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

最終更新：2026 年 3 月 5 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: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://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.

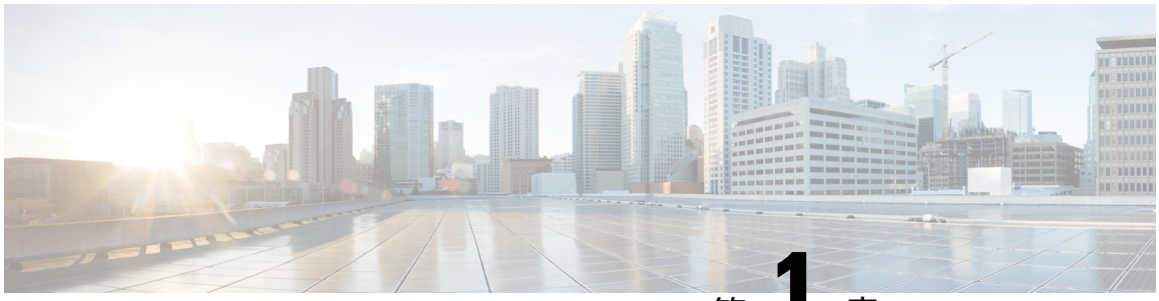
The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. 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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

Trademarks

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

（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
6.2(1)	ACI ファブリックに対して混合バージョン モードのサポートが有効になっています。古いバージョンと新しいバージョンのスイッチ ソフトウェアで ACI ファブリックを長期間にわたって運用し、トラフィック損失が発生することなく構成変更を実行できます。	Cisco ACI スイッチの混合バージョン中に許可される操作 （71 ページ）	

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
6.2(1)	アップグレード ワークフローは、全体的なアップグレード時間を短縮し、リアルタイムの進行状況とステータスの追跡を提供することで、プロセスを合理化します。信頼性を高めるために、包括的なアップグレード前チェック、監査証跡、および統合リカバリ ツールが含まれています。組み込みの検証チェックにより、アップグレードが開始される前に潜在的な問題をプロアクティブに検出します。	GUI を使用した APIC リリース 6.2 以降でのアップグレードまたは、ダウングレード （135 ページ）	
6.0(3)	メモリベースのスイッチ イメージのインストール	スイッチは、スタティック マッピングに基づくのではなく、スイッチのメモリ量に基づいて 32 ビットまたは 64 ビットのイメージをインストールします。	アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）
6.0(2)	リロードしないでスイッチ 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	一部のスイッチ ソフトウェア メンテナンス アップグレード（SMU）パッチでは、パッチのインストール後にスイッチをリロードする必要はありません。	該当なし
6.0(2)	Cisco APIC 検出の自動ファームウェア更新	製品の返品および交換（RMA）、クラスタ拡張、またはコミッションのいずれかによって新しい Cisco APIC をファブリックに追加すると、Cisco APIC は既存のクラスタの同じバージョンに自動的にアップグレードされます。	APIC 検出の自動ファームウェア更新 （175 ページ）

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
6.0(2)	32 ビットおよび 64 ビット Cisco ACIモードのスイッチ イメージ	現在、32 ビットと 64 ビットの両方のCisco ACIモード スイッチ イメージがあります。アップグレード プロセスにより、スイッチ モデルに応じて正しいイメージが自動的にインストールされます。 （注） Cisco APIC6.0（2）以降のイメージをダウンロードし、ダウンロードしたリリースにCisco APICクラスタをアップグレードします。アップグレードが完了する前に、Cisco ACIモード スイッチ イメージを Cisco APIC にダウンロードしないでください。	アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）
6.0(1)	Cisco ACI このドキュメントから「長期的リリース（Long-Lived Releases）」および「短期的リリース（Short-Lived Releases）」の章を削除	Cisco ACI 長期的リリースと短期的リリースの章を削除しました。6.0 リリース以降、Cisco ACI には長期リリースの概念がなくなりました。推奨されるリリースのみがあります。	次の推奨リリースのドキュメントを参照してください。 https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/recommended-release/b_Recommended_Cisco_ACI_Releases.html#Cisco_Reference.dita_4436dd5c-55c8-4598-802d-689a76dce826
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 （65 ページ）
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。	該当なし

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(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 Cisco ACI モード スイッチ リリース 15.2（1）以降、Cisco ACIモード 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 Cisco ACIモード スイッチ イメージに基づいて、Cisco 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 （179 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 （189 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 Cisco 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または、ダウングレード （115 ページ）
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または、ダウングレード （115 ページ）

Cisco APIC のリリースバージョン	特長	説明	参照先
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または、ダウングレード （103 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または、ダウングレード （115 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または、ダウングレード （103 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または、ダウングレード （115 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または、ダウングレード （103 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または、ダウングレード （115 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または、ダウングレード （103 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または、ダウングレード （115 ページ）

新機能および変更された機能に関する情報

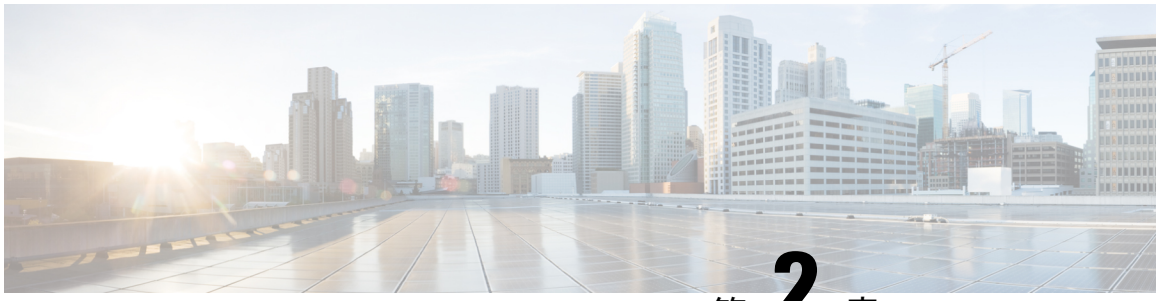
Cisco APIC のリリースバージョン	特長	説明	参照先
4.2(1)	検証は、アップグレードまたはダウングレード操作がトリガーされる前に実行されます。	リリース 4.2(1) 以降では、アップグレードまたはダウングレード操作をトリガーしようとすると、操作がトリガーされる前に、いくつかの検証が実行され、検証中に障害が見つかった場合は警告が表示されます。	• GUI を使用した APIC リリース 4.x または 5.0 でのアップグレードまたは、ダウングレード （103 ページ） • GUI を使用した APIC リリース 5.1 以降でのアップグレードまたは、ダウングレード （115 ページ）
該当なし	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	Cisco 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。Cisco 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	該当なし
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 （183 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。	該当なし

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
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	Cisco APIC リリース 4.0(1) から、バッシュを使用して Cisco APIC 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または、ダウングレード （103 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または、ダウングレード （115 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または、ダウングレード （103 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または、ダウングレード （115 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中に許可される操作 （71 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中に許可される操作 （71 ページ）
2.2（2e）	該当なし	このガイドの格納ファイルを再編成しました。このガイドの以前のリリースでは Cisco APIC クラスタ格納ファイルの高可用性は*Cisco APIC Getting* 開始ガイド、リリース *2.x* に以降されています。	該当なし
2.2(1n)	APIC クラスタのハイアベイラビリティ	Cisco APIC クラスタのハイ アベイラビリティ機能では、アクティブ/スタンバイ モードのクラスタで Cisco 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。

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
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。	N/A



第 2 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。
- Cisco APIC 6.0（2）以降、新しいタイプの SSL 証明書のサポート - ECDSA 証明書が有効になりました。この証明書は、Cisco APIC の以前のバージョンではサポートされていません。ECDSA 証明書を展開してからCisco APICの以前のバージョンにダウングレードすると、Cisco APICWeb サーバーは機能しません。Cisco APIC6.0（2）より前のバージョンにダウングレードする前に、RSA ベースの証明書を使用するようにCisco APIC Web サーバーを更新する必要があります。
- Cisco APIC 6.1(2) 以降では、最新の イメージにアップグレードする前に、グローバル AES 暗号化のチェックボックスを有効にする必要があります。これには、アップグレードを続行する前にグローバル AES 暗号化が有効になっていることを確認するための事前検証チェックが含まれています。

