 4 推奨される CISCO APIC および Cisco Nexus 9000 シリーズ ACI モード スイッチ リリース (Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases) ドキュメント

に移動し、ご使用の UCS プラットフォームおよび APIC ソフトウェア リリースの適切なエントリが含まれている行を見つけます。

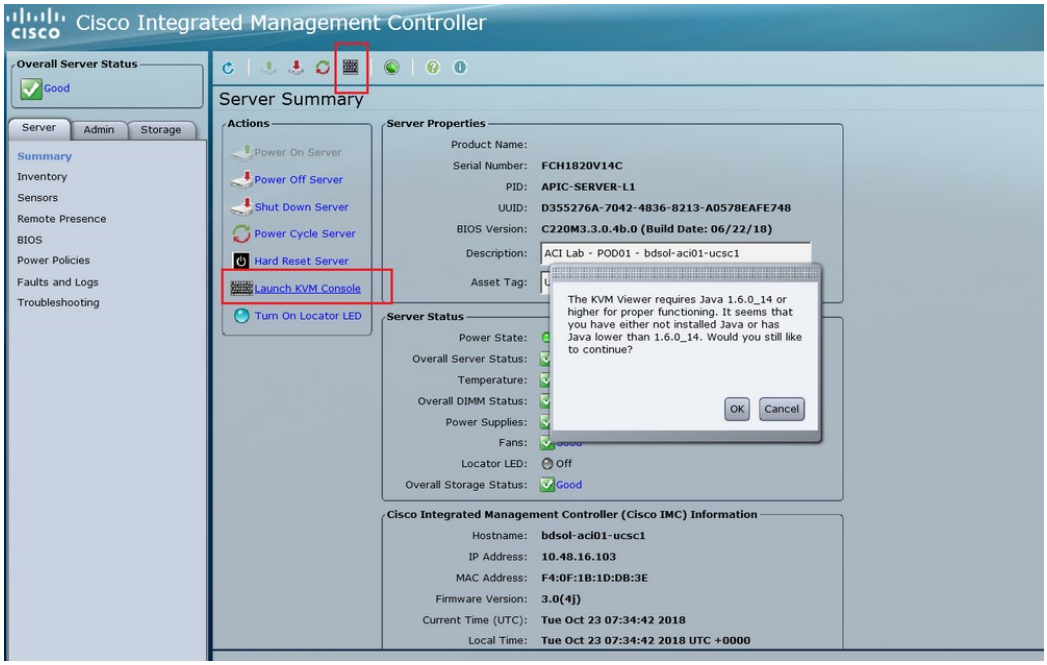
表に示されている UCS バージョンは、対応する APIC リリースに基づく、最新バージョンの CIMC ソフトウェアではない可能性があることに注意してください。たとえば、APIC リリースの 3.0 ブランチの場合、対応する CIMC ソフトウェアリリースは 3.0(3e) である可能性があります。これは必ずしも CIMC ソフトウェアの最新リリースではありませんが、APIC リリースの3.0 ブランチ CIMC ソフトウェアの正しいバージョンです。

ステップ 5 2 つのソースからの情報を比較して、正しいバージョンのイメージをダウンロードしていることを確認します。

2 つのソースの間で矛盾する情報が見つかった場合は、推奨される CISCO APIC および Cisco Nexus 9000 シリーズ ACI モード スイッチ リリース (Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases) のマニュアルに記載されている情報を、ご使用の UCS プラットフォームおよび APIC ソフトウェア リリースの正しいバージョンの HUU.iso イメージを示すものとして使用してください。

ステップ 6 https://software.cisco.com/downloadサイトから適切な、.iso イメージをダウンロードします。

ステップ 7 CIMC GUI から KVM コンソールを起動します。

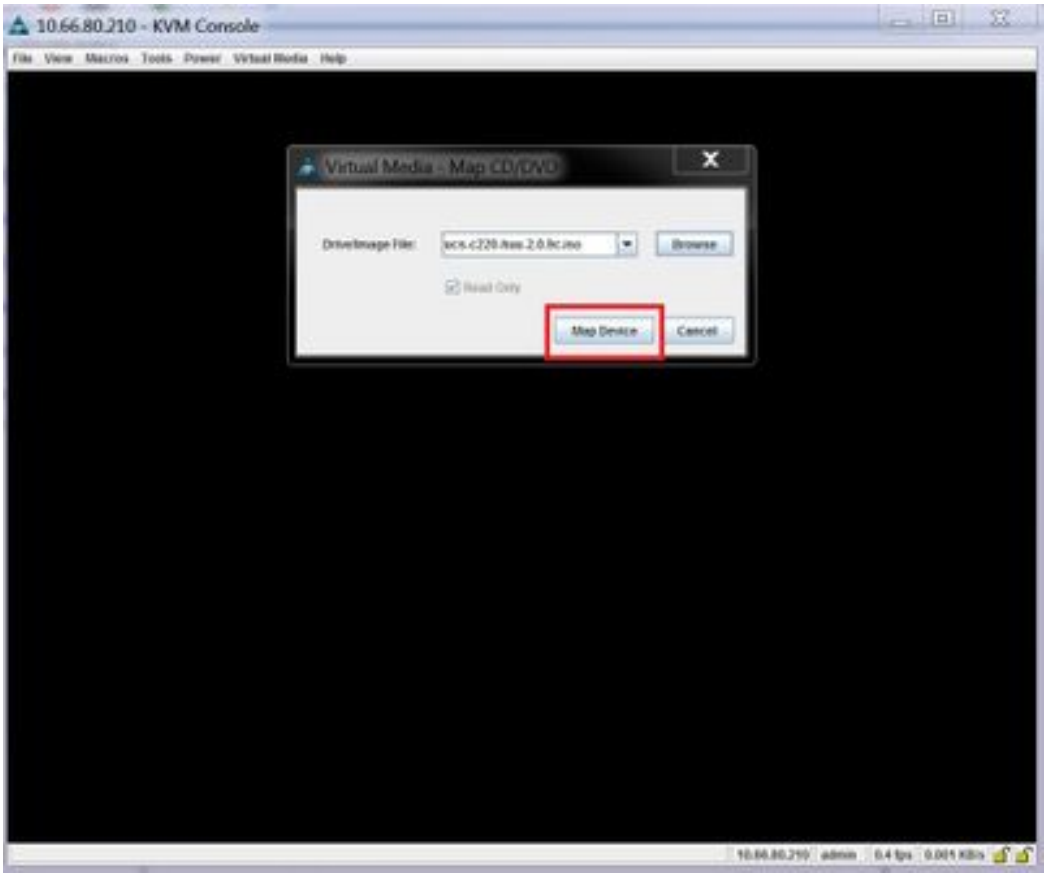


（注） KVM コンソールを開く際に問題が発生した場合は、通常、Java のバージョンで問題が発生しています。お使いのCIMCバージョンで使用可能なさまざまな回避策については、Cisco APIC リリース ノートを参照してください。これは APIC のドキュメンテーション ページで確認できます。

ステップ 8 KVM コンソールで、**[仮想メディア (Virtual Media)]** > **[仮想手バイスのアクティブ化 (Activate virtual Devices)]** をクリックし、セッションを受け入れます。

ステップ 9 **[仮想メディア (Virtual Media)]** > **[CD/DVD のマッピング (Map CD/DVD)]**をクリックし、PC でダウンロードしたイメージに移動します。

ステップ 10 ダウンロードした HUU.iso イメージを選択し、**[デバイスのマッピング (Map Device)]** をクリックして、ダウンロードした ISO を PC にマッピングします。



ステップ 11 **[マクロ (Macros)]** > **[静的マクロ (Static Macros)]** > **[Ctrl-Alt-Del]**をクリックして、サーバを再起動します。

このオプションを使用してサーバを再起動できない場合は、**[電源 (Power)]** > **[システムの電源サイクル (Power Cycle System)]** をクリックして、コールド リブートを実行します。

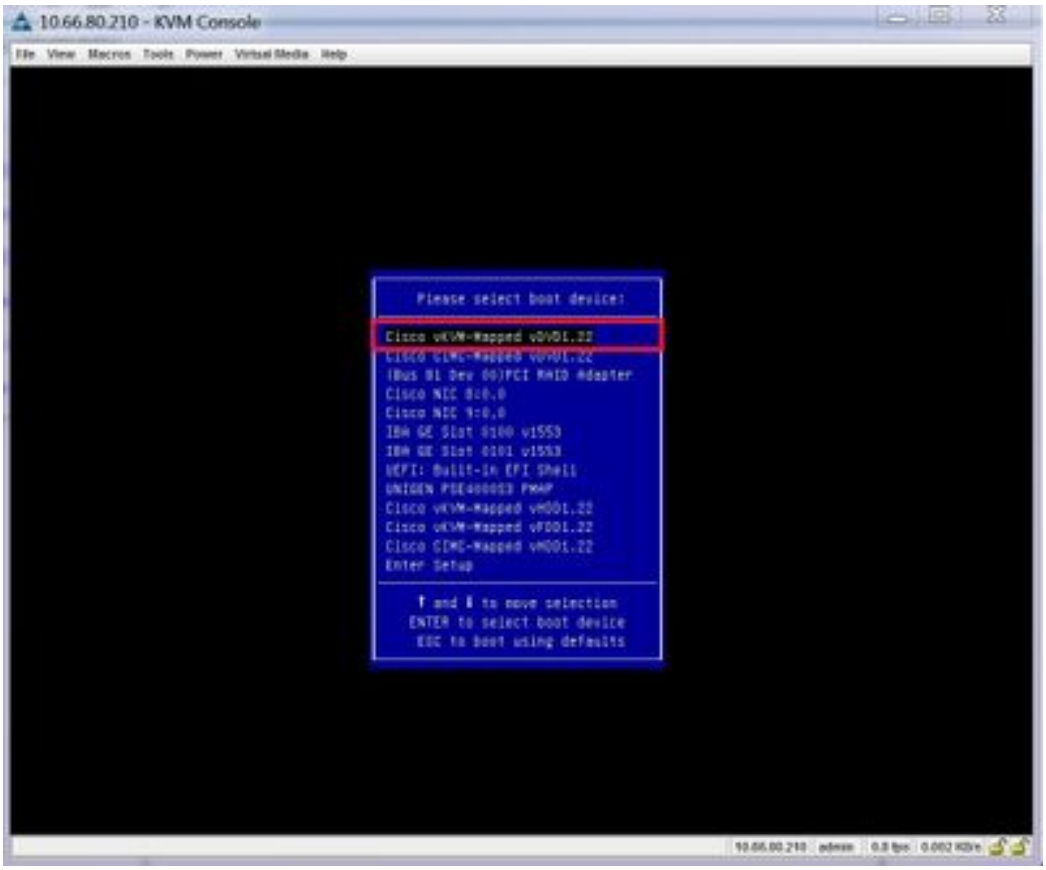
ステップ 12 **[F6]** を押してブート メニューを表示し、マップされた DVD を選択してブートできるようにします。

また、ユーザ定義マクロを作成して、リモートデスクトップアプリケーションを使用している場合は、**[マクロ (Macros)]** > **ユーザ定義マクロ (User Defined Macros)]** > **[F6]**を選択して、このアクションを実行することもできます。

ステップ 13 プロンプトが表示されたら、パスワードを入力します。

デフォルトのパスワードは `password` です。

ステップ 14 ブートデバイスを選択するように求められたら、次の図に示すように、 **[Cisco vKVM にマッピングされた vDVD (Cisco vKVM-Mapped vDVD)]** オプションを選択します。

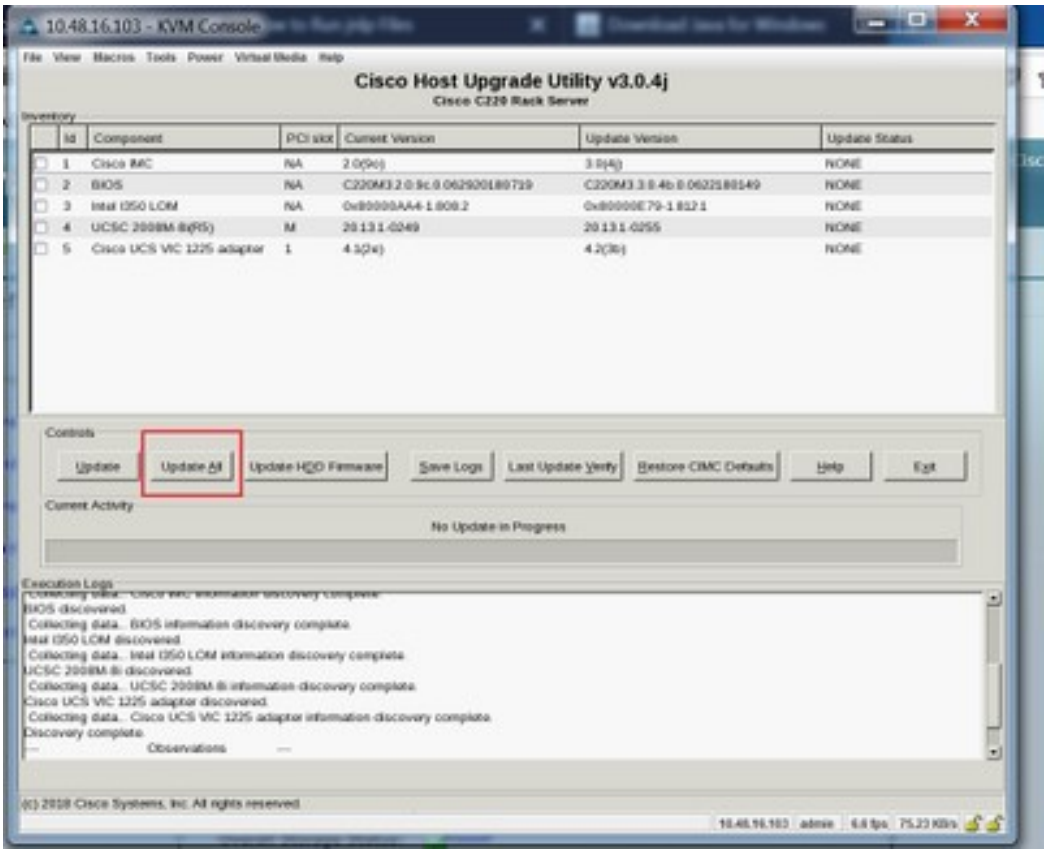


ステップ 15 プロセスが完了するのを待ち、プロンプトが表示されたら、利用規約に同意します。

HUU が ISO から抽出を行うには、10 ～ 15 分かかります。その後、ファームウェアやその他のツールがコピーするには、さらに 10 ～ 15 分かかります。

ステップ 16 ＨＵＵ 画面が表示されたら、適切な選択を行います。

すべてのコンポーネントのすべてのファームウェアを更新するには、**[すべて更新 (Update all)]** オプションを選択することをお勧めします。



ステップ 17 Cisco IMC セキュアブートを有効にするかどうかを確認するポップアップが表示された場合は、そのオプションに対して **[いいえ (No)]** を選択します。

Cisco UCS C-シリーズ サーバ統合管理コントローラ CLI 設定ガイド、リリース 4.0(Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 2.0(1) の「Cisco IMC セキュアブートの紹介 (Introduction to Cisco IMC Secure Boot)」のセクションを参照してください。

ステップ 18 HUU の **[更新ステータス (Update Status)]** 列に表示されている情報を使用して、更新の進行状況をモニタします。

ステップ 19 各コンポーネントのステータスが **[パス (PASS)]** になったら、**[終了 (Exit)]** をクリックして、サーバを再起動します。

サーバがリブートすると、CIMC GUI は終了します。CIMC に再度ログインし、アップグレードが正常に完了したことを確認する必要があります。

アップグレードが正常に完了したことを確認するには、GUI を使用するか、または CIMC HUU を起動し、**[最後の更新の確認 (Last Update Verify)]** を選択して、すべてのコンポーネントがアップグレードをパスしたことを確かめます。

CIMC 仮想メディアを使用した Cisco APIC ソフトウェアのインストール

Cisco Integrated Management Controller (CIMC) 仮想メディアを使用して Cisco APIC ソフトウェアをインストールするには、この手順に従ってください。

（注） 次の手順では、2 つのコンソール ウィンドウを開きます。

- KVM コンソール
- Serial over LAN（/sol）

この手順のほとんどの手順で、1つまたは他のコンソールウィンドウに特定のコマンドを入力して、2 つのコンソール ウィンドウの間を逆方向に反転させることができます。

始める前に

CIMC ソフトウェアのアップグレード （16 ページ） の情報を確認して、このセクションの手順を開始する前に、Cisco Integrated Management Controller (CIMC) ソフトウェアをアップグレードする必要があるかどうかを判断してください。

手順

ステップ 1 CCO から、関連する Cisco APIC .iso イメージを入手します。

ステップ 2 .iso イメージを HTTP サーバにコピーします。

ステップ 3 **KVM コンソール**にアクセスします。

a) コントローラの Cisco Integrated Management Controller (CIMC) GUI を開きます。

b) CIMC GUI から、**[サーバー (Server)]** > **[サマリ (Summary)]** > **[KVM の起動 (Launch KVM)]** を選択し、**[JAVA ベース KVM (JAVA based KVM)]** または **[HTML ベース KVM (HTML based KVM)]** のいずれかを選択して KVM コンソールにアクセスします。

大規模なファイルにはより信頼性の高いオプションであるため、可能な限り **Java ベースの KVM**オプションを使用することを推奨します。

ステップ 4 **Serial on LAN (SOL) コンソール**にアクセスします。

a) ターミナル ウィンドウから、CIMC コンソールにログインします。

```
# ssh admin@cimc_ip
```

ここで、 *cimc_ip*は CIMC IP アドレスです。次に例を示します。

```
# ssh admin@192.0.2.1
admin@192.0.2.1's password:
system#
```

b) 範囲を仮想メディアに変更します。

```
system# scope vmedia
system /vmedia #
```

c) .iso イメージを HTTP サーバにマップします。

```
system /vmedia # map-www volume_name http://http_server_ip_and_path iso_file_name
```

それぞれの説明は次のとおりです。

- *volume_name* は、ボリュームの名前です。
- *http_server_ip_and_path*は、HTTP サーバの IP アドレスと .iso ファイルの場所へのパスです。
- *iso_filename* は、.iso ファイルの名前です。

*http_server_ip_and_path*と*iso_filename*の間にスペースがあることに注意してください。

次に例を示します。

```
system /vmedia # map-www apic http://198.51.100.1/home/images/ aci-apic-dk9.4.0.3d.iso
Server username:
```

d) マッピングのステータスを確認します。

```
system /vmedia # show mappings detail
```

マップ ステータスは **[OK]** と表示されます。

e) SOL（Serial over LAN）に接続し、インストール プロセスを監視します。

```
system /vmedia # connect host
```

ステップ 5 **KVM コンソールで、[電源] > [パワー サイクル システム (コールド起動)]**[システムのリセット (Reset System)] を選択してコントローラの電源を再投入します。

ステップ 6 **SOL コンソールから**: ブートプロセス中に画面を観察し、適切な時点で**F6**を押してブート選択メニューを開始するように準備します。

起動プロセスが開始されると、最初に次のメッセージが表示されます。

```
Cisco Systems, Inc.
Configuring and testing memory..
Configuring platform hardware...
...
```

システム起動メッセージは、次の画面が表示されるまで表示され続けます。

```
...
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC COnfiguration, <F12>
 Network Boot
```

ステップ 7 **SOL コンソールから**: 上記のメッセージが表示されたら、**F6** キーを押して [起動選択 (boot selection)] メニューを表示します。

適切な時点でF6を押すことができる場合は、「**起動選択メニューの入力..**」と表示されます。お客様の機会がなく、適切な時点で **F6** を押すことができなかった場合は、ステップ 5 （25 ページ） に戻ってコントローラの電源を再投入し、**F6** キーを押してブート選択メニューを表示できるようになるまで、このプロセスを繰り返します。

ステップ 8 **SOL コンソールから**: 起動選択メニューで、ワンタイム起動デバイスとして**Cisco CIMC-Mapped vDVD 1.22** オプションを選択します。

```
/-----------------------------------\
| Please select boot device:        |
|-----------------------------------|
| (Bus 05 Dev 00)PCI RAID Adapter   |
| UNIGEN PHF16H0CM1-DTE PMAP        |
| Cisco vKVM-Mapped vHDD1.22        |
| Cisco CIMC-Mapped vHDD1.22        |
| Cisco vKVM-Mapped vDVD1.22        |
| Cisco CIMC-Mapped vDVD1.22        |
| Cisco vKVM-Mapped vFDD1.22        |
| UEFI: Built-in EFI Shell          |
| IBA GE Slot 0100 v1585            |
| IBA GE Slot 0101 v1585            |
| Enter Setup                       |
|-----------------------------------|
|    ^ and v to move selection      |
|    ENTER to select boot device    |
|     ESC to boot using defaults    |
\-----------------------------------/
```

また、BIOS パスワードを入力する必要があります。デフォルト パスワードは **password** です。

ステップ 9 **SOL コンソールから**: 次のように入力します。

a) インストール プロセスを高速化するために ISO URL を入力するかどうかを決定します。

起動プロセス中は次のメッセージが表示される場合があります。

```
To speed up the install, enter iso url in next ten minutes:
```

ここでは 2 つのオプションを選択できます。

- **ISO URL の入力**：このオプションを選択することをお勧めします。これによりインストール プロセスが高速化されます。次に、ここに入力する HTTP URL の例を示します。

  ```
  http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
  ```

  次の例に示すように、このオプションを選択するとプロトコルの種類を指定するように求められます。

  ```
  ? http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
  ++ awk -F '/|:' '{print $4}'
  + urlip=10.75.61.1
  + '[' -z http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
  + '[' -z 10.75.61.1 ']'
  + break
  + '[' -n http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
  + set +e
  + configured=0
  + '[' 0 -eq 0 ']'
  ```

```
+ echo 'Configuring network interface'
Configuring network interface
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to
re-enter the url: '
```

適切な SSH プロトコル タイプを選択します。

- [static]：このオプションを選択した場合は、インターフェイス名、管理 IP アドレス、およびゲートウェイを入力するよう求められます。次に、正しい管理インターフェイスを見つける方法の例を示します。

```
? static
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
Available interfaces
+ ls -l /sys/class/net
total 0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp11s0 ->
../../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:00.0/0000:0b:00.0/net/enp11s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp12s0 ->
../../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:01.0/0000:0c:00.0/net/enp12s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f0 ->
../../devices/pci0000:00/0000:00:01.0/0000:01:00.0/net/enp1s0f0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f1 ->
../../devices/pci0000:00/0000:00:01.0/0000:01:00.1/net/enp1s0f1
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 lo -> ../../devices/virtual/net/lo
+ read -p 'Interface to configure: ' interface
Interface to configure:
[anaconda] 1:main* 2:shell  3:log  4:storage-lo> Switch tab: Alt+Tab | Help:
 F1
```

上記の出力では、pci 番号が短いネットワーク インターフェイスが 2 つのアウトオブバンド管理インターフェイス（`enp1s0f0` (eth1-1) および `enp1s0f1`）に対応しています。両方のインターフェイスが正しく接続されている場合は、どちらかを選択できます。ただし、1 つのインターフェイスにのみケーブルが接続されている場合は、ケーブル接続されたポートに対応するインターフェイスを選択する必要があります。

- **[dhcp]**

また、この ISO URL の*http_server_ip_and_path*と*iso_filename*の間にスペースがないことにも注意してください (たとえば、`http://198.51.100.1/home/images/aci-apic-dk9.4.0.3d.iso`)。

- [Do not enter the ISO URL]：ISO の URL を入力しない場合は、10 分後にインストールプロセスが開始されます。

この時点で ISO の取得が開始されます。

```
+ read -p 'Interface to configure: ' interface
Interface to configure: enp1s0f0
+ read -p 'address: ' addr
address: 10.75.39.72/24
+ read -p 'gateway: ' gw
gateway: 10.75.39.254
```

```
+ ip addr add 10.75.39.72/24 dev enp1s0f0
+ ip link set enp1s0f0 up
+ ip route add default via 10.75.39.254
++ seq 1 2
+ for count in '$(seq 1 2)'
+ ping -c 1 10.75.61.1
PING 10.75.61.1 (10.75.61.1) 56(84) bytes of data.
64 bytes from 10.75.61.1: icmp_seq=1 ttl=125 time=0.875 ms

--- 10.75.61.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.875/0.875/0.875/0.000 ms
+ configured=1
+ break
+ '[' 1 -eq 0 ']'
+ echo 'Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso'
Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
+ wget -o /dev/null -O /tmp/cdrom.iso http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
```

KVM コンソールで **[ツール (Tools)]** > **[統計情報 (Stats)]** に移行することによって、プロセスのステータスを追跡できます。

b) SOL コンソールにメッセージ **poweroff**が表示されるまで待機してから、 **Ctrl** + **x** (**Ctrl** + **x**) を押して SOL を終了します。

c) 範囲を仮想メディアに変更します。

```
system# scope vmedia
system /vmedia #
```

d) 4.c （25 ページ） にマッピングした .iso イメージのマッピングを解除します。

```
system /vmedia # unmap volume_name
```

マッピングを保存する場合は、 [マッピングの保存 (save mapping)] プロンプトで yes と入力します。マッピングを保存しない場合は no を選択します。次に例を示します。

```
system /vmedia # unmap apic
Save mapping? Enther 'yes' or 'no' to confirm (CTRL-C to cancel) → yes
system /vmedia #
```

e) 再度 SOL に接続します。

```
system /vmedia #  connect host
```

ステップ 10 **KVM コンソール**で、**[電源]** > **[システムの電源をオンにする]** を選択してコントローラの電源を投入します。

ステップ 11 **SOL コンソールから**: 次のように入力します。

a) 起動プロセス中に **F6** を押して起動選択メニューを入力し、ワンタイム起動デバイスとして **[PCI RAID アダプター]** を選択します。

また、BIOS パスワードを入力する必要があります。デフォルト パスワードは **password** です。

b) ファブリック名、コントローラ数、トンネル エンドポイント アドレス プール、インフラ VLAN ID などの初期セットアップのオプションを入力し、インストール プロセスを完了します。

ACI ファブリックのクリーン初期化の実行

最初にファブリックを起動する際にファブリックのクリーン再起動を実行し、ファブリックが正常に動作しない場合、クリーン再起動がファブリックを再度起動する唯一のオプションとなります。これにより、Cisco APIC およびスイッチ ノードからすべての設定が削除されます。その後、最初から設定を開始するか、設定バックアップから再インポートする必要があります。

手順

ステップ 1 アウトオブバンド管理で各 Cisco APIC にログインし Cisco APIC DME アプリケーションを停止します。

例：

```
acidiag stop mgmt
```

ステップ 2 アウトオブバンド管理を使用して各スイッチにログインします。アウトオブバンド管理が使用できない場合は、コンソールを使用してログインします。次のコマンドセットのいずれかを使用して、スイッチをクリーン再起動します。

例：

```
leaf101# setup-clean-config.sh
In progress
In progress
Done
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

または

```
leaf101# acidiag touch clean
This command will wipe out this device, Proceed? [y/N] y
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

ステップ 3 次の通りに各 Cisco APIC にログインし、Cisco APIC を再起動します。

例：

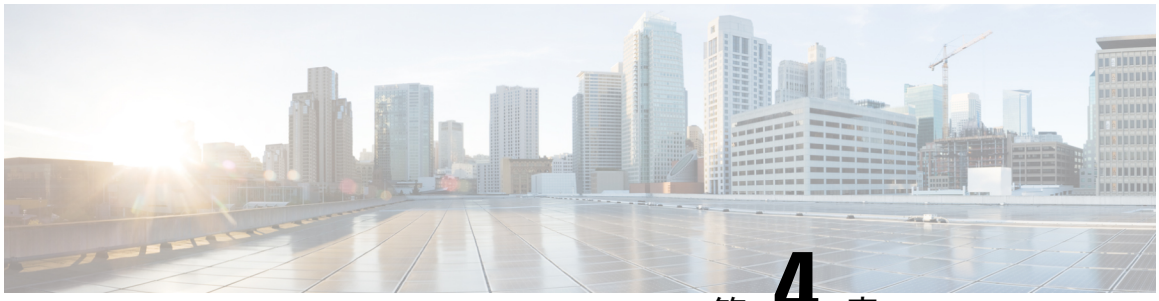
```
acidiag touch clean
acidiag reboot
```

また、初期設定パラメータを再設定する場合は、以下に示すように `acidiag touch setup` コマンドも含める必要があります。

```
acidiag touch clean
acidiag touch setup
acidiag reboot
```

（注） このエラーを無視する：「`acidiag: error: curl: (52) Empty reply from server`」

ファブリックがクリーン再起動されると、ノードは検出されません。ノードポリシーをポストする、UIを使用してスイッチを登録する、または設定のバックアップをインポートできます。



第 4 章

ACI ファームウェア アップグレードの概要

ファームウェア管理について

Cisco ACI にはいくつかの種類のファームウェアがあります。次に、このドキュメントで説明するファームウェアの概要を示します。この章では、主に上位 2 種類の Cisco ACI ファームウェア（Cisco APIC ファームウェアとスイッチ ファームウェア）に焦点を当てます。

ファームウェアのタイプ	説明	例
Cisco APIC ファームウェア	APIC アプライアンスで実行されている APIC のオペレーション システム。	APIC リリース 5.2(1g)： ***aci-apic-dk9.5.2.1g***
スイッチのファームウェア	Nexus 9000 シリーズで稼働する ACI スイッチのオペレーティング システム。	ACI スイッチ リリース 15.2(1g)： ***aci-n9000-dk9.15.2.1g.bin***
ソフトウェア メンテナンス アップグレード（SMU）パッチ	APIC または ACI スイッチの特定の障害のパッチ イメージ。 詳細については、ソフトウェア メンテナンス アップグレード パッチ （181 ページ）を参照してください。	5.2(1g) リリースを使用している APIC の CSCaa12345 パッチ： ***aci-apic-patch-CSCaa12345-5.2.1g-S.1.0.x86_64.tgz*** 15.2(1g) リリースを使用している ACI スイッチの CSCaa12345 パッチ： ***aci-n9000-patch-CSCaa12345-15.2.1g-S.1.1.1.rpm***

ファームウェアのタイプ	説明	例
サイレント ロール（SR）パッケージ	ACI スイッチの特定のハードウェア コンポーネント用のファームウェアのパッケージ。 詳細については、サイレント ロール パッケージのアップグレード（175ページ）を参照してください。	***aci-srpkg-dk9.1.0.0.bin***

Cisco ACI ファブリックをアップグレードするワークフロー

Cisco APIC は、ファブリック全体のアップグレードを一元的に管理します。Cisco APIC は、イメージのリポジトリとして（例：ファームウェア リポジトリ）、およびブート サーバとして機能します。リーフ スイッチとスパイン スイッチにはACI インフラ ネットワークを使用した Cisco APIC への接続性があり、アップグレードするときスイッチは Cisco APIC からファームウェアをダウンロードします。このセクションでは、アップグレードを正常に完了するための推奨手順を説明します。

1. ターゲットAPICおよびACIスイッチのバージョンを選択します。
    1. APICとACIスイッチの両方を同じバージョンにアップグレードする必要があります。
    2. 相互に互換性のあるAPICおよびACIスイッチのバージョンは、xy（z）および1x.y（z）の形式で記述されます。たとえば、APICバージョン5.2（1g）はACIスイッチバージョン15.2（1g）に対応します。
    3. リリースノート（APICおよびACIスイッチ）で、未解決の問題や欠陥がないか、ターゲットバージョンを確認します。 https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#Release_Notes https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html
2. 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ックスを参照してください。
    1. 現在のバージョンとターゲット バージョンが離れすぎている場合は、『*APIC* アップグレード/ダウングレード サポート マトリクス』で推奨されている中間バージョンに APIC とスイッチの両方をアップグレードする必要があります。詳細については、「マルチ アップグレード （40 ページ）」を参照してください。
    2. *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には、ターゲット APIC バージョンに使用する必要がある UCS HUU バージョンも示されます。
3. ACI アップグレード アーキテクチャを確認します。

実行すべきでないことと期待すべきことを理解するには、ACI アップグレード アーキテクチャ （53 ページ） を参照してください。

4. バックアップ用に設定をエクスポートします。

   詳細については、 『Cisco ACI Configuration Files：Import and Export』を参照してください。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b_KB_Using_Import_Export_to_Recover_Config_States.htmlAES暗号化が有効になっていることを確認します。

5. 事前にAPICイメージにパッケージされているものを除き、APIC 上のすべての App Center アプリを無効化します。

   詳細については、App Center アプリの注意事項 （41 ページ）を参照してください。

6. APIC と ACI スイッチ ファームウェアの両方を APIC にダウンロードします。

   詳細については、各リリースの『*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。

   - 4.x より前のリリース：APIC で APIC とスイッチイメージをダウンロードする （107 ページ）
   - リリース 4.x または 5.0： APIC で APIC とスイッチ イメージをダウンロードする （115 ページ）
   - リリース 5.1 以降： APIC で APIC とスイッチ イメージをダウンロードする （128 ページ）

7. APICから各スイッチにACIスイッチファームウェアをダウンロードします。

   スイッチリリース14.1（1）以降、スイッチはアップグレード前にAPICからイメージをダウンロードできます。詳細については、ルール 5：スイッチイメージを事前にダウンロードして時間を節約します （37 ページ）を参照してください。

8. ップグレード前の検証の実行

   詳細については、アップグレード前のチェックリスト （71 ページ）を参照してください。

9. サポートマトリックスで推奨されている場合は、APIC の HUU（CIMC、BIOS、ネットワークアダプタ、RAID コントローラ、ディスク）を介してすべてのサーバーコンポーネントをアップグレードします。

   詳細については、CIMC ソフトウェアのアップグレード （16 ページ）を参照してください。

10. APIC をアップグレードします。

    詳細については、各リリースの『*Cisco APIC* のアップグレード』の項を参照してください。

    - 4.x より前のリリース：リリース 4.x より前のリリースからの Cisco APIC のアップグレード （108 ページ）

- リリース 4.x または 5.0： リリース 4.x または 5.0 からの Cisco APIC のアップグレード （118 ページ）
- リリース 5.1 以降： リリース 5.1x 以降からの Cisco APIC のアップグレード （130 ページ）

11. ACIスイッチをアップグレードします。
    1. すべてのAPICが完全に適合するまで待ちます。
    2. 詳細については、各リリースの『リーフおよびスパイン スイッチのアップグレード』の項を参照してください。
       - 4.x より前のリリース：リリース 4.x より前の APIC を使用したリーフおよびスパイン スイッチのアップグレード （111 ページ）
       - リリース 4.x または 5.0： リリース 4.x または 5.0 を実行している APIC によるリーフおよびスパイン スイッチのアップグレード （121 ページ）
       - リリース 5.1 以降： リリース 5.1x 以降を実行している APIC によるリーフおよびスパイン スイッチのアップグレード （132 ページ）
12. これがマルチステップアップグレードの場合は、上記の手順を繰り返して、APICとスイッチの両方の即時バージョンへのアップグレードが完了し、APICクラスタステータスが完全に適合した後に、中間バージョンからターゲットバージョンにアップグレードします。

（注） Cisco ACI ファブリックの導入環境に Cisco AVS/AVS が含まれている場合は、Cisco AVS/AVS を Cisco APIC との互換性があるバージョンにアップグレードしてください。Cisco AVS / AVEをアップグレードするには、『Cisco ACI Virtual Edge Installation Guide』の「Recommended Upgrade Sequence for Cisco APIC、the Fabric Switches、and Cisco ACI Virtual Edge」を参照してください。https://www.cisco.com/c/en/us/td/docs/dcn/aci/aci-virtual-edge/3x/installation/cisco-aci-virtual-edge-installation-guide-32x/m_ave_upgrade.html

ACI スイッチ アップグレードの注意事項

ACI スイッチのアップグレードのガイドラインは次のとおりです。

- 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 （35 ページ）
- 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 （35 ページ）
- 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 （36 ページ）
- ルール 4：スイッチ更新グループの同時キャパシティを理解する （36 ページ）

- ルール 5：スイッチ イメージを事前にダウンロードして時間を節約します （37 ページ）
- ACI スイッチのグレースフル アップグレード （38 ページ）
- ACI スイッチのグレースフル アップグレード （38 ページ）

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

次に例を示します。

- グループ ODD：リーフ 101、リーフ 103、スパイン 1001
- Group EVEN：リーフ 102、リーフ 104、スパイン 1002

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

- 各ポッドでは、少なくとも 1 つの MP-BGP ルート リフレクタ（RR）スパイン スイッチを常に稼働させてください。
- IPN 接続のスパイン スイッチを少なくとも 1 つ、各ポッドで常に稼働させてください。
- 特定のポッドにスパイン スイッチが 1 つしかない場合（マルチポッドの場合）、スパイン スイッチのグレースフル アップグレードを実行しないでください。

  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 （38 ページ）を参照してください。

次に例を示します。

グループの更新	ポッド 1	ポッド 2
ODD	リーフ 101、リーフ 103、リーフ 105 **スパイン 1001（RR、IPN）** **スパイン 1003**	リーフ 201、リーフ 203、リーフ 205 **スパイン 2001（RR、IPN）** **スパイン 2003**
EVEN	リーフ 102、リーフ 104、リーフ 106 **スパイン 1002（RR、IPN）** **スパイン 1004**	リーフ 202、リーフ 204、リーフ 206 **スパイン 2002（RR、IPN）** **スパイン 2004**

ここで、

- **RR** は、ルート リフレクタ スパイン スイッチを意味します。
- **IPN** は、IPN に接続されたスパイン スイッチを意味します。

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

- 常に同じ vPC ペアのリーフ スイッチの 1 つを稼働状態に維持します
- 各 Cisco Application Policy Infrastructure Controller (APIC) に接続されているリーフスイッチの 1 つを常に稼働させます。

次に例を示します。

グループの更新	ポッド 1	ポッド 2
ODD	**リーフ 101（vPC 11、APIC1）** **リーフ 103（vPC 12、APIC2）** **リーフ 105（vPC 13）** スパイン 1001	**リーフ 201（vPC 21、APIC3）** **リーフ 203（vPC 22）** **リーフ 205（vPC 23）** スパイン 2001
EVEN	**リーフ 102（vPC 11、APIC1）** **リーフ 104（vPC 12、APIC2）** **リーフ 106（vPC 13）** スパイン 1002	**リーフ 202（vPC 21、APIC3）** **リーフ 204（vPC 22）** **リーフ 206（vPC 23）** スパイン 2002

ここで、

- **vPC xx** は、1 つの vPC ペアを意味します。
- **APICx** とは、Cisco APIC に接続されたリーフスイッチのことです。

ルール 4：スイッチ更新グループの同時キャパシティを理解する

全般

- 各アップグレード/メンテナンス グループに含められるのは、最大 80 スイッチ ノードです。
- 同時キャパシティ（同時にアップグレードされるスイッチ）は、同じ更新/メンテナンス グループ内で同時にアップグレードする必要があるスイッチの数を決定します。ただし、同時キャパシティ設定では、同じグループのどのスイッチを同時にアップグレードするかを管理できないため、同時キャパシティ設定に依存するのではなく、異なるスケジュールでスイッチをアップグレードするために個別の更新グループを作成することを推奨します。
- 同じ vPC ペアの両方のリーフ ノードが同じスイッチ アップグレード グループにある場合、同時キャパシティに関係なく、一度に 1 つのリーフ ノードのみがアップグレードされます。
- Cisco APIC リリース 4.1(1) 以降、グレースフルアップグレードが適用され、同じポッドに他の動作可能なスパインスイッチがない場合、同時キャパシティ設定に関係なく、アップグレードは拒否されます。

- Cisco APIC リリース 4.0(1) 以降からリリース 3.2(x) 以前のものにダウングレードする場合、リリース間でサポートされる QoS クラスの違いにより、ファブリックで小規模のトラフィックドロップが発生する可能性があります。詳細については、CSCwa32037 を参照してください。

Cisco APIC リリース 4.2(5) よりも前のリリース：

- 同じ更新グループ内でも、スイッチは一度に 1 つのポッドのみアップグレードされます。
- グループあたりのデフォルトの同時キャパシティは 20 です。

同じグループに 20 を超えるスイッチがある場合は、アップグレード スケジューラを使用して容量を無制限に変更できます。

詳細については、『リーフおよびスパイン スイッチ ソフトウェア バージョンのアップグレード』を参照してください。

- 4.x より前のリリース：リリース 4.x より前の APIC を使用したリーフおよびスパイン スイッチのアップグレード （111 ページ）
- リリース 4.x または 5.0： リリース 4.x または 5.0 を実行している APIC によるリーフおよびスパイン スイッチのアップグレード （121 ページ）

Cisco APIC リリース 4.2(5) 以降：

- 同じ更新グループ内のスイッチは、ポッドに関係なく同時にアップグレードされます。
- グループあたりのデフォルトの同時キャパシティは無制限です。

Cisco APIC リリース 4.2(5) からの上記の拡張機能は、Cisco APIC が 4.2(5) 以降にアップグレードされるとすぐに有効になります。たとえば、Cisco APIC が 4.2(5) にアップグレードされ、スイッチがまだリリース 13.2(10) である場合、スイッチが 13.2(10) から 14.2(5) にアップグレードされると、上記の拡張機能が有効になります。

この機能拡張により、スイッチのアップグレードにかかる時間を短縮できます。

ルール 5：スイッチ イメージを事前にダウンロードして時間を節約します

Cisco APIC とスイッチイメージを Cisco APIC のファームウェアリポジトリにダウンロードした後でも、スイッチは Cisco APIC からイメージをダウンロードする必要があります。以降のリリースでは、この操作は実際のアップグレード手順とは別に実行できます。これは事前ダウンロードと呼ばれ、Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）のステップ 7 に相当します。

スイッチ リリース 14.1(1) より前：

未サポートアップグレードがトリガーされると、スイッチは Cisco APIC からイメージをダウンロードします。

スイッチ リリース 14.(1) ～ 15.0(x)：

- 事前ダウンロードは、アップグレード スケジューラを使用して実行できます。

- 推奨されるアップグレード手順の順守：

  1. 遠い将来（10年先など）に設定されたスケジューラで更新グループを作成します。これにより、スイッチは Cisco APIC からイメージをすぐにダウンロードします。
  2. メンテナンス ウィンドウでアップグレードを開始する時間になったら、同じグループを編集し、**[アップグレード開始時間（Upgrade Start Time）]** を **[今すぐ（Now）]** に変更します。

- スイッチの現在のバージョンが 14.2(5) 以降の場合、Cisco APIC GUI に事前ダウンロードの進行状況が表示されます。

スイッチ リリース 15.1(1) 以降：

- 事前ダウンロードは、スケジューラを使用せずに GUI ワークフローでネイティブに構築されます。

  1. 更新グループを作成し、[**ダウンロードの開始（Begin Download）**] をクリックすると、スイッチは Cisco APIC からイメージをダウンロードします。
  2. 事前ダウンロードが完了すると、各スイッチに **[インストール準備完了（Ready to Install）]** と表示されます。
  3. 同じグループに対して **[インストールの開始（Begin Install）]** を実行して、アップグレードをトリガーします。

スイッチ リリース 14.1(1) からの上記の拡張（事前ダウンロード）は、Cisco APIC とスイッチの両方が対応するバージョンにアップグレードされた後にのみ有効になります。たとえば、Cisco APIC が 4.2(7) にアップグレードされ、スイッチが 13.2(10) にある場合、スイッチを 13.2(10) から 14.2(7) にアップグレードするための事前ダウンロードは使用できません。一方、Cisco APIC が 5.2(1) にアップグレードされ、スイッチが 14.2(7) のままの場合、[**ダウンロードの開始（Begin Download**）] を使用して、 14.2(7) から 15.2(1) へのスイッチのアップグレードのため、新しい Cisco APIC GUI を介して事前ダウンロードが実行します。

ACI スイッチのグレースフル アップグレード

アップグレード手順を実行するときにユーザ トラフィックからスイッチを分離する場合は、次の状況でサポートされているものとサポートされていないものをよりよく理解するために、使用可能なさまざまな用語と方法を理解しておくと役立ちます。

- **グレースフル挿入と削除（GIR）**：ユーザー トラフィックからスイッチを分離するために使用される操作。
- **メンテナンス モード**：デバッグ目的でユーザー トラフィックからスイッチを分離するために使用されます。Cisco APIC **[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）]にある** > **GUI の[ファブリックメンバーシップ（Fabric Membership）]** ページの **[メンテナンス（GIR）（Maintenance（GIR））]** フィールドを有効にすることで、スイッチを**メンテナンスモード**にできます

（スイッチを右クリックして **[メンテナンス（GIR）Maintenance（GIR）]** を選択します）。

スイッチを**メンテナンスモード**にすると、そのスイッチは動作可能な ACI ファブリック インフラストラクチャの一部とは見なされず、通常の Cisco APIC 通信は受け入れられません。したがって、この状態にあるスイッチのファームウェアアップグレードを実行しようとすると、障害が発生したり、不完全なステータスで無限にスタックしたりする可能性があるため、この状態のスイッチに対するファームウェアアップグレードの実行はサポートされていません。

- **グレースフルアップグレード**：アップグレード手順中にユーザトラフィックから隔離されたスイッチをリロードするために使用されます。スイッチは、ファームウェア アップグレードプロセス中の特定の時点で自動的にリブートするようにプログラムされています。この操作は、リブートの前に自動的に GIR を実行します。Cisco APIC GUI の **[管理（Admin）]>[ファームウェア（Firmware）]** で、更新グループ内のスイッチの **[グレースフルメンテナンス（Graceful Maintenance）]** オプション（リリース 5.1 より前のリリース）または **[グレースフルアップグレード（Graceful Upgrade）]** オプション（リリース 5.1 以降）を確認できます。

  スイッチがユーザ トラフィックから分離された後、ユーザ トラフィックが冗長パスを通過するようにリロードされる前に手順を停止する場合、このような操作は現在 ACI ではサポートされていません。

ACI 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

ACI スイッチ アップグレードの注意事項 （34 ページ） のすべての注意事項は、**グレースフルアップグレード**にも適用されます。ただし、このセクションでは、**グレースフルアップグレード**に特に重要ないくつかの注意事項について詳しく説明します。

- 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 （35 ページ） で提案されているように、特にマルチポッド設定で**グレースフルアップグレード**を実行している場合は、ポッドのすべてのスパイン スイッチを一度にアップグレードしないでください。

  そうしないと、アップグレードが失敗し、スパインスイッチがファブリックから無期限に隔離されたままになります。これは**グレースフルアップグレード**プロセスの一部のため、IPN 接続性は正常にアップグレードされる各スパイン スイッチで明示的にダウンされるため、ファブリックから分離できます。この方法でアップグレードすると、スパインスイッチ自体を含むポッド全体が、他のポッド内の Cisco APIC およびスイッチとの通信を失い、自己回復の手段がなくなります。

  このため、**グレースフルアップグレード**を実行している場合、スイッチが個別にアップグレードされるように、同じポッドのスパイン スイッチから異なるメンテナンス/更新グループに配置する必要があります。ポッドにスパイン スイッチが 1 つしかない場合は、アップグレードの前に **[グレースフル アップグレード（Graceful Upgrade）]**（または **[グレースフル メンテナンス（Graceful Maintenance）]**）オプションを無効にする必要があります。この手順に従わない場合は、CSCvn28063 に示されている回避策を参照してください。

  この問題を回避するために、Cisco APIC 4.1(1) リリースでは、**グレースアップグレード**が適用された際に、ポッドの最後のスパインスイッチのアップグレードを拒否する安全なメ

カニズムが導入されました。このブロックメカニズムについても、ルール 4：スイッチ更新グループの同時キャパシティを理解する （36 ページ） で説明します。

- 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 （36 ページ） で提案されているように、同じ Cisco APIC に接続された 2 つ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、Cisco APIC 接続リーフスイッチを異なるメンテナンス/更新グループに配置する必要があります。

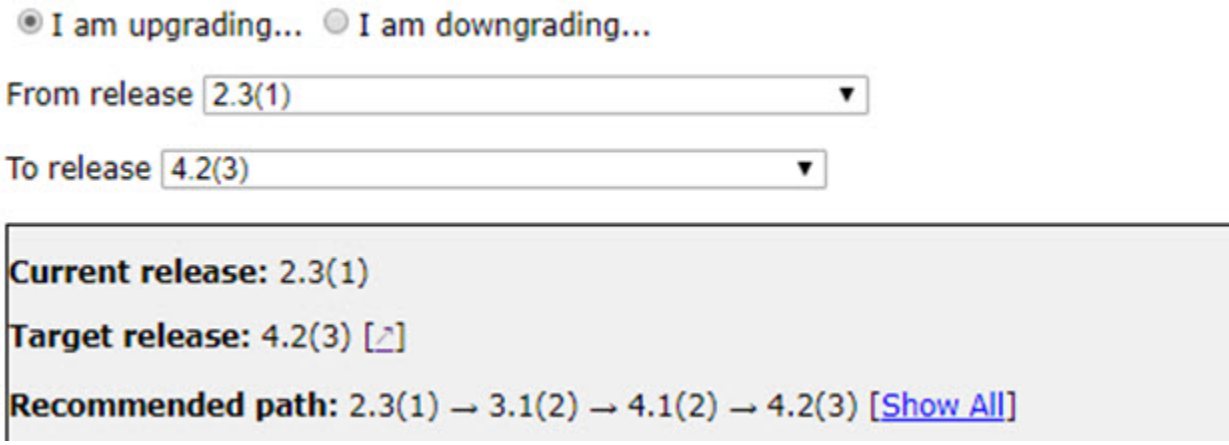
マルチ アップグレード

Cisco ACI ファブリックでは基本的に、すべてのノード (APIC、リーフ スイッチ、およびスパイン スイッチ) が同じソフトウェア リリースまたは互換性のあるソフトウェア リリースである必要があります。この場合、APIC ノードの標準リリース形式は x.y(z)、リーフおよびスパイン スイッチは、スイッチ固有の標準リリース形式の 1x.y(z) になります。たとえば、APIC ノードがソフトウェアリリース 4.2(1) である場合、リーフ スイッチとスパイン スイッチは、スイッチ固有の互換性のあるソフトウェアリリースである 14.2(1) である必要があります。

APIC アップグレード/ダウングレード サポート マトリックスには、現在のバージョンとターゲット バージョンでサポートされているアップグレードおよびダウングレード パスが表示されます。これら 2 つのバージョンが離れすぎている場合、ターゲット バージョンへの直接アップグレードはサポートされない可能性があります。

現在のリリースからの直接のアップグレードパスが存在しないリリースにアップグレードする場合は、すべての APIC とスイッチを、直接アップグレードパスが存在する、サポート対象の中間リリースにアップグレードしたうえで、そのリリースから目的のリリースにアップグレードする必要があります。状況によっては、目的のリリースにアップグレードする前に、複数の中間リリースにアップグレードしなければならない場合があります。この場合、複数の対象 APIC とスイッチの両方をそのつど同じリリースにアップグレードします。

たとえば、*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に、リリース 2.3(1) からリリース 4.2(3) へのアップグレードのための複数の中間リリースが示されている場合、次のような状況が考えられます。



この状況では、次の方法でアップグレードを実行します。

1. APIC を 3.1(2) リリースにアップグレードし、スイッチを 13.1(2) リリースにアップグレードします。
2. 3.1 (2)/13.1 (2) へのアップグレード後に、すべての APIC およびスイッチが**完全に適合した**状態で、動作していることを確認します。
3. 4.1(2) および 14.1(2) についても同じ手順を繰り返します。
4. 4.2(3) および 14.2(3) についても同じ手順を繰り返します。

大規模ファブリックのアップグレード

多数のスイッチのある巨大なファブリックをアップグレードまたはダウングレードする場合や、数日かけてアップグレードまたはダウングレードを行う場合など、ファブリック内で異なるリリースを同時に使用することになる状況があります。このような状況では、ファブリック内には常に、多くとも 2 つの異なる APIC とスイッチ ソフトウェア リリースが存在し得ます。ただし、これらの状況でサポートされる操作は限られています。詳細については、「Cisco ACI スイッチの混合バージョンで許可される操作 （65 ページ）」を参照してください。

App Center アプリの注意事項

Cisco APIC ノードの https://dcappcenter.cisco.com/ からアプリケーションを実行している場合は、次のようにします。

- それらの APIC ノードで APIC ソフトウェアをアップグレードまたはダウングレードする前に、これらのアプリケーションを無効にします。
- これらの APIC ノードで APIC ソフトウェアをアップグレードまたはダウングレードする際に、アプリをインストールしたり、削除したりしないでください。
- これらの APIC ノードで APIC ソフトウェアをアップグレードまたはダウングレードする際に、アプリ イメージのアップグレードを実行しないでください。
- 3.2(1) リリース以前のリリースからアップグレードし、アップグレード前にアプリケーションがインストールされていた場合、アプリケーションは機能しなくなります。アプリケーションを再度使用するには、それらをアンインストールしてから再インストールする必要があります。
- APIC リリース 5.2(1) 以降にアップグレードする場合、外部スイッチ アプリケーション バージョン 1.1 をインストールしている場合は、APIC リリース 5.2(1) 以降にアップグレードする前に、アプリケーションを削除し、バージョン 1.2 を再インストールする必要があります。

ファブリック全体 (APIC ノードとスイッチ) の APIC ソフトウェアのアップグレードまたはダウングレードプロセスが完了したら、それらを無効にした場合は、アプリを再度有効にしま

す。APIC ソフトウェアのアップグレードまたはダウングレードプロセスが完了した後、アプリケーションをインストールまたは削除したり、アプリ イメージのアップグレードを実行したりできます。

現在のソフトウェア バージョンの決定

このセクションの手順を使用して、ファブリック内のスイッチおよび APIC で現在実行されているソフトウェア ビルドを確認します。

• 現在のソフトウェア バージョンの決定 （42 ページ）
• スイッチの現在のソフトウェア バージョンの確認 （42 ページ）

現在のソフトウェア バージョンの決定

ファブリックの APIC で現在実行されているソフトウェア バージョンを確認できます。

- Cisco APIC GUI ウィンドウの右上隅にあるアイコン (⚙) をクリックし、[**バージョン情報 (About)**] を選択します。
- **[Controllers]** ページに移動します。
  - リリース 5.1(1) 以前のリリースの場合、**[管理（Admin）]** > **[ファームウェア（Firmware）]** > **[インフラストラクチャ（Infrastructure）]** > **[コントローラ（Controllers）]** に移動します。ソフトウェア バージョンは、このページの表の **[現在のファームウェア (Current Firmware)]** カラムに表示されます。
  - リリース5.1(1) 以降の場合は、**[管理（Admin）]** > **[ファームウェア（Firmware）]** に移動し、左側のナビゲーション ウィンドウで **[ダッシュボード（Dashboard）]** をクリックします。ソフトウェアバージョンは、ページの**[コントローラ（Controllers）]** 領域の **[ファームウェア（Firmware）]** フィールドに表示されます。

    この同じページの**[コントローラ（Controllers）]** 領域を検索することで、個々の APIC で実行されているソフトウェア バージョンを確認することもできます。各 APIC で実行されているソフトウェアバージョンは、**[現在のバージョン（Current Version）]** 列に表示されます。

スイッチの現在のソフトウェア バージョンの確認

ファブリック内のリーフ スイッチおよびスパイン スイッチで現在実行されているソフトウェア バージョンを確認するには：

- リリース5.1(1) より前のリリースの場合は、**[管理（Admin）]** > **[ファームウェア（Firmware）]** > **[インフラストラクチャ（Infrastructure）]** > **[ノード（Nodes）]** に移動します。ソフトウェア バージョンは、このページの表の **[現在のファームウェア (Current Firmware)]** カラムに表示されます。

- リリース5.1(1) 以降の場合は、**[管理（Admin）]** > **[ファームウェア（Firmware）]** に移動し、左側のナビゲーション ウィンドウで**[ダッシュボード（Dashboard）]**をクリックします。ソフトウェア バージョンは、ページの **[ノード（Nodes）]** 領域の **[ファームウェア（Firmware）]** フィールドに表示されます。
- リリース 5.2(1) 以降では、**[管理（Admin）]** **[ファームウェア（Firmware）]** > **[ノード（Nodes）]** > **タブの[ノード サマリ（Node Summary）]**も使用できます。

スケジューラによるアップグレードについて

スケジューラを使用すると、Cisco APIC クラスタやスイッチのアップグレードなど、操作の時間枠を指定します。これらの時間枠は、1-回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。このセクションでは、アップグレードのスケジューラの仕組みについて説明します。スケジューラに関する詳細情報については、『Cisco アプリケーション セントリック インフラストラクチャの基礎』を参照してください。

（注） クラスタのアップグレードを実行する場合、 Cisco APIC はクラスタに参加するためすべて同じバージョンである必要があります。ファブリックに参加する際の自動アップグレードはありません。

- Cisco APIC クラスタ アップグレード：Cisco APIC のデフォルトのスケジューラ オブジェクトがあります。一般的なスケジューラ オブジェクトには複数のプロパティがありますが、開始時間のプロパティのみ Cisco APIC クラスタ アップグレードに設定可能です。開始時間を指定する場合、 Cisco APIC アップグレード スケジューラは 1 日の期間に指定された開始時刻からアクティブになります。コントローラに対して runningVersion != desiredVersion の場合、このアクティブな 1 日のウィンドウの間いつでもクラスタ アップグレードを開始します。スケジューラのその他のパラメータは Cisco APIC アップグレードに設定できません。スケジューラを使用しない 1 回のトリガを使用して、Cisco APIC アップグレードを実行できることにも注意してください。この 1 回のトリガは、[今すぐアップグレード] とも呼ばれます。
- スイッチのアップグレード：スケジューラはメンテナンス グループに関連付けることができます。スイッチのメンテナンス グループに接続されているスケジューラには、「startTime」、「concurCap」および「duration」などいくつかの設定可能なパラメータがあります。これらのパラメータは下記に説明されています。
  - startTime：アクティブなウィンドウの開始。
  - concurCap：同時にアップグレードするノードの数。
  - Duration：アクティブなウィンドウの長さ。

  グループ内のスイッチに対して runningVersion != desiredVersion の場合、このアクティブな 1 日のウィンドウの間いつでもスイッチはアップグレードの対象となります。アップグレードの対象ノード間で、次の制約がアップグレードの候補の選択に適用されます。

- 「concurCap」ノード以上には現在アップグレードできません。
- 1 回でアップグレードされるのは仮想ポート チャネル（vPC）ペアの 1 つのノードのみです。
- Cisco APIC クラスタはノードのアップグレードを開始する前に正常な状態である必要があります。

（注） GUI、CLI、または REST API を使用して、即時アップグレードとスケジューラベースのアップグレードのオプションがあります。たとえば、CLI では、EXEC モードで **firmware upgrade switch-group** コマンドを使用して、スイッチグループをすぐにアップグレードできます。このコマンドは、設定されたスケジュール済みアップグレードよりも優先されます。

スケジューラに関する注意事

1回限りのアップグレードスケジュールまたは定期的アップグレードスケジュールのいずれを設定しているかに応じて、アップグレードスケジュールを過去の日付に設定した場合、システムの反応は異なります。

- 過去の日付を使用して*1* 回限りのアップグレードスケジュールを設定すると、システムによって設定が拒否されます。
- 定期的アップグレードまたは1度だけのアップグレードのスケジュールに過去の日付が設定されている場合、スケジューラはただちにアップグレードをトリガします。たとえば、水曜日に正午にいて、正午の火曜日ごとに定期アップグレードスケジュールを設定した場合、スケジューラは最初にアップグレードをすぐにトリガーし、その時点から火曜日ごとにアップグレードを実行します。

GUI を使用したスケジューラ–の構成

トリガー スケジューラを使用すると、管理者による介入なしで 1 つ以上のノードをアップグレードして再起動できる、1 回限りまたは繰り返しの期間を定義できます。

手順

ステップ 1 [**トリガー スケジューラの作成 (Create Trigger Scheduler)**] ウィンドウにアクセスします。

ステップ 2 [**トリガー スケジューラの作成 (Create Trigger Scheduler)**] ウィンドウで、[**名前 (name)**] フィールドにスケジューラ ポリシーの名前を入力し、[スケジュール ウィンドウ (schedule Windows)]

領域で [+] をクリックして [**スケジュールの作成 (Create Schedule)create schedule**]ウィンドウを表示します。

ステップ 3 [**ウィンドウ タイプ (Window Type)**] フィールドで、1 回限りまたは定期スケジュール ウィンドウのどちらを設定するかに応じて、[**1 回限り (One Time)**] または [**定期 (Recurring)**] をクリックします。

ステップ 4 [**ウィンドウ名 (Window Name)**] フィールドで、このスケジュール ウィンドウの名前を入力します。

このフィールドの最大文字数は 16 です。

ステップ 5 [スケジュール (schedule)] ウィンドウを実行する日付と時刻を決定します。

日付と時刻を設定するためのオプションは、ワンタイムまたは定期スケジュール ウィンドウのどちらを設定するかによって異なります。

- *1*回限りのスケジュール ウィンドウを設定している場合は、[**日付 (Date)**)]フィールドに、1回限りのスケジュール ウィンドウが発生する日付を入力します。このフィールドでは、YYYY-MM-DD HH: MM: SS AM/PM の形式を使用するか、下矢印をクリックしてカレンダーから日付と時刻を選択します。

  （注） [1 回限りのスケジュール (one-time schedule)] ウィンドウの過去の日付と時刻 (現在の日付と時刻の前) を入力すると、システムはそのエントリを拒否します。

- [定期スケジュール *(Recurring Schedule)*] ウィンドウを設定している場合は、次のフィールドに必要な情報を入力します。

  - [**日 (Day**)]: 定期スケジュールウィンドウを実行する日付を選択します。定期スケジュールウィンドウを毎週実行する特定の日を選択するか、または定期的なスケジュールウィンドウを毎日、すべての偶数日または週のすべての奇数の曜日に実行するかを選択します。
  - [**時間 (hour**)]: 軍事 24 時間のクロック値 (0-23) を使用して、スケジュールウィンドウを繰り返す時間を入力します。
  - [**分 (minute**)]: 定期スケジュールウィンドウを発生させる分を入力します。

  たとえば、毎日午後 11:30 の火曜日に定期スケジュールウィンドウを設定する場合は、次のように選択します。

  - **Day**: 火曜日
  - **時間**:22
  - **分**:30

（注） 定期スケジュールウィンドウの過去の日付と時刻 (現在の日時よりも前) を入力すると、スケジューラはすぐにアップグレードをトリガーします。たとえば、水曜日に正午にあり、火曜日ごとの午後 11:30 に定期アップグレードスケジュールを設定した場合、スケジューラは最初にアップグレードをトリガーし、その時点から火曜日ごとの午後 11:30 にアップグレードを実行します。

ステップ 6 [**最大同時ノード (Maximum Concurrent nodes)**] フィールドに、同時アップグレードを行うことが許可されるノードの最大数を入力します。

このフィールドに **0** を入力すると、ノードが APIC ノードであるか、リーフまたはスパインスイッチであるかに応じて、ソフトウェアによってデフォルト値が自動的に選択されます。

- リリース 4.2(5) より前のリリースでは、このフィールドのデフォルト値「0」は APIC ノードの場合は 1、リーフまたはスパイン スイッチの場合は 20 と解釈されます。このフィールドに入力できる POD ごとの最大ノード数は 200 です。
- リリース 4.2(5) 以降では、このフィールドのデフォルト値「0」は、APIC ノードでは 1 と解釈されます。リーフまたはスパイン スイッチの場合、このフィールドのデフォルト値の「0」の解釈は 20 から無制限に変更されています。つまり、このフィールドに「0」を入力すると、一度にアップグレードできるリーフ スイッチまたはスパイン スイッチの数は無制限になります。

ステップ 7 [**最大実行時間 (Maximum Running time)**] フィールドで、スケジュール ウィンドウの最大継続時間を入力します。これは、アップグレードプロセスを開始するために許可する時間の長さです。

このフィールドでは、DD: HH: MM: SS の形式を使用し、最大 24 時間 (01:00:00:00) を使用します。[スケジューラ (scheduler)] ウィンドウで時間制限を適用しない場合は、[無制限 (unlimited)] を入力します。

たとえば、これらのフィールドに次の値を入力したとします。

- **最大同時ノード (Maximum Concurrent Nodes)**数:20
- **最大実行時間 (Maximum Running Time)**: 00:00:30:00

この場合、このスケジュール ウィンドウでは、20 個のノードを同時にアップグレードできます。これらの 20 ノードは、上記のフィールドに入力した開始時刻から 30 分以内にアップグレードプロセスが正常に開始した場合にのみアップグレードされます。アップグレードプロセスが 30 分以内に正常に開始されない場合、この時点では 20 ノードはアップグレードされません。また、定期スケジュール ウィンドウを設定した場合、次回スケジューラ ウィンドウが繰り返しに設定されたときに、システムはこれらの 20 ノードのアップグレードを試行します。

[**最大実行時間 (Maximum Running Time)**] フィールドに入力した値は、グループ内のスイッチがアップグレードするために必要な時間には影響しません。たとえば、[最大実行時間 (Maximum Running Time)] フィールドに値 **5** を入力した場合は、アップグレードが 5 分後に開始されない場合、システムはスイッチのアップグレードプロセスを放棄することのみを意味します。これは、システムが 5 分後にアップグレードプロセスを停止することを意味するものではありません。通常、各スイッチのアップグレードには約 10 分かかります。

ステップ 8 **[トリガー スケジューラ–の作成 (Create Trigger Scheduler)]** ウィンドウで必要な情報の入力が完了したら、**[OK]** をクリックします。

[**トリガー スケジューラ–の作成 (Create Trigger Scheduler)**] ウィンドウが再度表示され、新しく設定されたスケジュール ウィンドウがスケジュール ウィンドウ テーブルに表示されます。

ステップ 9 このトリガー スケジューラに対して追加のスケジュール ウィンドウを作成するかどうかを決定します。

このトリガー スケジューラに対してより多くのスケジュール ウィンドウを作成する場合は、[スケジュール ウィンドウ (Schedule Windows)] 領域で [+] をクリックして、[**スケジュール ウィンドウの作成 (Create Schedule Window)**] ウィンドウを再度表示します。

たとえば、毎日 2 回開始するようにアップグレードを設定する場合や、毎日 12:00 AM と PM の場合、または特定の曜日にアップグレードを設定する場合は、より多くのスケジュールウィンドウを作成することができます。

ステップ 10 必要なスケジュールウィンドウの設定が完了したら、[**トリガー スケジューラの作成 (Create Trigger Scheduler**)] ウィンドウで [**送信 (Submit)**] をクリックします。

[**ノード アップグレードの選択 (Select Node Upgrade)**] ウィンドウが再度表示されます。

ステップ 11 [**ノード アップグレードの選択 (Select Node Upgrade)**] ウィンドウで、[**スケジューラ (Scheduler)**] フィールドを見つけて、先ほど設定したトリガースケジュールを選択します。

ステップ 12 [**ノード アップグレードの選択 (Select Node Upgrade)**] ウィンドウで必要な追加設定を完了し、[**送信 (Submit)**] をクリックします。

NX-OS スタイルの CLI を使用したスケジューラ–の構成

スケジュールにより、設定のインポート/エクスポートまたはテクニカル サポートの収集などの操作を 1 つ以上の指定した時間帯に発生させることができます。

スケジュールには、一連のタイム ウィンドウ（オカレンス）が含まれます。これらのウィンドウは、1回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。期間や実行するタスクの最大数などのウィンドウで定義されているオプションにより、スケジュール設定されたタスクの実行時期が決定されます。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、APIC が 1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する1つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

- 絶対（1 回）時間帯：絶対時間帯は、1 回しか発生しないスケジュールを定義します。これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。
- 繰り返し時間帯：繰り返し時間帯は、繰り返しのスケジュールを定義します。この時間帯は、タスクの最大数に達するまで、または時間帯に指定された日の終わりに達するまで継続します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **scheduler** *schedule-name* 例： `apic1(config)# scheduler controller schedule myScheduler`	新しいスケジューラを作成するか、既存のスケジューラを設定します。
ステップ 3	[**no**] **description** *text* 例： `apic1(config-scheduler)# description 'This is my scheduler'`	このスケジューラの説明を追加します。テキストにスペースが含まれている場合は、単一引用符で囲む必要があります。
ステップ 4	[**no**] **absolute window** ウィンドウ名 例： `apic1(config-scheduler)# absolute window myAbsoluteWindow`	絶対（1 回）の時間帯スケジュールを作成します。
ステップ 5	[**no**] **max concurrent nodes** *count* 例： `apic1(config-scheduler-absolute)# max concurrent nodes 300`	同時に処理できるノード（タスク）の最大数を設定します。指定できる範囲は 0 ～ 65535 です。ノード数を制限しない場合は 0 に設定します。
ステップ 6	[**no**] **max running time** *time* 例： `apic1(config-scheduler-absolute)# max running time 00:01:30:00`	dd:hh:mm:ss の形式でタスクの最大実行時間を設定します。指定できる範囲は 0 ～ 65535 です。時間の制限がない場合は 0 に設定します。
ステップ 7	[**no**] **time start** *time* 例： `apic1(config-scheduler-absolute)# time start 2016:jan:01:12:01`	[[[yyyy:]mmm:]dd:]HH:MM 形式で開始時刻を設定します。
ステップ 8	**exit** 例： `apic1(config-scheduler-absolute)# exit`	スケジューラ コンフィギュレーション モードに戻ります。
ステップ 9	[**no**] **recurring window** ウィンドウ名 例： `apic1(config-scheduler)# recurring window myRecurringWindow`	繰り返し時間帯のスケジュールを作成します。

	コマンドまたはアクション	目的
ステップ 10	[**no**] **max concurrent nodes** *count* 例： `apic1(config-scheduler-recurring)# max concurrent nodes 300`	同時に処理できるノード（タスク）の最大数を設定します。指定できる範囲は 0 ～ 65535 です。ノード数を制限しない場合は 0 に設定します。
ステップ 11	[**no**] **max running time** *time* 例： `apic1(config-scheduler-recurring)# max running time 00:01:30:00`	dd:hh:mm:ss の形式でタスクの最大実行時間を設定します。指定できる範囲は 0 ～ 65535 です。時間の制限がない場合は 0 に設定します。
ステップ 12	[**no**] **time start** { **daily** *HH:MM* | **weekly**（使用状況を参照） *HH:MM*} 例： `apic1(config-scheduler-recurring)# time start weekly wednesday 12:30`	期間（毎日または毎週）と開始時刻を設定します。**weekly** を選択した場合、次のオプションから選択します。 • **monday** • **tuesday** • **wednesday** • **thursday** • **friday** • **saturday** • **sunday** • **even-day** • **odd-day** • **every-day**