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

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 サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M1/L1、M2/L2 または、M3/L3にインストールする。

この手順では、ブート前実行環境（PXE）サーバーを使用してCisco Application Policy Infrastructure Controller（APIC）ソフトウェアをAPICサーバー M1/L1、M2/L2、または M3/L3 にインストールします。

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。

PXE サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M4/L4 にインストールする。

この手順では、Preboot Execution Environment（PXE）サーバーを使用してCisco Application Policy Infrastructure Controller（APIC）ソフトウェアをAPICサーバー M4/L4 にインストールします。

手順

ステップ 1 PXE サーバーに DNSMasq パッケージと HTTP サーバー パッケージをインストールします。

ステップ 2 インストールする ISO を、PXE サーバーがファイルをホストするパス （`/var/www/html` など）にダウンロードします。

ステップ 3 必要に応じて ISO を解凍またはマウントします。

例：

```
$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -oloop /var/www/html/aci-apic-dk9.6.0.2b.iso /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
```

ステップ 4 インストーラの EFI ファイルを、`/srv/tftp` などの PXE サーバーの TFTP パスにコピーします。

例：

```
$ cp -av /mnt/efi/EFI/BOOT/*.EFI /srv/tftp/
```

ステップ 5 ISOのマウント解除。

例：

```
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

ステップ 6 DNSMasq を構成します。

例：

次のテキストは構成例です。必要に応じて設定を変更してください。これを `/etc/dnsmasq.conf` 構成ファイルに保存して、デフォルトの構成を上書きします。

```
interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

# UEFI PXE clients only.
dhcp-vendorclass=BIOS,PXEClient:Arch:00000

# Boot directly into shim.
dhcp-boot="BOOTX64.EFI"
```

```
# Use this option to pass parameters to the installer. Currently only
# atxi.wipe= and atomix.isourl are supported.
dhcp-option-force=129,"atomix.isourl=http://ipaddress-of-PXE-server/path/to/install/iso"

# Create a DHCP range and set the gateway.
dhcp-range=rack-rack1-data0,192.168.41.0,static,255.255.255.0,infinite
dhcp-option=rack-rack1-data0,3,192.168.41.1

# Static mapping for clients.
dhcp-host=52:54:00:a2:34:c0,,192.168.41.2,brick2-data2,infinite
dhcp-host=52:54:00:a2:34:02,,192.168.41.3,brick2-data3,infinite
dhcp-host=52:54:00:a2:34:03,,192.168.41.4,brick2-data4,infinite
```

ステップ 7 PXE サーバを再起動します。

ステップ 8 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。

PXE サーバを使用する Cisco APIC のインストール

PXE サーバを使用して、UEFI、UEFI セキュアブート、およびレガシー BIOS システムの Cisco Application Policy Infrastructure Controller （APIC）ISO をインストールできます。

次のソフトウェアがシステムにインストールされていることを確認します。

```
sudo apt install -y dnsmasq lighttpd syslinux-common pxelinux
```

DNSMasq の構成

新しい **dnsmasq** 構成を作成するには、以下のコマンドを実行します。

```
$ sudo systemctl stop dnsmasq
$ sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
$ sudo mkdir -p /srv/tftp
```

次のコード スニペットでは、ISO をホストしている HTTP サーバの IP の詳細を入力し、HTTP サーバの IP に到達できる必要があるクライアントの DHCP サブネット範囲を構成する必要があります。変更を含む構成ファイルを保存した後、次のコマンドを実行します。

```
sudo systemct restart dnsmasq
```

```
interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

dhcp-match=x86PC,  option:client-arch, 0  # matches legacy BIOS x86
dhcp-match=BC_EFI, option:client-arch, 7  # matches UEFI x86-64

# Load different PXE boot image depending on client architecture
pxe-service=tag:x86PC,X86PC,   "Install Linux on x86 BIOS",    pxelinux.0
pxe-service=tag:BC_EFI,BC_EFI, "Install Linux on x86-64 UEFI", bootx64.efi

# Set bootfile name only when tag is "bios" or "uefi"
```

```
dhcp-boot=tag:x86PC,pxelinux.0      # for Legacy BIOS detected by dhcp-match above
dhcp-boot=tag:BC_EFI,bootx64.efi    # for UEFI arch detected by dhcp-match above

# Enable PXELinux client options
dhcp-option=tag:x86PC,208,f1:00:74:7e  # pxelinux.magic string

# set boot params, note the ip/network is tied to the netplan config in this layer
dhcp-option-force=129,"atxi.wipe=true atomix.isourl=http://<IP of your HTTP
server>/atomix.iso"

# an example IPV4 subnet range
dhcp-range=192.168.41.3,192.168.41.50,12h
dhcp-lease-max=25
```

HTTP設定

デフォルトの **lighttpd** 構成ファイルは、ポート 80 のすべてのインターフェイスでリッスンするため、変更する必要はありません。

（注） ファイルの名前は、 `dhcp-option-force=129` 設定の `/etc/dnsmasq.conf` 値と一致する必要があります。この値は DHCP 設定を介してマシンに渡され、URL を使用して **iso** ファイルをダウンロードします。

インストーラ **ISO** ファイルを次のパスにコピーします。

```
/var/www/html/<ISONAME.iso>
```

PXELINUX の構成

BIOS/レガシーを介して再起動するシステムは、pxelinux を使用してインストーラを取得します。上記の **DNSMasq** 構成ファイルの **tftp** の場所が、これらのファイルと構成をコピーするか、必要に応じてコマンドを調整するために使用されていることを確認します。

```
sudo mkdir -p /srv/tftp
sudo cp -av /usr/lib/PXELINUX/* /srv/tftp/
sudo cp /usr/lib/syslinux/modules/bios/* /srv/tftp/
sudo mkdir -p /srv/tftp/pxelinux.cfg
```

次の設定を `/srv/tftp/pxelinux.cfg/default` の場所にコピーし、HTTP サーバーの IP と ISO へのパスに一致するように HTTP URL を変更します。

```
DEFAULT atomix-install

label atomix-install
  kernel vmlinuz
  append initrd=initrd.img ro verbose debug console=tty0 console=ttyS0,115200n8
atomix.isourl=http://<HTTP_IP>/<ISO NAME>
  sysappend 3
```

ISO からのコンテンツの抽出

ISO を取得したら、次に示すように、ISO からいくつかのファイルを抽出し、特定のディレクトリに配置する必要があります。

```
$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -oloop /var/www/html/<ISO filename> /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
$ cp -av /mnt/efi/EFI/BOOT/BOOTX64.efi /srv/tftp/bootx64.efi
$ cp -av /mnt/efi/EFI/BOOT/GRUBX64.efi /srv/tftp/grubx64.efi
```

```
$ cp -av /mnt/iso/isolinux/vmlinuz /srv/tftp/vmlinuz
$ cp -av /mnt/iso/isolinux/initrd.img /srv/tftp/initrd.img
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

テスト

構成を適用したら、テスト システムをインストーラで起動し、ネットワーク設定を構成し、HTTP を介して ISO をシステムにダウンロードして、インストールを続行する必要があります。

PXE サーバーでは、次の **dnsmasq** サービスを使用できます。

```
sudo journalctl --follow -u dnsmasq
```

（注） 一部の **dnsmasq** ログエントリには、次のようなエラーが表示される場合があります。ただし、これらのエラーは致命的ではなく、ファームウェアの UEFI PXE クライアントは再試行します。

```
Feb 17 01:01:25 ubuntu dnsmasq-dhcp[1201]: 1836224829 sent size: 10 option: 43 vendor-encap
  06:01:08:0a:04:00:50:58:45:ff
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: error 8 User aborted the transfer received
from 192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/bootx64.efi to
192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/bootx64.efi to 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: error 3 User provided memory block is too
small received from 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/grubx64.efi to
192.168.41.3
Feb 17 01:02:09 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/grubx64.efi to 192.168.41.3
```

PXE クライアントでは、シリアル コンソール出力にインストールが表示され、特に ISO を取得する方法が表示されます。

これは、インストーラ **iso** ファイルを取得する方法を示すインストーラ出力の一部です。

```
++ cmdline=' BOOT_IMAGE=vmlinuz initrd=initrd.img ro verbose debug console=tty0
console=ttyS0,115200n8 atomix.isourl=http://192.168.41.2/atomix.iso ip=192.168.41.41:192.'
++ case "$cmdline" in
++ val='http://192.168.41.2/atomix.iso
ip=192.168.41.41:192.168.41.2:192.168.41.2:255.255.255.0 BOOTIF=01-52-54-00-12-34-56 '
++ val=http://192.168.41.2/atomix.iso
++ echo http://192.168.41.2/atomix.iso
+ ksurl=http://192.168.41.2/atomix.iso
+ '[' -z http://192.168.41.2/atomix.iso ']'
+ '[' -n http://192.168.41.2/atomix.iso ']'
+ '[' -z '' ']'
+ dhclient
[    3.573160] 8021q: adding VLAN 0 to HW filter on device ens4
+ tmpiso=/tmp/atomix.iso
++ seq 1 3
+ for count in $(seq 1 3)
+ '[' http: = https ']'
+ busybox wget --output-document=/tmp/atomix.iso http://192.168.41.2/atomix.iso
Connecting to 192.168.41.2 (192.168.41.2:80)
atomix.iso           100% |*******************************|  842M  0:00:00 ETA
+ break
+ mkdir -p /cdrom
```

```
+ mount -o loop,ro /tmp/atomix.iso /cdrom
[    4.896038] ISO 9660 Extensions: RRIP_1991A
+ echo 'Found install image through PXE'
Found install image through PXE
...
```

仮想メディアを使用する Cisco APIC ソフトウェアのインストール

仮想メディア（vMedia）を使用した Cisco Application Policy Infrastructure Controller（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 マップされた vDVD** 機能を使用して .iso イメージをマウントします。ローカル コンピュータのファイルをマップする、 **vKVM マップされた vDVD** 機能を使用しないでください。これは、大きなイメージの場合信頼性の高いできず、インストールに失敗する原因になります。また、Cisco APIC ではサポートされていません。
- 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） インストール時間を大幅に短縮するには、インストーラの起動後にISOイメージのURLを2回目に入力することをお勧めします。この高速化により、 HTTP と HTTPS の両方がサポートされますが、ユーザー/パスワード認証はサポートされません。

迅速化プロセスをスキップし、ユーザー/パスワード認証を有効にするには、次のプロセスを使用します。

- **Cisco APIC 6.0(2) より前のリリースの場合**：

  コンソールに「To speed up the install, enter the ISO URL:」というプロンプトが表示されます。10分後に入力が提供されない場合、インストーラはCIMC 仮想メディア（vMedia）マッピングを介してISOコンテンツを読み取る低速パスを続行します。10 分間の待機期間中に任意の時点で **Enter** キーを押しても、低速パスのインストールプロセスがすぐに続行されます。10分間の待機期間が経過してから **Enter** キーを押しても効果はありません。

- **Cisco APIC 6.0.(2) の場合**：

  コンソールに次のプロンプトが表示されます。「To speed up the install, enter iso url. ローカルメディアを使用するには、'skip' と入力してください："このプロンプトには入力が必要です。URL または「skip」という単語を指定する必要があります。指定しないと、無期限に待機します。

- **すべての Cisco APIC バージョンの場合**：

  短縮をスキップした場合、それ以上の入力は必要ありません。ISO URL を指定した場合は、 ISO を提供するホストへの接続を持つインターフェイスを起動するために、ホストネットワーク構成も提供する必要があります。 **[DHCP]**（使用可能な場合）または **[静的（Static）]** のいずれかを選択してプロンプトに応答し、適切なインターフェイスを選択して、必要に応じて詳細なプロンプトに応答します。この時点で、インストーラはISOを完全にダウンロードし、それ以上の入力を必要とせずにインストールします。

CIMC ソフトウェアのアップグレード

（注） Cisco APIC リリース 6.2(1) 以降では、 CIMC に個別にログインする代わりに、 APIC を介して Cisco APIC CIMC をアップグレードできます。詳細については、リリース 6.2x 以降からの Cisco APIC CIMC のアップグレードまたは、ダウングレード （138 ページ）を参照してください。

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 225 M6（第 4 世代アプライアンス APIC-SERVER-M4 および APIC-SERVER-L4）
- 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 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-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-M4	UCS-C225-M6	中規模の CPU、SSD、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 2 世代コントローラで構成されるクラスタ。
APIC-SERVER-L4	UCS-C225-M6	大規模の CPU、SSD/NVME、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-G5	UCS-C225-M8	大規模の CPU、NVME、およびいずれかのサイズのメモリ

APIC プラットフォーム	対応する UCS プラットフォーム	説明
		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。

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。

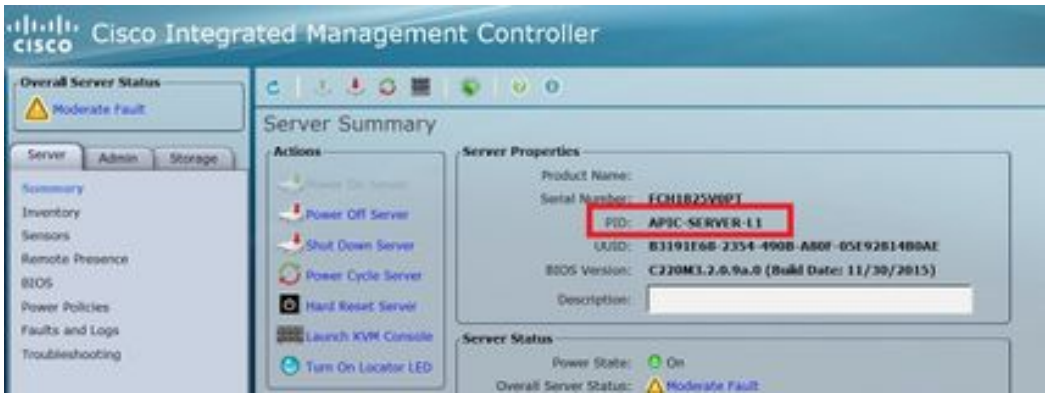
手順

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。

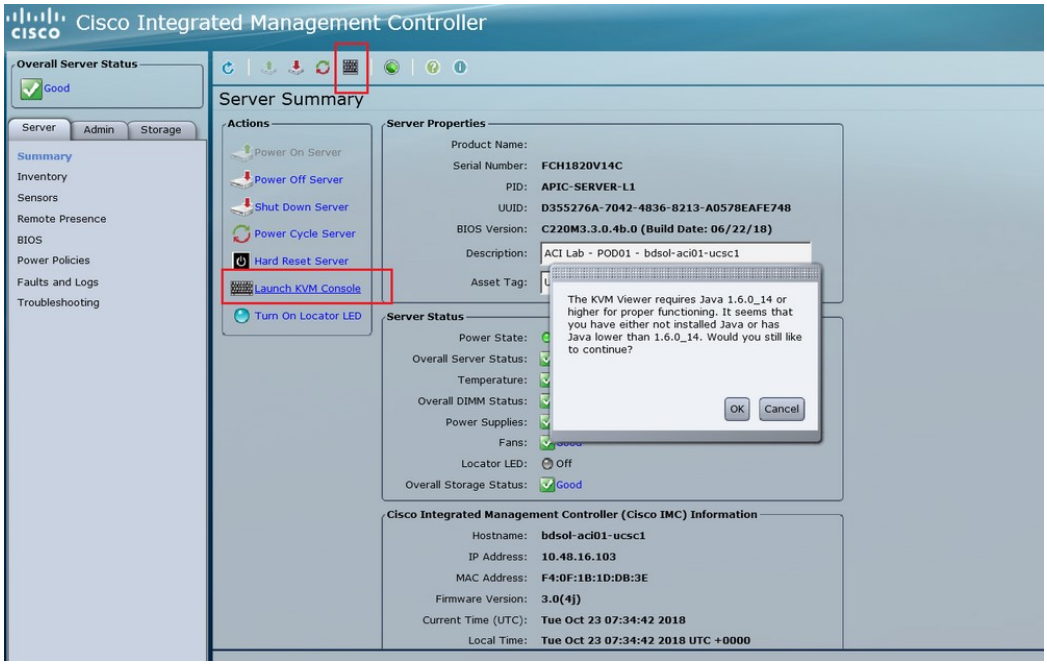
表に示されている UCS バージョンは、対応する APIC リリースに基づく、最新バージョンの CIMC ソフトウェアではない可能性があることに注意してください。たとえば、APIC リリースの 3.0 ブランチの場合、対応する CIMC ソフトウェアリリースは 3.0(3e) である可能性があります。これは必ずしも CIMC ソフトウェアの最新リリースではありませんが、APIC リリースの3.0 ブランチ CIMC ソフトウェアの正しいバージョンです。