例

次に、毎週水曜日に実行するよう繰り返しスケジューラを設定する例を示します。

```
apic1# configure
apic1(config)# scheduler controller schedule myScheduler
apic1(config-scheduler)# description 'This is my scheduler'
apic1(config-scheduler)# recurring window myRecurringWindow
apic1(config-scheduler-recurring)# max concurrent nodes 300
apic1(config-scheduler-recurring)# max running time 00:01:30:00
apic1(config-scheduler-recurring)# time start weekly wednesday 12:30
```

REST API を使用したスケジューラ–の構成

スケジュールにより、設定のインポート/エクスポートまたはテクニカル サポートの収集などの操作を 1 つ以上の指定した時間帯に発生させることができます。

スケジュールには、一連のタイム ウィンドウ（オカレンス）が含まれます。これらのウィンドウは、1回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。期間や実行するタスクの最大数などのウィンドウで定義されているオプションにより、スケジュール設定されたタスクの実行時期が決定されます。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、APIC が 1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する 1 つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

- 絶対（1 回）時間帯：絶対時間帯は、1 回しか発生しないスケジュールを定義します。これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。
- 繰り返し時間帯：繰り返し時間帯は、繰り返しのスケジュールを定義します。この時間帯は、タスクの最大数に達するまで、または時間帯に指定された日の終わりに達するまで継続します。

手順

ステップ 1 リポジトリにスイッチ イメージをダウンロードします。

例：

```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http" url="http://<ip
address>/<ver-no>"/>
</firmwareRepoP>
```

ステップ 2 次のポリシーを、POST 送信することにより、ノード ID が 101、102、103、104 の スイッチから構成されるファームウェア グループを作成し、ノード ID 101、102、103、104 によるメンテナンス グループを作成します。

例：

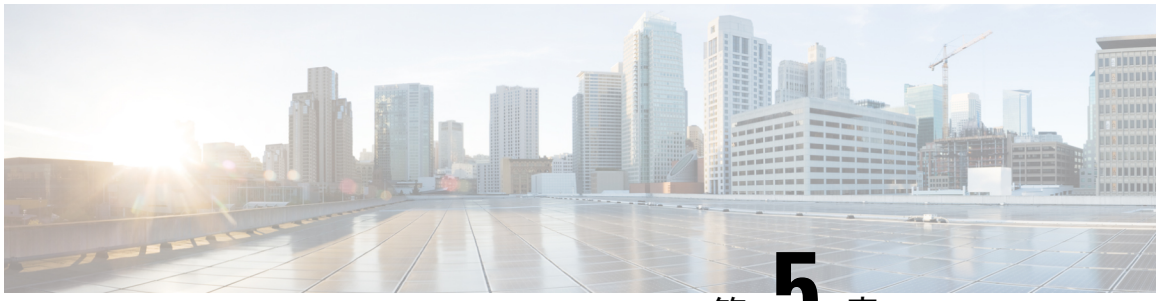
```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
<firmwareFwP
    name="AllswitchesFwP"
    version="<ver-no>"
    ignoreCompat="true">
</firmwareFwP>
```

```
<firmwareFwGrp
    name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
<firmwareRsFwgrpp
    tnFirmwareFwPName="AllswitchesFwP">
</firmwareRsFwgrpp>
</firmwareFwGrp>

<maintMaintP
    name="AllswitchesMaintP"
    runMode="pauseOnlyOnFailures" >
</maintMaintP>

<maintMaintGrp
    name="AllswitchesMaintGrp">
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
<maintRsMgrpp
    tnMaintMaintPName="AllswitchesMaintP">
</maintRsMgrpp>
</maintMaintGrp>
</fabricInst>
```

ステップ 3 スケジューラに基づいてすべてのスイッチをアップグレードするには、次のようなポリシーをポストします。

例：

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<trigSchedP annotation="" descr="" dn="uni/fabric/schedp-EveryEightHours"
name="EveryEightHours" nameAlias="" ownerKey="" ownerTag="" userdom="">
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="17"
minute="0" name="third" nameAlias="" nodeUpgInterval="0" procBreak="none"
procCap="unlimited" timeCap="00:01:00:00.000" userdom=""/>
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="9" minute="0"
 name="second" nameAlias="" nodeUpgInterval="0" procBreak="none" procCap="unlimited"
timeCap="00:01:00:00.000" userdom=""/>
 <trigRecurrWindowP annotation="" concurCap="unlimited" day="every-day" hour="1" minute="0"
 name="first" nameAlias="" nodeUpgInterval="0" procBreak="none" procCap="unlimited"
timeCap="00:01:00:00.000" userdom=""/>
</trigSchedP>
```



第 5 章

ACI アップグレード アーキテクチャ

APIC アップグレードの概要

APIC クラスタのアップグレードを実行する場合は、アップグレードされた APIC のデータがターゲット イメージと互換性があることを保証するとともに、各 APIC を個別にアップグレードするために発生する特定のシーケンスのイベントがあります。これらのイベントのほとんどはバックグラウンドで発生するため、APIC クラスタのアップグレードをトリガーするときに表示される内容を理解することが重要です。

1. ファームウェア リポジトリにイメージを追加します。イメージはすべての APIC クラスタ メンバーに同期されます。
2. 特定のターゲット バージョンへのアップグレードがトリガーされます。
3. クラスタ内の各 APIC は、最初の grub パーティションに新しいイメージをインストールするプロセスを実行します。これは、アップグレードプロセスを高速化するために並行して行われることに注意してください。
4. イメージのインストールが完了すると、各 APIC は順番にデータベース ファイルのデータ変換プロセスを順番に実行します。これが発生すると、次のイベントが発生します。
    1. データ管理エンジン（DME）プロセスがシャットダウンします。これには、すべての API 要求を処理する nginx Web サーバが含まれます。このため、UI / API、およびその APIC で実行される他のバックエンドアプリケーションにアクセスできなくなります。

2. データベース ファイルが初期バージョンからターゲット バージョンに変換されます。これにかかる時間は、ACI ファブリックに展開された設定のサイズによって異なります。このため、変換を完了するまでの合計時間は導入環境によって異なります。

（注） **この段階で *APIC* に対して実行される破壊的なアクションがないことが重要です。**詳細については、「アップグレード/ダウングレード中に回避する必要がある操作（62 ページ）」を参照してください。

3. APIC は、データベース変換プロセスが正常に完了した後にリロードし、ターゲット バージョンで定義されたソフトウェアのバージョンで起動します。

5. リロードを実行した APIC がオンラインに戻ると、ステップ 4 で説明した一連のイベントがクラスタ内の次の APIC で発生します。このプロセスは、クラスタのすべてのメンバーがアップグレードされるまで繰り返されます。

APIC アップグレードの詳細な概要

次の項では、APIC アップグレードの詳細な概要を示します。

APIC のアップグレード段階の説明

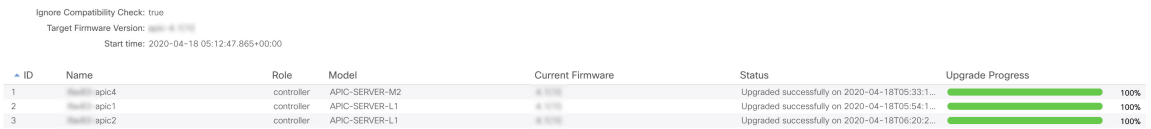
アップグレード プロセス中に APIC が実行する段階は、現在実行しているソフトウェアのバージョンとアップグレード先のソフトウェアのバージョンによって異なります。

- 4.2(5) より前のリリースからリリース 4.2(5) 以降へのアップグレード （54 ページ）
- 4.2(5) より前のリリースからリリース 4.2(5) 以降へのアップグレード （57 ページ）

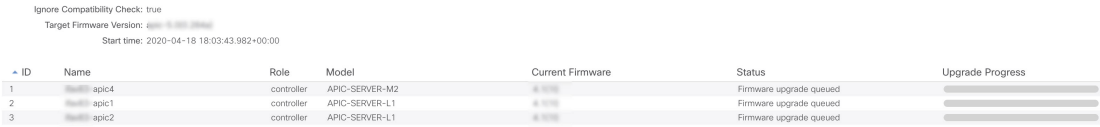
4.2(5) より前のリリースからリリース 4.2(5) 以降へのアップグレード

ソフトウェアの現在実行中のバージョンが Cisco APIC リリース 4.2(5) よりも前で、リリース 4.2(5)以降にアップグレードする場合、このセクションでは、アップグレード プロセス中に各 APIC が実行する段階について説明します。

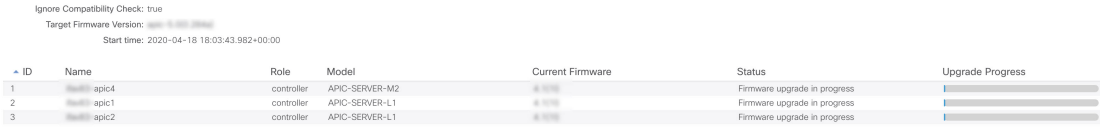
- アップグレードを開始する前に、各 APIC は 100% で表示されます。これは、各 APIC で以前に実行されたインストール、アップグレード、またはダウングレードが正常に完了したことを示します。



- アップグレードプロセスを開始すると、すべての APIC のステータスが 100% から 0% に変わり、次の段階を経ます。
  - ステータスは、最初に [ファームウェア アップグレードのキュー作成（Firmware upgrade queued）] と表示されます。

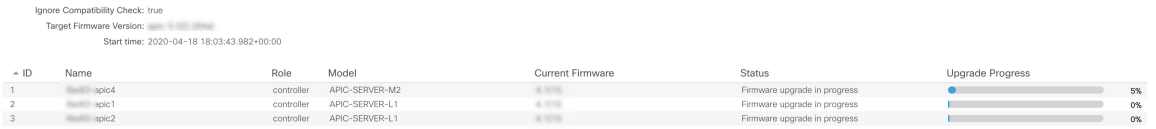


  - ステータスが [ファームウェア アップグレードの進行中（Firmware upgrade in progress）] に変わります。

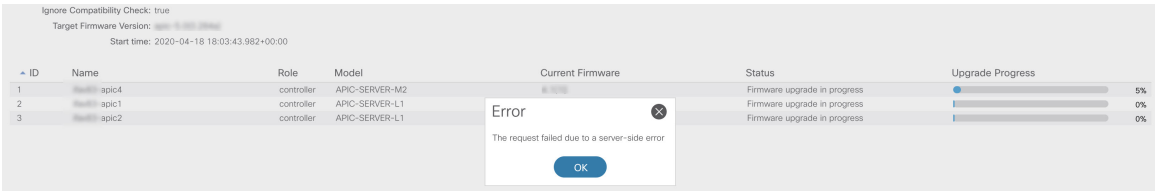


- 次に、インストーラによって最初に選択された APIC がアップグレードを開始し、次の図に示すように 5% に進みます。

（注） アップグレード プロセスを開始するために最初に選択される APIC は、インストーラによって最初に呼び出される APIC に応じてランダムに選択されます。つまり、クラスタ内で最初にアップグレードを開始する APIC は、必ずしも番号が最も小さいAPICではありません。



この段階では、次のようなエラーおよび警告メッセージが表示されることがあります。



これは正常な動作であり、アップグレード プロセスの一環として APIC がリブートされるためです。

クラスタ内の最初の APIC が 5% に達すると、各 APIC はアップグレード プロセスの次の段階に進み、**[アップグレードの進行状況（Upgrade Progress）]** 領域に表示されます。

- **インストーラによって呼び出される最初の APIC**: 0% → 5% → 100%

- **クラスタ内の残りの APIC**: 0% → 100%

次の表に、このアップグレード プロセスの各段階で行われる処理の詳細を示します。

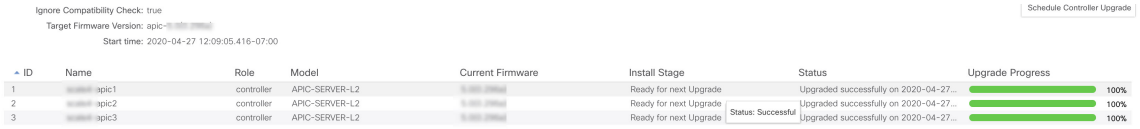
アップグレードの経過表示	説明
0%	アップグレード インストーラが開始し、アップグレード プロセスが開始されたときに表示されます。
5%	この段階では、クラスタ内のすべての APIC に対して次の設定が行われます。インストーラによって呼び出された最初の APIC のステータスは 5% のままで、クラスタ内の残りの APIC のステータスは 0% のままです。 • インストーラによって最初に呼び出された APIC は、新しい APIC との互換性を保つためのデータベース変換の準備や、各 APIC のファームウェア イメージのステータス チェックなどの内部健全性チェックを実行します。 • 内部健全性チェックが完了し、ターゲット バージョンが APIC にプリロードされます。 • クラスタ内のすべての APIC は、インストーラによって最初に呼び出された APIC、次に 2 番目の APIC、3 番目の APIC の順に順次アップグレードされます。この段階では、各 APIC は、その前の APIC が完了するのを待ってから、アップグレードを開始します。つまり、最初の APIC ノードが最初にアップグレードを開始し、最初の APIC がアップグレード プロセスを完了するまで 2 番目と 3 番目の APIC が待機します。最初の APIC ノードがこの段階を完了すると、2 番目の APIC は ¥ がアップグレードプロセスを開始し、3 番目の APIC は待機します。 • すべての APIC は、アップグレード プロセスのデータ変換フェーズを順番に実行します。アップグレード プロセスのこの段階で、アップグレード プロセスが失敗すると、システムは以前のバージョンのソフトウェアにロールバックします。 この段階のデータ変換部分が完了すると、この段階で各 APIC がリブートします。各 APIC がリブートすると、次のように表示されます。 • 次のエラーと警告メッセージが表示される場合があります。 不明な理由により、サーバ側のエラーまたは `Web` ソケット接続が閉じられたため、要求が失敗しました これは正常な動作であり、アップグレードプロセスの一環として APIC がリブートされるためです。 • APIC は、GUI の APIC コントローラのリストから一時的に表示されなくなり、リブートが完了してアップグレードが正常に完了すると、リストに再表示されます。 ブラウザが接続されている Cisco APIC がアップグレードされて再起動すると、ブラウザには最初にエラー メッセージが表示されます。その後、この APIC にログインするために使用したブラウザには何も表示されません。ただし、必要に応じて、クラスタ内の残りの APIC にログインして、アップグレード プロセスの進行状況をモニタし続けることができます。

アップグレードの経過表示	説明
100 %	APIC がアップグレード プロセス全体を正常に完了したときに表示されます。

4.2(5) より前のリリースからリリース 4.2(5) 以降へのアップグレード

ソフトウェアの現在の実行バージョンが Cisco APIC リリース 4.2(5) 以降で、それ以降のリリースにアップグレードする場合、このセクションでは、アップグレードプロセス中に各 APIC が実行する段階について説明します。

- アップグレードを開始する前に、各 APIC は 100% で表示されます。これは、各 APIC で以前に実行されたインストール、アップグレード、またはダウングレードが正常に完了したことを示します。



- アップグレードプロセスを開始すると、次の図に示すように、すべての APIC のステータスが 100% から 0% に変わります。

- 次に、インストーラによって最初に選択された APIC がアップグレードを開始し、次の図に示すように 5% に進みます。

（注） アップグレード プロセスを開始するために最初に選択される APIC は、インストーラによって最初に呼び出される APIC に応じてランダムに選択されます。つまり、クラスタ内で最初にアップグレードを開始する APIC は、必ずしも番号が最も小さいAPICではありません。

- インストーラによって 2 番目に選択された APIC がアップグレードを開始し、5% に進みます。
- インストーラによって 3 番目に選択された APIC がアップグレードを開始し、5% に進みます。

クラスタ内に 3 つ以上の APIC がある場合、クラスタ内のすべての APIC が 5% になるまでプロセスが続行されます。

クラスタ内のすべての APIC が 5% に達すると、各 APIC はアップグレード プロセスの次の段階に進み、**[アップグレードの進捗状況（Upgrade Progress）]** 領域に表示されます。

- **インストーラによって最初に呼び出される APIC**: 0% → 5% → 10% → 25% → 50% → 75% → 100%
- **クラスタ内の残りのAPIC**: 0% → 5% → 25% → 50% → 75% → 100%

次の表に、このアップグレード プロセスの各段階で行われる処理の詳細を示します。

アップグレードの経過表示	インストールステージ	インストールステージ ステータス	説明
0%	次のアップグレードの準備完了	キュー（Queued）	アップグレード インストーラが開始し、アップグレード プロセスが開始されたときに表示されます。
5%	互換性の確認	コントローラのハードウェアとソフトウェアの互換性を確保する	アップグレード インストーラが開始し、アップグレード プロセスが開始されたときに表示されます。
10%	コントローラの正常性の確認	アップグレードの準備のための内部健全性チェックの実行	この段階では、インストーラによって呼び出された最初のAPICが、新しいファームウェアと互換性があるデータベース変換の準備や各 APIC のファームウェア イメージ ステータス チェックなどの内部健全性チェックを実行します。最初の APIC はこの段階で 10% に移行しますが、クラスタ内の他の APIC は5% のままになります。
25 %	アップグレードの実行	コントローラにターゲット バージョンをインストールします	内部健全性チェックが完了し、ターゲット バージョンが APIC にプリロードされたことが表示されます。 クラスタ内の他の APIC で設定チェックとアップグレード前の設定を実行している最初の APIC は、この段階で10% から25% に移行しますが、クラスタ内の残りの APIC は、この段階では5% から25% に直接移動します。
50%	アップグレードする他のコントローラの待機	他のコントローラが設定の移行を完了するまで待機	クラスタ内の APIC は、インストーラによって最初に呼び出された APIC、次に 2 番目の APIC、3 番目の APIC の順に順次アップグレードされます。この段階では、各 APIC は、その前の APIC が完了するのを待ってから、アップグレードを開始します。つまり、最初の APIC ノードが最初にアップグレードを開始し、最初の APIC がアップグレード プロセスを完了するまで 2 番目と 3 番目の APIC が待機します。最初の APIC ノードがこの段階を完了すると、2 番目の APIC は ¥ がアップグレードプロセスを開始し、3 番目の APIC は待機します。

アップグレードの経過表示	インストールステージ	インストールステージ ステータス	説明
75%	設定の移行	コントローラで変換を実行しています	アップグレードプロセスのデータ変換フェーズで表示されます。ここでも、クラスタ内のすべてのAPIC間のアップグレードプロセスの順番が異なるため、1つのAPICはこの段階で50%から75%に移行しますが、他の2つの APIC は50% のままになります。最初のAPICがアップグレードプロセスのこのフェーズを完了すると、クラスタ内の2番目の APIC がこのフェーズを開始し、50%から75% に移行します。2 番目の APIC がアップグレードプロセスのこのフェーズを完了するまで、残りの APIC は 50% のままになります。 アップグレードプロセスのこの段階(50% ステージと 75% ステージの間) で、アップグレードプロセスが失敗すると、システムは以前のバージョンのソフトウェアにロールバックします。 この段階のデータ変換部分が完了すると、この段階で各 APIC がリブートします。各 APIC がリブートすると、次のように表示されます。 • 次のエラーと警告メッセージが表示される場合があります。 不明な理由により、サーバ側のエラーまたは `Web` ソケット接続が閉じられたため、要求が失敗しました これは正常な動作であり、アップグレード プロセスの一環として APIC がリブートされるためです。 • APIC は、GUI の APIC コントローラのリストから一時的に表示されなくなり、リブートが完了してアップグレードが正常に完了すると、リストに再表示されます。 ブラウザが接続されている Cisco APIC がアップグレードされて再起動すると、ブラウザには最初にエラー メッセージが表示されます。その後、このAPICにログインするために使用したブラウザには何も表示されません。ただし、必要に応じて、クラスタ内の残りのAPIC(APICがリロードされた時点でまだ50%だった APIC) にログインして、アップグレード プロセスの進行状況をモニタし続けることができます。
100 %	次のアップグレードの準備完了	Successful（成功）	APICがアップグレードプロセス全体を正常に完了したときに表示されます。

5.2(4) リリース以降のデフォルト インターフェイスポリシー

5.2(4) 以降のリリースにアップグレードすると、Cisco Application Policy Infrastructure Controller (APIC) によって次のデフォルトのインターフェイスポリシーが自動的に作成されます。

- CDP (cdpIfPol)
  - system-cdp-disabled
  - system-cdp-enabled
- LLDP (lldpIfPol)
  - system-lldp-disabled
  - system-lldp-enabled
- LACP (lacpLagPol)
  - system-static-on
  - system-lacp-passive
  - system-lacp-active
- リンク レベル (fabricHIfPol)
  - system-link-level-100M-auto
  - system-link-level-1G-auto
  - system-link-level-10G-auto
  - system-link-level-25G-auto
  - system-link-level-40G-auto
  - system-link-level-100G-auto
  - system-link-level-400G-auto
- ブレイクアウトポート グループマップ (infraBrkoutPortGrp)
  - system-breakout-10g-4x
  - system-breakout-25g-4x
  - system-breakout-100g-4x

アップグレード中に、これらのポリシーのいずれかとまったく同じ名前とパラメータを持つポリシーがすでに存在する場合、システムはそれらのポリシーの所有権を取得し、ポリシーは読み取り専用になります。そうではなく、`system-cdp-disabled` の設定が「有効」になっている

など、パラメータが異なる場合、ポリシーは引き続きユーザーポリシーになります。つまり、ユーザーはポリシーを変更できます。

スイッチ アップグレードの概要

ACI スイッチ ノードのアップグレードを実行すると、アップグレード中のデバイスで発生するイベントの特定のシーケンスがあります。これらのイベントのほとんどはバックグラウンドで発生するため、ACI スイッチ ノードのアップグレードをトリガーするときに表示される内容を理解することが重要です。

1. イメージが APIC からスイッチにプッシュされます。
2. スイッチのファイル システムとブートフラッシュをチェックして、イメージを抽出するのに十分な領域があることを確認します。
3. イメージが抽出され、プライマリ GRUB パーティションがターゲット バージョンに更新されます。古いバージョンはリカバリ パーティションに移動されます。
4. BIOS および EPLD イメージは、必要に応じてアップグレードされます。
5. スイッチはクリーン リロードを実行し、新しいバージョンのソフトウェアを実行している ACI ファブリックに再参加します。

リリース 2.1(4) 以降では、サードパーティ製ミクロン ソリッド ステート ドライブ (SSD) ファームウェア自動更新のサポートが追加されました。標準的な Cisco APIC ソフトウェア アップグレードプロセスの一環として、アップグレード時にスイッチが再起動します。そのブート時のプロセスでは、システムは現在の SSD ファームウェアもチェックし、必要に応じて SSD ファームウェアへのアップグレードを自動的に実行します。システムが SSD ファームウェアのアップグレードを実行すると、スイッチは後でもう一度クリーン リブートします。

スイッチ アップグレードの詳細な概要

次の項では、スイッチ アップグレードの詳細な概要を示します。

スイッチのアップグレード段階の説明

ACI スイッチ ノードのアップグレード中は、完了した段階に基づいてアップグレードの進行状況が進みます。

次の表に、このアップグレード プロセスの各段階で行われる処理の詳細を示します。

アップグレードの経過表示	インストール ステージ	説明
0%	ファームウェアアップグレードのキュー	ファームウェアが APIC からスイッチにダウンロードされているときに表示されます。
5%	ファームウェアアップグレードが進行中です	アップグレード インストーラが開始し、アップグレード プロセスが開始されたときに表示されます。
45%	ファームウェアアップグレードが進行中です	ブートフラッシュチェックが完了し、イメージ抽出ステージが開始された後に表示されます。
60%	ファームウェアアップグレードが進行中です	イメージ抽出ステージが完了し、grub パーティションが新しいソフトウェア情報で更新されています。
70%	ファームウェアアップグレードが進行中です	ソフトウェアがスイッチで更新されました。
80%	ファームウェアアップグレードが進行中です	EPLD と BIOS のアップグレードが開始されました。
95 %	ファームウェアアップグレードが進行中です	EPLD と BIOS のアップグレードが完了し、スイッチのリブートが開始されました。
100%	アップグレード成功	ターゲット バージョンのソフトウェアを実行しているクリーン リロード後に、スイッチがファブリックに再参加しました。

APIC ダウングレード段階の説明

ACI APIC およびスイッチのダウングレードの段階は、ソフトウェアのバージョンが実行中のバージョンよりも低いという点で APIC アップグレードの概要 （53 ページ） で説明されているアップグレードの段階と同じです。

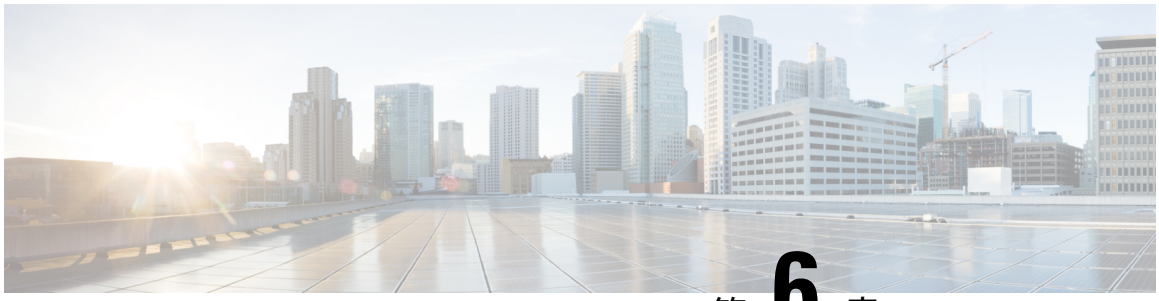
アップグレード/ダウングレード中に回避する必要がある操作

いずれかの時点で、アップグレード/ダウングレードが停止または失敗したと思われる場合は、以下に示すアクションを実行しないことが重要です。

- クラスタ内の APIC をリロードしないでください。
- クラスタ内の APIC をデコミッションしないでください。
- ファームウェアのターゲット バージョンを元のバージョンに戻さないでください。

代わりに、次のガイドラインに従ってください。

1. 必要に応じて、「トラブルシューティング」の項で説明されているインストーラ ログ ファイルを表示します（APIC インストーラ ログ ファイル （167 ページ） および ACI スイッチ インストーラのログ ファイル（168 ページ） を参照）。これは、アップグレードされているデバイスでまだ進行中のアクティビティがあるかどうかを理解するのに役立ちます。
2. 「トラブルシューティング」セクションで説明されているテクニカル サポート ファイルを収集します（テクニカル サポート ファイルの収集 （168 ページ） を参照）。
3. アップグレードが正常に完了しない場合は、Cisco TAC に連絡し、作成後に TAC ケースにテクニカル サポート ファイルをアップロードします。



第 6 章

Cisco ACI スイッチの混合バージョンで許可される操作

Cisco ACI スイッチの混合バージョンで許可される操作

Cisco ACI ファブリックには基本的に、すべてのノード (APIC、リーフスイッチ、およびスパインスイッチ) が同じソフトウェアリリースまたは互換性のあるソフトウェアリリース上にある必要があります。この場合、APIC ノードの標準リリース形式は x.y(z)、リーフおよびスパインスイッチには、スイッチ固有の標準リリース形式の 1x.y(z) があります。たとえば、APIC ノードがソフトウェアリリース 4.1(1) 上にある場合、リーフ スイッチとスパイン スイッチは、スイッチ固有のバージョン 14.1(1) である必要があります。

ただし、この状況では通常、スイッチ ノードを複数の異なるグループ (メンテナンス グループ) に分割することになるため、多数のスイッチ ノードを持つ大きな ACI ファブリックのソフトウェアをアップグレードしようとすると、これは困難な要件となる可能性があります。これにより、一度に1つのアップグレードを実行して、サービスの中断を回避できますスイッチ ノードまたはメンテナンス グループの数、およびネットワーク トラフィック、サービス、およびアプリケーションの検証プロセスに応じて、1 日のメンテナンス グループをアップグレードできますが、その他のメンテナンス グループのアップグレードを待つ必要がある場合があります。

リリース 2.2(1) 以降では、ソフトウェアのアップグレードによりすべての ACI スイッチが同じバージョンになっていない場合でも、一部の操作を実行できます。この動作は、リリース 2.3(1) で拡張され、この状況で実行できるさらに多くの操作をサポートするようになりました。次の表では、リリース 2.2(1) および 2.3(1) 以降のスイッチが混在リリースにある場合に実行できる操作について説明します。

Cisco ACI スイッチの混合バージョンで許可される操作

（注）

- アップグレード パスごとに混合バージョンでサポートされる操作 （66 ページ） で説明されているサポートされている操作を実行するには、最初にすべての APIC ノードを新しいバージョンにアップグレードする必要があります。すべての APIC ノードが正常にアップグレードされ、完全にアップグレードされるまで、操作を実行しないでください。
- 混合バージョンでサポートされる操作は、異なるソフトウェア バージョンを実行する vPC ペア リーフ スイッチには適用されません。 vPC ペア スイッチは、すべての操作で同じソフトウェア バージョンを実行している必要があります。

  古いバージョンのみサポートしている古い世代のスイッチから、新しいバージョンのみサポートしている新世代スイッチに移行する必要があるため、異なるバージョンの vPC ペアのリーフ スイッチを交換する場合（たとえば、4.2(1) を実行しているリーフ スイッチを 5.0(1) を実行している別のリーフ スイッチのセットに交換する場合）、一度に1つのスイッチを交換しないでください。このようなシナリオでは、1 つのリーフ スイッチから同じ vPC 内の別のリーフ スイッチへのユーザ トラフィックのスムーズなフェールオーバーは保証されません。代わりに、すべてのワークロードを既存のリーフ スイッチの別のセットに移動し（トラフィックの中断を避けるため）、最初に両方のスイッチを削除してから、古いスイッチと同じノード ID で vPC に新しいスイッチを登録する必要があります。
- アップグレード パスごとに混合バージョンでサポートされる操作 （66 ページ） でリストされている操作を実行できるのは、古い (from) バージョンですでにサポートされていた機能に関連している場合だけです。
- 3.0 以前のリリースでは、ファブリック内の ACI ノードのバージョンの違いを通知する赤いバナーの警告が表示されています。このバナーの警告は、リリース 3.0 以降に削除されました。

アップグレード パスごとに混合バージョンでサポートされる操作

アップグレード パス		サポートされる操作
移行前	移行後	
2.2(x)	サポートされているアップグレード パスのすべてのバージョン	• 設定のエクスポート • テクニカル サポートの収集 • 物理的なネットワークの変更(再起動、ケーブル交換など) • メジャー リリースの前に導入された機能のポリシー変更*

Cisco ACI スイッチの混合バージョンで許可される操作

アップグレード パス		サポートされる操作
2.3(x) 以降	サポートされているアップグレード パスのすべてのバージョン	• 設定のエクスポート • テクニカル サポートの収集 • 物理的なネットワークの変更(再起動、ケーブル交換など) • メジャー リリースの前に導入された機能のポリシー変更* • 機能のポリシー変更: リリース 2.3(x) 以降からのアップグレードでバージョンが混在する場合にサポートされる操作 （67 ページ）

* この操作がサポートされるのは、アップグレードが同じリリースの列車内にある場合 (たとえば 3.2(5d) から 3.2(5f) へのアップグレードであり、リリースは 3.2(5) リリースのトレーニングの一部ですが、そのリリースの**d**と**f**のバージョンの間でアップグレードが発生します)。

リリース 2.3(x) 以降からのアップグレードでバージョンが混在する場合にサポートされる操作

リリース 2.3(1) 以降、Application Policy Infrastructure Controller は上記のネットワーク設定機能と混合 OS 動作中の変更に一覧表示したものに加えて、次の機能をサポートします。

機能	操作
コントラクト	• フィルタ、件名、コントラクトを作成、更新、削除します。 • コントラクトをエクスポートおよびインポートします。 • EPG に関係する提供および消費されたコントラクトを追加および削除します。 • vzAny で提供および消費されたコントラクトを追加および削除します。
エンドポイント グループ	• EPG の作成と削除。 • VMM、物理、外部、L2 外部、L3 外部ドメインの関連付けを追加および削除します。 • スタティック ポートの割り当ておよびノードへの静的リンクを追加、削除、更新します。 • 1 つの EPG から別の EPG にエンドポイントを移動します。 • uSeg EPG からベースに EPG にエンドポイントを移動します。

Cisco ACI スイッチの混合バージョンで許可される操作

機能	操作
マイクロセグメンテーション	uSeg EPG を追加および更新します。
VMotion	リーフ スイッチ全体の vMotion。
VM 操作	仮想マシンのオンおよびオフ。
ブリッジ ドメイン	ブリッジ ドメインを作成、更新、削除します。
VMM ドメイン	次の操作は、VMware vDS および Cisco AV でのみサポートされます。 • VMM ドメインを作成し削除します。 • VLAN プールを作成し更新します。 • マルチキャスト プールを追加し削除します。 • vMware vCenter を追加し更新します。 • vSwitch ポリシーを追加し更新します。
レイヤ2またはレイヤ3アウト	L2 外部および L3 外部ドメインを追加、更新、削除します。
アクセスポリシー	• スイッチ ポリシー、インターフェイス ポリシー、ポリシー グループ、接続エンティティプロファイル（AEP）を追加、更新、削除します。
トラブルシューティング	• SPAN 設定を追加、更新、削除します。 • syslog サーバーを追加、更新、削除します。

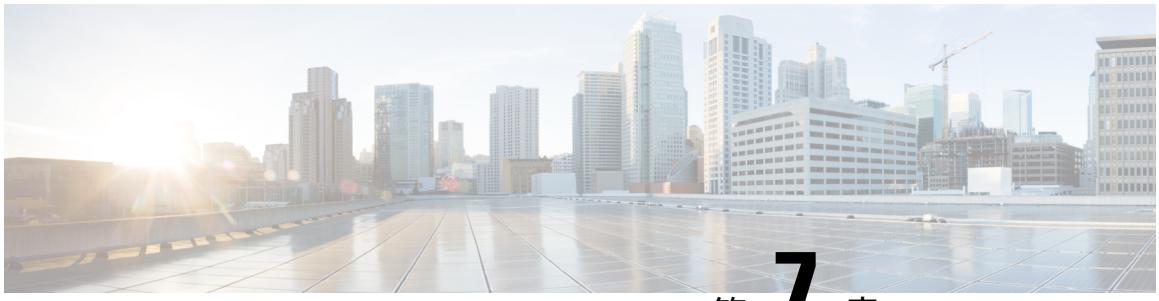
Cisco ACI スイッチの混合バージョンで許可される操作

機能	操作
物理ネットワーク	• ポート ステータスを有効化および無効化します。 • 物理サーバのオンおよびオフ。 • リーフ スイッチおよびリーフ スイッチ間で物理サーバを移動します。 • スパイン スイッチとリーフ スイッチのリロード。 • スパイン スイッチ LC カード、FC カード、CS カードと SUP カードのリロード。 • スパイン スイッチとリーフ スイッチのデコミッション。 • **[コントローラから削除（Remove from Controller）]** オプションを使用してスパイン スイッチとリーフ スイッチを削除する。 • 新しいスパイン スイッチおよびリーフ スイッチの登録 • 仮想ポート チャネル（vPC）ドメインの追加と削除。 • プライマリ リンク、セカンダリ リンク、および仮想ポート チャネル（vPC）内のすべてのリンクをフラップします。 • すべてのポート チャネル リンクをフラップし、ポート チャネルで 1 つのリンクをフラップして、FEX で NIF ポートをフラップし、ラック上部の全面パネル ポートをフラップします。
ファブリック ポリシー	• NTP サーバ、SNMP、BGP ルート リフレクタ、L2 MTU ポリシーを追加、更新、削除します。 • Cisco APIC 接続設定を更新します。

次の定義は、Cisco APIC リリースについて説明するために使用されます。

- Cisco APIC メジャー リリースには、新しいソフトウェア機能およびその他のハードウェアの更新のサポートが含まれています。メジャー リリースの例には、2.2(1n) と 2.1(1h) が含まれます。
- Cisco APIC マイナーまたはメンテナンス リリース（MR）には、バグ修正や既存のリリースからのパッチが含まれています。マイナーまたはメンテナンス リリースの例には、2.0(1m) と 2.0(2f) が含まれます。
- Cisco APIC パッチ リリースには、特定の不具合の修正が含まれています。パッチのリリースの例には、2.1(1h) と 2.1(1i) が含まれます。

Cisco ACI スイッチの混合バージョンで許可される操作



第 7 章

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 （72 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 （75 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（75 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 （76 ページ）				☑
互換性（ターゲット ACI バージョン）（76 ページ）		4.2(4)	☑	☑
互換性（CIMC バージョン） （76 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） （76 ページ）		4.2(4)	☑	☑
互換性（リモート リーフ スイッチ）（76 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） （77 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（77 ページ）			☑	☑
アップグレード前に無効にする必要がある設定 （78 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 （35 ページ）				☑
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 （35 ページ）		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 （36 ページ）				☑
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 （78 ページ）		4.2(4)	☑	☑
APIC ディスク領域の使用状況（F1527、F1528、F1529） （79 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 （80 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 （82 ページ）		5.2(3e)		☑
APIC 間の APIC ファームウェア同期（83 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（83 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）（84 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 （85 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） （86 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） （87 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） （89 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） （90 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）（91 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） （92 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） （93 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） （94 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） （95 ページ）	F3544	5.1(1)	☑	☑
一般的なスケーラビリティの制限値（96 ページ）				☑
重複する VLAN プール （96 ページ）				☑
L3Out MTU の不一致 （97 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 （98 ページ）	CSCvm28482 – 4.1(2) 以降			☑
L3Out の誤ったルート マップ方向（CSCvm75395） （99 ページ）	CSCvm75395 – 4.1(1) 以降			☑
互換性（リモート リーフ スイッチ）（76 ページ）	CSCvs16767 – 14.2(2)			☑
EP Announce バージョンの不一致（CSCvi76161） （99 ページ）	CSCvi76161 – 13.2(2) 以降			☑
Intersight Device Connector をアップグレード中です。 （100 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 （38 ページ）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
```