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。

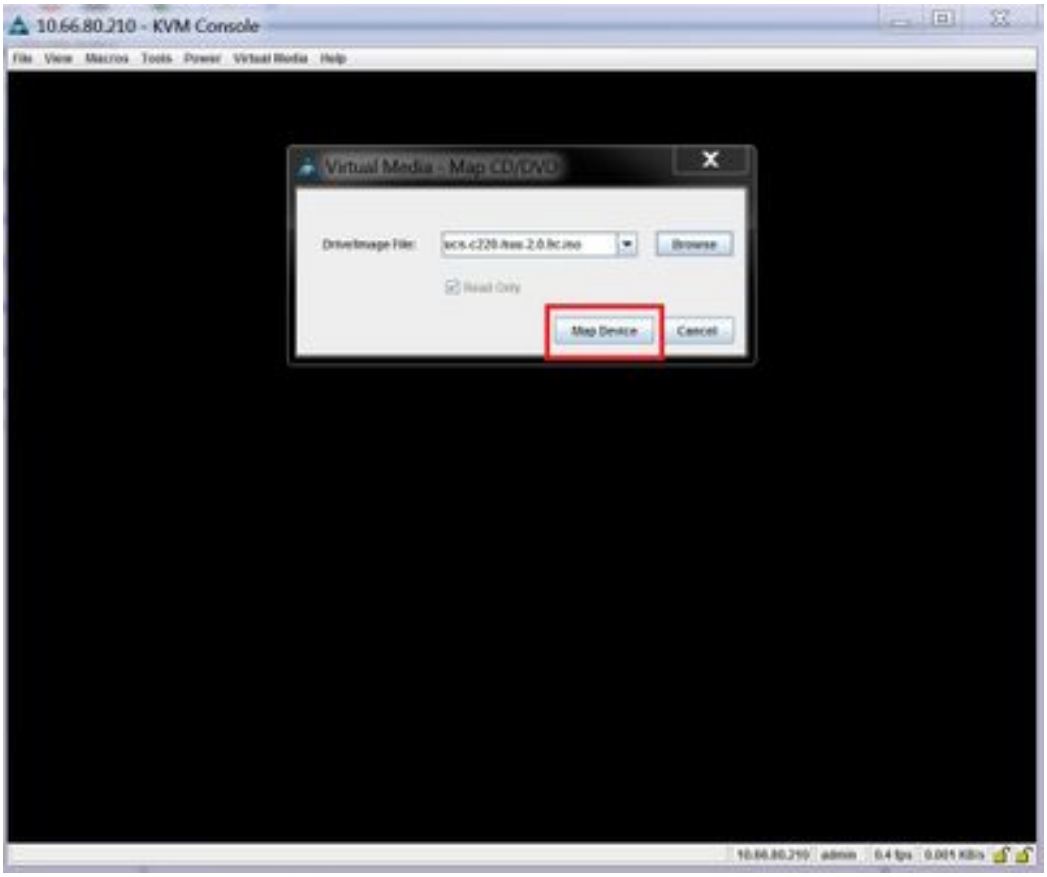


（注）
KVM コンソールを開く際に問題が発生した場合は、通常、Java のバージョンで問題が発生しています。お使いの CIMC バージョンで使用可能なさまざまな回避策については、Cisco APIC リリース ノートを参照してください。これは APIC のドキュメンテーション ページで確認できます。

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。

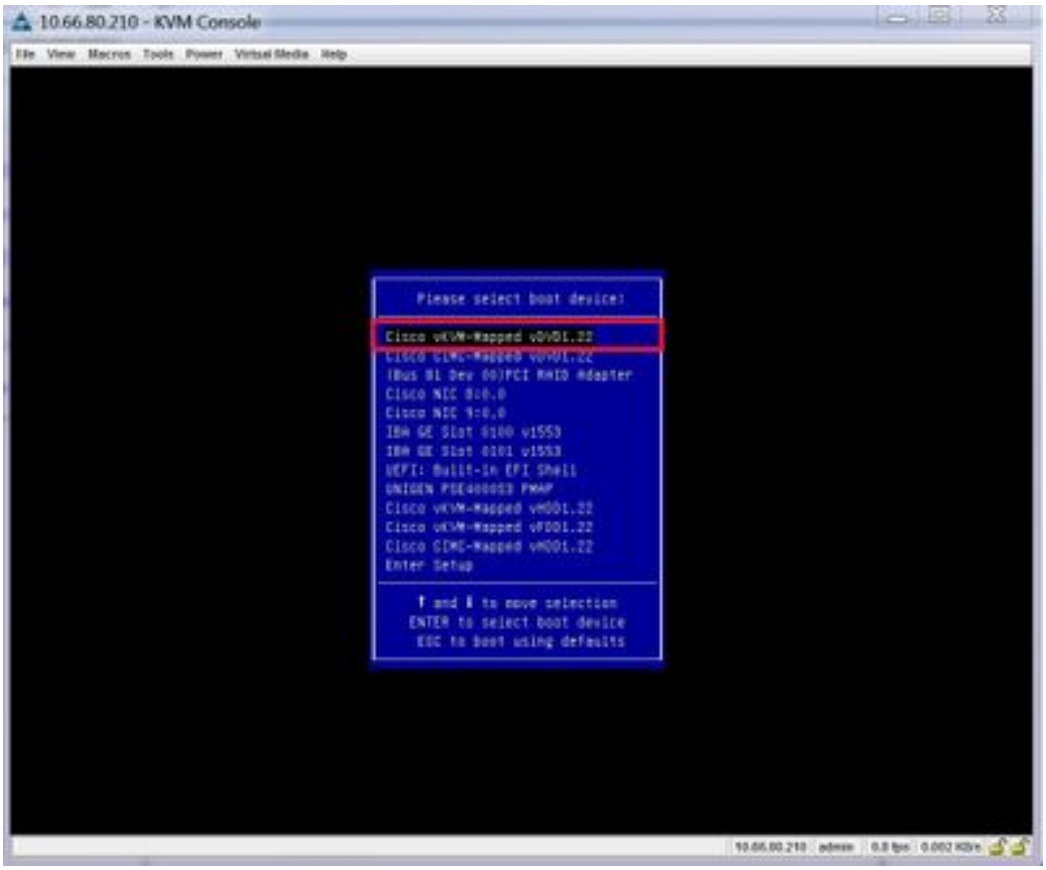
ステップ 12 **[F6]** を押してブート メニューを表示し、マップされた DVD を選択してブートできるようにします。

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。

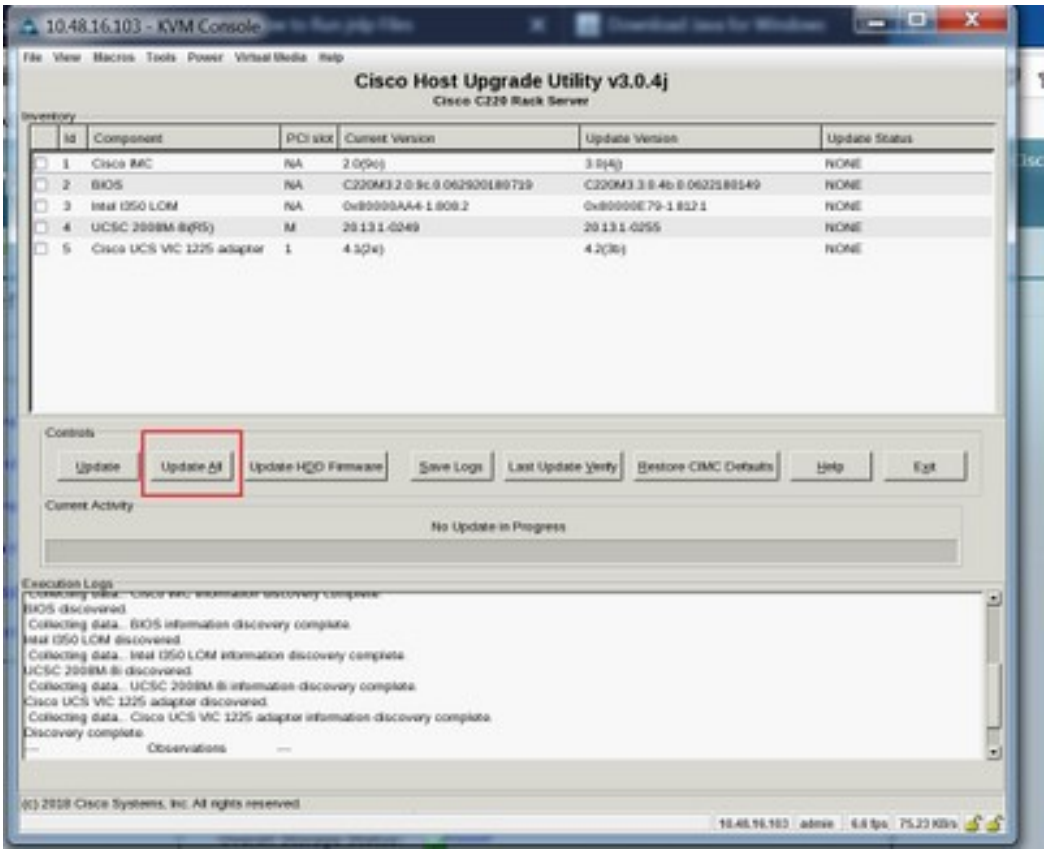


ステップ 15 プロセスが完了するのを待ち、プロンプトが表示されたら、利用規約に同意します。

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。

- vKVM 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 （22 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。

- APIC-M4/L4 サーバは CIMC 接続で構成する必要があります。
- Cisco APIC ISO は、APICM4/L4 サーバ CIMC 管理インターフェイスおよび OOB 管理インターフェイスから到達可能な HTTP サーバで使用可能である必要があります。
- Cisco.com から関連する Cisco APIC.iso イメージを取得し、.iso イメージを HTTP サーバにコピーします。

手順

ステップ 1 vKVM 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 からの APIC-M1、M2、M3、L1、L2、または L3 サーバの場合、**[サーバ（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。

c) APIC-M4/L4 サーバの場合、CIMC GUI から**[サーバ（Server）] > [サマリ（Summary）] > [KVM の起動（Launch vKVM）]** を選択し、HTTP ベース vKVM コンソールにアクセスします。

ステップ 2 **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 3 **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 4 **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 5 **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 3 （31 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 6 **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 7 **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。このオプションは、Cisco APIC バージョン 5.3(x)、6.0(2) 以降ではサポートされていません。

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) 2.c （31 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 8 **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 9 **SOL コンソールから**: 次のように入力します。

a) 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：

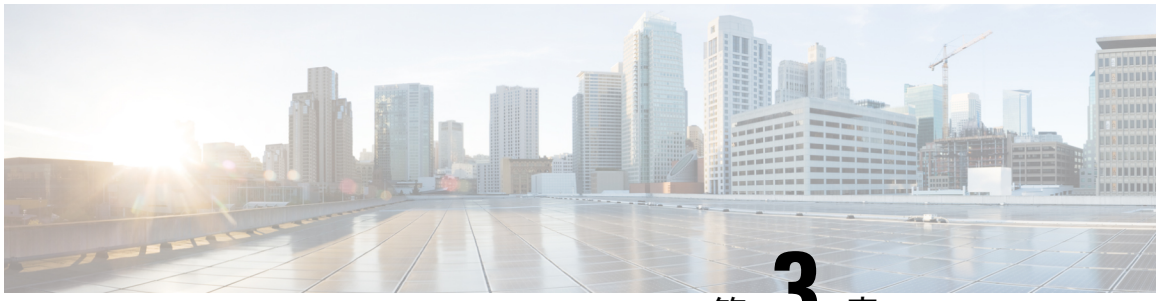
```
acidiag touch clean
acidiag reboot
```

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 3 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***

ファームウェアのタイプ	説明	例
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 （189 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***
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（183 ページ）を参照してください。	***aci-srpkg-dk9.1.0.0.bin***

アップグレードまたはダウングレードするワークフローを Cisco ACI ファブリック

Cisco APIC は、ファブリック全体のアップグレードとダウン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、アップグレードまたは、ダウン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、アップグレードまたは、ダウン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 Cisco APIC および ACI スイッチ リリースを選択します。
    1. Cisco APIC と ACI スイッチの両方を同じリリースにアップグレードまたは、ダウングレードする必要があります。
    2. 相互に互換性のある Cisco 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、Cisco APIC リリース 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 リリースを確認します。
2. 現在のリリースからサポートされているアップグレードとダウン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（APIC Upgrade/Downgrade Support Matrix）]* を参照してください。

1. 現在のリリースとターゲット リリース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 マトリックス（*APIC Upgrade/Downgrade Support Matrix*）*]* で推奨されている中間バージョンに Cisco APIC とスイッチの両方をアップグレードまたは、ダウングレードする必要があります。詳細については、「マルチ アップグレードとダウングレード （47 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（*APIC Upgrade/Downgrade Support Matrix*）*]* には、ターゲット Cisco APIC リリース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/ダウングレード アーキテクチャ （61 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 Cisco APIC イメージにパッケージされているものを除き、Cisco APIC 上のすべての App Center アプリを無効化します。

   Cisco APIC リリース 6.1(2) 以降では、App Center が廃止ているため、これは適用されません。

   詳細については、App Center アプリの注意事項 （48 ページ）を参照してください。

6. Cisco APIC と ACI スイッチ ファームウェアの両方を Cisco 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 （95 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 （103 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 （116 ページ）
   - リリース6.0(2)以降では、Cisco APICアップグレードが正常に完了した後に、32ビットと64ビットの両方のスイッチイメージをダウンロードします。詳細については、「32 ビットと 64 ビットの両方の ACI モード スイッチ イメージをダウンロードする （6.0(2) 以降） （82 ページ）」を参照してください。
   - リリース 6.2 以降： APIC で APIC とスイッチ イメージをダウンロードする （116 ページ）

7. Cisco 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または、ダウングレード前にCisco 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 （44 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/ダウングレード前のチェックリスト （81 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、Cisco 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 コンポーネントをアップグレードまたは、ダウングレードします。

   Cisco APIC がリリース 6.2(1) 以降を実行している場合は、 APIC を介して CIMC ソフトウェアをアップグレードできます。詳細については、リリース 6.2x 以降からの Cisco APIC CIMC のアップグレードまたは、ダウングレード （138 ページ）を参照してください。

   それ以外の場合は、 CIMC ユーザー インターフェイスを使用した CIMC のアップグレードの詳細については、CIMC ソフトウェアのアップグレード （22 ページ） を参照してください。

10. Cisco APIC をアップグレードまたはダウングレードします。

    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 のアップグレードまたは、ダウングレード （97 ページ）
    - リリース 4.x または 5.0： Cisco APIC のリリース 4.x または 5.0 からのアップグレードまたはダウングレード （106 ページ）
    - リリース 5.1 以降： リリース 5.1x 以降からの Cisco APIC のアップグレードまたは、ダウングレード （118 ページ）
    - リリース 6.2 以降： リリース 6.2x 以降からの Cisco APIC のアップグレードまたはダウングレード （140 ページ）

11. 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/ダウングレード前のチェックリスト （81 ページ）を参照してください。

12. ACI モード スイッチをアップグレードまたはダウングレードします。

    1. すべての Cisco 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または、ダウングレード（99 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 Cisco 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または、ダウングレード（110 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または、ダウングレード（121 ページ）
- リリース 6.2 以降：リリース 6.2x 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または、ダウングレード（143 ページ）