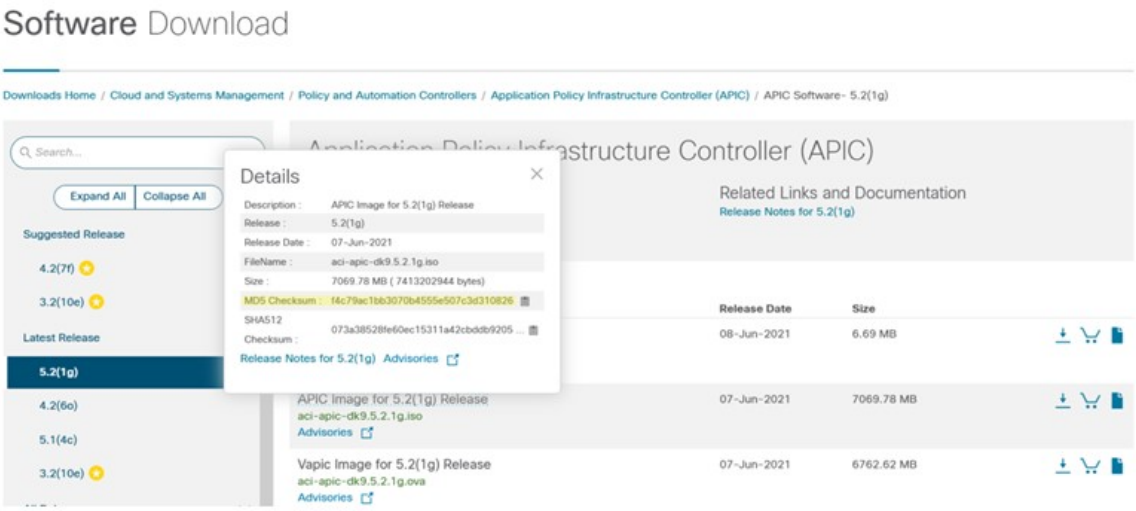
APIC およびスイッチ ファームウェアの MD5sum チェック

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 （107 ページ）
     - 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 （115 ページ）
     - GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ）

- 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）（94 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）（95 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。

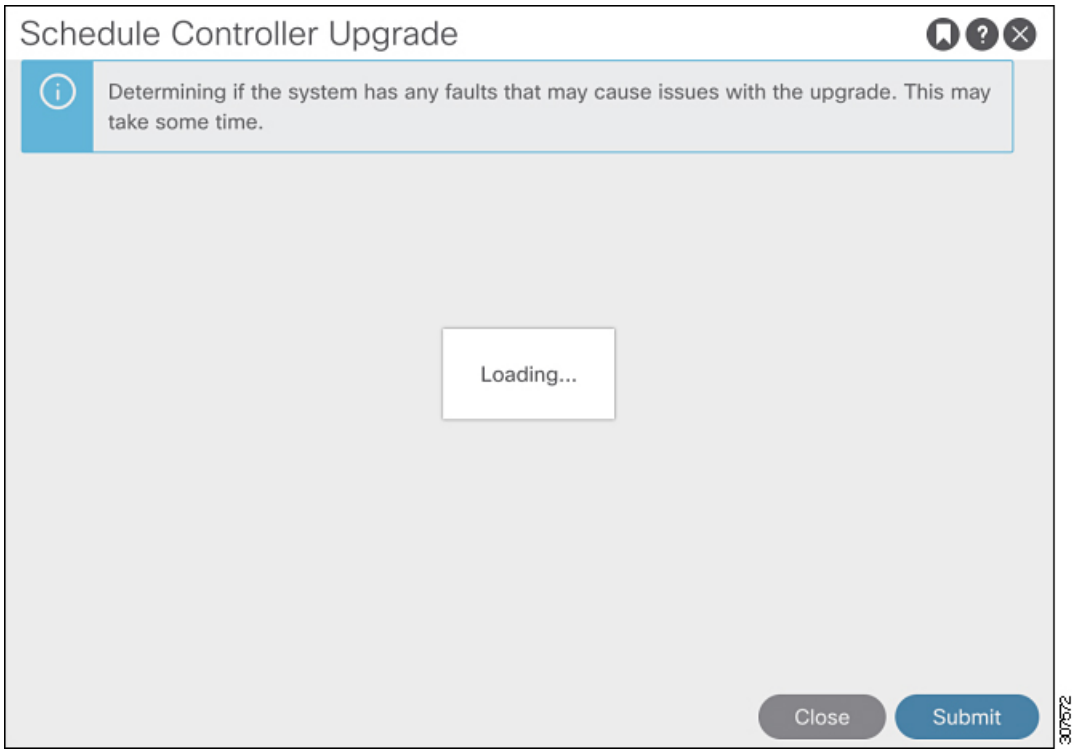
- イメージをダウングレードする前に、Cisco APIC に接続されているサポートされていないリーフ スイッチをデコミッションし、ケーブルをファブリックの一部である他のリーフ スイッチに移動する必要があります。

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

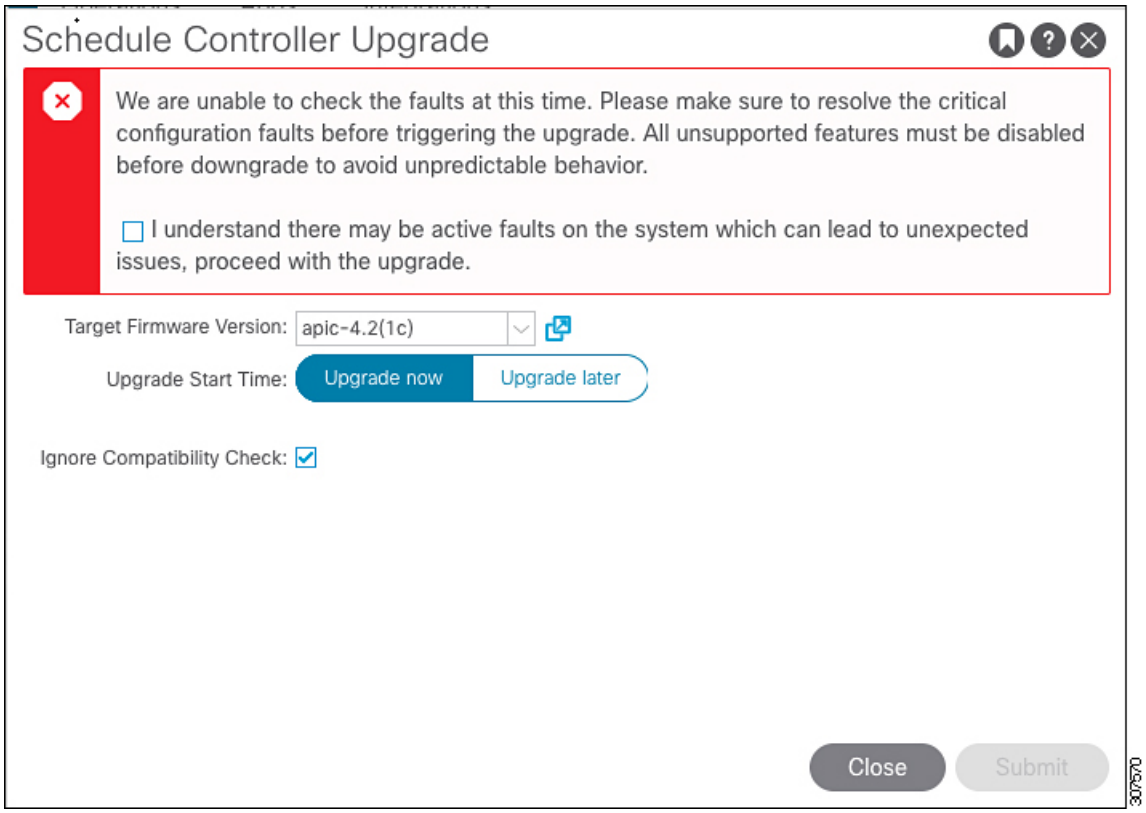
警告メッセージが GUI で表示される場合は、次の 3 つの状況が考えられます。

- 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。

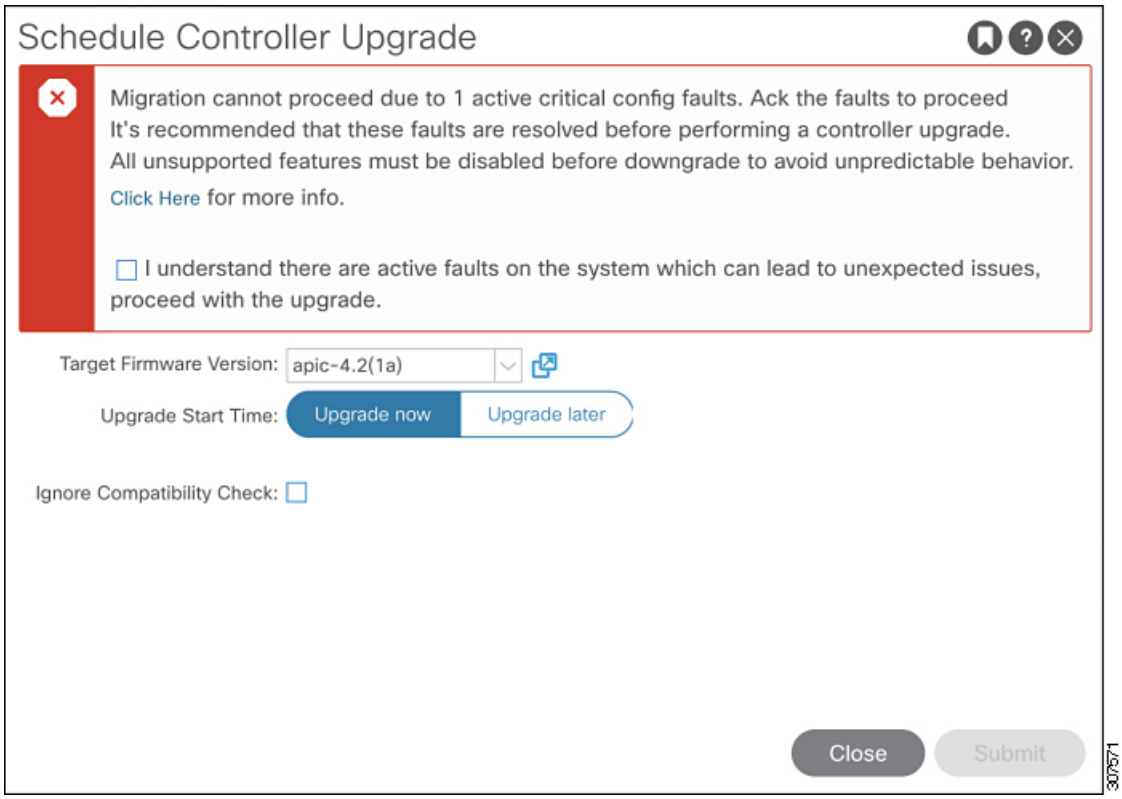
- 何らかの理由でクエリが失敗した場合は、次のようなメッセージが表示されることがあります。



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
```

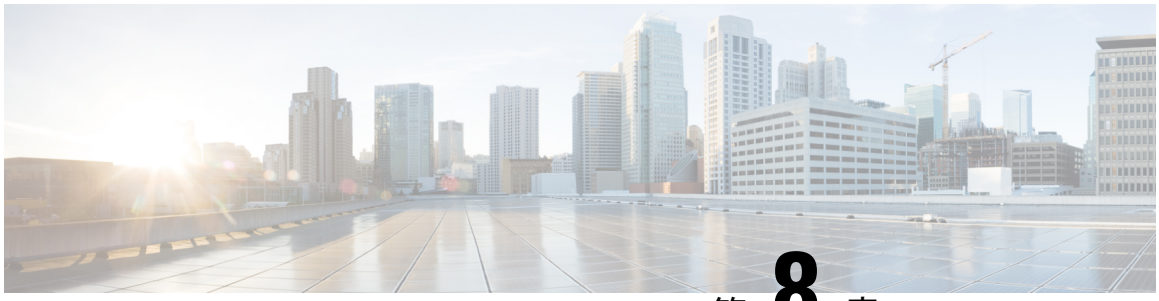
ファブリックの障害が検出された場合は、次のようなエラーメッセージが表示されることがあります。

```
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
```



第 8 章

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

（注） 次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

APIC で APIC とスイッチ イメージをダウンロードする

この手順は、APIC および ACI スイッチのファームウェア イメージを外部ファイル サーバまたはローカル マシンから、PIC のファームウェア レポジトリにダウンローするためのものです。

手順

ステップ 1 メニュー バーで、**[管理 (ADMIN)]** > **[ファームウェア (Firmware)]** を選択し、**[ナビゲーション (Navigation)]** ペインで、**[コントローラ ファームウェア (Controller Firmware)]** をクリックします。
[作業（Work）] ペインの Cisco APIC には、各コントローラにロードされた現在のファームウェアが表示されます。ファームウェアが最後にアップグレードされたときの状態も表示されます。

ステップ 2 **[ナビゲーション (Navigation)]**ペインで、**[ダウンロード タスク (Download Tasks)]** をクリックします。

ステップ 3 **[作業 (Work)]** ペインで、**[全般 (General)]** > **[アクション (Actions)]** を選択し、**[外部ファームウェア ソースの作成 (Create Outside Firmware source)]** をクリックして、次のアクションを実行します。

ステップ 4 **[外部ファームウェア ソースの作成 (Create Outside Firmware source)]** ダイアログ ボックスで、次の操作を実行します。

a) **[ソース名 (Source Name)]** フィールドに、Cisco APIC イメージ ファイルの名前（*apic_image*）を入力します。

b) **[プロトコル (Protocol)]** フィールドで、**[HTTP]** オプション ボタンをクリックします。

（注） http ソースまたはセキュア コピー プロトコル（SCP）ソースからソフトウェア イメージをダウンロードする場合は、該当するオプション ボタンをクリックし、**<SCP サーバ>:/<パス>** の形式を使用します。URL の例としては、**10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso** のようになります。

c) **[URL]** フィールドに、イメージをダウンロードする URL を入力します。**[送信 (Submit)]** をクリックします。

Cisco APIC のファームウェア イメージがダウンロードされるのを待ちます。

ステップ 5 **[ナビゲーション (Navigation)]**ペインで、**[ダウンロード タスク (Download Tasks)]** をクリックします。[Work] ペインで、[Operational] をクリックして、イメージのダウンロード状態を表示します。

[ナビゲーション (Navigation)] ペインで、ダウンロードが 100% に達したら、**[ファームウェア リポジトリ (Firmware Repository)]**をクリックします。

[作業 (Work)] ペインに、ダウンロードされたバージョン番号およびイメージ サイズが表示されます。

リリース 4.x より前のリリースからの Cisco APIC のアップグレード

（注） リリース 4.0 以降にアップグレードする場合は、APIC アップグレードを実行する前に、既存のスイッチ ファームウェアとメンテナンス グループをすべて削除してください。

詳細については、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 （77 ページ）を参照してください。

ファブリック内の APIC のソフトウェアをアップグレードするには、次の GUI ベースのアップグレード手順を使用します。

何らかの理由で、これらのGUIベースのアップグレード手順を使用してファブリック内のAPICのソフトウェアをアップグレードできない場合（新しい注文または製品返品と交換（RMA）を通じて APIC を受け取った場合、GUI を使用してアップグレードを実行するためにファブリックに参加できない場合）、APIC ソフトウェアをアップグレードする代わりに、CIMC を使用してAPICでソフトウェアのクリーンインストールを実行できます。これらの手順については、インストール Cisco APIC 仮想メディアを使用してソフトウェア （15 ページ） を参照してください。

始める前に

次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	**[ナビゲーション (Navigation)]** ペインで、**[コントローラ ファームウェア (Controller Firmware)]** をクリックします。**[作業 (Work)]** ペインで、**[アクション (Actions)]** > **[コントローラ ファームウェア アップグレード ポリシー (Upgrade Controller Firmware Policy)]** を選択します。**[コントローラ ファームウェア アップグレード ポリシー (Upgrade Controller Firmware Policy)]** ダイアログボックスで、次の操作を実行します。	**[ステータス（Status）]** ダイアログボックスに **[変更が保存されました（Changes Saved Successfully）]** というメッセージが表示され、アップグレード プロセスが開始されます。アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。

	コマンドまたはアクション	目的
ステップ 2	**[ナビゲーション (Navigation)]**ペインの **[コントローラ ファームウェア (Controller Firmware)]** をクリックして、アップグレードの状態を **作業 ([Work)]** ペインで確認します。	（注） コントローラのアップグレードはランダムに行われます。Cisco APIC のアップグレードにはそれぞれ約 10 分かかります。コントローラのイメージがアップグレードされると、クラスタからドロップし、新しいバージョンで再起動します。その間、クラスタ内の他の Cisco APIC は動作しています。コントローラが再起動すると、クラスタに再び参加します。その後、クラスタが収束し、次のコントローラのイメージのアップグレードを開始します。クラスタがすぐに収束せず、完全な適合状態にならなければ、その後のアップグレードは、クラスタが収束して完全な適合状態になるまで待機状態になります。この間、アップグレードされる各 Cisco APIC の **[ステータス（Status）]** カラムに**[クラスタ コンバージェンスの待機（Waiting for Cluster Convergence）]**というメッセージが表示されます。 （注） ブラウザが接続されている Cisco APIC がアップグレードされて再起動すると、ブラウザにエラー メッセージが表示されます。
ステップ 3	ブラウザの URL フィールドに、すでにアップグレード済みの Cisco APIC の URL を入力し、プロンプトに応じてその Cisco APIC にサインインしてください。	

リリース 4.x より前の APIC を使用したリーフおよびスパイン スイッチのアップグレード

（注） これは、リリース 4.x より前のリリースで実行されている APIC GUI を使用したスイッチのアップグレード手順です。APIC がすでにバージョン 4.x 以降にアップグレードされている場合、スイッチがリリース 14.x より前のバージョンを実行している場合でも、GUI の手順は異なります。このような場合は、次のような対応するセクションを確認します。

- リリース 4.x または 5.0： 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 （115 ページ）
- リリース 5.1 以降： GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ）

始める前に

次の注意事項を確認し、それに従ってください。

- 全コントローラが新しいファームウェア バージョンにアップグレードされるまで待機してから、スイッチのファームウェアのアップグレードに進みます。
- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

手順

ステップ 1 **ナビゲーション**] ペインで、右クリックして **ファブリック ノード ファームウェア**] をクリックし、 **ファームウェア アップグレード ウィザード** 。
作業] ペインで、 **ファームウェア グループの作成** ダイアログボックスが表示されます。

ステップ 2 [Create Firmware Group] ダイアログボックスで、次の操作を実行します。

a) [Nodes] の下にある [Select All] タブをクリックして、[Selected] 列のファブリック内の全ノードを選択します。[Next] をクリックします。

b) 「Firmware Group] の下にある [Group Name] フィールドにグループ名を入力します。

c) [**互換性チェックを無視する (Ignore Compatibility Check)**] フィールドで、互換性チェック機能を無効にするように特別に指示されていない限り、デフォルトの設定を **オフ** (チェック解除) の設定のままにします。

（注） 次に、ボックスにチェックマークを入力して、互換性チェック機能を無効にする] を選択すると、 互換性の確認を無視 に移動して、システム内で発生する可能性がありますシステムには、サポートされていないアップグレードを加えるのリスクを実行する] フィールドで、使用不可の状態。

d) [Target Firmware Version] フィールドで、ドロップダウン リストから、スイッチをアップグレードするための目的のイメージ バージョンを選択します。[Next] をクリックします。

e) **メンテナンス グループ** 、すべてのスイッチでは 2 つのメンテナンス グループを作成します。たとえば、偶数番号のデバイスを含むグループと、奇数番号のデバイスを含む別のグループを作成します。

（注） 1 つのメンテナンス グループは、同時すべてリーフとスパイン スイッチをアップグレードは、中に推奨してリーフとスパイン スイッチをダウンをソフトウェアの中にすることをファブリック全体を防ぐために複数の (2 つまたは複数) メンテナンスのグループに分割することアップグレードします。リーフとスパイン スイッチでのほぼ同じグループで構成される 2 つ以上のメンテナンス グループにリーフおよびスパイン スイッチを分割することにより、ソフトウェアのアップグレード中に、ファブリックの継続的な動作半分をアップグレードすることによって (以下) ファブリック ノードの一度に 1 つ.

f) [Create Maintenance Group] タブをクリックします。

g) **[メンテナンス グループの作成 (Create Maintenance Group)]** ダイアログ ボックスの **[グループ名 (Group Name)]** フィールドにグループの名前を入力します。

h) [Run mode] フィールドで、デフォルト モードである [Pause only Upon Upgrade Failure] オプション ボタンを選択します。

i) アップグレード操作中に発生するリブート前に、ファブリックからノードを分離する場合は、**[グレースフル メンテナンス（Graceful Maintenance）]** チェックボックスをオンにします。そうすることで、トラフィックはその他利用可能なスイッチにプロアクティブに迂回されます。

j) **[送信 (Submit)]** をクリックします。

k) [Finish] をクリックします。

[Work] ペインに、全スイッチがアップグレードが予定されているファームウェア グループおよびメンテナンス グループの名前とともに表示されます。

ステップ 3 **[Navigation]** ペインで、**[Fabric Node Firmware]** > **[Firmware Groups]**を展開し、作成したファームウェア グループの名前をクリックします。
[Work] ペインに、以前に作成されたファームウェア ポリシーの詳細が表示されます。

ステップ 4 **[Navigation]** ペインで、**[Fabric Node] [ファームウェア** > **[メンテナンス グループ]** を展開し、作成したメンテナンスグループをクリックします。
[Work] ペインに、メンテナンス ポリシーの詳細が表示されます。

ステップ 5 作成したメンテナンス グループを右クリックし、[Upgrade Now] をクリックします。

ステップ 6 [Upgrade Now] ダイアログボックスで、「Do you want to upgrade the maintenance group policy now?」 に対する [Yes] をクリックします。[OK] をクリックします。

（注） [Work] ペインで、[Status] にグループ内の全スイッチが同時にアップグレードされていく状況が表示されます。グループ内のデフォルトの同時実行数は 20 に設定されます。したがって、20 台のスイッチが同時にアップグレードされ、その後また 20 台のスイッチの組がアップグレードされます。ファブリックに仮想ポートチャネル（vPC）構成が存在する場合、アップグレード プロセスでは、同時設定にかかわらず vPC ドメインにある 2 台のスイッチのうち一度に 1 台のスイッチのみがアップグレードされます。障害が発生した場合、スケジューラがサスペンドし、Cisco APIC 管理者の手動操作が必要になります。通常、各スイッチのアップグレードには約 10 分かかります。スイッチはアップグレードすると再起動し、接続が切断されて、クラスタ内のコントローラはグループ内のスイッチとしばらくの間、通信しません。スイッチが起動後にファブリックに再加入した場合、コントローラ ノードから全スイッチが一覧で表示されます。

ステップ 7 [Navigation] ペインで、[Fabric Node Firmware] をクリックします。
[Work] ペインで、一覧表示される全スイッチを確認します。[Current Firmware] 列に、アップグレードイメージの詳細が、各スイッチに対して表示されます。ファブリック内のスイッチが新しいイメージにアップグレードされることを確認します。

リリース 4.x より前の APIC によるカタログのアップグレード

カタログはアップグレード互換性チェックで使用され、**[互換性チェックを無視（Ignore Compatibility Check）]** でオン/オフを切り替えることができます。カタログイメージは APIC イメージに組み込まれ、Cisco APIC イメージがアップグレードされるとアップグレードされます。ただし、何らかの理由でカタログイメージが APIC イメージとともにアップグレードされなかった場合は、カタログを手動でアップグレードするオプションがあります。この手順はめったに使用されず、以降のリリースの APIC GUI では使用できません。

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[Firmware]** を選択します。[Navigation] ペインで、[Catalog Firmware] をクリックします。

ステップ 2 [Work] ペインで、**[Actions]** > **[Change Catalog Firmware Policy]** を選択します。

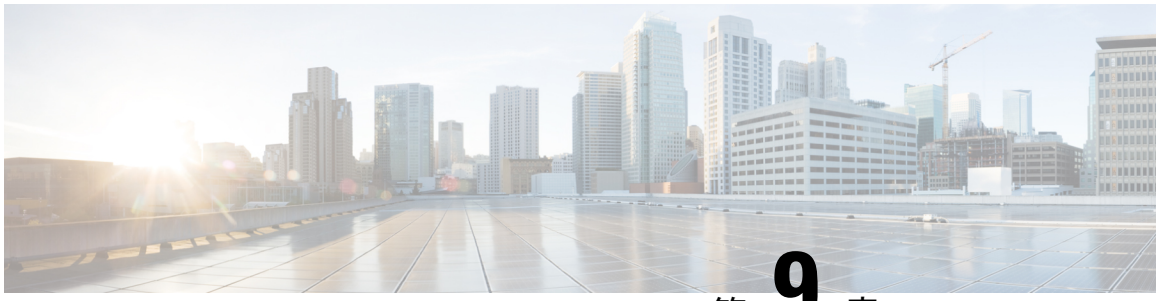
ステップ 3 [Change Catalog Firmware Policy] ダイアログボックスで、次の操作を実行します。

a) [Catalog Version] フィールドで、目的のカタログ ファームウェアの バージョンを選択します。

b) ファームウェアをただちにアップグレードするために、[Apply Policy] フィールドの [Apply Now] オプション ボタンをクリックします。**[送信 (Submit)]** をクリックします。

c) [Work] ペインで、[Target Firmware version] フィールドが [Current Firmware Version] フィールドのイメージ バージョンに一致する画像が表示されるまで待機します。

これでカタログのバージョンが、アップグレードされました。



第 9 章

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

（注） 次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）
- イメージをアップグレードする前に、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。

- APIC で APIC とスイッチ イメージをダウンロードする （115 ページ）
- リリース 4.x または 5.0 からの Cisco APIC のアップグレード （118 ページ）
- リリース 4.x または 5.0 を実行している APIC によるリーフおよびスパイン スイッチのアップグレード （121 ページ）

APIC で APIC とスイッチ イメージをダウンロードする

この手順は、APIC および ACI スイッチのファームウェア イメージを外部ファイル サーバまたはローカル マシンから、PIC のファームウェア レポジトリにダウンローするためのものです。

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
[サマリー（Summary）] ウィンドウが表示され、次の情報が表示されます。

- [ノード（Nodes）] タイル：物理ノードで使用されているファームウェア バージョンに関する情報を提供します。

- [仮想ノード（Virtual Nodes）] タイル：仮想ノードで使用されているファームウェア バージョンに関する情報を提供します。
- [コントローラ（Controller）] タイル：このコントローラで使用されているファームウェア バージョンに関する情報を提供します。カタログのバージョンに関する情報も提供します。
- [コントローラ ストレージ（Controller Storage）] タイル：各コントローラのストレージ容量に関する情報を提供します。

ステップ 2 [イメージ（Images）] タブをクリックし、[アクション（Actions）] アイコンをクリックし、スクロールダウン メニューから [ファームウェアを APIC に追加（Add Firmware to APIC）] を選択します。
[ファームウェアを APIC に追加（Add Firmware to APIC）] ポップアップ ウィンドウが表示されます。

ステップ 3 ファームウェア イメージをローカル ロケーションからインポートするかリモート ロケーションからインポートするかを決めます。

- 「ローカル」ロケーションからファームウェアイメージをインポートする場合は、[ファームウェア イメージの場所（Firmware Image Location）] フィールドの [ローカル（Local）] オプション ボタンをクリックします。[参照...（Browse...）] ボタンをクリックし、インポートするファームウェアイメージがあるローカル システムのフォルダに移動します。ステップ 4 （117 ページ）に進みます。
- 「リモート」ロケーションからファームウェアイメージをインポートする場合は、[ファームウェアイメージの場所（Firmware Image Location）] フィールドの [リモート（Remote）] オプション ボタンをクリックし、次の操作を実行します。

a) [ダウンロード名（Download Name）] フィールドで、スクロールダウン メニューに表示されるオプションを使用して既存のダウンロードを選択するか、 Cisco APIC イメージ ファイルの名前（*apic_image*など）を入力してダウンロードを新しく作成します。

（注） [ダウンロード名（Download Name）] フィールドに既存のダウンロード名を入力してから、フィールドの横にあるゴミ箱アイコンをクリックして、既存のダウンロード タスクを削除することもできます。

新しいダウンロードを作成している場合は下記のフィールドが表示されます。

b) [プロトコル（Protocol）] フィールドで、[HTTP] または [セキュア コピー（Secure copy）] のどちらかのオプション ボタンをクリックします。

c) [URL] フィールドに、イメージのダウンロード元の URL を入力します。

- 前の手順で [HTTP] オプション ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する http ソースを入力します。
- 前の手順で **[セキュア コピー（Secure copy）]** ラジオ ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する Secure Copy Protocol（SCP）ソースを入力します。

HTTP ソースと SCP ソースの両方の形式は次のとおりです。

```
<HTTP/SCP サーバ IP または FQDN>:/<path>/<filename>
```

URL の例は、`10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso` です。

プロトコルとして **SCP** を選択した場合は、次のフィールドが表示されます。

d) [Username] フィールドに、セキュア コピーのユーザ名を入力します。

e) [認証タイプ（Authentication Type）] フィールドで、ダウンロードの認証タイプを選択します。次のタイプを選択できます。

- **パスワードを使用**
- **SSH 公開/秘密キー ファイルを使用**

デフォルトは、[**パスワードの使用 (Use Password)**] です。

f) [パスワードを使用（Use Password）] を選択した場合は、[パスワード（Password）] フィールドにセキュア コピーのパスワードを入力します。

g) **[SSH 公開/秘密キー ファイルを使用（Use SSH Public/Private Key Files）]** を選択した場合は、次の情報を入力します。

- **SSH キーのコンテンツ**: SSH 秘密キーのコンテンツ。
- **SSH キーのフレーズ**: SSH 秘密キーの生成に使用される SSH キー パスフレーズ

（注） 提供された SSH 秘密キーに基づいて、APIC はこのトランザクションのために一時的な SSH 公開キーを内部的に作成し、リモート サーバとの接続を確立します。リモート サーバが「authorized_keys」の 1 つとして対応する公開キーをもつことを確認する必要があります。認証チェックが実行されると、APIC の一時公開キーが削除されます。

次のように入力して、いずれかの APIC で SSH 秘密キー（ー`/.ssh/id_rsa`）および対応する SSH 公開キー（ー`/.ssh/id_rsa.pub`）を生成できます。