13. これが **[マルチステップ アップグレード（Multistep Upgrade）]** の場合は、上記の手順を繰り返して、Cisco APIC とスイッチの両方の即時リリースへのアップグレードまたは、ダウングレードが完了し、Cisco APIC クラスタ ステータスが **[完全に適合した（Fully Fit）]** 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または、ダウングレードします。

（注） Cisco ACI ファブリックの展開環境に Cisco AVS/AVS が含まれている場合は、Cisco AVS/AVS を Cisco APIC との互換性があるリリースにアップグレードまたは、ダウングレードしてください。Cisco AVS / AVEをアップグレードまたは、ダウングレードするには、[Cisco ACI 仮想エッジ インストール ガイド（Cisco ACI Virtual Edge Installation Guide）]の**[Cisco APIC、ファブリック スイッチと Cisco ACI 仮想エッジの推奨されているアップグレード順序（Recommended Upgrade Sequence for Cisco APIC, the Fabric Switches, and Cisco ACI Virtual Edge）]**を参照してください。

ACI スイッチ アップグレードとダウングレードのガイドライン

ACI スイッチのアップグレードとダウン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（42 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（42 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（42 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（43 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（44 ページ）
- ACI スイッチのグレースフル アップグレードまたは、ダウングレード（45 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 アップグレードまたは、ダウングレード（45 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 リモート リーフ スイッチです。
- 同時キャパシティ（同時にアップグレードまたは、ダウン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または、ダウン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または、ダウン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または、ダウン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または、ダウングレード 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または、ダウングレードされます。
- Cisco APIC リリース 4.1（1）以降、グレースフルアップグレードまたは、ダウン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、アップグレードまたは、ダウングレードは拒否されます。

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または、ダウングレードされます。
- 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または、ダウングレード （99 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 Cisco 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または、ダウングレード （110 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または、ダウングレードされます。
- 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、アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 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または、ダウン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または、ダウン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 アップグレードまたは、ダウングレード

アップグレードまたは、ダウングレード手順を実行するときにユーザー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。**[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 Cisco APIC 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または、ダウングレードを実行しようとすると、プロセスで機能不全が発生したり、不完全なステータスで無限に止まる可能性があるため、スイッチ上でのこの状態のスイッチに対するファームウェア アップグレードまたは、ダウン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 アップグレードとダウングレードのガイドライン （41 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 （42 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 （43 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 （42 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。

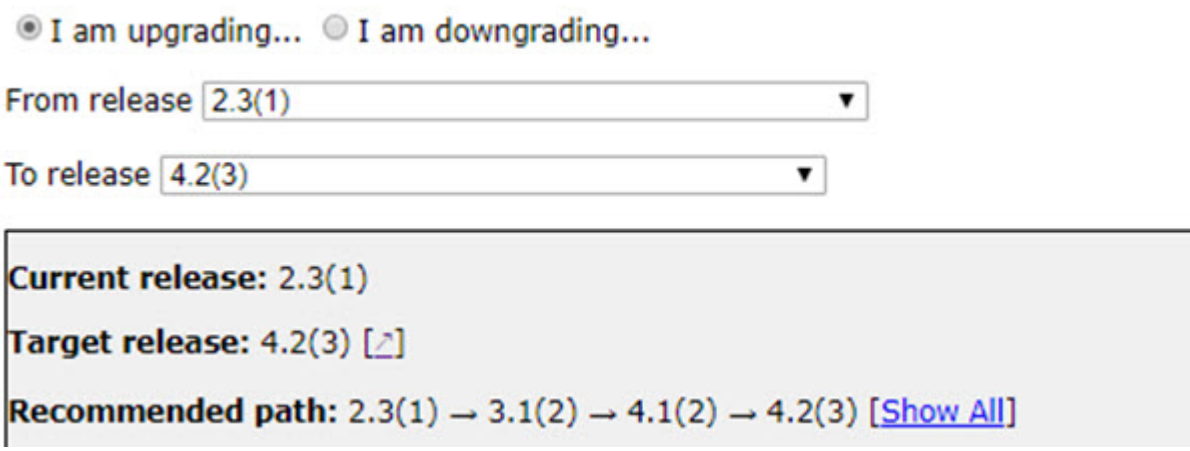
マルチ アップグレードとダウングレード

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または、ダウン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または、ダウングレード

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中に許可される操作 （71 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。

（注） Cisco ACIリリース 6.1(2) 以降、App Center が廃止たため、これは適用されなくなりました。

- 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 （49 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 （49 ページ）

現在のソフトウェア バージョンの決定

（注） クラスタをアップグレードする場合、クラスタに参加するには、すべての Cisco APIC が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。ファブリックに参加するときの自動アップグレードは、 APIC リリース 6.0(2) までは使用できません。詳細については、APIC 検出の自動ファームウェア更新 （175 ページ）を参照してください。

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。

スケジューラを使用してアップグレードまたは、ダウングレードすることについて

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また、ダウングレードなど、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、アップグレードまたは、ダウン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） ACI 6.2(1) リリース以降、アップグレードまたはダウングレードのスケジューラはサポートされていません。

- 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。

APIC リリース 5.1 以降、GUI スケジューラ オプションはサポートされなくなりました。

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：	[[[yyyy:]mmm:]dd:]HH:MM 形式で開始時刻を設定します。

	コマンドまたはアクション	目的
	apic1(config-scheduler-absolute)# **time start 2016:jan:01:12:01**	
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。
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。