```
ssh-keygen -t rsa -b 2048 -C "<username>@<apic_name>"
```

または、別のマシンでそれらを生成できます。いずれの方法の場合も、ダウンロード構成ごとに生成された秘密キーを提供する必要があります。

ステップ 4 **[送信 (Submit)]** をクリックします。
Cisco APIC のファームウェア イメージがダウンロードされるのを待ちます。

ステップ 5 必要に応じて [イメージ（Images）] タブを再度クリックして、イメージのダウンロード ステータスを表示します。

ダウンロードが 100% に達したら、表内でダウンロードしたファームウェア イメージの行をダブルクリックして、その特定ファームウェア イメージの [ファームウェアの詳細（Firmware Details）] ページを表示します。

リリース 4.x または 5.0 からの Cisco APIC のアップグレード

ファブリック内の APIC のソフトウェアをアップグレードするには、次の GUI ベースのアップグレード手順を使用します。

何らかの理由で、これらの GUI ベースのアップグレード手順を使用してファブリック内の APIC のソフトウェアをアップグレードできない場合（新しい注文または製品返品と交換（RMA）を通じて APIC を受け取った場合、GUI を使用してアップグレードを実行するためにファブリックに参加できない場合）、APIC ソフトウェアをアップグレードする代わりに、CIMC を使用して APIC でソフトウェアのクリーンインストールを実行できます。これらの手順については、インストール Cisco APIC 仮想メディアを使用してソフトウェア （15 ページ） を参照してください。

始める前に

次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）
- イメージをアップグレードする前に、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。

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
[サマリー（Summary）] ウィンドウが表示され、次の情報が表示されます。

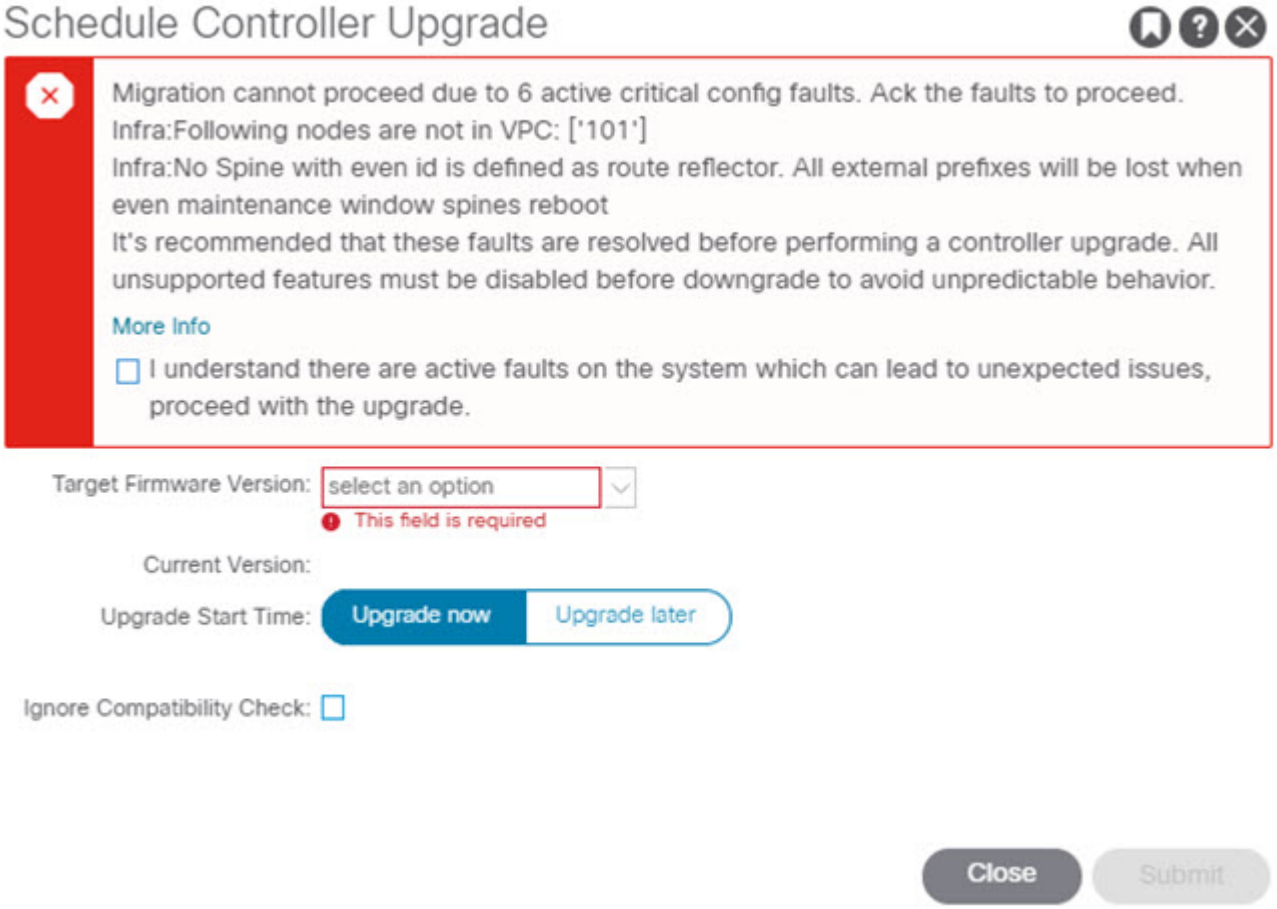
- **[ノード（Nodes）]** タイル：物理ノードで使用されているファームウェア バージョンに関する情報を提供します。
- **[仮想ノード（Virtual Nodes）]** タイル：仮想ノードで使用されているファームウェア バージョンに関する情報を提供します。
- **[コントローラ（Controller）]** タイル：このコントローラで使用されているファームウェア バージョンに関する情報を提供します。カタログのバージョンに関する情報も提供します。
- **[コントローラ ストレージ（Controller Storage）]** タイル：各コントローラのストレージ容量に関する情報を提供します。

ステップ 2 **[インフラストラクチャ（Infrastructure）]** タブをクリックし、**[コントローラ（Controllers）]** サブタブを選択していない場合はクリックして選択します。

ステップ 3 **[アクション（Actions）]>[コントローラ アップグレードのスケジュール（Schedule Controller Upgrade）]** を選択します。

[コントローラ アップグレードのスケジュール（Schedule Controller Upgrade）] ダイアログボックスが表示されます。

場合によっては、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。



お使いのバージョンの APIC アップグレード前検証ツールによってチェックされる項目と、スクリプトを使用するか手動で AppCenter アップグレード前検証ツールを使用して確認する必要があるその他の項目については、アップグレード前のチェックリスト （71 ページ） を参照してください。

ステップ 4 **[コントローラ アップグレードのスケジュール（Schedule Controller Upgrade）]** ダイアログボックスで、次の操作を実行します。

a) **[ターゲットのファームウェア バージョン (Target Firmware Version)]** フィールドで、ドロップダウン リストから、アップグレードするイメージ バージョンを選択します。

b) **[アップグレード開始時刻（Upgrade Start Time）]** フィールドで、2 つのオプション ボタンのいずれかをクリックします。

- **[今すぐアップグレード（Upgrade now）]**
- **[後でアップグレード（Upgrade later）]**：アップグレードを実行する日付と時刻を選択します。

  次に、**[後でアップグレード (Upgrade later)]** フィールドのさまざまなエントリに関連したシナリオの例と、各シナリオでのシステムの反応の例を示します。

  - **[開始時刻 (Start Time)] が現在の時刻より前のポイントに設定された場合**: アップグレードポイントが過去のポイントに設定されていると、システムによって設定が拒否されます。
  - **[開始時刻 (Start Time)] が現在の時刻より 後のポイントに設定された場合**: アップグレードは、設定した時点で開始されます。

c) [**互換性チェックを無視する (Ignore Compatibility Check)**] フィールドで、互換性チェック機能を無効にするように特別に指示されていない限り、デフォルトの設定を **オフ** (チェック解除) の設定のままにします。

（注） 次に、ボックスにチェックマークを入力して、互換性チェック機能を無効にする] を選択すると、 互換性の確認を無視 に移動して、システム内で発生する可能性がありますシステムには、サポートされていないアップグレードを加えるのリスクを実行する] フィールドで、使用不可の状態。

[ステータス（Status）] ダイアログボックスに **[変更が保存されました（Changes Saved Successfully）]** というメッセージが表示され、アップグレードプロセスが開始されます。アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。

ステップ 5 必要に応じて、**[インフラストラクチャ（Infrastructure）]** ペインで **[コントローラ（Controllers）]** サブタブを再度クリックして、アップグレードのステータスを確認します。

コントローラのアップグレードはランダムな順番で行われます。Cisco APIC のアップグレードにはそれぞれ約 10 分かかります。コントローラのイメージがアップグレードされると、クラスタからドロップし、新しいバージョンで再起動します。その間、クラスタ内の他の Cisco APIC は動作しています。コントローラが再起動すると、クラスタに再び参加します。その後、クラスタが収束し、次のコントローラのイメージのアップグレードを開始します。クラスタがすぐに収束せず、適合状態にならない場合、アップグレードはクラスタが収束して完全に正常になるまで延期されます。この間、アップグレードされる各 Cisco APIC の **[ステータス（Status）]** カラムには、**[クラスタ コンバージェンスの待機（Waiting for Cluster Convergence）]** というメッセージが表示されます。

Cisco APIC リリース 4.2(5) 以降では、コントローラのアップグレードプロセスのステータスに関する追加情報が提供される場合があります。APICアップグレードのさまざまな段階の詳細については、APIC のアップグレード段階の説明 （54 ページ） を参照してください。

（注） 実際のアップグレードプロセスは、以前のリリースと同じように、リリース4.2(5)のままです。ただし、リリース4.2(5)以降では、アップグレードプロセス中の段階を示す追加情報が提供されました。

ステップ 6 ブラウザの URL フィールドに、すでにアップグレード済みの Cisco APIC の URL を入力し、プロンプトに応じてその Cisco APIC にサインインしてください。

リリース 4.x または 5.0 を実行している APIC によるリーフおよびスパイン スイッチのアップグレード

（注） これは、リリース 4.x または 5.0 で実行されている APIC GUI を使用したスイッチのアップグレード手順です。APIC がすでにバージョン 5.1 以降にアップグレードされている場合、スイッチがリリース 14.x または 15.0 より前のバージョンを実行している場合でも、GUI の手順は異なります。このような場合は、GUI を使用した APIC リリース 5.1 以降でのアップグレード （127 ページ） などの対応するセクションを確認します。

始める前に

次の注意事項を確認し、それに従ってください。

- 全コントローラが新しいファームウェアバージョンにアップグレードされるまで待機してから、スイッチのファームウェアのアップグレードに進みます。
- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

手順

ステップ 1 作業を進める前に、全コントローラが新しいファームウェアバージョンにアップグレードされていることを確認します。
全コントローラが先に新しいファームウェア バージョンにアップグレードされるまでは、スイッチのファームウェアをアップグレードしないでください。

ステップ 2 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
[サマリー（Summary）] ウィンドウが表示され、次の情報が表示されます。

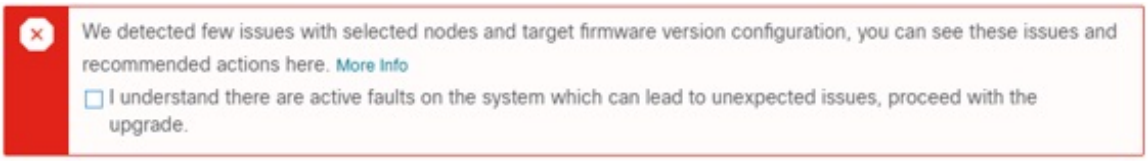
- [ノード（Nodes）] タイル：物理ノードで使用されているファームウェア バージョンに関する情報を提供します。

- [仮想ノード（Virtual Nodes）] タイル：仮想ノードで使用されているファームウェア バージョンに関する情報を提供します。
- [コントローラ（Controller）] タイル：このコントローラで使用されているファームウェア バージョンに関する情報を提供します。カタログのバージョンに関する情報も提供します。
- [コントローラ ストレージ（Controller Storage）] タイル：各コントローラのストレージ容量に関する情報を提供します。

ステップ 3 [Infrastructure] タブをクリックし、[Nodes] サブタブをクリックします。

ステップ 4 [**アクション (Actions)**] をクリックし、[**ノードのアップグレードをスケジュール (Schedule Node Upgrade)**] を選択して、次の操作を実行します。

場合によっては、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。



お使いのバージョンの APIC アップグレード前検証ツールによってチェックされる項目と、スクリプトを使用するか手動で AppCenter アップグレード前検証ツールを使用して確認する必要があるその他の項目については、アップグレード前のチェックリスト （71 ページ） を参照してください。

a) [**グループ タイプ (Group Type)**] フィールドで、[**スイッチ (Switch)**] または [**vPod**] のいずれかを選択します。

b) このフィールドが使用可能な場合は、[**アップグレード グループ (Upgrade Group)**] フィールドで、[**既存 (Existing)**] または [**新規 (New)**] のいずれかを選択します。

リリース 4.1 (2) 以降では、[**アップグレード グループ (Upgrade group)**] フィールドを使用して、既存または新規のアップグレードグループを使用しているかどうかを選択できます。

- [**既存 (existing)**]: 既存のアップグレードグループを使用する場合に選択します。既存のアップグレード グループのプロパティを変更する場合は、この例の [**アップグレード グループ名 (Upgrade Group Name)**] フィールドで既存のアップグレードグループを選択し、このページの残りのフィールドに変更を加えます。
- [**新規 (New)**]: 新しいアップグレード グループを作成する場合に選択します。この場合は、[**アップグレード グループ名 (Upgrade Group name)**] フィールドに新しいアップグレードグループの名前を入力し、このページの残りのフィールドに情報を入力して新しいアップグレード グループを作成します。

c) [**アップグレード グループ名 (Upgrade Group name)**] フィールドで、既存のアップグレードグループのスクロールダウン メニューからアップグレードグループ名を選択するか、新しいアップグレード グループのテキスト ボックスに名前を入力します。

[アップグレード グループ名（Upgrade Group Name）] フィールドで、スクロールダウン メニューに表示されるオプションを使用して既存のアップグレード グループを選択するか、フィールドの隅にある「**x**」をクリックしてフィールドをクリアし、アップグレード グループの名前を入力します

既存のポッド メンテナンス グループを選択した場合は、そのメンテナンス グループに関連付けられているフィールドに自動的に入力されます。

d) サイレント ロール パッケージのアップグレードを実行するかどうかを決定します。

（注） 通常のスイッチ ソフトウェア アップグレードではなく、ACI スイッチ ハードウェア SDK、ドライバなどの内部パッケージのアップグレードを実行する必要がある場合にのみ、[**手動サイレント ロール パッケージ アップグレード (Manual Silent Roll Package Upgrade)**](SR パッケージ アップグレード) を選択します。SR パッケージのアップグレードを実行する場合、メンテナンス グループは SR パッケージのアップグレード専用であり、通常のスイッチ ソフトウェア アップグレードは実行できません。詳細については、サイレント ロール パッケージのアップグレード （175 ページ）を参照してください。

e) [Target Firmware Version] フィールドで、ドロップダウン リストから、スイッチをアップグレードするための目的のイメージ バージョンを選択します。

f) [**互換性チェックを無視する (Ignore Compatibility Check)**] フィールドで、互換性チェック機能を無効にするように特別に指示されていない限り、デフォルトの設定を **オフ** (チェック解除) の設定のままにします。

（注） 次に、ボックスにチェック マークを入力して、互換性チェック機能を無効にする] を選択すると、 互換性の確認を無視 に移動して、システム内で発生する可能性がありますシステムには、サポートされていないアップグレードを加えるのリスクを実行する] フィールドで、使用不可の状態。

g) アップグレード操作中に発生するリブート前に、ファブリックからノードを分離する場合は、**[グレースフル メンテナンス（Graceful Maintenance）]** チェックボックスをオンにします。そうすることで、トラフィックはその他利用可能なスイッチにプロアクティブに迂回されます。

h) [実行モード（Run Mode）] フィールドで、ノード セットのメンテナンス プロセスが正常に完了した後で自動的に次のノード セットに進むための実行モードを選択します。

次のオプションがあります。

- **障害時に一時停止せず、クラスタの状態を待機しない（Do not pause on failure and do not wait on cluster health）**
- **アップグレードの失敗時に一時停止します**

デフォルトは [アップグレードの失敗時のみ一時停止Pause only Upon Upgrade Failure）] です。

i) [**アップグレード開始時刻 (Upgrade Start Time)**] フィールドで、[**今すぐ (Now)**] または [**後でスケジュール (Schedule for Later)**] のいずれかを選択します。

一度にアップグレードできるスイッチの数は、リリースによって異なります。

- リリース 4.2(5) 以前のリリースでは、グループ内のデフォルトの同時実行は 20 に設定されています。したがって、20 台のスイッチが同時にアップグレードされ、その後また 20 台のスイッチの組がアップグレードされます。
- リリース 4.2(5) およびそれ以降では、グループ内のデフォルトの同時実行数が20から無制限 (一度にアップグレードできるリーフまたはスパインスイッチのデフォルト数は無制限) に変更されました。

上記の値は、**[今すぐ（Now）]** と **[後でスケジュール（Schedule for Later）]**の両方に適用されます。

[後でスケジュール (Schedule For Later)] を選択した場合は、既存のトリガー スケジューラを選択するか、または [トリガー スケジューラを作成 (Create trigger scheduler)] をクリックして新しいトリガー スケジューラを作成します。

j) リリース 4.1(2) 以降の場合は、[すべてのノード (All Nodes)] エリアの右側にある [+] アイコンをクリックします。

[アップグレード グループにノードを追加 (Add Nodes to Upgrade Group)] ページが表示されます。

k) **[アップグレード グループにノードを追加 (Add Nodes To Upgrade Group)]** ページ (リリース 4.1 (2) 以降) または **[ノード選択 (Node Selection)**] フィールド (4.1(2) 以前のリリースの場合) で、**[範囲 (Range)]** または **[手動 (Manual)]** を選択します。

- [範囲（Range）] を選択した場合は、[グループ ノード ID（Group Node Ids）] フィールドに範囲を入力します。
- [手動（Manual）]を選択した場合は、選択可能なリーフ スイッチとスパイン スイッチのリストが [すべてのノード（All Nodes）] 領域に表示されます。このアップグレードに含めるノードを選択します。

  表示されるノードは、[グループ タイプ（Group Type）] フィールドで [スイッチ（Switch）] を選択した場合は物理リーフ スイッチおよびスパイン スイッチであり、[Vpod] を選択した場合は仮想リーフ スイッチまたは仮想スパイン スイッチです。

l) **[送信 (Submit)]** をクリックします。

その後、メイン **ファームウェア** のページに戻ります。

Cisco APIC リリース 4.2(5) 以降では、**[作業 (Work)]** ペインに **[ダウンロード進行状況 (download progress)]** フィールドがあります。これにより、ノード アップグレードのファームウェアのダウンロードの進行状況に関するステータスが表示されます。

- ファームウェアのダウンロードが何らかの理由で失敗した場合、**[ダウンロード進行状況 (Download Progress)]** フィールドのステータスに [赤] と表示されます。この場合、ステータスバーの上にカーソルを置くと、エラーポップアップが表示されます。この場合、**[ダウンロード進行状況: ダウンロード失敗 (Download status: download-failed)]** というメッセージが表示されます。

- ファームウェアのダウンロードが成功すると、**[ダウンロード進行状況 (Download Progress)]** フィールドのステータスバーが緑色に変わり、**100%**が表示されます。この場合、ステータスバーの上にカーソルを置くと、**「[ダウンロード進行状況: ダウンロード済み」**というメッセージが表示されます。

また、イメージをダウンロードするための `/firmware` パーティションに十分なスペースがない場合は、この画面に通知が表示されることがあります。`/firmware` パーティションが 75% を超えていないことを確認します。パーティションが 75% を超えている場合は、リポジトリから未使用のファームウェア ファイルを一部削除する必要があります。これは、圧縮されたイメージを保存し、イメージを抽出するための適切なスペースを提供します。

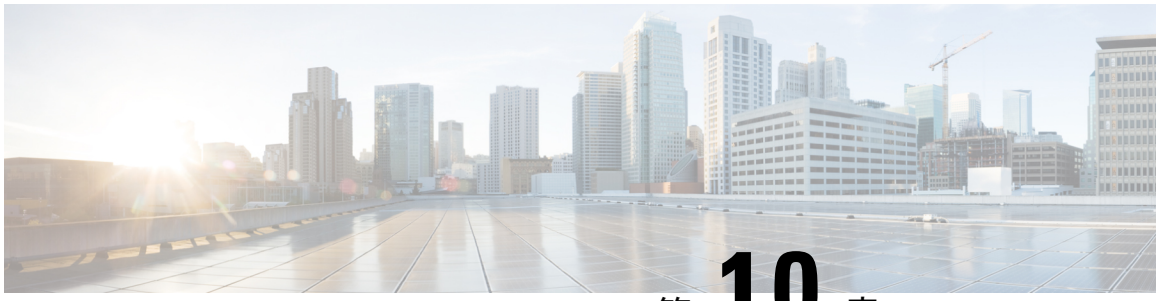
Admin > **Firmware** > **Infrastructure** > **Nodes** の下のテーブルには、各ノードが属しているアップグレードグループを示す **[アップグレードグループ（Upgrade Group）]**（以前はPODメンテナンスグループとして表示されていました）の列があります。特定のノードのこの列を右クリックすると、次のオプションが表示されます。

- アップグレード グループの編集（4.1(2) より前のリリース）
- アップグレード グループの表示（リリース4.1 (2) 以降）
- アップグレード グループの削除（Delete Upgrade Group）

リリース4.1(2)よりも前では、このオプションを使用してアップグレードグループを編集し、ターゲットバージョンを変更してノードのアップグレードをトリガーできます。リリース4.1(2)以降では、この列は既存のアップグレード グループの詳細を表示するためにのみ使用できます。任意のリリースで選択したアップグレード グループを削除できます。

ステップ 5 リリース 4.1 (2) 以降の場合、アップグレード グループからノードを削除するには、次のようにします。

a) アップグレード グループから削除するテーブル内のノードを選択します。
b) [すべてのノード (All Nodes)] エリアの右側にある [ゴミ箱 (trashcan)] アイコンをクリックします。
c) [送信（Submit）] をクリックします。



第 10 章

GUI を使用した APIC リリース 5.1 以降でのアップグレード

（注） 次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）
- リリース 5.1 以降、GUI を使用した ACI ファームウェア アップグレードでは、アップグレード用のスケジューラを設定するオプションは提供されていません。代わりに、スイッチでイメージの事前ダウンロードなどのスケジューラを使用する利点は、すべてネイティブ ワークフローに組み込まれています。
- イメージをアップグレードする前に、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。

ダッシュボードへのアクセス

[Admin] > **[Firmware]** > **[Dashboard]** に移動して、ファブリック内の APIC ノードとスイッチのファームウェア ステータスを示すダッシュボードにアクセスできます。

ダッシュボードには、各 APIC のファームウェア リポジトリの使用状況も表示されます。

APIC で APIC とスイッチ イメージをダウンロードする

この手順は、APIC および ACI スイッチのファームウェア イメージを外部ファイル サーバまたはローカル マシンから、PIC のファームウェア レポジトリにダウンローするためのものです。

手順

ステップ 1 シスコ ソフトウェア ダウンロード サイト（5.2(1g) リリースなど）から目的のターゲット バージョンをファイル サーバまたはローカル マシンにダウンロードします。

ステップ 2 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
ダッシュボード ウィンドウが表示され、コントローラおよびリーフとスパイン スイッチ（ノード）に関する一般情報を示します。

ステップ 3 左側のナビゲーション バーの **イメージ** をクリックします。
[Image] ウィンドウが表示され、以前にダウンロードしたイメージが表示されます。

ステップ 4 **[アクション（Actions）]** アイコンをクリックし、スクロールダウン メニューから **[ファームウェアを追加（Add Firmware]** を選択します。
[ファームウェア イメージを追加（Add Firmware Image）] ポップアップ ウィンドウが表示されます。

ステップ 5 ファームウェア イメージをローカル ロケーションからインポートするかリモート ロケーションからインポートするかを決めます。

- コンピューターからファームウェア イメージをインポートする場合は、**[ロケーション（Location）]** フィールドで、**[ローカル（Local）]** ラジオ ボタンをクリックします。**[ファイルの選択（Choose File）]** ボタンをクリックし、インポートするファームウェア イメージがあるローカル システムのフォルダに移動します。ステップ 6 （129 ページ）に進みます。
- リモート ロケーションからファームウェア イメージをインポートする場合は、リモート ロケーションからファームウェア イメージをインポートするために使用する方法に応じて、**[セキュア コピー（Secure copy）** または **[HTTP]** をクリックします。
  - **[セキュア コピー（Secure copy）]** ラジオ ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する Secure Copy Protocol（SCP）ソースを入力します。
    1. [URL] フィールドに、イメージのダウンロード元の URL を入力します。

       SCP ソースの形式は次のとおりです。

       ```
       <SCP server IP or FQDN>:/<path>/<filename>
       ```

       URL の例は `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso` です。
    2. [Username] フィールドに、セキュア コピーのユーザ名を入力します。
    3. [認証タイプ（Authentication Type）] フィールドで、ダウンロードの認証タイプを選択します。次のタイプを選択できます。

- **[Password]**
- **SSH 公開/秘密ファイル**

デフォルトは、「**Password**」です。

- **[パスワード（Password）]** を選択した場合は、**[パスワード（Password）]** フィールドにセキュア コピーのパスワードを入力します。
- **[SSH 公開/秘密ファイル（SSH Public PrivateFiles）]** を選択した場合は、次の情報を入力します。
  - **Ssh Key Contents**：SSH 秘密キーの内容。
  - **Ssh Key Passphrase**：SSH 秘密キーの生成に使用される SSH キー パスフレーズ。

    （注） 提供された SSH 秘密キーに基づいて、APIC はリモート サーバとの接続を確立するために、このトランザクションのために一時的な SSH 公開キーを内部的に作成します。リモート サーバが「authorized_keys」の 1 つとして対応する公開キーをもつことを確認する必要があります。認証チェックが実行されると、APIC の一時公開キーが削除されます。

  次のように入力して、いずれかの APIC で SSH 秘密キー（~/.ssh/id_rsa）および対応する SSH 公開キー（~/.ssh/id_rsa.pub）を生成できます。

  ```
  ssh-keygen -t rsa -b 2048 -C "<username>@<apic_name>"
  ```

  または、別のマシンでそれらを生成できます。いずれの方法の場合も、ダウンロード構成ごとに生成された秘密キーを提供する必要があります。

- 前の手順で **[HTTP]** オプション ボタンを選択した場合は、ソフトウェア イメージのダウンロードに使用する http ソースを入力します。

  HTTP ソースの形式は次のとおりです。

  ```
  <HTTP server IP or FQDN>:/<path>/<filename>
  ```

  URL の例は `10.1.2.3:/path/to/the/image/aci-apic-dk9.5.0.1a.iso` です。

ステップ 6 **[送信 (Submit)]** をクリックします。

APIC は、設定されたソースから指定されたファームウェア イメージのダウンロードを開始します。ダウンロードの進行状況が **[ダウンロード ステータス（Download Status）]** カラムに表示されます。

リリース 5.1x 以降からの Cisco APIC のアップグレード

ファブリック内の APIC のソフトウェアをアップグレードするには、次の GUI ベースのアップグレード手順を使用します。

何らかの理由で、これらの GUI ベースのアップグレード手順を使用してファブリック内の APIC のソフトウェアをアップグレードできない場合（新しい注文または製品返品と交換（RMA）を通じて APIC を受け取った場合、GUI を使用してアップグレードを実行するためにファブリックに参加できない場合）、APIC ソフトウェアをアップグレードする代わりに、CIMC を使用して APIC でソフトウェアのクリーンインストールを実行できます。これらの手順については、インストール Cisco APIC 仮想メディアを使用してソフトウェア （15 ページ） を参照してください。

始める前に

次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
ダッシュボード ウィンドウが表示され、コントローラおよびリーフとスパインスイッチ（ノード）に関する一般情報を示します。

ステップ 2 左側のナビゲーションウィンドウで、**[コントローラ（Controllers）]**をクリックします。
[コントローラ（Controllers）] ウィンドウが表示され、コントローラのファームウェア情報が示されます。

ステップ 3 **[更新のセットアップ（Setup Update）]** ボタンをクリックします。
[コントローラ ファームウェアの更新のセットアップ（Setup Controller Firmware Upgrade）] ウィンドウの **[バージョン設定（Version Selection）]** ステップが表示され、システムにダウンロードしたすべてのソフトウェア イメージが表示されます。

（注） 代わりに、次のエラー メッセージが表示されます。

```
No firmware images available. Please check the Images tab.
```

アップグレードに使用できるイメージがありません。APIC で APIC とスイッチイメージをダウンロードする （128 ページ） で説明している手順を使用して、アップグレードに使用するイメージを追加します。

ステップ 4 ファームウェアの更新に使用するイメージを選択し、**[次へ（Next)]**をクリックします。
[検証（Validation）] ステップが表示されます。

ステップ 5 **[検証（Validation）]** 画面に表示される情報を確認します。

リリース 5.1(1) 以降では、特定の検証チェックが実行され、**[検証（Validation）]** 画面に表示されます。各検証チェックが成功したか失敗したかを示すメッセージが表示されます。

失敗した検証チェックについては、アップグレードに進む前に、これらの障害または問題に対処することを推奨します。

[検証（Validation）] ウィンドウで発生した障害または問題に対処したら、**[次へ（Next）]** をクリックして **[確認（Confirmation）]** ウィンドウに進みます。

ステップ 6 **[確認（Confirmation）]** ウィンドウで、情報が正しいことを確認し、**[インストールの開始（Begin Install）]** をクリックします。

[コントローラ（Controllers）] ウィンドウが再び表示され、アップグレードのステータスが表示されます。

アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。Cisco APIC のアップグレードにはそれぞれ約 10 分かかります。コントローラのイメージがアップグレードされると、クラスタからドロップし、新しいバージョンで再起動します。その間、クラスタ内の他の Cisco APIC は動作しています。コントローラが再起動すると、クラスタに再び参加します。その後、クラスタが収束し、次のコントローラのイメージのアップグレードを開始します。クラスタがすぐに収束せず、適合状態にならない場合、アップグレードはクラスタが収束して完全に正常になるまで延期されます。この間、アップグレードされる各 Cisco APIC の **[アップグレード ステータス（Upgrade Status）]** カラムに**[クラスタ コンバージェンスの待機（Waiting for Cluster Convergence）]**というメッセージが表示されます。

ブラウザが接続されている APIC がアップグレードされて再起動すると、ブラウザには最初にエラー メッセージが表示されます。その後、この APIC にログインするために使用したブラウザには何も表示されません。ただし、必要に応じて、クラスタ内の残りの APIC にログインして、アップグレード プロセスの進行状況をモニタし続けることができます。

コントローラのアップグレードプロセスのステータスに関する追加情報が提供される場合があります。APICアップグレードのさまざまな段階の詳細については、APIC のアップグレード段階の説明 （54 ページ） を参照してください。

（注） 実際のアップグレードプロセスは、以前のリリースと同じように、リリース 5.1(1) のままです。ただし、リリース 5.1(1) 以降では、アップグレードプロセス中の段階を示す追加情報が提供されました。

ステップ 7 ブラウザの URL フィールドに、すでにアップグレード済みの Cisco APIC の URL を入力し、プロンプトに応じてその Cisco APIC にサインインしてください。

ステップ 8 すべての APIC がアップグレードを完了し、**完全に適合**するまで待ちます。

リリース5.1x以降を実行しているAPICによるリーフおよびスパイン スイッチのアップグレード

リーフおよびスパイン スイッチへのイメージの事前ダウンロード

この手順では、実際のアップグレード（ソフトウェアのインストール）を開始せずに、独自のタイミングでAPICのファームウェア リポジトリからリーフおよびスパイン スイッチにスイッチイメージをダウンロードする方法について説明します。これは事前ダウンロードと呼ばれます。APIC リリース 5.1(1) よりも前では、この操作はスケジューラを介してトリガーする必要がありました。ただし、APIC リリース 5.1(1) 以降では、ネイティブ GUI ワークフローを使用して、スイッチ更新グループを作成し、事前ダウンロードを実行できます。

この操作中、スイッチは稼働したままで、リブートは実行されません。

始める前に

次の注意事項を確認し、それに従ってください。

- 全コントローラが新しいファームウェアバージョンにアップグレードされるまで待機してから、スイッチのファームウェアのアップグレードに進みます。
- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
ダッシュボード ウィンドウが表示され、コントローラおよびリーフとスパインスイッチ（ノード）に関する一般情報を示します。

ステップ 2 左側のナビゲーションウィンドウで、**[ノード（Nodes）]**をクリックします。
[ノード（Nodes）] ウィンドウが表示され、リーフおよびスパイン スイッチのアップグレード グループのファームウェア情報が示されます。

ステップ 3 **[Actions]**アイコンをクリックし、スクロールダウン メニューから**[更新グループの作成（Create Update Group）]**を選択します。
[ノード ファームウェアの更新のセットアップ（Setup Node Firmware Update）] ウィンドウの **[バージョン選択（Version Selection）]** ステップが表示され、システムにダウンロードしたすべてのソフトウェア イメージが表示されます。

ステップ 4 **[バージョンの選択（Version Selection）]** ステップで、アップグレード グループの名前を入力し、ファームウェア アップデートに使用するイメージを選択して、**[次へ（Next）]**をクリックします。

[ノード選択（Node Selection）] ステップが表示されます。

ステップ 5 **[ノード選択（Node Selection）]** ステップで、**[ノードの追加（Add Nodes）]** ボタンをクリックします。
[ノードの選択（Select Nodes）] ステップが表示されます。

ステップ 6 **[ノードの選択（Select Nodes）]** ステップで、このアップグレード グループの一部として含めるノードを選択します。
このウィンドウでは、ノード範囲またはノード名でフィルタリングすることもできます。**[ノード選択（Node Selection）]** ステップが再び表示されます。

ステップ 7 **[ノード選択（Node Selection）]** ステップで、アップグレードするノードがリストされていることを確認します。

このアップグレードグループから削除するノードの行にあるごみ箱アイコンをクリックして、このグループからノードを削除することもできます。

ステップ 8 （任意）次に示す詳細オプションのいずれかが必要な場合は、**[詳細設定（Advanced Settings）]** をクリックして **[詳細設定（Advanced Settings）]** ウィンドウを表示します。

通常、これらの詳細オプションを設定する必要はありません。オプションを無効にするか、デフォルト値を使用することを推奨します。

[詳細設定（Advanced Settings）] ウィンドウで、必要に応じて次のいずれかの操作を実行します。

- **[互換性チェックを無視する (Ignore Compatibility Check)]** フィールドで、互換性チェック機能を無効にするように特別に指示されていない限り、デフォルトの設定を **いいえ** の設定のままにします。

  （注） Cisco APIC イメージに組み込まれているカタログに基づき、現在実行中のバージョンのシステムから、特定の新しいバージョンのアップグレードパスがサポートされているかどうかを確認する互換性チェック機能があります。次に、ボックスにチェック マークを入力して、互換性チェック機能を無効にする] を選択すると、 **互換性の確認を無視** に移動して、システム内で発生する可能性がありますシステムには、サポートされていないアップグレードを加えるのリスクを実行する] フィールドで、使用不可の状態。

- **グレースフル アップグレード（グレースフル チェック）**

  ファームウェアのインストールがトリガーされたときに**グレースフルアップグレード**を実行するには、このオプションを有効にします。

  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 （38 ページ） を参照し、このオプションを有効にする際は必ずガイドラインに従ってください。展開しない場合、アップグレードが失敗することがあります。

- [実行モード（Run Mode）] フィールドで、ノード セットのメンテナンス プロセスが正常に完了した後で自動的に次のノード セットに進むための実行モードを選択します。

  次のオプションがあります。

- **アップグレード失敗時の一時停止**：いずれかのスイッチでアップグレードが失敗した場合、またはAPICクラスタのステータスが完全に適合しなくなった場合（たとえば、すべての APIC 接続リーフ スイッチは同時にアップグレードされます。ACI スイッチ アップグレードの注意事項 （34 ページ） では推奨されていません）、更新グループがスイッチ アップグレードを承認しません。
- **障害時に一時停止せずクラスタの状態で待機しない**：いずれかのスイッチにアップグレードの失敗または一時的な APIC クラスタの問題があったため、更新グループはグループ全体のスイッチ アップグレードを停止しません。

アップグレードする同じグループ内のスイッチのセットを各更新グループにダイナミックに決定するのではなく、1つの更新グループに同時にアップグレードする必要があるスイッチをグループ化することを推奨するため（たとえば、同時容量設定を使用）、**[障害時に一時停止せずクラスタの状態で待機しない（Do not pause on failure and do not wait on cluster health）]** を選択することをお勧めします。このようなベスト プラクティスに従う場合、**[アップグレード障害時の一時停止（Pause On Upgrade Failure）]** はあまり価値がありません。

[詳細設定（Advanced Settings）] ウィンドウでいずれかのアクションの実行が完了したら、**[完了（Done）]** をクリックします。その後、メイン **ファームウェア** のページに戻ります。

ステップ 9 **[ノード選択（Node Selection）]** ステップのすべてが正しいことを確認したら、**[次へ（Next）]** をクリックします。
[検証（Validation）] ステップが表示されます。

ステップ 10 **検証**ステップで提供される情報を確認します。

このページには、アップグレードに影響する可能性のある障害または問題が表示されます。アップグレードを続行する前に、表示される障害または問題に対処することを推奨します。

お使いのバージョンの APIC アップグレード前検証ツールによってチェックされる項目と、スクリプトを使用するか手動で AppCenter アップグレード前検証ツールを使用して確認する必要があるその他の項目については、アップグレード前のチェックリスト （71 ページ） を参照してください。

[検証（Validation）] ステップで発生した障害または問題に対処したら、**[次へ（Next）]** をクリックして **[確認（Confirmation）]** ステップに進みます。

ステップ 11 **[確認（Confirmation）]** ステップで、情報が正しいことを確認し、**[ダウンロードの開始（Begin Download）]** をクリックします。

システムは、前の画面で選択したすべてのノードへのソフトウェアのダウンロードを開始し、各ノードのダウンロード ステータスを表示します。

（注） Cisco APIC リリース 4.2(6) より前のリリースからアップグレードする場合、ダウンロード ステータスはダウンロード中として表示されますが、ダウンロードが完了したことを示す次の段階には進みません。これは、Cisco APIC リリース 4.2(6) よりも前のリリースからアップグレードする場合の既知の問題であり、想定される動作です。リーフおよびスパイン スイッチへのイメージのインストール（136ページ） の手順に従って、ダウンロードが完了したらソフトウェアのインストールプロセスを開始します。

（注） リリース 4.x または 5.0 を実行している APIC によるリーフおよびスパイン スイッチのアップグレード （121 ページ） で説明されている手順を使用して 5.1x より前のリリースから別のアップグレード グループのノードをアップグレードする場合は、以前に次の選択を行いました。

- **[アップグレード開始時刻（Upgrade Start Time）]** フィールドの **[今すぐ（Now）]**
- **[最大実行時間（Maximum Running Time）]** フィールドで **[無制限（unlimited）]**

次の動作が表示される場合があります。

- **最初のアップグレード グループ**：これらの手順で **[ダウンロードの開始（Begin Download）]** をクリックすると、ソフトウェアはイメージのダウンロードを開始し、イメージのダウンロードが完了した後、最初のアップグレード グループのノードにソフトウェアを自動的にインストールします。これは予期しない動作です。
- **2 番目のアップグレード グループ**：これらの手順で **[ダウンロードの開始（Begin Download）]** をクリックすると、イメージのダウンロードが開始されますが、イメージのダウンロードが完了すると、2番目のアップグレード グループのノードにソフトウェアが自動的にインストールされません。これは予想される動作です。次の手順で リーフおよびスパイン スイッチへのイメージのインストール （136 ページ） の情報を使用してソフトウェアをインストールします。

最初のアップグレード グループの動作は予期しないものですが、有害ではありません。最初のアップグレードグループのノードは、このシナリオで自動的に実行されるソフトウェア インストール プロセスの一部としてリブートすることに注意してください。

ステップ 12 グループ内のアップグレードするすべてのノードのダウンロードが正常に完了したことを確認します。

[ステータス（Status）]列に **[失敗（Failed）]** と表示されているノードがある場合は、いくつかのオプションがあります。

- ページの下部にある **[すべて再試行（Retry All）]** をクリックして、アップグレードグループ内のすべてのノードのダウンロードを再試行します。
- ページの下部にある **[すべてキャンセル（Cancel All）]** をクリックして、アップグレードグループ内のノードのダウンロードをキャンセルします。
- ダウンロードフェーズで成功したノードのアップグレードを続行できるように、このアップグレードグループから失敗したノードを手動で削除する場合は、このアップグレードから手動で削除するノードの横にある鉛筆アイコンをクリックします。グループ化して **[削除（Remove）]** をクリックします。

トラブルシューティングについては、ダウンロード障害の一般的な原因 （162 ページ） を参照してください。

グループ内のすべてのノードの **[ダウンロード完了（Download Complete）]**のステータスが表示されると、画面の上部に **[インストール準備完了（Ready to Install）]** と表示されます。

リーフおよびスパイン スイッチへのイメージのインストール

すべてのスイッチで事前ダウンロードが完了し、アップグレード ステータスが **[インストール準備完了（Ready to Install）]** になったら、アップグレードをトリガーする手順を実行して、ファームウェアをインストールし、スイッチをリブートできます。

通常、この手順の数時間または数日前にダウンロードを実行します。アップグレード前の検証はダウンロード前に実行されているため、検証に違反していないことを確認してください。この時点でアップグレード前の検証を再度実行する場合は、App Center のアップグレード前の検証ツールまたはスクリプトを使用します。これは、APIC の組み込みのアップグレード前の検証ツールによってスイッチ イメージが再ダウンロードされるためです。

始める前に

次の注意事項を確認し、それに従ってください。

- Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
- アップグレード前のチェックリスト （71 ページ）
- アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）

最初に、リーフおよびスパイン スイッチへのイメージの事前ダウンロード （132 ページ） で事前ダウンロード手順を完了する必要があります。

手順

ステップ 1 アップグレードプロセスの一部としてノードをリブートできるメンテナンスウィンドウがある場合は、**[すべてインストール（Install All）]**をクリックしてソフトウェアのインストールを開始します。

[ノード ファームの更新（Node Firmware Update）] ウィンドウで、アップグレードグループ内のノードのアップグレードの進行状況をモニタできます。このウィンドウを閉じ、左側のナビゲーションウィンドウで **[ノード（Nodes）]** をクリックして、テーブルの **[ステータス（Status）]** 列でアップグレードグループの全体的なステータスを確認することもできます。

ステップ 2 すべてのノードのステータスが **[完了済み（Completed）]** になったら、**[完了（Done）]** をクリックし、次の更新グループに進みます。

アプリケーションのインストール動作について

特定のアプリケーションはAPICにインストールでき、App Center（https://dcappcenter.cisco.com/）からダウンロードできます。これらのアプリケーションは、次の2つのカテゴリに分類されます。

- **ユーザがインストールしたアプリケーション**：App Center から手動でダウンロードし、APIC にアップロードするアプリケーション。
- **事前にパッケージ化されたアプリケーション**：プラグイン ハンドラによって APIC に自動的にインストールされるアプリケーション。

REST API または APIC GUI を使用してアプリケーションをインストールできます。

- REST API を使用してアプリケーションをインストールするには、次の例のような XML を使用して投稿を送信します。ダウンロードタスクのトリガー時に選択するプロトコルは、アプリケーション イメージをホストするファイル サーバによって異なります。次のポストは、プロトコルが SCP である例を示しています。

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="MY-APP" proto="scp" url="URL:PATH-TO-APP-IMAGE"
user="MY-USER-NAME" password="MY-PASSWORD"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

次の例は、プロトコルが HTTP である同様の投稿を示しています。

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
    <fabricInst>
        <firmwareRepoP>
            <firmwareOSource name="httpuploadapp" proto="http"
url="{{downloadserver}}/{{filename}}" status="created,modified"/>
        </firmwareRepoP>
    </fabricInst>
</polUni>
```

- APIC GUI を使用してアプリケーションをインストールするには：
  - 5.2 より前の APIC リリースの場合：
    1. **[管理（Admin）]** > **[ダウンロード（Downloads）]**をクリックします。

       [ダウンロード（Downloads）] 画面が表示されます。
    2. **[ダウンロード（Downloads）]** 作業ウィンドウの右端にある **[タスク（Task）]** アイコン（）をクリックし、**[APIC にファイルを追加する（Add File to APIC）]** を選択します。

[ルールの追加（Rule User）] ダイアログが表示されます。

3. **[ダウンロード名（Download Name）]** フィールドにダウンロードファイルの名前を入力します。
4. **[プロトコル（Protocol）]** フィールドで、**[安全なコピー（Secure Copy）]** を選択します。
5. **[URL]** フィールドに、ダウンロード ファイル イメージの場所へのパスを入力します。
6. ユーザ名とパスワードを**[ユーザ名（Username）]**および**[パスワード（Password）]** フィールドに入力し、**[送信（Submit）]** をクリックします。
7. **[操作（Operational）]** タブをクリックし、**[ダウンロード（Downloads）]** 作業ウィンドウの右端にある **[更新（Refresh）]** アイコン（）をクリックしてステータスを確認します。

   ダウンロードすると、アプリケーションが自動的にインストールされます。これはおよそ 5 分で完了します。

• APIC リリース 5.2 以降の場合：

1. **[アプリケーション（Apps）]**>**[ダウンロード（Downloads）]**をクリックします。

   [ダウンロード（Downloads）] 画面が表示されます。
2. **[ダウンロード（Downloads）]** 作業ウィンドウの右端にある **[タスク（Task）]** アイコン（）をクリックし、**[APIC にファイルを追加する（Add File to APIC）]** を選択します。

   [ルールの追加（Rule User）] ダイアログが表示されます。
3. **[ダウンロード名（Download Name）]** フィールドにダウンロードファイルの名前を入力します。
4. **[プロトコル（Protocol）]** フィールドで、**[安全なコピー（Secure Copy）]** を選択します。
5. **[URL]** フィールドに、ダウンロード ファイル イメージの場所へのパスを入力します。
6. ユーザ名とパスワードを**[ユーザ名（Username）]**および**[パスワード（Password）]** フィールドに入力し、**[送信（Submit）]** をクリックします。
7. **[操作（Operational）]** タブをクリックし、**[ダウンロード（Downloads）]** 作業ウィンドウの右端にある **[更新（Refresh）]** アイコン（）をクリックしてステータスを確認します。

   ダウンロードすると、アプリケーションが自動的にインストールされます。これはおよそ 5 分で完了します。

APIC の App Center からアプリケーションをインストールする場合、そのアプリケーションのインストール時の動作は、いくつかの要因によって異なります。

- アプリケーションが、**ユーザがインストールしたアプリケーション**であるか、**事前にパッケージ化されたアプリケーション**であるか
- APIC のアプリケーションの新規インストール、アップグレード、またはダウングレードのいずれであるか

ユーザがインストールしたアプリケーション

通常は APIC に事前インストールされていないアプリケーションを手動でインストールする場合、そのインストールに関する動作は次の状況によって異なります。

- APIC にこのアプリケーションがまだインストールされていない場合、これは新規インストールと見なされ、アプリケーションは通常の方法で APIC にインストールされます。
- このアプリケーションがすでに APIC にインストールされており、現在 APIC にインストールされているアプリケーションが**以前**のバージョンのアプリケーションである場合、この新しいバージョンのアプリケーションを APIC にアップロードすると、APIC でアプリケーションがアップグレードされます。
- APIC にこのアプリケーションがすでにインストールされており、APIC に現在インストールされているアプリケーションが**新しい**バージョンである場合は、この以前のバージョンのアプリケーションを APIC にアップロードすると、APIC でアプリケーションのダウングレードがトリガーされます。

Pre-Packaged Apps

クラスタ内のすべての APIC を新しい APIC イメージにアップグレードすると、プラグイン ハンドラは、新しい APIC イメージに付属する事前にパッケージ化されたアプリケーション イメージをチェックします。

- 新しい APIC イメージでアプリケーションが使用可能であることをプラグイン ハンドラが検出したが、そのアプリケーションが現在 APIC にインストールされていない場合、プラグインハンドラは APIC でそのアプリケーションのインストールをトリガーします。
- 新しい APIC イメージでアプリケーションが使用可能で、そのアプリケーションがすでに APIC にインストールされていることをプラグイン ハンドラが検出した場合、プラグイン ハンドラは、新しい APIC イメージで使用可能なアプリケーションが APIC に現在インストールされているアプリケーションであるか確認します。
  - 新しい APIC イメージ内のアプリケーションのバージョンが、現在 APIC にインストールされているアプリケーションより**新しい**リリースである場合、プラグインハンドラは APIC でそのアプリケーションのアップグレードをトリガーします。リリース 5.2(3) 以降、事前にパッケージ化されたアプリは、APIC がアップグレードされる前に、そのセットアップ時に実行されていたアプリのバージョンに関係なく、すべての APIC がセットアップでアップグレードされた後、APIC イメージにバンドルされている任意のアプリイメージにアップグレードされます。

- 新しいAPICイメージ内のアプリケーションのバージョンが、APICに現在インストールされているアプリケーションよりも前のリリースである場合、プラグインハンドラはAPIC上のアプリケーションに対してアクションを実行しません。プラグインハンドラは、新しいAPICイメージで使用可能な以前のバージョンにAPICのアプリケーションをダウングレードしません。これは、新しいバージョンのアプリケーションをインストールできるようにするためです。インストールするアプリケーションのバージョンは、APICイメージが事前にパッケージ化されたバージョンよりも新しい場合があり、プラグインハンドラは以前のバージョンのAPICに現在インストールされているアプリケーションの新しいバージョンに自動的にを上書きしません。

たとえば、クラスタ内のAPICがリリースバージョン1.2(3)で実行されており、APICリリース1.2(3)で事前にパッケージ化されたアプリケーション**AcmeApp**が使用可能であると仮定します。4.5(6)はリリース1.2(3)で実行されているAPICで通常の事前パッケージ化されているAcmeAppのバージョンです。

後日AcmeAppをアップグレードし、AcmeAppの最新バージョン（AcmeAppの4.6(1)バージョン）をApp Centerで入手できるとします。APICとAcmeAppが次のバージョンになるように、AcmeAppの最新バージョンを手動でダウンロードしてインストールします。

- クラスタ内のAPICは、APICリリース1.2(3)でまだ実行中です。
- これらのAPICのAcmeAppがAcmeAppバージョン4.6(1)に更新されました。

後日、APICをリリース1.2(3)からリリース1.2(4)にアップグレードするとします。ただし、1.2(4)で稼働するAPICの場合、通常事前パッケージ化されているAcmeAppのバージョンは4.5(7)です。この場合、APICには通常APICリリース1.2(4)で事前パッケージ化されている4.5(7)以降のバージョン4.6で実行されているAcmeAppのバージョンがあるため、プラグインハンドラはAPICで実行されているAcmeAppのバージョンに変更を加えません。

事前にパッケージ化されたアプリケーションのアプリケーションポリシーを変更できることに注意してください。

- REST APIでは、次の3つのオプションのいずれかを使用して`apPrepackagedPlugins MO`を変更することで、事前にパッケージ化されたアプリケーションのアプリケーション ポリシーを変更できます。
  - **install-all**：これはデフォルト値です。このオプションは、前述の方法で事前にパッケージ化されたアプリケーションをインストールまたはアップグレードします。

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="install-all"/>
  </apPluginPolContainer>
</polUni>
```

  - **remove-all**：このオプションは、事前にパッケージ化されたすべてのアプリケーションをAPICから削除します。

```
POST {{apic-url}}/api/policymgr/mo/.xml
```

```
<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="remove-all"/>
  </apPluginPolContainer>
</polUni>
```

- **skip-installation**：このオプションは、将来の APIC イメージのアップグレードでプラグイン ハンドラが自動的にインストールまたはアップグレードするのを無効にします。

```
POST {{apic-url}}/api/policymgr/mo/.xml

<polUni>
  <apPluginPolContainer>
      <apPrepackagedPlugins PrepackagedAppsAction="skip-installation"/>
  </apPluginPolContainer>
</polUni>
```

- APIC GUI を使用します。

1. **[アプリケーション（Apps）]** > **[インストールされたアプリケーション（Installed Apps）]**に移動します。

   [Apps] ページが表示されます。

2. **[設定（Settings）]** アイコン（🛠）をクリックし、**[事前パッケージ化されたアプリケーション ポリシーの変更（Change Prepackaged Apps Policy）]** を選択します。

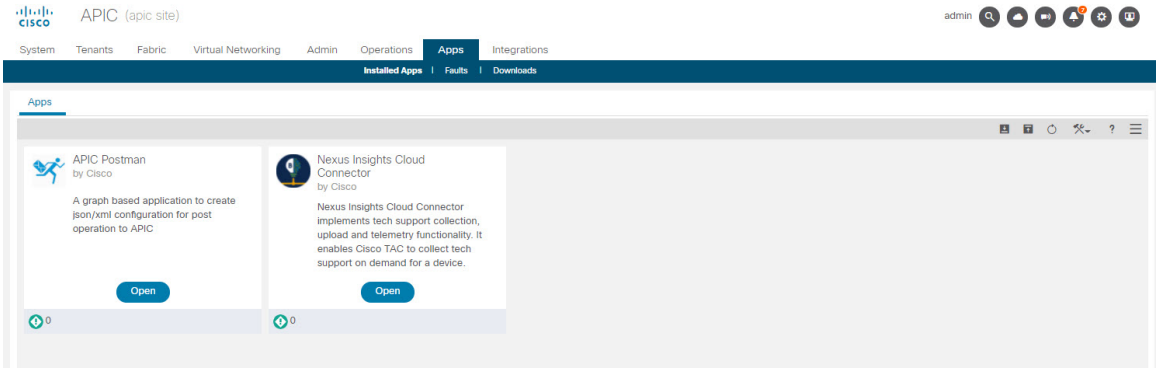
   [事前パッケージ化されたアプリケーション ポリシー（Prepackaged Apps Policy）] ページが表示されます。

3. 次のオプションのいずれかを選択します（上記の REST API 情報のオプションの説明を参照）。

   - すべてインストール
   - すべて削除
   - インストールをスキップ

非表示の事前パッケージ済みアプリケーションの使用

ユーザがインストールしたアプリケーションでも、事前にパッケージ化されたアプリケーションでも、インストールするアプリケーションについては、通常、**[アプリケーション（App）][インストールされているアプリケーション（Installed Apps）]** に移動して表示される APIC GUI の **[アプリケーション（Apps）]** ウィンドウにそのアプリケーションが表示されます。



このウィンドウに表示されるアプリケーションに対して、それらのアプリケーションを開く、有効にする、削除するなどの特定のアクションを実行できます。

ただし、APIC GUI の **[アプリケーション（Apps）]** ウィンドウに表示されない、事前にパッケージ化された特定のアプリケーション（リリース 5.2(1) 以降で使用可能になった ApicVision アプリケーションなど）があります。これらの非表示のアプリケーションは **[アプリケーション（Apps）]** ウィンドウには表示されませんが、そのアプリケーションに問題がある場合（[アプリケーション（Apps）] **[障害（Faults）]**）は、**[障害（Faults）]** ウィンドウに表示されることがあります。

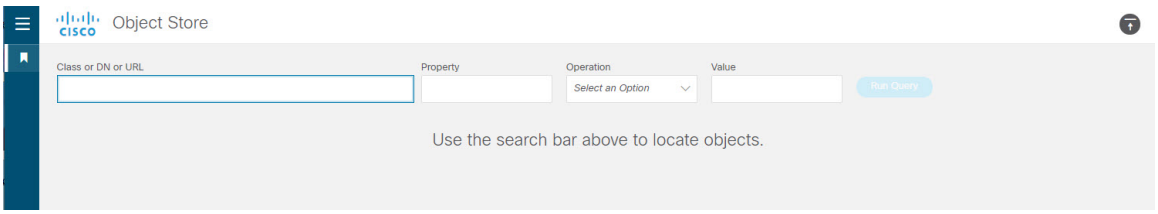
（注） リリース 5.2(1) で使用可能になった、事前にパッケージ化された ApicVision アプリは、App Store からダウンロードできません。そのため、ApicVision アプリを変更したり、削除したりしないでください。事前にパッケージ化された ApicVision アプリに問題や障害がある場合は、Cisco TAC サポートにお問い合わせください。

管理対象オブジェクト（MO）を直接クエリするために使用できる APIC オブジェクト ストア ブラウザである Visore を使用して、これらの非表示の事前パッケージ アプリケーションを検索して操作できます。Visore の詳細については、『アプリケーション ポリシー インフラストラクチャ コントローラ *Visore* ツール紹介』を参照してください。

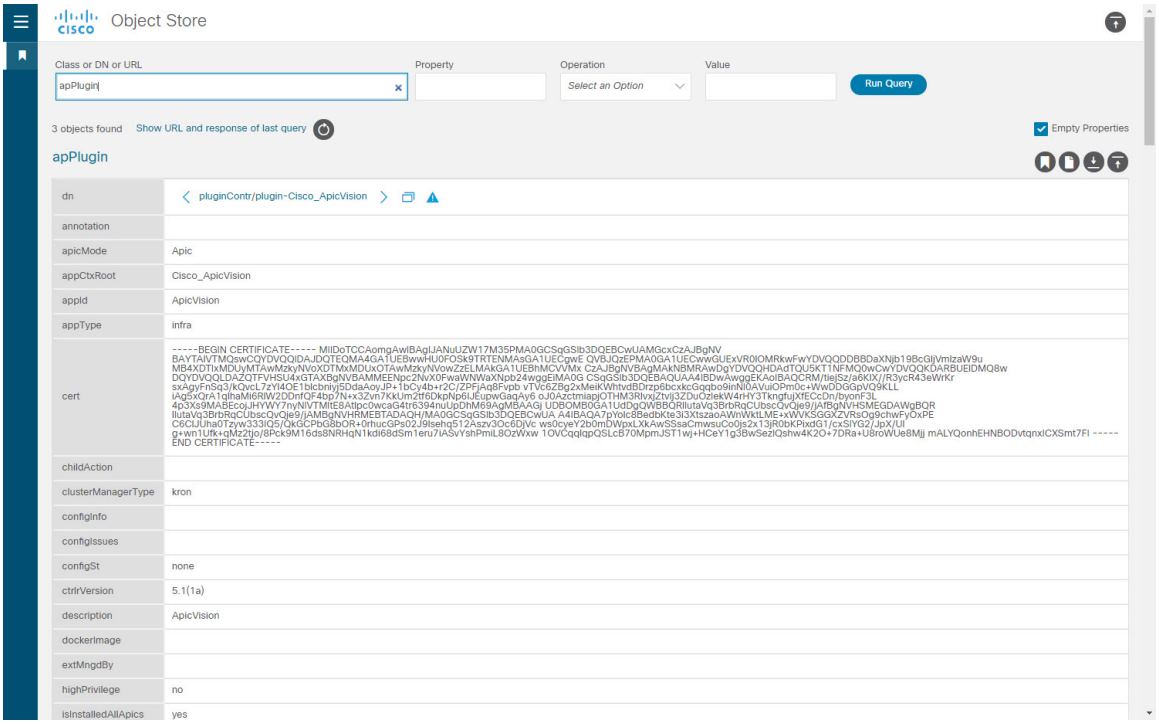
Visore にアクセスするには、APIC GUI へのログインに通常使用する URL に `/visore.html` を追加します。

```
https://<APIC or Switch IP ADDRESS>/visore.html
```

Visore にログインすると、[オブジェクト ストア（Object Store）] ウィンドウが表示されます。



そこから、[クラスまたは DN または URL（Class or DN or URL）] フィールドに **apPlugin** と入力し、**[クエリの実行（Run Query）]** をクリックすることで、APIC にインストールされているアプリケーションの MO をクエリできます。Visore は、この MO で検出されたオブジェクトの数を示す出力を返します。これは、通常の APIC GUI の **[アプリケーション（Apps）]** ウィンドウに表示されない非表示のアプリケーションを含む、APIC にインストールされているアプリケーションの合計数です。



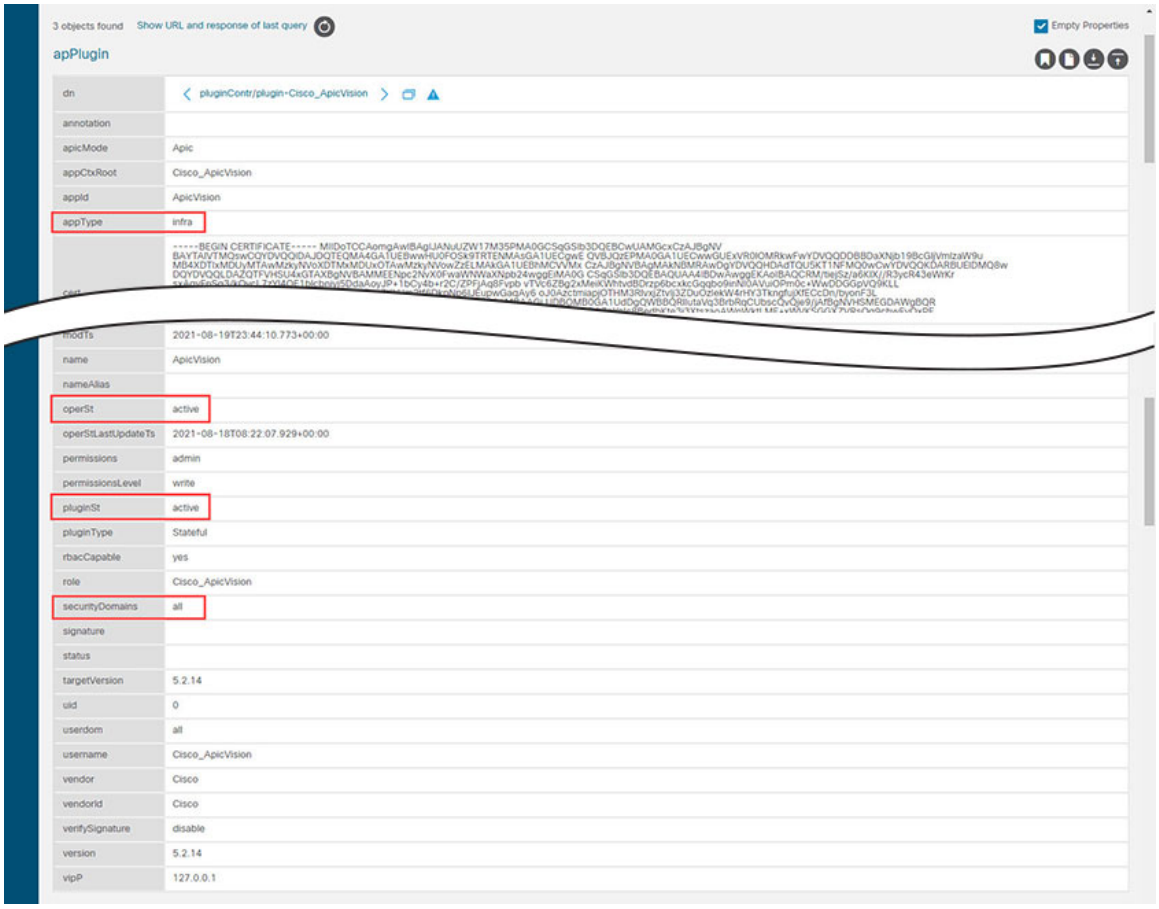
たとえば、上記の例の **[アプリケーション（Apps）]** ウィンドウに表示される情報には 2 つのアプリケーションがインストールされていますが、Visore の `apPlugin` クエリから返される情報には、アプリケーション MO で見つかった 3 つのオブジェクトが表示されます。アプリケーションの 2 つのリストを比較すると、ApicVision アプリは通常の APIC GUI の **[アプリ（Apps）]** ウィンドウには表示されず、Visore の出力に表示されるため、ApicVision アプリは事前にパッケージ化された非表示のアプリです。

Visore の出力に表示される特定のフィールド（アプリケーションの目的の状態を示す **pluginSt** フィールドや、アプリケーションの動作状態を示す **operSt** フィールドなど）を使用して、この非表示の事前パッケージ アプリケーションに関する詳細情報を取得できるようになりました。

たとえば、次のように表示される場合は、アプリケーションが稼働中であることを確認できます。

- このアプリケーションの障害は、**[障害（Faults）]** ウィンドウ（**[アプリケーション（Apps）]** > **[障害（Faults）]**）に表示されません。
- **[operSt]** フィールドの状態はアクティブとして表示されます。
- **[pluginSt]** フィールドの状態はアクティブとして表示されます。

さらに、アプリケーションを有効にするときにセキュリティ ドメインを選択する必要があります。また、以下で説明するように、アプリケーションを有効にすると、**securityDomains** フィールドにその値が入力されます（apPlugin MO のインスタンスの **pluginSt** フィールドを `active` に設定した場合）。プラグイン ハンドラは、インフラ アプリケーションのセキュリティ ドメインとして `all` を選択します（apPlugin MO インスタンスの `[appType]` フィールドで **[インフラ（infra）]** に設定されているアプリケーションの場合）。



これらの非表示のアプリケーションは、通常の APIC GUI の **[アプリケーション（Apps）]** ウィンドウでは表示できないため、APIC GUI を使用して非表示のアプリケーションを開いたり、有効にしたり、削除したりするなどの特定のアクションを実行できません。ただし、REST API を使用して非表示のアプリケーションで次のアクションを実行できます。

- 非表示のアプリケーションを有効にするには、次の例のような XML を使用して投稿を送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="active"
securityDomains="{{security-domains}}"/>
</apPluginContr>
```

ここで、pluginSt がアクティブになります。

- 非表示のアプリケーションを無効にするには、次の例のように XML を使用して投稿を送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/plgnhandler/mo/.xml -->
<apPluginContr>
    <apPlugin appCtxRoot="{{vendordomain}}_{{appid}}" pluginSt="inactive"/>
</apPluginContr>
```

ここで、pluginSt は非アクティブです。

次の点に注意してください。

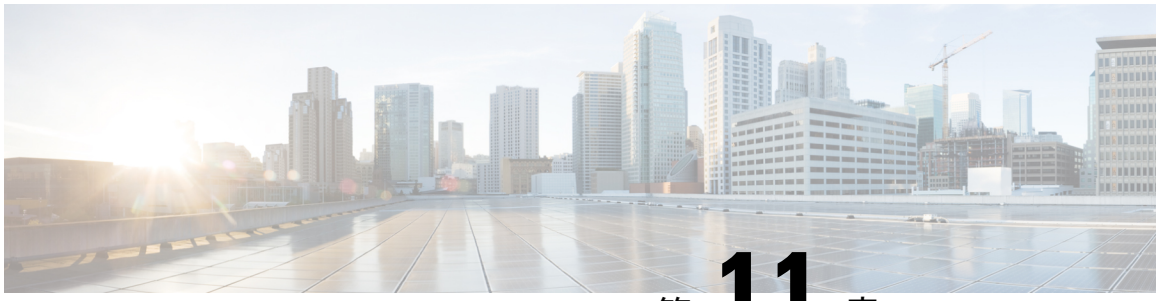
- 非表示のアプリケーションを無効にする場合、セキュリティドメインは必要ありません。
- 上記のいずれかの投稿のアプリケーションの appCtxRoot 値を検索するには、apPlugin MO のインスタンスを照会し、対象のアプリケーションに対応する apPlugin MO のインスタンスの appCtxRoot フィールドのエントリを使用します。

  この情報を取得するには、管理ユーザとして ssh を使用して APIC にログインし、moquery -c apPlugin | grep appCtxRoot コマンドを入力します。

```
# moquery -c apPlugin | grep appCtxRoot
appCtxRoot           : Cisco_NIBASE
appCtxRoot           : Cisco_ApicVision
```

- 非表示のアプリケーションを削除するには、次の例のように XML を使用して投稿を送信します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/node/mo/.xml -->
<firmwareRepo>
    <firmwareFirmware name="{{vendordomain}}_{{appid}}" deleteIt="true"/>
</firmwareRepo>
```



第 11 章

REST API を使用したソフトウェアのアップグレード

REST API を使用して、ソフトウェアをアップグレードすることができます。

REST API を使用した Cisco APIC ソフトウェアのアップグレード

手順

ステップ 1 リポジトリに Cisco APIC イメージをダウンロードします。

例：

```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="APIC_Image_download" proto="http" url="http://<ip
address>/<ver-no>"/>
</firmwareRepoP>
```

ステップ 2 コントローラの目的のバージョンを設定するには、次のポリシーを POST 送信します。

例：

```
POST URL: https://<ip address>/api/node/mo/uni/controller.xml
<firmwareCtrlrFwP
    version="<ver-no>"
    ignoreCompat="true">
</firmwareCtrlrFwP>
```

ステップ 3 コントローラのアップグレードをただちに起動する次のポリシーを POST 送信します。

例：

```
POST URL : https://<ip address>/api/node/mo/uni/controller.xml
<maintCtrlrMaintP
    adminState="up" adminSt="triggered">
</maintCtrlrMaintP>
```

REST API を使用したスイッチ ソフトウェアのアップグレード

手順

ステップ 1 リポジトリにスイッチ イメージをダウンロードします。

例：

```
POST URL: https://<ip address>/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http" url="http://<ip
address>/<ver-no>"/>
</firmwareRepoP>
```

ステップ 2 ソフトウェア リリースに応じて、必要なノード ID を持つファームウェア グループとメンテナンス グループを作成するための適切なポリシーを投稿します。

- リリース 4.0(1) 以前のリリースの場合、次のポリシーを、POST 送信することにより、ノード ID が 101、102、103、104 の スイッチから構成されるファームウェア グループを作成し、ノード ID 101、102、103、104 によるメンテナンス グループを作成します。

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
<firmwareFwP
    name="AllswitchesFwP"
    version="<ver-no>"
    ignoreCompat="true">
</firmwareFwP>

<firmwareFwGrp
    name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
```

```
<firmwareRsFwgrpp
    tnFirmwareFwPName="AllswitchesFwP">
</firmwareRsFwgrpp>
</firmwareFwGrp>

<maintMaintP
    name="AllswitchesMaintP"
    runMode="pauseOnlyOnFailures" >
</maintMaintP>

<maintMaintGrp
    name="AllswitchesMaintGrp">
        <fabricNodeBlk name="Blk101"
            from_="101" to_="101">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk102"
            from_="102" to_="102">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk103"
            from_="103" to_="103">
        </fabricNodeBlk>
        <fabricNodeBlk name="Blk104"
            from_="104" to_="104">
        </fabricNodeBlk>
<maintRsMgrpp
    tnMaintMaintPName="AllswitchesMaintP">
</maintRsMgrpp>
</maintMaintGrp>
</fabricInst>
```

- リリース 4.0(1) 以降のリリースの場合、次のポリシーを、POST 送信することにより、ノード ID が 101、102、103、104 の スイッチから構成されるファームウェア グループを作成し、ノード ID 101、102、103、104 によるメンテナンス グループを作成します。

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<fabricInst>
       <maintMaintP
              version="<ver-no>"
              name="AllswitchesFwP"
              runMode="pauseOnlyOnFailures">
       </maintMaintP>
       <maintMaintGrp name="AllswitchesMaintGrp">
              <fabricNodeBlk name="Blk101" from_="101" to_="101">
              </fabricNodeBlk>
              <fabricNodeBlk name="Blk102" from_="102" to_="102">
              </fabricNodeBlk>
              <fabricNodeBlk name="Blk103" from_="103" to_="103">
              </fabricNodeBlk>
              <fabricNodeBlk name="Blk104" from_="104" to_="104">
              </fabricNodeBlk>
              <maintRsMgrpp tnMaintMaintPName="AllswitchesMaintGrp">
              </maintRsMgrpp>
       </maintMaintGrp>
</fabricInst>
```