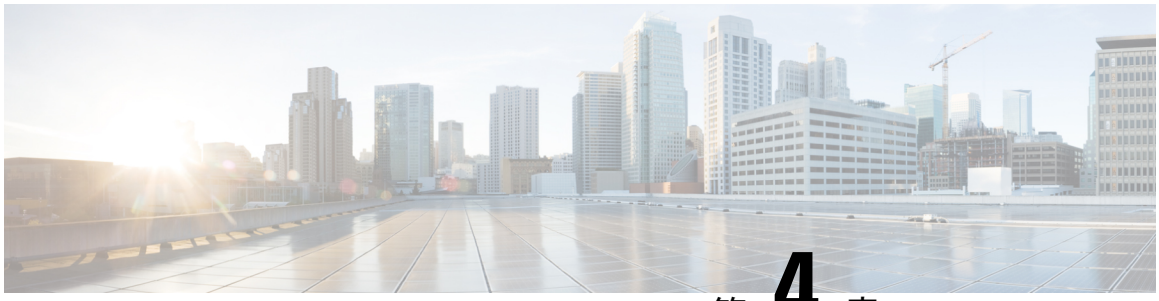
例：

```
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 4 章

ACI アップグレード/ダウングレード アーキテクチャ

APIC アップグレードとダウングレードの概要

APIC クラスタのアップグレードまたは、ダウングレードを実行する場合は、アップグレードまたは、ダウングレードされた 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または、ダウン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または、ダウン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または、ダウン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、アップグレードまたは、ダウングレードプロセスを高速化するために並行して行われます。
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構成、運用データ、監査ログなどのレコードオブジェクトを含むデータベース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。

   ソース バージョンが APIC リリース 6.0(3) 以降の場合、データベース変換プロセスが強化され、以前のリリースと比較してこのプロセスの待機時間が短くなることがあります。

   ソース バージョンが APIC リリース 6.2(1) 以降の場合、 APIC 1 はアップグレードの一元的なオーケストレーション ポイントとして機能し、 APIC クラスタ全体に分散されるすべてのデータベースのデータベース変換を一度に実行します。他の APIC は、それ自体にローカルな特別な APIC に対してのみ変換を実行します。これにより、クラスタ同期の問題のリスクを軽減することで、より堅牢な変換プロセスが提供されます。

（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、「アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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、4 （61 ページ） 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。その間、オンラインに戻ったAPICは、データベースの最終チェックとしてアップグレード後のアクティビティを開始します。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または、ダウングレードされるまで繰り返されます。
6. Cisco APIC 6.0(6) より前は、すべての APIC がオンラインに戻り、アップグレード後のアクティビティに関係なく完全に適合したときに、 APIC クラスタのアップグレードが完了したと見なされました。Cisco APIC 6.0(6) 以降、各 APIC ノードでアップグレード後のアクティビティが完了するまで、 APIC クラスタのアップグレードのステータスは「Post Upgrade Pending」に移行します。その後、アップグレードステータスが最終的に「Completed」になります。

（注） スイッチのアップグレードを続行する前に、 APIC でのアップグレード後のアクティビティを正常に完了する必要があります。一般に、 APIC クラスタとスイッチのアップグレードは同じメンテナンス期間中に発生しない可能性があるため、 APIC クラスタのアップグレード前とスイッチのアップグレード前に、それぞれ pre-upgrade validation script を実行することをお勧めしウィンドウ。ただし、Cisco APIC 6.0(6) より前では、同じメンテナンス ウィンドウ内で行われる場合でも、スイッチのアップグレード前にスクリプトを実行することを強くお勧めします。このスクリプトは、アップグレード前の検証だけでは、アップグレード後のアクティビティのステータスも確認して、APIC クラスタのアップグレード後にファブリックによりスイッチのアップグレードを続行する準備ができていることを確認するためです。

7. Cisco APIC 6.1(2) 以降、すべてのアクティブな APIC ノードがアップグレードされた後、スタンバイ APIC ノードで同じアップグレード手順が実行されます。詳細については、『Cisco APIC 6.1 向けスタートアップ ガイド』を参照してください。

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 のアップグレードとダウングレード段階の説明

Cisco ACI リリース 6.2(1) 以降、 APIC アップグレード プロセスが強化されました。ここでは、APIC アップグレード プロセスについて説明します。アップグレードはいくつかの段階に進み、それぞれ前の段階を完了した上に構築されます。

1. アップグレード プロセスは常に APIC1 で開始されます。
2. APIC1 は、いくつかのクラスタ全体のアップグレード段階を実行し、アップグレードされる最初の APIC です。
3. APIC1 はそれ自体をアップグレードする準備ができると、内部 API コールを使用して制御を APIC2 に渡します。
4. その後、APIC1 はノード アップグレード モードで動作し、独自のアップグレードを完了します。
5. この間、UI は APIC 2 にリダイレクトされます。
6. APIC2 は制御を APIC1 に返し、UI がリダイレクトされます。
7. APIC1 は、同じ方法でクラスタ内の残りの APIC のアップグレードを続行します。
8. すべての APIC がターゲット バージョンにアップグレードされると、APIC1 は最終クラスタ全体の段階を実行し、アップグレード サイクルを完了します。

次の表に、アップグレード プロセスの各段階で何が発生するかを示します。

名前（Name）	ステージ レベル	説明
致命的な障害のチェック	クラスタ全体	アップグレード前の検証を開始して、アップグレードを実行できることを確認します。
クラスタ アップグレードの準備	クラスタ全体	アップグレードのコールバックを確認し、クラスタのバージョンを要求されたアップグレード バージョンに設定します。
アップグレードの準備	ノードのレベル	すべての状態のアップグレード前の状態を設定します。
新しい OS のステージング	ノードのレベル	抽出されたターゲット イメージを使用してデータ変換のための環境をセットアップします。
データベースをフリーズする	ノードのレベル	データ変換のためにデータベースをフリーズし、Perperdown の完了を監視します。
APIC サービスを停止する	ノードのレベル	サービスをシャットダウンします。
ステージ データベース変換	ノードのレベル	データ変換のための設定
データベース変換	ノードのレベル	データ変換を行います。
新しい OS のインストール	ノードのレベル	新しい OS をインストールします。
再起動	ノードのレベル	アップグレードに基づいて、コンテナまたは kexec を再起動して、リロード操作を実行します。
OS 構成を確定する	ノードのレベル	状態の確定が完了しました。
クリーンアップ	ノードのレベル	アップグレード後のアクティビティを確認します。

名前（Name）	ステージ レベル	説明
HyperFlex クラスタの健全性の検証	ノードのレベル	すべてのノードが正常な状態であることを確認します。
データベースのアップグレードのファイナライズ	ノードのレベル	クラスタが正常であることを確認します。
クラスタのアップグレード検証	ノードのレベル	クラスタのアップグレード後のチェックを実行します。
クラスタ状態の確定	クラスタ全体	すべてのシャードでアップグレード後が完了しているかどうかを確認し、APIC バージョンを確認します。
クラスタ状態の検証中	クラスタ全体	すべての APIC でアップグレードのコールバックをリセットする

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 アップグレードとダウングレードの概要

ACI スイッチ ノードのアップグレードとダウングレードを実行すると、アップグレードとダウン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とダウン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または、ダウングレード中は、完了した段階に基づいてアップグレードまたは、ダウン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または、ダウン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。

アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項

- Cisco APIC 6.2 以降のリリースから 6.2(1) 以前のリリースへのダウングレードはサポートされていません。詳細については、ダウングレードのチェックリスト （85 ページ）を参照してください。
- いずれかの時点で、アップグレードまたは、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Application Policy Infrastructure Controller（APIC） をリロードしないでください。
  - クラスタ内の Cisco 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、これら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 （171 ページ） および ACI スイッチ インストーラのログ ファイル （172 ページ） を参照）。これは、アップグレードまたは、ダウン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 （172 ページ） を参照）。
  3. アップグレードまたは、ダウン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。

- ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの 1 つのシャードにのみ保存されます。このため、アップグレードまたはダウングレードのために Cisco APICが再起動している間は、ログ レコードにアクセスできません。他のオブジェクトを介して読み取ることができる他のCisco APICとは異なります。
- Cisco APIC6.0（2）リリース以降にアップグレードするには、次の手順を実行する必要があります。

  1. Cisco APIC6.0（2）以降のイメージをダウンロードし、ダウンロードしたリリースにAPICクラスタをアップグレードします。この手順が完了する前に、Cisco Application Centric Infrastructure(ACI) モード スイッチ イメージを Cisco APIC にダウンロードしないでください。6.0（2）リリースには 32 ビットと 64 ビットの両方のスイッチ イメージがありますが、6.0（2）より前のリリースは 64 ビット イメージをサポートしていません。その結果、この時点で 64 ビット イメージをダウンロードすると、エラーや予期しない結果が生じる可能性があります。ただし、6.0(1) リリースを除き Cisco APIC に 5.2(8)以降のリリースがある場合は、この手順の前に、それ以前の他のアップグレー