ステップ 3 すべてのスイッチのアップグレードをただちにトリガする次のポリシーを POST します。

例：

```
POST URL : https://<ip address>/api/node/mo/uni/fabric.xml
<maintMaintP
    name="AllswitchesMaintP" adminSt="triggered">
</maintMaintP>
```

アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。

REST API を使用したカタログ ソフトウェア バージョンのアップグレード

通常、カタログ イメージは、Cisco APIC イメージのアップグレード時にアップグレードされます。ただし、管理者がカタログイメージをアップグレードしなければならない場合もあります。

手順

カタログ イメージをアップグレードします。

例：

```
http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareCatFwP
    version="catalog-1.0(1e)"  ignoreCompat="yes" />
</firmwareCatFwP>
```

API を使用したファームウェア バージョンおよびアップグレード ステータスの確認

確認内容	URL の例
コントローラで現在実行中のファームウェアのバージョン	GET URL：https://<ip address>/api/node/class/firmwareCtrlrRunning.xml
スイッチで現在実行中のファームウェアのバージョン	GET URL：https://<ip address>/api/node/class/firmwareRunning.xml
コントローラとスイッチのアップグレードの状態	GET URL：https://<ip address>/api/node/class/maintUpgJob.xml

アップグレードの例

コントローラ アップグレードの例

Cisco APIC イメージをリポジトリにダウンロードする

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="APIC_Image_download" proto="http"
url="http://172.21.158.190/aci-apic-dk9.1.0.0.72.iso"/>
</firmwareRepoP>
```

スイッチ イメージをリポジトリにダウンロードする

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareRepoP>
 <firmwareOSource name="Switch_Image_download" proto="http"
url="http://172.21.158.190/aci-n9000-dk9.11.0.0.775.bin"/>
</firmwareRepoP>
```

コントローラ ファームウェア ポリシー：コントローラの目的のバージョン設定

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/controller.xml
<firmwareCtrlrFwP
     version="apic-1.0(0.72)"
     ignoreCompat="true">
</firmwareCtrlrFwP>
```

コントローラのメンテナンスポリシー：コントローラのアップグレードのトリガを今すぐ開始する

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/controller.xml
<maintCtrlrMaintP
 adminState="up" adminSt="triggered">
</maintCtrlrMaintP>
```

コントローラで現在実行中のバージョンを取得する

```
(all controllers) GET URL :
http://trunk6-ifc1.insieme.local/api/node/class/firmwareCtrlrRunning.xml
(a controller) GET URL :
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-1/sys/ctrlrfwstatuscont/ctrlrrunning.xml
```

コントローラのアップグレードのステータスを取得する

```
(all controllers) GET URL : http://trunk6-ifc1.insieme.local/api/node/class/maintUpgJob.xml
(a controllers) GET URL :
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-1/sys/ctrlrfwstatuscont/upgjob.xml
```

スイッチのアップグレード例

スイッチのファームウェア グループ: スイッチで同じファームウェア ポリシー グループ

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareFwGrp name="AllswitchesFwGrp" >
        <fabricNodeBlk name="Blk101to104” from_="101" to_="104” />
       <firmwareRsFwgrpp tnFirmwareFwPName="AllswitchesFwP” />
</firmwareFwGrp>
```

スイッチのファームウェアのファームウェア ポリシー: セットが必要なバージョン

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<firmwareFwP name="AllswitchesFwP” version="n9000-11.0(0.775)” ignoreCompat="true">
</firmwareFwP>
```

スイッチのメンテナンス グループ: スイッチで同じメンテナンス ポリシー グループ

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintGrp name="AllswitchesMaintGrp">
        <fabricNodeBlk name="Blk101to104” from_="101" to_="104” />
        <maintRsMgrpp tnMaintMaintPName="AllswitchesMaintP” />
</maintMaintGrp>
```

スイッチのメンテナンス ポリシー: **maitenance** のセットアップのスケジュール

```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintP name="AllswitchesMaintP” runMode="pauseOnlyOnFailures" >
</maintMaintP>
```

今すぐ開始: メンテナンス グループでトリガーのアップグレード

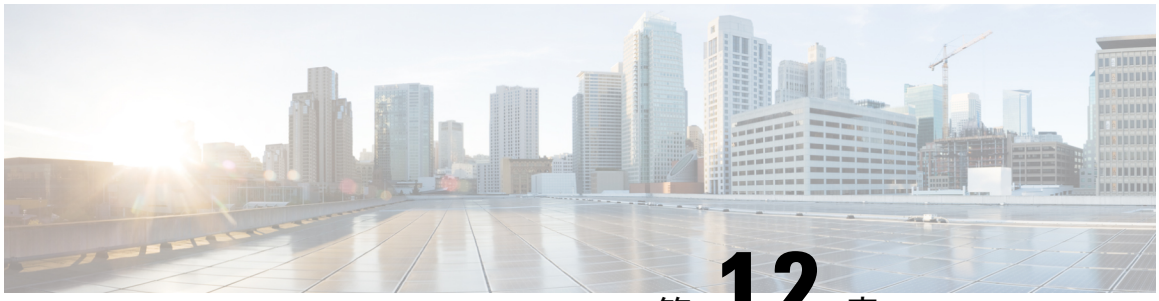
```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintP name="AllswitchesMaintP" adminSt="triggered">
</maintMaintP>
```

スイッチで現在実行中のバージョンを取得します。

```
(all switches) GET UR : http://trunk6-ifc1.insieme.local/api/node/class/firmwareRunning.xml
(a switch) GET URL:
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-101/sys/fwstatuscont/running.xml
```

スイッチのアップグレードのステータスを取得します。

```
(all switches) GET URL: http://trunk6-ifc1.insieme.local/api/node/class/maintUpgJob.xml
(a switch) GET URL:
http://trunk6-ifc1.insieme.local/api/node/mo/topology/pod-1/node-101/sys/fwstatuscont/upgjob.xml
```



第 12 章

CLI を使用するソフトウェアのアップグレード

CLI を使用して、ソフトウェアをアップグレードできます。

（注）
- 次の注意事項を確認し、それに従ってください。
  - Cisco ACI ファブリックをアップグレードするワークフロー （32 ページ）
  - アップグレード前のチェックリスト （71 ページ）
  - アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）
- GUI を使用してアップグレードのポリシーを作成する場合、CLI を使用して同じポリシーを変更することはできません（逆も）。

NX-OS を使用した Cisco APIC ソフトウェアのアップグレード

手順

ステップ 1 送信元からコントローラにイメージをダウンロードします。

例：

```
admin@ifc1:~> scp <username>@<Host IP address that has the image>:/<absolute path to the
 image including image file name>  .
admin@ifc1:~> pwd
/home/admin
admin@ifc1:~> ls
<ver-no>.bin
```

ステップ 2 リポジトリ情報を表示します。

例：

```
apic1# show firmware repository
```

ステップ 3 リポジトリにファームウェア イメージを追加します。

```
apic1# firmware repository add <name of the image file>
```

例：

```
apic1# firmware repository add aci-apic-dk9.2.0.1r.iso
```

ステップ 4 アップグレードするコントローラを設定します。

```
apic# configure
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version <name of the image file>
```

例：

```
apic# configure
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version aci-apic-dk9.2.2.2e.bin
```

ステップ 5 コントローラをアップグレードします。

例：

```
apic1(config-firmware-controller)# exit
apic1(config-firmware)# exit
apic1(config)# exit
apic1# firmware upgrade controller-group
```

アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。アップグレードはバックグラウンドで実行されます。

ステップ 6 コントローラのアップグレードを確認します。

例：

```
apic1# show firmware upgrade status
 Pod         Node        Current-Firmware      Target-Firmware       Status
         Upgrade-Progress(%)
 ----------  ----------  --------------------  --------------------
-------------------------  --------------------
 1           1           apic-2.3(0.376a)                            success
         100
 1           2           apic-2.3(0.376a)                            success
         100
 1           3           apic-2.3(0.376a)                            success
         100
 1           101         n9000-12.3(0.102)     n9000-12.3(0.102)     success
         100
 1           102         n9000-12.3(0.102)     n9000-12.3(0.102)     success
```

```
          100
 1           103         n9000-12.3(0.100)     n9000-12.3(0.102)     upgrade in progress
        5
 1            104         n9000-12.3(0.102)     n9000-12.3(0.102)     success
          100
 1            201         n9000-12.3(0.102)     n9000-12.3(0.102)     success
          100
 1           202         n9000-12.3(0.100)     n9000-12.3(0.102)     upgrade in progress
        5
apic1#
```

NX-OS スタイル CLI を使用したスイッチのアップグレード

手順

ステップ 1 送信元からコントローラにイメージをダウンロードします。

例：

```
admin@ifc1:~> scp <username>@<Host IP address that has the image>:/<absolute path to the
 image including image file name>  .
admin@ifc1:~> pwd
/home/admin
admin@ifc1:~> ls
<ver-no>.bin
```

ステップ 2 リポジトリ情報を表示します。

例：

```
apic1# show firmware repository
```

ステップ 3 リポジトリにファームウェア イメージを追加します。

```
apic1# firmware repository add <name of the image file>
```

例：

```
apic1# firmware repository add aci-apic-dk9.2.0.1r.iso
```

ステップ 4 アップグレードのスイッチのグループを設定します。

```
apic1# configure
apic1(config)# firmware
apic1(config-firmware)# switch-group <name of the switch group>
apic1(config-firmware-switch)# switch <switches to add to group>
apic1(config-firmware-switch)# firmware-version <name of the image file>
```

例：

```
apic1# configure
apic1(config)# firmware
apic1(config-firmware)# switch-group group1
```

```
apic1(config-firmware-switch)# switch 101-104,201,202
apic1(config-firmware-switch)# firmware-version aci-n9000-dk9.12.2.2e.bin
```

上記の **switch** コマンドで **no** 引数を使用して、次のようにグループからスイッチを削除することもできます。

```
apic1(config-firmware-switch)# no switch 203,204
```

ステップ 5 現在のノード セットでアップグレードが失敗した場合に次のノード セットに進むかどうかを指定します。

```
apic1(config-firmware-switch)# [no] run-mode {pause-never | pause-on-failure}
```

例：

```
apic1(config-firmware-switch)# run-mode pause-on-failure
```

ステップ 6 アップグレードにスケジューラを割り当てるか、すぐにアップグレードするかを決定します。

- アップグレードをいつ実行するのかを指定するには、スケジューラが存在する必要があります。

  スケジューラの詳細については、「スケジューラによるアップグレードについて（43 ページ）」を参照してください。

  既存のスケジューラをアップグレードに割り当てるには、次の手順を実行します。

  ```
  apic1(config-firmware-switch)# schedule <scheduler-name>
  ```

  次に例を示します。

  ```
  apic1(config-firmware-switch)# schedule myNextSunday
  ```

- スイッチ グループをすぐにアップグレードするには、EXEC モードに戻り、コマンド **firmware upgrade switch-group** を入力します。

  （注） この状況では、**firmware upgrade switch-group** コマンドはすぐにアップグレードを実行します。

  これは、設定済みのスケジュールされたアップグレードよりも優先されます。

  ```
  apic1(config-firmware-switch)# exit
  apic1(config-firmware)# exit
  apic1(config)# exit
  apic1# firmware upgrade switch-group <name of the switch group>
  ```

  次に例を示します。

  ```
  apic1(config-firmware-switch)# exit
  apic1(config-firmware)# exit
  apic1(config)# exit
  apic1# firmware upgrade switch-group group1
  ```

ステップ 7 スイッチ グループのアップグレード ステータスを確認します。

```
apic1# show firmware upgrade status switch-group <name of the switch group>
```

このコマンドから生成される出力は、リリースによって異なります。

- リリース 4.2(5) よりも前のリリースでは、次のような出力が表示されます。

```
apic1# show firmware upgrade status switch-group group1
 Pod         Node        Current-Firmware      Target-Firmware       Status
             Upgrade-Progress(%)
 ----------  ----------  --------------------  --------------------
-------------------------  --------------------
 1           1           apic-2.3(0.376a)                            success
             100
 1           2           apic-2.3(0.376a)                            success
             100
 1           3           apic-2.3(0.376a)                            success
             100
 1           101         n9000-12.3(0.102)     n9000-12.3(0.102)     success
             100
 1           102         n9000-12.3(0.102)     n9000-12.3(0.102)     success
             100
 1           103         n9000-12.3(0.100)     n9000-12.3(0.102)     upgrade in
progress        5
 1           104         n9000-12.3(0.102)     n9000-12.3(0.102)     success
             100
 1           201         n9000-12.3(0.102)     n9000-12.3(0.102)     success
             100
 1           202         n9000-12.3(0.100)     n9000-12.3(0.102)     upgrade in
progress        5
apic1#
```

- リリース4.2 (5) 以降では、次のような出力が表示されます。ここでは、**[Download-Status]** および**[Download-Progress(%)]** 列を使用して追加情報を提供します。

```
apic1# show firmware upgrade status switch-group group1
  Pod         Node        Current-Firmware      Target-Firmware       Status
              Upgrade-Progress(%)   Download-Status            Download-Progress(%)

 ----------  ----------  --------------------  --------------------
-------------------------  --------------------  -------------------------
--------------------
 1           101         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1          107         n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                 100
 1           108         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1           112         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1           113         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1           121         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1          122         n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                 100
 1          123         n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                 100
 1           124         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1           126         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100

 1           127         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                 100
```

```
 1           128         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1           130         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           171         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           172         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           173         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           174         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           175         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           196         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           197         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1           201         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 2           303         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1           501         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1           502        n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                  100
 1          1001         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1          1002        n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                  100
 1          1901         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1          1902         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1          1903         n9000-15.0(0.138)     n9000-15.0(0.144)     upgrade in
progress        45                    downloaded                  100

 1          3999        n9000-15.0(0.138)     n9000-15.0(0.144)     waiting in queue
           0                     downloaded                  100
apic1#
```

NX-OS スタイル CLI を使用したカタログ ソフトウェア バージョンのアップグレード

デフォルトで、コントローラをアップグレードすると、自動的に対応するカタログ コントローラのバージョンにアップグレードされます。つまり、リポジトリにコントローラのイメージを追加すると、リポジトリにもカタログ イメージが追加されます。

別のカタログ イメージをコピーし、リポジトリに追加することもできます。

手順

ステップ 1 カタログ イメージをリポジトリに追加します。

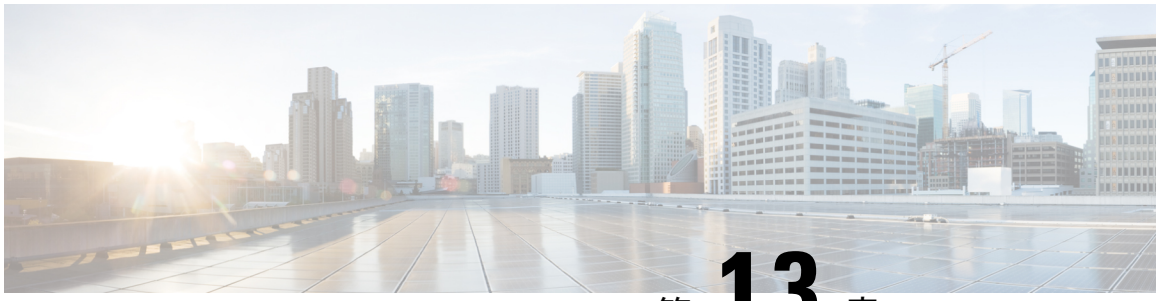
例：

```
apic1(config)# firmware
apic1(config-firmware)# catalog-version aci-catalog-dk9.2.2.2e.bin
```

ステップ 2 カタログ アップグレード ステータスを確認します。

例：

```
apic1# show catalog
Catalog-version : 2.2(2e)
apic1#
```



第 13 章

アップグレード プロセス中にフォールトのトラブルシューティング

一般的な障害の考慮事項

（注） アップグレードの失敗をトラブルシューティングする際は、システムの安定性を確保するために、アップグレード/ダウングレード中に回避する必要がある操作 （62 ページ）で回避するように先に進む前に操作のリストを確認してください。

ACI スイッチ アップグレードの場合、メンテナンス ポリシーごとに 1 つのスケジューラが存在します。デフォルトでアップグレードフォールトが検出されると、スケジューラを停止し、そのグループのノードはアップグレードを開始しません。スケジューラは、アップグレードフォールトの場合に手動介入によるデバッグを必要とします。手動介入が完了したら、一時停止されたスケジューラを再開させる必要があります。

スイッチのステータスが「queued」になっている場合は、以下を確認します。

- コントローラのクラスタが正常かどうか。APIC コントローラ クラスタは、正常な状態にする必要があります。API に「waitingForClusterHealth＝yes」と表示されている場合、または GUI で [Waiting for Cluster Convergence] に対して [Yes] が表示されている場合は、コントローラのクラスタが正常ではないことを示しています。正常になるまで、アップグレードを開始していないスイッチのステータスは「queued」のままになります。

- スイッチのメンテナンス グループが一時停止していないか。スイッチがアップグレードに失敗すると、グループは一時停止状態になります。
- **[管理（Admin）]** > **[ファームウェア（Firmware）]** > **[履歴（History）]** > **[イベント（Events）]** > **[スケジューラ（Schedulers）]** に移動して、各メンテナンス グループのイベントログを確認します。イベントログは、アップグレードの状態が進行していない理由に関する詳細情報を提供します。

ダウンロード障害の一般的な原因

ダウンロード障害の一般的な原因は、次のようなものがあります。

- リモート サーバの権限が不十分です
- リモート サーバでディレクトリまたはファイルが見つかりません
- APIC のディレクトリがいっぱいです
- リクエストのタイムアウト/許容可能な時間内にダウンロードが完了できなかった
- サーバ エラー/不明なサーバ エラー
- 無効な Ack
- ユーザー名/パスワード認証の問題

問題が解決したら、ダウンロード タスクを再起動してダウンロードを再トリガーできます。

クラスタの収束の確認

一般的な障害の考慮事項（161 ページ） で説明したように、ACI スイッチ ノードを正常にアップグレードするには、APIC コントローラ クラスタが正常である必要があります。GUI を使用して、クラスタ コンバージェンスを確認できます。

さらに定期メンテナンス後に、クラスタの収束の進行状況をモニタできます。GUI に **[コントローラ ファームウェア]** 画面が表示され、1 つのクラスタの収束プロセスごとに一連のメッセージが示されます。これらのメッセージは [Status] フィールドに表示されます。

This may take a while. すべてのクラスタが正常に収束されると、**[コントローラ ファームウェア]** 画面の **[クラスタ コンバージェンスの待機]** フィールドに「**No**」と表示されます。

スケジューラ ステータスの確認

コントローラのアップグレードを一時停止することの確認

コントローラのアップグレードは、GUI または REST API のいずれかを使用して一時停止を確認することができます。

GUI を使用してコントローラのアップグレード スケジューラー時停止しているかどうかを確認するには

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[Firmware]** を選択します。

ステップ 2 [Navigation] ペインで、**[Fabric Node Firmware]** > **[Controller Firmware]** を展開します。

ステップ 3 スケジュールされたメンテナンス ポリシーが一時停止して かどうかが表示されます **アップグレードに失敗しました** で、 **ステータス** 内の列、 **作業** ペインで、特定の Cisco APIC 。

ものが正しく進行していることが表示されます **ファームウェア アップグレード queued、クラスタ コンバージェンスを待機中** で [Status] カラムで、 **作業** ペインで、特定の Cisco APIC 。

ステップ 4 問題を特定して、この問題を修正します。

ステップ 5 をクリックします **アクション**] タブをクリックします **コントローラ ファームウェア ポリシーのアップグレード** 。

REST API を使用してコントローラのアップグレード スケジューラー時停止しているかどうかを確認するには

手順

コントローラ メンテナンス ポリシーのためにスケジューラが一時停止されていることを確認するには、次の API を POST 送信します。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

次のような返品が表示されます。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group
```

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/fabric/
maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00" polName="
ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="local"
maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status="" uid="0"
waitOnClusterHealth="no" windowName=""/>
</imdata>
```

スイッチのアップグレードの一時停止確認

GUI または REST API のいずれかを使用して、スイッチのアップグレードの一時停止を確認できます。

GUI を使用してスイッチ アップグレード スケジューラの一時停止を確認する

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。

ステップ 2 [ナビゲーション] ペインで、**[ファブリック ノード ファームウェア]** > **[メンテナンス グループ]** を展開します。

ステップ 3 **[メンテナンス グループ]** を展開して、**[すべてのスイッチ]** をクリックします。

ステップ 4 **[作業]** ペインで、**[スケジューラのステータス]** が **[一時停止]** を読み取っているか確認します。

（注） **[スケジューラのステータス]** が **[実行中]** を読み取り、グループ内のノードがアップグレードを続行または完了している場合、デバイスが実行されアップグレードが続行または完了します。

ステップ 5 デバイスに移動し、手順 1 ～ 4 を繰り返します。

この時点で、**[スケジューラのステータス]** は **[実行中]** を読み取ります。

ステップ 6 右上の **[アクション]** ドロップダウンリストを使用して、**[アップグレード スケジューラの再開]** を選択します。

ステップ 7 右上の **[アクション]** ドロップダウン リストを使用して、**[今すぐアップグレード]** を選択します。

REST API を使用してスイッチのアップグレードスケジューラが時停止しているか確認する

手順

スイッチ メンテナンス ポリシーのためにスケジューラが一時停止されていることを確認するには、次の API を POST 送信します。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

次のような返品が表示されます。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/
fabric/maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00"
polName="ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
 windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="
local" maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status=""
uid="0" waitOnClusterHealth="no" windowName=""/>
</imdata>
```

スコントローラのメンテナンス ポリシーのために一時停止したスケジューラの再開

GUI または REST API のいずれかを使用してコントローラ メンテナンス ポリシーの一時停止スケジューラを再開することができます。

コントローラのアップグレード スケジューラ Resume を GUI を使用して一時停止しています

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[Firmware]** を選択します。

ステップ 2 [Navigation] ペインで、**[Fabric Node Firmware]** > **[Controller Firmware]** を展開します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

ステップ 4 [Controller Maintenance Policy] 領域で、[Running Status] フィールドの表示が [Paused] であることを確認します。

ステップ 5 [Actions] タブをクリックし、[Resume Upgrade Scheduler] をクリックします。

ステップ 6 をクリックします **アクション**] タブを選択します **コントローラ ファームウェア ポリシーのアップグレード** ドロップダウンリストから。

ステップ 7 [アクション（Actions）] タブをクリックし、ドロップダウン リストから [今すぐ適用（Apply Now）] を選択します。

REST API を使用して一時停止したコントローラのアップグレード スケジューラを再開する

手順

ステップ 1 コントローラ メンテナンス ポリシーのために一時停止されたスケジューラを再開するには、次の API をPOST 送信します。

この例では、メンテナンス ポリシーは ConstCtrlrMaintP です。

例：

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="ConstCtrlrMaintP" status="deleted" />
</maintUpgStatusCont>
```

ステップ 2 Cisco APIC コントローラ ソフトウェアをアップグレードするために最初に使用される REST API を使用します。

スイッチのメンテナンスポリシーのために一時停止したスケジューラの再開

一時停止したスイッチのアップグレード スケジューラを再開するために GUI を使用する

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。

ステップ 2 **[ナビゲーション]** ペインで、**[ファブリック ノード ファームウェア]** > **[メンテナンス グループ]** > ***[maintenance_group_name]*** を展開します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

ステップ 4 [Maintenance Policy] 領域で、[Running Status] フィールドの表示が [Paused] であることを確認します。

ステップ 5 **[メンテナンス ポリシー]** 領域で、**[スケジューラのステータス]** フィールドに **[一時停止]** が表示され、**[クラスタ コンバージェンスの待機]** フィールドに **[いいえ]** が表示されていることを確認します。

ステップ 6 [Actions] タブをクリックし、[Resume Upgrade Scheduler] をクリックします。

ステップ 7 **[アクション]** タブをクリックして、ドロップダウン リストから **[今すぐアップグレード]** を選択します。

REST API を使用して一時停止したスイッチ アップグレード スケジューラを再開する

手順

ステップ 1 スイッチ メンテナンス ポリシーのために一時停止されたスケジューラを再開するには、次の API をPOST 送信します。

この例では、メンテナンス ポリシーは swmaintp です。

例：

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="swmaintp" status="deleted" />
</maintUpgStatusCont>
```

ステップ 2 最初に使用した REST API を使用してスイッチ ソフトウェアをアップグレードします。

ログ ファイルの確認

APIC インストーラ ログ ファイル

ソフトウェア リリース 4.0 以降、APIC のアップグレード ログ（インストーラ ログ）は、ライブ アクセスを可能にするために、ユーザがアクセス可能な場所に移動されました。APIC のアップグレードが期待どおりに進行しているかどうかを判断するために、それらをオープンまたはテールにすることができます。アップグレードに応じて、アップグレードプロセス全体を含む 1 つまたは 2 つのログ ファイルが作成されます。

常に予想されるファイルの名前は *insieme_*_installer.log* に似ており、4.x 以降のアップグレードでは、*atom_installer.log* が追加されます。すべてのバージョンのシナリオで、*insieme_*_installer.log* を最初にチェックする必要があります。このログには、*atom_installer.log* に記録される atom_installer が呼び出されたことを示すメッセージが含まれます。

ログ ファイルは、各 APIC の */firmware/logs/YYYY-MM-DDTHH-MM-SS-MS* ディレクトリに保存されます。フォルダのタイムスタンプは、その特定のアップグレードがトリガーされたタイムスタンプに対応します。

```
admin@apic1:logs> pwd
/firmware/logs

admin@apic1:logs> ls -l
2021-04-15T07:42:57-50
2021-05-28T10:18:33-50

admin@apic1:logs> ls -l ./2021-05-28T10:18:33-50
atom_installer.log
insieme_4x_installer.log
```

上記の例では、最近のアップグレードが 2021 年 5 月 28 日 10:18 頃にトリガーされました。対応するログファイルは、そのディレクトリ内に含まれています。個々のログ ファイルは、コンテンツを表示するために選択した Linux ファイル ビューアで開くことができます。代わりに、ログを実際に監視してアップグレードが進行中であることを確認する場合は、***tail –f insieme_zx_installer.log*** を発行して、ログ ファイルに書き込まれている内容をリアルタイムで表示します。

ACI スイッチ インストーラのログ ファイル

すべての ACI スイッチ バージョンで、インストーラ ログ ファイルの表示がサポートされています。ACI スイッチのインストーラ ログは、`/mnt/pss` ディレクトリにあります。ファイルを開くか、*tail –f installer_detail.log* を発行して、ログ ファイルに出力されている現在の内容をリアルタイムで確認できます。

```
leaf101# pwd
/mnt/pss

leaf101# ls -asl installer_detail.log
142 -rw-rw-rw- 1 root root 144722 Apr 29 07:58 installer_detail.log
```

テクニカル サポート ファイルの収集

テクニカル サポート ファイルを収集するには、「On-Demand TechSupport」機能を使用することを推奨します。次のガイドに記載されているように、最初にこの方法を使用してみてください。『API CUI からの ACI show tech の収集』

ただし、APIC のアップグレードが失敗した場合は、クラスタの全体的な状態が低下する可能性があります。つまり、クラスタのステータスが「Data Layer Partially Diverged / Data Layer Partially Degraded Leadership」の状態になる可能性があります。この場合、オンデマンド テクニカル サポート ポリシーを使用してテクニカル サポート ファイルを収集できる可能性は低くなります。この場合、各 APIC ノードでローカルのテクニカル サポート ファイルを個別に収集できます。この方法は、次のガイドに記載されています。『個々の ACI ノードの CLI からの Local show tech の収集』

HUU アップグレード後の CIMC / BIOS 設定

通常 APIC は、APIC として適切に機能するために必要な CIMC および BIOS 設定で事前に設定する必要があります。ただし、CIMC と BIOS の設定が期待値から外れるシナリオやアクションがあります。

（注） HUU アップグレードを実行すると、BIOS TPM 設定が無効になることがあります。APIC が HUU 後の APIC OS に再起動する問題を示している場合は、APIC をリセットして BIOS 設定を検証します。

予想される CIMC 値

管理 - 専用

デフォルトの管理者パスワード - パスワード

LLDP - 無効

予想される BIOS 値

TPM –有効

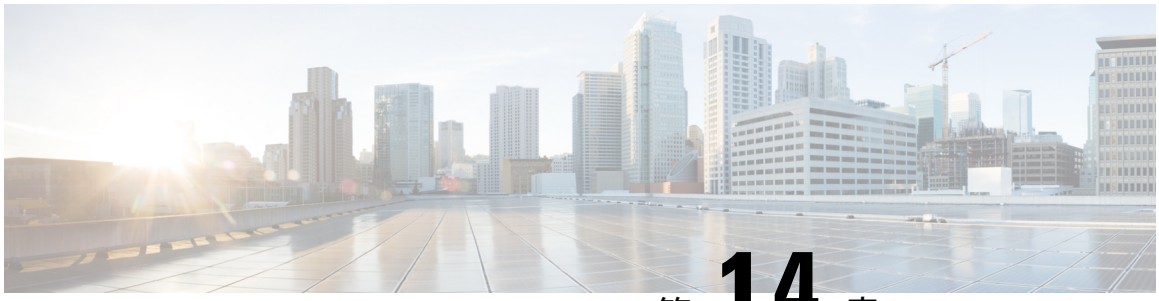
TPM 状態-所有

検証

次の一連のコマンドを使用して、APIC の CIMC を ssh してこれらの設定を検証できます。

```
C220-FCH1838V001# scope bios

C220-FCH1838V001 /bios # show main detail
Set-up parameters:
    Power ON Password Support: Disabled
    TPM Support: Enabled <<<<<<<<<<<<

C220-FCH1838V001# scope cimc

C220-FCH1838V001 /cimc # show network detail
Network Setting:
    ...
    NIC Mode: dedicated <<<<<<<<<<<<
    NIC Redundancy: none
    ...

C220-FCH1838V001# scope chassis

C220-FCH1838V001 /chassis # show adapter detail
PCI Slot 1:
    Product Name: UCS VIC 1225
    Product ID: UCSC-PCIE-CSC-02
    ...
    VNTAG: Disabled
    FIP: Enabled
    LLDP: Disabled <<<<<<<<<<<<
    PORT CHANNEL: N/A    <<<<<<<<<<<<   Validate for Gen 3 APICs
```

```
Configuration Pending: no
Cisco IMC Management Enabled: no
...
```



第 14 章

FPGA/EPLD/BIOS ファームウェアの管理

FPGA / EPLD / BIOS ファームウェアの管理について

Cisco スイッチには複数の Progurammable Logical Device（PLD）が含まれているので、すべてのモジュールでハードウェア機能を使用できます。PLD には、電子プログラマブルロジックデバイス（EPLD）とフィールドプログラマブルゲートアレイ（FPGA）が含まれます。シスコは定期的なイメージのアップグレードは、ハードウェアの機能強化を組み込むか、既知の問題を解決するために定期的に提供されます。

Cisco ACI では、FPGA / EPLD / BIOS ファームウェアを個別にまたは明示的に手動で管理する必要はありません。代わりに、ACI スイッチが APIC によって管理され、APIC を介してスイッチの通常のファームウェア アップグレードが実行される場合、ACI スイッチ イメージ自体に含まれる適切なFPGA / EPLD / BIOS ファームウェア（aci-n9000-dk9.14.2.1i.bin など）が自動的に適用されます。

ただし、APIC によってトリガーされたアップグレードを実行せずにスイッチが ACI スイッチ イメージで起動すると、ACI スイッチで実行されている FPGA / EPLD / BIOS ファームウェアは、ACI スイッチ イメージの適切なバージョンでアップグレードされません。これにより、FPGA / EPLD / BIOS のバージョンが一致しなくなる可能性があります。これは、新しい注文（返品および交換（RMA））でスイッチを受け取った場合、またはスイッチをスタンドアロン NX-OS ソフトウェアから ACI スイッチ ソフトウェアに変換した場合に発生することがあります。

Cisco APIC リリース 5.2(1) および ACI スイッチ リリース 15.2(1) より前のリリースでは、スイッチを一度ダウングレードしてから、APIC を使用して目的のバージョンにアップグレードし、FPGA / EPLD / BIOS のバージョンを適切なものにアップグレードする必要がありました。

Cisco APIC リリース 5.2(1) および ACI スイッチ リリース 15.2(1) から、ACI スイッチは APIC を介して実行されるアップグレード操作ではない場合でも、次のコンポーネントの通常の起動シーケンス中に、起動している ACI スイッチイメージに基づいて、FPGA / EPLD / BIOSを自動的にアップグレードします。

- **リーフ スイッチとボックス型スパイン スイッチ**：EPLD / FPGA / BIOS はスイッチ自体で自動的にアップグレードされます。
- **モジュラタイプ スパイン スイッチ**：EPLD / FPGA / BIOS は次のコンポーネントで自動的にアップグレードされます。
  - スーパーバイザ モジュール
  - ラインカード モジュール
  - ファブリック モジュール

上記のサポート対象コンポーネントのいずれかが起動すると、システムは自動的に次のアクションを実行して、EPLD/FPGA/BIOS イメージが Cisco ACI または NX-OS イメージと同期しているかどうかを判断します。

1. システムは BIOS のバージョンを比較し、イメージが同期していないことを検出すると、BIOS レベルでアップグレードを実行します。
2. システムは EPLD/FPGA のバージョンを比較し、イメージが同期していないことを検出すると、EPLD/FPGA レベルでアップグレードを実行します。
3. システムがいずれかのレベル（BIOS レベルまたはEPLD/FPGA レベル）でアップグレードを実行する必要がある場合、システムはそのコンポーネント（スイッチ、スーパーバイザ モジュール、ラインカード モジュール、またはファブリック モジュール）の電源の再投入を実行します。

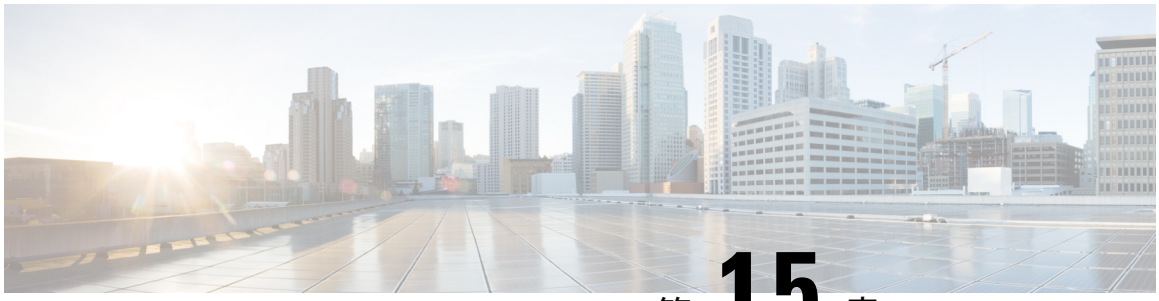
通常の起動シーケンス中のこれらの自動 FPGA / EPLD / BIOS アップグレードは、コンポーネントごとに実行されます。たとえば、新しいラインカードモジュールが挿入され、スーパーバイザモジュールからダウンロードされたベース ACI スイッチイメージを使用して起動すると、新しいラインカード モジュールのみの電源がオンになり、ベース ACI スイッチ イメージから FPGA / EPLD / BIOS が適用されます。他のモジュールは影響を受けません。

FPGA / EPLD / BIOS ファームウェア管理時の注意事項と制約事項

- 以下のコンポーネント特有の考慮事項に注意してください。
  - **スーパーバイザ モジュールの場合**：ACI スイッチはコールドスタンバイで動作するため、アクティブなスーパーバイザモジュールがリロードされると、ボックス全体がリロードされます。そのため、通常の起動シーケンス中に FPGA / EPLD / BIOS のアップグレードがアクティブ スーパーバイザ モジュールとスタンバイ スーパーバイザ モジュールの両方に必要な場合、またはアクティブモジュールのみに必要な場合は、アクティブ スーパーバイザ モジュールとスタンバイ スーパーバイザ モジュールの両方で同時に電源がオンになります。スタンバイ モジュールでのみ FPGA / EPLD / BIOS のアップグレードが必要な場合は、スタンバイ モジュールでのみ電源がオンになり、アクティブ モジュールは稼働したままになります。

- **システム コントローラの場合**：モジュラ スイッチのシステム コントローラ（SC）の FPGA / EPLD / BIOS は、通常のブート シーケンス中にアップグレードされません。システム コントローラの EPLD / FPGA / BIOS バージョンがベース ACI スイッチ イメージと一致しない場合でも、APIC を使用してスイッチ自体のアップグレードを実行する必要があります。

- メモリ テクノロジー デバイス（MTD）の断続的なマウントに関する既知の問題があります。この問題では、特定の MTD ベースのボード上の一部のライン カード モジュールおよびファブリック モジュールで自動 FPGA / EPLD / BIOS アップグレードがトリガーされません。Embedded MultiMediaCard（EMMC）または MTD に問題がある場合、FPGA / EPLD / BIOS の自動アップグレードはトリガーされません。
- 上位ボード レベルで `show system reset-reason` コマンドを入力すると、自動 FPGA / EPLD /BIOS アップグレードがトリガーされたときのリセットの理由に関する情報が表示されます。ただし、ライン カードレベルまたはファブリック モジュール レベル（たとえば、`show system reset-reason module 3`）でコマンドを入力しても、情報は生成されません。



第 15 章

サイレント ロール パッケージのアップグレード

サイレント ロール パッケージのアップグレードについて

Cisco APIC リリース 4.1(2) では、サイレント ロール パッケージ アップグレード (SR アップグレード) 機能が導入されています。SR アップグレードを使用すると、ACI スイッチのソフトウェア OS 全体をアップグレードしなくても、ACI スイッチのハードウェア SDK、ドライバなどの内部パッケージのアップグレードを手動で実行できます。通常、ACI スイッチのソフトウェア OS のアップグレード機能は、内部パッケージも処理するため、SR アップグレードを実行する必要はありません。

Cisco APIC リリース 4.1(2) では、SR アップグレード機能は次の 2 つのスイッチをサポートしています。

- N9K-C93216TC-FX2
- N9K-C93360YC-FX2

Cisco APIC GUI を使用してサイレント ロール パッケージのアップグレードの設定

始める前に

- 全コントローラが新しいファームウェアバージョンにアップグレードされるまで待機してから、スイッチのファームウェアのアップグレードに進みます。
- SR パッケージのアップグレードに使用する SR パッケージ (aci-srpkg-dk9.1.0.0 など) をダウンロードします (必要に応じて、APIC で APIC とスイッチイメージをダウンロードする（115 ページ）に記載されている手順を使用します)。
- 「Cisco ACI ファブリックをアップグレードするワークフロー（32 ページ）」で、中断を最小限に抑えながらアップグレードを正常に完了するための推奨手順を確認します。

手順

ステップ 1 作業を進める前に、全コントローラが新しいファームウェアバージョンにアップグレードされていることを確認します。
全コントローラが先に新しいファームウェア バージョンにアップグレードされるまでは、スイッチのファームウェアをアップグレードしないでください。

ステップ 2 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。

ステップ 3 [ワーク (Work)] ペインで、**[インフラストラクチャ (Infrastructure)]** > **[ノード (Nodes)]** をクリックします。

ステップ 4 **[アクション (Actions)]** をクリックし、**[ノードのアップグレードをスケジュール (Schedule Node Upgrade)]** を選択して、次の操作を実行します。

a) **[グループ タイプ (Group Type)]** フィールドで、**[ローカル (local)]** を選択します。

b) このフィールドが使用可能な場合は、**[グループのアップグレード (Upgrade Group)]** フィールドで **[既存 (Existing)]** または **[新規 (New)]** のいずれかを選択します。

- **[既存 (existing)]**一既存のアップグレード グループのノードのアップグレードをスケジュールすることができます。
- **[新規 (new)]**: 新しいアップグレード グループを作成できます。

c) **[アップグレード グループ名 (Upgrade Group Name)]** フィールドで、ドロップダウン メニューで指定されたオプションを使用して既存のアップグレード グループを選択するか、または新しいアップグ レードグループを作成するための名前を入力します。

4.1(2) 以前のリリースでは、新しいアップグレード グループを作成するために、フィールドの隅にある **x** をクリックしてフィールドをクリアし、新しいアップグレード グループの名前を入力します。

既存のポッド メンテナンス グループを選択した場合は、そのメンテナンス グループに関連付けられているフィールドに自動的に入力されます。

d) [**手動サイレント ロール パッケージのアップグレード (Manual Silent Roll Package Upgrade)**] チェックボックスをオンにします。

（注） **手動サイレント ロール パッケージのアップグレード (Manual Silent Roll Package Upgrade)**を選択した場合:

- [**サイレント ロール パッケージのバージョン (Silent Roll Package version)**] ドロップダウンリストに、SRアップグレードパッケージのバージョンのリストが表示されます。
- 次のフィールドは無効になっています。
  - **ターゲットのファームウェア バージョン**
  - **互換性チェックの無視**
  - **グレースフル メンテナンス**

e) [**サイレント ロール パッケージのバージョン (Silent Roll Package Version)**] ドロップダウン リストをクリックして、SR パッケージのアップグレード用のパッケージを選択します。

f) [実行モード（Run Mode）] フィールドで、ノード セットのメンテナンス プロセスが正常に完了した後で自動的に次のノード セットに進むための実行モードを選択します。

次のオプションがあります。

- **障害時に一時停止せず、クラスタの状態を待機しない（Do not pause on failure and do not wait on cluster health**）
- **アップグレードの失敗時のみ一時停止（Pause only Upon Upgrade Failure**）

デフォルトは [アップグレードの失敗時のみ一時停止Pause only Upon Upgrade Failure）] です。

g) [**アップグレード開始時刻 (Upgrade Start Time)**] フィールドで、[**今すぐ (Now)**] または [**後でスケジュール (Schedule for Later)**] のいずれかを選択します。

[予定をスケジュール（Schedule for Later）] を選択した場合は、[スケジューラ（Scheduler）] スクロールダウン メニューを使用してトリガー値を選択します。

h) [**すべてのノード (All Nodes)**] テーブルの右側にあるプラス アイコンをクリックします。

[**アップグレード グループにノードを追加 (Add Nodes to Upgrade Group)**] ページが表示されます。

i) [**アップグレード グループにノードを追加 (Add Nodes To Upgrade Group)**] ページで、次のいずれかを選択します。

- [**範囲 (Range)**] を選択した場合は、[**グループ ノード ID (Group Node Ids)**] フィールドに範囲を入力します。

- [手動 (Manual)] を選択した場合は、選択可能なリーフ スイッチとスパイン スイッチのリストが [**すべてのノード (All Nodes)**] 領域に表示されます。このアップグレードに含めるノードを選択します。

  表示されるノードは、物理リーフ スイッチとスパイン スイッチであることに注意してください。

j) **[送信 (Submit)]** をクリックします。

ステップ 5 アップグレード グループからノードを削除するには、次のようにします。

a) アップグレード グループから削除するテーブル内のノードを選択します。
b) [**すべてのノード (All Nodes)**] テーブルの右側にあるゴミ箱アイコンをクリックします。
c) [送信（Submit）] をクリックします。

CLI を使用したサイレント ロール パッケージのアップグレードの設定

このセクションでは、SR パッケージのアップグレードを設定および設定解除する方法と、CLI を使用して SR パッケージのアップグレードおよび SR パッケージのバージョンを設定した後にアップグレードをトリガーする方法について説明します。

SR パッケージのアップグレードの詳細については、サイレント ロール パッケージのアップグレードについて （175 ページ） を参照してください。

手順

ステップ 1 SR パッケージのアップグレードを設定するには、次のようにします。

```
Switch# configure
Switch(config)# firmware
Switch(config-firmware)# switch-group new
Switch(config-firmware-switch)# sr-version aci-srpkg-dk9.1.0.0.bin
Switch(config-firmware-switch)# sr-upgrade
Switch(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group new
# Time: Wed Mar 13 15:55:59 2019
  firmware
    switch-group new
      sr-version aci-srpkg-dk9.1.0.0.bin
      sr-upgrade
      exit
    exit
```

ステップ 2 SR パッケージのアップグレードを設定解除するには、次のようにします。

```
Switch# configure
Switch(config)# firmware
Switch(config-firmware)# switch-group new
Switch(config-firmware-switch)# no sr-upgrade
Switch(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group new
# Time: Wed Mar 13 16:17:01 2019
  firmware
    switch-group new
      sr-version aci-srpkg-dk9.1.0.0.bin
      exit
    exit
```

ステップ 3 SRパッケージのバージョンとSRパッケージのアップグレードを設定した後にアップグレードをトリガーするには、次のようにします。

（注） SRパッケージのアップグレードが設定されている場合は、アップグレードをトリガーするためにSRパッケージのバージョンを空にすることはできません。SRパッケージのアップグレードが設定されていない場合は、ファームウェアバージョン (スイッチバージョン) を空にすることはできません。

```
Switch# firmware upgrade switch-group new
```

REST API を使用したサイレント ロール パッケージのアップグレードの設定

ここでは、REST API を使用する SR パッケージのアップグレードを設定する方法について説明します。

SR パッケージのアップグレードの詳細については、サイレント ロール パッケージのアップグレードについて （175 ページ） を参照してください。

手順

SR パッケージのアップグレードを設定するには、次のようにします。

```
<fabricInst>
                <maintMaintP
                srVersion="srpkg-1.0(1)"
                srUpgrade="yes"
                name="m1"
                runMode="pauseOnlyOnFailures">
                </maintMaintP>
                <maintMaintGrp name="m1">
               <fabricNodeBlk name="Blk101"
               from_="101" to_="101">
               </fabricNodeBlk>
                <maintRsMgrpp
                tnMaintMaintPName="m1">
```

```
                </maintRsMgrpp>
                </maintMaintGrp>
</fabricInst>
```

第 16 章

ソフトウェア メンテナンス アップグレード パッチ

ソフトウェア メンテナンス アップグレード パッチについて

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降では、特定の不具合に対する修正を含むソフトウェア メンテナンス アップグレード（SMU）パッチをインストールできます。SMU パッチは、従来のパッチ リリースよりもはるかに迅速にリリースできるため、特定の問題をタイムリーに解決できます。SMU パッチは、Cisco.com からダウンロードできます。通常、パッチが解決する問題を簡単に識別できるように、解決した障害の ID 番号をファイル名に含めます。SMU パッチには新しい機能は含まれていません。

SMU パッチは、Cisco APIC および Cisco ACI モード スイッチで使用できます。Cisco APIC にパッチを適用すると、パッチはクラスタ内のすべての Cisco APIC にインストールされ、Cisco

APIC はパッチのインストールを完了するために自動的にリブートされます。スイッチにパッチを適用する場合は、インストールを完了するためにスイッチをリブートする必要がありますが、複数の SMU パッチのインストールを開始するまでリブートを遅らせることができます。

必要に応じて、SMU パッチをアンインストールできます。パッチのインストールと同様に、Cisco APIC またはスイッチを再起動してアンインストールを完了する必要があります。

ソフトウェア メンテナンスのアップグレード パッチに関する注意事項と制限事項

ソフトウェア メンテナンス アップグレード（SMU）パッチには、次のガイドラインと制限事項が適用されます。

- **グレースフル アップグレード**機能は、SMU パッチのインストールおよびアンインストールではサポートされません。
- **スイッチ検出時の自動ファームウェア更新**機能は、SMU パッチのインストールまたはアンインストールの更新グループに属するスイッチでは実行されません。

GUI を使用した Cisco APIC ソフトウェア メンテナンス アップグレード パッチのインストール

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降では、次の手順を使用して、Cisco Application Policy Infrastructure Controller（APIC）にソフトウェア メンテナンス アップグレード（SMU）パッチをインストールできます。

手順

ステップ 1 patch to the ().SMU パッチに対応するファームウェア イメージを Cisco APIC に追加します。パッチは他のファームウェア イメージとともに一覧に記載されます（SMU パッチおよびその他）。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。

ステップ 2 コントローラ ファームウェア更新をセットアップします。**[バージョンの選択（Version Selection）]** 画面で、**[更新タイプ（Update Type）]** の場合 **[ソフトウェア メンテナンス アップグレード（インストール）（Software Maintenance Upgrade (Install)）]** を選択し、**[ファームウェアの選択（Select Firmware）]** セクションの SMU パッチを選択します。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。

GUI を使用したスイッチ ソフトウェア メンテナンス アップグレード パッチのインストール

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降では、次の手順を使用して、Cisco Application Centric Infrastructure（ACI）モード スイッチにソフトウェア メンテナンス アップグレード（SMU）パッチをインストールできます。

SMU パッチのインストールまたはアンインストールでは、通常のファームウェア アップグレードと同じ更新グループが使用されます。1 個のノードは 1 つの更新グループにのみ属することが可能なため、SMU パッチを特定のノードに適用するとき、既存のグループからそのノードを削除し、ノード専用の新しいグループを作成することで、他のノードが影響を受けなくならないようにします。今後ファブリック全体の定期的なファームウェア アップグレードを実行する必要があるとき、SMU パッチ インストールに使用される専用更新グループを削除し、元のグループのいずれかにノードを追加できます。既存グループのすべてのノードに SMU パッチが必要な場合、新しい更新グループを作成することなく、同じ更新グループを使用することができます。

手順

ステップ 1 SMU パッチに対応するファームウェア イメージを Cisco Application Policy Infrastructure Controller（APIC）に追加します。Cisco APIC には、パッチが他のファームウェア イメージとともに記載されます（SMU パッチおよびその他）。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。

ステップ 2 ノード ファームウェアの更新をセットアップします。**[バージョンの選択（Version Selection）]** 画面で、**[更新タイプ（Update Type）]** の場合 **[ソフトウェア メンテナンス アップグレード（インストール）（Software Maintenance Upgrade (Install)）]** を選択し、**[ファームウェアの選択（Select Firmware）]** セクションの SMU パッチを選択します。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。

[確認（Confirmation）] 画面で **[ダウンロードの開始（Begin Download）]** をクリックすると、選択したスイッチにパッチがダウンロードされます。[作業（Work）] ペインの **[ファームウェアの更新（Firmware Updates）]** タブが表示されます。

ステップ 3 [作業（Work）] ペインで、作成したアップグレード グループをクリックします。

[ノード ファームウェアの更新（Node Firmware Update）] ダイアログに、アップグレード グループの情報が表示されます。

ステップ 4 スイッチのステータスが [インストールの準備完了（Ready to Install）] になったら、**[アクション（Actions）]** をクリックし、次のいずれかのアクションを選択します。

- **インストールおよびリロード**：SMU パッチのインストール後にスイッチがリブートされます。1 つの SMU パッチのみをインストールする場合、または複数のパッチの最終パッチをインストールする場合は、このアクションを選択します。
- **インストールおよびリロードのスキップ**：SMU パッチのインストール後、スイッチはリブートされません。複数の SMU パッチをインストールし、このパッチが最終パッチでない場合は、このアクションを選択します。この場合、追加のパッチごとにこの手順全体を繰り返し、最後のパッチをインストールするまで **[インストールおよびリロードのスキップ（Install and Skip Reloa）]** を選択し続けます。最後のパッチとして、**[インストールおよびリロード（Install and Reload）]** を選択します。必要に応じて、このアクションを選択し、パッチのインストール後にスイッチを手動でリブートできます。

GUI を使用した Cisco APIC ソフトウェア メンテナンス アップグレード パッチのアンインストール

Cisco Application Policy Infrastructure Controller（APIC）5.2(1) リリース以降では、次の手順を使用して、Cisco APIC からソフトウェア メンテナンス アップグレード（SMU）パッチをアンインストールできます。

手順

コントローラ ファームウェア更新をセットアップします。**[バージョンの選択（Version Selection）]** 画面で、**[更新タイプ（Update Type）]** の場合 **[ソフトウェア メンテナンス アップグレード（インストール）（Software Maintenance Upgrade (Uninstall)）]** を選択し、アンインストールのため **[ファームウェアの選択（Select Firmware）]** セクションの SMU パッチを選択します。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。この手順はアップグレードを目的としていますが、パッチのアンインストールでは、ここで指定されている場合を除き、同じ手順を使用します。

GUI を使用したスイッチ ソフトウェア メンテナンス アップグレード パッチのアンインストール

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降では、次の手順を使用して、Cisco Application Centric Infrastructure（ACI）モード スイッチからソフトウェア メンテナンス アップグレード（SMU）パッチをアンインストールできます。アンインストールのプロセスには、アップグレード グループを作成し、そのグループを使用して SMU パッチをアンインストールすることが含まれます。

SMUパッチのインストールまたはアンインストールでは、通常のファームウェア アップグレードと同じ更新グループが使用されます。1 個のノードは 1 つの更新グループにのみ属することが可能なため、SMU パッチを特定のノードに適用するとき、既存のグループからそのノードを削除し、ノード専用の新しいグループを作成することで、他のノードが影響を受けません。今後ファブリック全体の定期的なファームウェア アップグレードを実行する必要があるとき、SMU パッチ インストールに使用される専用更新グループを削除し、元のグループのずれかにノードを追加できます。既存グループのすべてのノードに SMU パッチが必要な場合、新しい更新グループを作成することなく、同じ更新グループを使用することができます。

手順

ステップ 1 ノード ファームウェアの更新を設定します。**[バージョンの選択（Version Selection）]** 画面で、**[更新タイプ（Update Type）]** の場合 **[ソフトウェア メンテナンス アップグレード（インストール）（Software Maintenance Upgrade (Uninstall)）]** を選択し、アンインストールのため **[ファームウェアの選択（Select Firmware）]** セクションの SMU パッチを選択します。

手順については、GUI を使用した APIC リリース 5.1 以降でのアップグレード（127 ページ）を参照してください。パッチをアンインストールする場合でも、手順はアップグレード手順とほぼ同じです。

[確認（Confirmation）] 画面が表示されたら、次の手順に進みます。

ステップ 2 表示される情報が正しい場合は、**[アンインストールとリロードをスキップ（Uninstall and Skip Reload）]** または **[アンインストールの開始（Begin Uninstall）]** をクリックします。それ以外の場合は、前の画面のいずれかに戻り、必要に応じて設定を変更します。

- **[アンインストールおよびリロードをスキップ（Uninstall and Skip Reload）]**：SMU パッチがアンインストールされた後、スイッチはリブートされません。複数の SMU パッチをアンインストールする場合にこのアクションを選択します。このパッチは最終パッチではありません。この場合、追加のパッチごとにこの手順全体を繰り返し、最後のパッチをアンインストールするまで、**[アンインストールおよびリロードのスキップ（Uninstall and Skip Reload）]** を選択し続けます。最後のパッチとして、**[アンインストールの開始（Begin Uninstall）]** を選択します。必要に応じて、このアクションを選択し、最終パッチがアンインストールされた後にスイッチを手動でリブートできます。

- **アンインストールの開始**：SMU パッチがアンインストールされた後、スイッチがリブートされます。1 つの SMU パッチのみをアンインストールする場合、または複数のパッチの最終パッチをアンインストールする場合は、このアクションを選択します。

REST API を使用した Cisco APIC ソフトウェア メンテナンス アップグレード パッチのインストールまたはアンインストール

次のREST API XML の例では、Cisco Application Policy Infrastructure Controller（APIC）にソフトウェア メンテナンス アップグレード（SMU）パッチをインストールし、インストールの完了後に Cisco APIC をリブートします。

```
<polUni>
    <ctrlrInst>
        <firmwareCtrlrFwP
          version="apicpatch-CSCab12345-9.0.0-5.2.0.155d.x86_64">
        </firmwareCtrlrFwP>
        <maintCtrlrMaintP
          adminState="up" smuOperation="smuInstall" adminSt="triggered" >
        </maintCtrlrMaintP>
    </ctrlrInst>
</polUni>
```

次のテーブルでは、SMU パッチ固有の要素とパラメータを説明します。

エレメント	パラメータ	説明
`firmwareCtrlrFwP`	`version`	SMUパッチのファイル名を指定します。
`maintCtrlrMaintP`	`smuOperation`	パッチをインストールするかアンインストールするか指定します。設定可能な値は次のとおりです。 • `smuInstall`：パッチをインストールします。 • `smuUninstall`：パッチをアンインストールします。

REST API を使用したスイッチ ソフトウェア メンテナンス アップグレードパッチのインストールまたはアンインストール

次の REST API XML の例では、スイッチにソフトウェア メンテナンス アップグレード（SMU）パッチをインストールし、インストールの完了後にスイッチをリブートします。

```
<polUni>
    <fabricInst>
        <maintMaintP
          version="n9000-patch-CSCsysinfo12-15.2.0.151-S1.1.1.x86_64"
          smuOperation="smuInstall"
          smuOperationFlags="smuReloadImmediate"
          name="Leaf202"
          adminSt="triggered">
        </maintMaintP>

        <maintMaintGrp name="Leaf202">
            <fabricNodeBlk name="blk202" from_="202" to_="202">
            </fabricNodeBlk>
            <maintRsMgrpp tnMaintMaintPName="Leaf202">
            </maintRsMgrpp>
        </maintMaintGrp>
    </fabricInst>
</polUni>
```

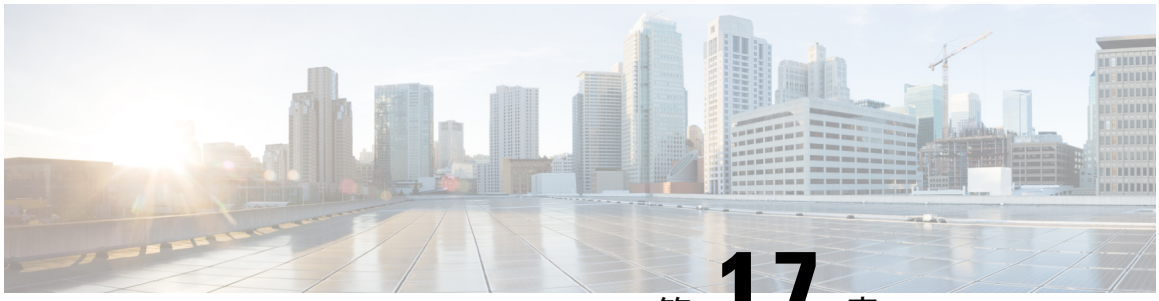
次のテーブルでは、SMU パッチ固有の要素とパラメータを説明します。

エレメント	パラメータ	説明
maintMaintP	version	SMU パッチのファイル名を指定します。
maintMaintP	smuOperation	パッチをインストールするかアンインストールするか指定します。設定可能な値は次のとおりです。 • smuInstall：パッチをインストールします。 • smuUninstall：パッチをアンインストールします。

エレメント	パラメータ	説明
maintMaintP	smuOperationFlags	パッチのインストール後にスイッチをリブートするかどうかを指定します。設定可能な値は次のとおりです。 • smuReloadImmediate：SMU パッチのインストール後にスイッチがリブートされます。1 つの SMU パッチのみをインストールする場合、または複数のパッチの最終パッチをインストールする場合は、この値を指定します。 • smuReloadSkip：スイッチは SMU パッチのインストール後に再起動されません。複数の SMU パッチをインストールし、このパッチが最終パッチでない場合は、この値を指定します。この場合、追加のパッチごとに適切な XML をポストし、最終パッチをインストールするまで smuReloadSkip を指定し続けます。最後のパッチには、smuReloadImmediate を指定します。必要に応じて、smuReloadSkip を指定し、パッチのインストール後にスイッチを手動でリブートできます。
maintMaintP	name	メンテナンス グループの名前を指定します。
fabricNodeBlk	from_ および to_	パッチをインストールまたはアンインストールするスイッチ ノード ID の範囲を指定します。

エレメント	パラメータ	説明
maintRsMgrpp	tnMaintMaintPName	メンテナンス グループの名前を指定します。値は、maintMaintP 要素の name パラメータの値と一致する必要があります。

表で指定されているパラメータ値の一部を変更することで、パッチをインストールまたはアンインストールするかどうかを指定でき、パッチのインストールまたはアンインストール後にスイッチをリブートしないように指定できます。



第 17 章

スイッチ ハードウェアのアップグレード

仮想ポートチャネル移行：第一世代スイッチから第二世代スイッチへのノードの移行

最初にファブリックは、2つの第2世代スイッチ間のvPCを使用して設定されます。トラフィック フローは、これらの vPC のみがデータ トラフィックに使用されるように設計されます。第一世代のスイッチを第二世代のスイッチに移行するには、次の手順が必要です。

この手順では、vPC プライマリおよび vPC セカンダリが vPC ペアの第一世代のスイッチであり、前述のようにトラフィックを送信します。

このスイッチでサポートされるトランシーバ、アダプタ、およびケーブルを確認するには、『Cisco トランシーバ モジュール互換性情報』を参照してください。

トランシーバの仕様と取り付けに関する情報を確認するには、『Cisco トランシーバ モジュール インストール ガイド』を参照してください。

始める前に

仮想ポートチャネル（vPC）を構成する 2 つの第 2 世代 Cisco Nexus 9000 シリーズスイッチがあります。同じケーブルを使用して 2 つの第二世代 Cisco Nexus 9000 シリーズ スイッチに移行しようとしています。

第 1 世代 Cisco Nexus 9000 シリーズスイッチには、PID（製品 id）に EX または FX が含まれていないスイッチが含まれています。

第 2 世代 Cisco Nexus 9000 シリーズスイッチには、PID に EX または FX があるスイッチが含まれています。

移行している vPC 第 1 世代スイッチに接続されているすべての APIC コントローラをファブリック内の他のスイッチに移動し、APIC クラスタが「完全に適合」になるまで待ちます。

手順

ステップ 1 APIC GUI から、vPC セカンダリの**コントローラからの削除**操作を実行します。スイッチは APIC によってクリーン リブートされます。操作が完了するまで約 10 分待ちます。このアクションでは、すべてのトラフィックでデータ トラフィックにその他の第一世代スイッチを使用するように促します。vPC セカンダリからケーブルを外します。

ステップ 2 スイッチ固有のハードウェア取り付けガイドにある「スイッチ シャーシの取り付け」セクションに記載されている手順の順序を逆にして、第一世代のスイッチを取り外します。

ステップ 3 スイッチ固有のハードウェア取り付けガイドの「スイッチ シャーシの取り付け」セクションに記載されている手順に従って、第二世代スイッチを取り付けます。

ステップ 4 第一世代のスイッチから取り外した緩んでいないケーブルを、第二世代スイッチの同じポートに接続します。

ステップ 5 新しい第二世代スイッチを APIC に登録します。新しいノードを同じノード名およびノード ID に登録します。このスイッチはファブリックの一部になります。ポリシーは新しいスイッチにプッシュされ、生成スイッチの不一致があるため、vPC レッグはダウンしたままになります。この時点で、vPC プライマリは引き続きデータトラフィックを送信します。

ステップ 6 APIC GUI から、vPC プライマリの**コントローラからの削除**操作を実行します。このスイッチは、APIC によってクリーンにリブートされます。

操作が完了するまで約 10 分待ちます。第二世代スイッチの vPC レッグは、以前にダウン状態になっています。このアクションにより、すべてのトラフィックが新しい第二世代スイッチに移動するように求められます。新しい第二世代スイッチの vPC ポートは、リモート デバイス上で展開された VLAN に対して STP が無効になっている場合、約 10 ～ 22 秒で起動し、ファブリック内のフローに応じて 10 ～ 40 秒の範囲でトラフィックがドロップすることに注意してください。STP がリモート デバイスの VLAN で有効になっている場合、ファブリック内のフローに応じて、トラフィック損失は 40 ～ 75 秒の範囲になります。

ステップ 7 その他の第一世代スイッチからケーブルを外します。

ステップ 8 手順 2 で行ったように、第一世代スイッチを取り外します。

ステップ 9 手順 3 で行ったように、第二世代スイッチを取り付けます。

ステップ 10 手順 4 で行ったように、緩んだケーブルを接続します。

ステップ 11 新しい第二世代スイッチを APIC に登録します。新しいノードを同じノード名およびノード ID に登録します。このスイッチはファブリックの一部になります。ポリシーが新しいスイッチにプッシュされ、vPC レッグが起動し、トラフィックの通過を開始します。

異なるソフトウェアバージョンの古いスイッチから新しいスイッチへの移行

古い世代のスイッチから新しい世代のスイッチに移行する場合、一般的な移行手順は次のとおりです。

1. APIC とスイッチの両方を、新しいスイッチをサポートするバージョンにアップグレードします。
2. 古いスイッチを、両方とも同じバージョンを実行している新しいスイッチに置き換えます。

ただし、この手順は、新しいスイッチに必要な新しいバージョンで既存のスイッチがサポートされていない場合には適用されません。この状況の例としては、Cisco ACI スイッチ 15.0(1) 以降でサポートされなくなった Cisco Nexus 9300（-E 付きまたはサフィックスなし）などの第 1 世代 ACI スイッチから、リリース 15.0(1) 以降でのみサポートされる新しいスイッチの一部に移行する場合があります。

以下の手順ではこの状況での指示を提供します。

このセクションの手順では、新しいスイッチを最初に追加するのではなく、最初にスイッチを削除することを推奨しています。この推奨事項は、次の理由に基づいています。

- アップグレード中に新しいスイッチを登録する場合（つまり、ファブリック内のバージョンが混在する場合）、サポートされる設定変更は制限されます。詳細については、「Cisco ACI スイッチの混合バージョンで許可される操作 （65 ページ）」を参照してください。
- このため、古いスイッチを削除する前に新しいスイッチを新しいノード ID でファブリックに登録しても、必要なすべての設定を新しいノード ID に追加できない場合があります。つまり、ファブリック全体のアップグレードが完了するまで、ワークロードを新しいスイッチに移動することはできません。新しいスイッチが同じノード ID を再利用できるように古いスイッチが最初に削除された場合、新しいスイッチは追加の設定なしで同じノード ID に必要なすべての既存の設定をダウンロードできます。
- 理論的には、アップグレードを開始する前に、新しいノード ID を使用して APIC で必要な設定を事前プロビジョニングできます。ただし、事前にこれらの設定をテストすることはできません。したがって、この項のこの手順では、ワークロードを他の既存のスイッチに移動し、古いスイッチを同じノード ID を持つ新しいスイッチに置き換えることを推奨します。

始める前に

- 『アップグレードサポートマトリクス』を使用して、現在のバージョンを新しいバージョンに直接アップグレードできることを確認します。現在のバージョンを最初に中間バージョンにアップグレードする必要がある場合は、最初に APIC とスイッチの両方を中間バージョンにアップグレードします。

- **[自動ファームウェア更新（Auto Firmware Update）]** が有効になっている場合は、現在のバージョンでサポートされていない新しいハードウェアに交換されたスイッチのノード ID の **[管理（Admin）]** > **[ファームウェア（Firmware）]** の下にある更新グループを必ず削除してください。それ以外の場合、**[自動ファームウェア更新（Auto Firmware Update）]** は、ノード ID の更新グループに設定されている現在の（古い）バージョンに新しいハードウェアをダウングレードしようとします。

手順

ステップ 1 スイッチの交換の準備をします。

- 新しいスイッチに以前のファブリックからの設定が残っている場合は、コマンド **setup-clean-config.sh** を実行して**リロード**します。
- 新しいスイッチがターゲット バージョンで現在ロードされていない場合、APIC でターゲット バージョンの **[自動ファームウェア更新（Auto Firmware Update）]** を有効にすることで、ファブリックに参加するとき、ターゲットバージョンに自動的に新しいスイッチがアップグレードされるようにします。上記の **[自動ファームウェア更新（Auto Firmware Update）]** に関する前提条件を参照してください。もしくは、事前に新しいスイッチにターゲット バージョンを手動でロードする必要があります。

ステップ 2 新しいスイッチに必要なターゲットバージョンに Cisco APIC をアップグレードします。

ステップ 3 新しいバージョンでサポートされている ACI スイッチをアップグレードします。

新しいバージョンでサポートされて**いない** ACI スイッチはアップグレードしないでください。

ステップ 4 新しいバージョンでサポートされていない ACI スイッチの 1 つを削除します。

a) 交換するスイッチ ノード（新しいバージョンでサポートされなくなったスイッチの 1 つ）を選択します。

b) リーフ スイッチを交換する場合は、他の既存のリーフ スイッチにワークロードを移動します。

（注） vPC ペアのリーフ スイッチの場合、同じ vPC ペアの両方のリーフ スイッチのすべてのワークロードを別のリーフ スイッチのセットに移動します。vPC ペアのリーフ スイッチを異なるバージョンに交換する場合、一度に 1 つのスイッチを交換することはサポートされていません。

c) スイッチからケーブルを取り外し、スイッチの電源をオフにします。

スイッチが APIC に接続されているリーフ スイッチである場合、APIC が別のリーフ スイッチを介して ACI スイッチに接続していることを確認します。

d) **[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）]** > **[到達不能なノード（Unreachable Nodes）]** に移動し、リーフ スイッチが到達不能であることを確認します。

[ノード名] と **[ノード ID]** のノードを作成します。

e) ノードを選択し、**[アクション（Actions）]**をクリックして、**[コントローラから削除（Remove From Controller）]** を選択します。

Cisco APIC からノードが削除されるまで 5 ～ 10 分間待機します。

f) 交換するスイッチが vPC ペアのリーフ スイッチである場合は、同じ vPC ペアの他のリーフ スイッチに対して 4.c （194 ページ） ー 4.e （195 ページ） を繰り返します。

ステップ 5 取り外したスイッチを交換します。

a) 電源をオフにしたリーフ スイッチを新しいリーフスイッチに物理的に交換します。

b) 必要なケーブルを接続し、新しいリーフ スイッチの電源を入れます。

c) Cisco APIC にログインし、GUI の次のページに移動します。

[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）] > [ノード保留登録（Nodes Pending Registration）]

d) 新しいリーフ スイッチが表示されていることを確認します。

e) 新しいリーフ スイッチに、同じ**ノード名**と**ノード ID** を 4.d （194 ページ） から割り当てます。

f) すべての関連ポリシーが新しいスイッチにプッシュされるまで数分間待ちます。

確認するには、**[オペレーション（Operations）] > [容量ダッシュボード（Capacity Dashboard）] > [リーフ容量（Leaf Capacity）]** に移動します。

ステップ 6 これが vPC ペアのリーフ スイッチである場合は、もう一方の古いスイッチに対して ステップ 5 （195 ページ） を繰り返します。

ステップ 7 他のすべての古いスイッチに対して ステップ 4 （194 ページ） ー ステップ 6 （195 ページ） を繰り返します。

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。

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。