ド手順と同じように 6.0(2) の前に Cisco APIC にスイッチイメージをダウンロードできます。

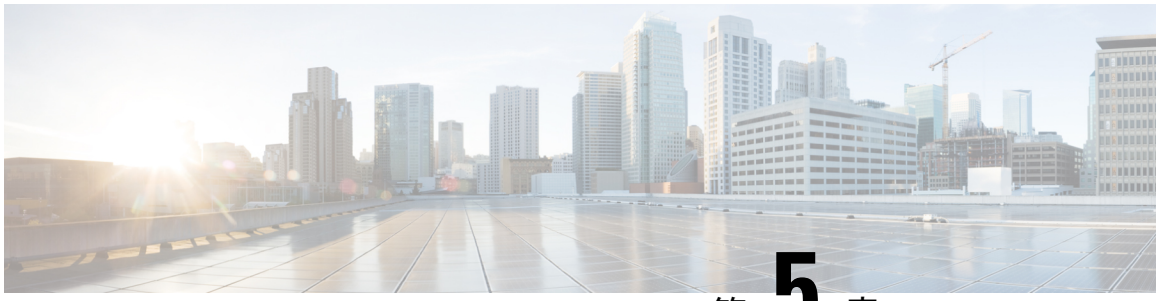
2. 32 ビットと 64 ビットの両方のCisco ACIモード スイッチ イメージをCisco APIC にダウンロードします。一つのイメージしかダウンロードしない場合、アップグレード中にエラーが生じることがあります。

   6.0(3)リリース以降、スイッチはスタティック マッピングに基づくのではなく、スイッチの使用可能なメモリに基づいてCisco APICからインストールするイメージを決定します。スイッチの使用可能なメモリが24GB以下の場合、スイッチは32ビットイメージをインストールします。スイッチの使用可能なメモリが32 GB以上の場合、スイッチを最初に 32 ビット イメージにアップグレードしてから、再度 64 ビット イメージにアップグレードできます。この場合、アップグレードプロセス中に2回のリブートが発生します。

   モジュラ スパイン スイッチは、スイッチの使用可能なメモリに関係なく、64ビットイメージをインストールします。

3. メンテナンス グループを作成し、通常どおりアップグレード手順をトリガーします。Cisco APICは、アップグレードプロセス中に適切なイメージをそれぞれのスイッチに自動的に展開します。

- アップグレード プロセス中にスイッチ ファームウェア グループを変更すると、アップグレード プロセスが完了せず、予期しないアップグレード動作が発生する可能性があります。



第 5 章

Cisco ACI スイッチの混合バージョン中に許可される操作

Cisco ACI スイッチの混合バージョン中に許可される操作

Cisco Application Centric Infrastructure（ACI）ファブリックには基本的に、すべてのノード（Cisco Application Policy Infrastructure Controller （APIC）、リーフスイッチ、およびスパインスイッチ）に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が必要です。この場合、Cisco APIC ノードの標準リリース フォーマットは 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 フォーマットの 1x.y（z）があります。たとえば、Cisco 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Cisco 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。

この要件を満たすユーザーを支援するためのオプションは 2 つあります。

- **混合バージョンのサポートの強化** ：混合バージョン V1 と V2 の古いバージョン V1 でサポートされているすべての機能、構成、および操作をサポートします。
- **限定された混合バージョンのサポート** ：以下に示す一部の機能、構成、および操作をサポートします。

Cisco ACI スイッチの混合バージョン中に許可される操作

混合バージョンのサポート条件

Enhanced Mixed Version Support と **Limited Mixed Version Support** の 両方が、以下の条件で利用可能です。

- 同時に最大 2 つのバージョン。例えば、V1 および V2 がサポートされます。V1、V2 および V3 はサポートされていません。
- APIC は常に V2 である必要がありますが、スイッチは V1 または V2 のいずれかです。V2 は新しいバージョンです。
- vPC ペアの両方のスイッチが同じバージョンである必要があります（両方が V1 または両方が V2）。

表 *2*: 制限付き混合バージョン サポートまたは拡張混合バージョン サポート

V1	V2	サポートされる操作
2.2(x) 以降	マトリクスで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	混合バージョンの限定的なサポート
マトリックスで拡張混合バージョンのサポートとして特に言及されているバージョン ペア。	マトリックスで拡張混合バージョンのサポートとして特に言及されているバージョン ペア。	混合バージョンのサポートの強化

混合バージョンのサポートの強化

APICリリース 6.2(1) 以降、混合バージョンのサポート条件 （72 ページ） で説明されている条件下で、**拡張混合バージョン サポート**が 導入されました。

上記の条件が満たされている場合、Cisco ACIファブリックは、V1 と V2 の混合バージョン（V1 が古く、V2 が新しい）のうち、古いバージョン V1 でサポートされているすべての機能、構成、および操作をサポートします。

強化された混合バージョン サポート により、ユーザーは、APIC と一部のスイッチが V2 を実行している場合でも、制限なくすべてのバージョンが V1 で実行されているかのようにファブリックを操作できます。これは、次のような状況に役立ちます。

- すべてのスイッチをアップグレードするには、複数のメンテナンス ウィンドウが必要です。
- V2 は、新しいスイッチ モデルにのみ必要です。
- V2 は、スイッチのサブセットにのみ必要です。

Cisco ACI スイッチの混合バージョン中に許可される操作

混合バージョンの限定的なサポート

混合バージョンのサポートの制限は、リリース 2.2(1) から利用可能になりました。混合バージョンのサポート条件に記載されている条件が満たされている場合、操作が古い（元の）バージョンですでにサポートされていた機能に関するものであれば、すべての Cisco ACI スイッチが同じバージョンにアップグレードされていない場合でも、以下にリストされている一部の限定された操作を実行できます。

（注） 次に示す操作は、アップグレード シナリオ専用です。ファブリックをダウングレードする場合、つまり APIC がスイッチよりも古いバージョンを実行している場合、これらは適用されずサポートされません。APIC が新しいバージョンを実行している間のスイッチのダウングレードはサポートされていません。

表 *3 :* リリース *2.2(x)* からのアップグレードにおける限定的な混合バージョン サポート対象のサポート操作

機能	操作
トラブルシューティング	• 設定のエクスポート • テクニカル サポートの収集
物理ネットワーク	リブート、ケーブル交換など
その他	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。 *この操作は、アップグレードが同じリリース トレイン内にある場合にのみサポートされます。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。

Cisco ACI スイッチの混合バージョン中に許可される操作

表 *4 :* リリース*2.3(x)* 以降からのアップグレードにおける限定的な混合バージョン サポート対象のサポート操作

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、レイヤ 2 外部、レイヤ 3 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。
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。

Cisco ACI スイッチの混合バージョン中に許可される操作

機能	操作
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	レイヤ 2 外部および レイヤ 3 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。 • 設定のエクスポート • テクニカル サポートの収集

Cisco ACI スイッチの混合バージョン中に許可される操作

機能	操作
物理ネットワーク	

機能	操作
	• 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。 リロードがステートレスである場合、つまり、構成が消去されて Cisco APIC から再度プルされるクリーン リロードである場合、スイッチのリリースは と同じである必要があります。 • スパイン スイッチ ライン カード、ファイバ チャンネル 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 スイッチを削除します。 • 新しいスパイン スイッチおよびリーフ スイッチの登録 新しいスイッチには、Cisco APIC と同じリリースが必要です。 • 仮想ポート チャネル 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 リンクをフラッピングし、ポート チャネルで 1 つのリンクをフラッピングして、FEX で NIF ポートをフラッピングし、リーフ スイッチの全面パネル ポートをフラッピングします。

機能	操作
	• ケーブルを交換します。
ファブリック ポリシー	• NTP サーバー、SNMP、BGP ルート リフレクタ、レイヤ 2 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。
その他	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* *この操作は、アップグレードが同じリリーストレイン内にある場合にのみサポートされます。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。

Cisco ACI-Mode スイッチの混合バージョンの注意事項と制約事項

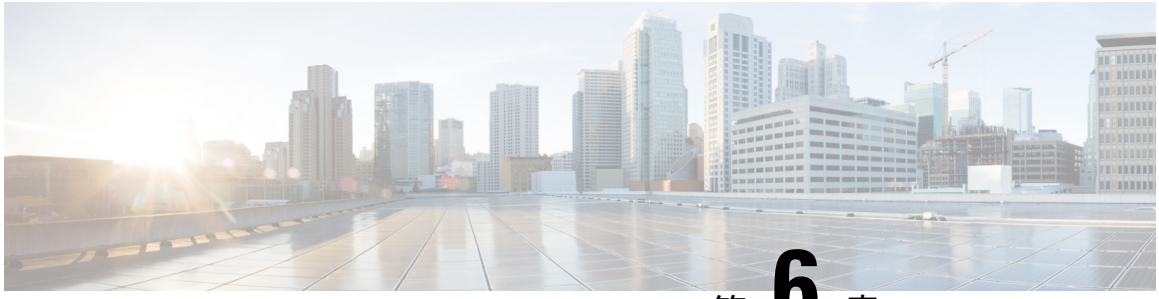
- 次の定義は、Cisco APIC リリースについて説明するために使用されます。
  - Cisco APIC メジャー リリースには、新しいソフトウェア機能およびその他のハードウェアの更新のサポートが含まれています。メジャー リリースの例には、2.2（1n）と 2.1（1h）が含まれます。
  - Cisco APIC マイナーまたはメンテナンス リリース（MR）には、バグ修正や既存のリリースからのパッチが含まれています。マイナーまたはメンテナンス リリースの例には、2.0（1m）と 2.0（2f）が含まれます。
  - Cisco APIC パッチ リリースには、特定の不具合の修正が含まれています。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。
- 3.0 以前のCisco APICリリースでは、ファブリック内のCisco 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、Cisco APICリリース 3.0 以降に削除されました。
- Cisco APICが5.2（4）以降のリリースを実行しており、スイッチで15.2（4）より前のCisco ACIモード スイッチ ソフトウェア リリースを実行している場合、ピア ノードが廃止されると、vPC ドメインのインターフェイスは一時停止/ダウンになります。vPC ピア ノードのグレースフル挿入（メンテナンス モード）でも、スイッチが自動的にデコミッションさ

れ、リブートされ、再稼働されるため、同じ問題が発生します。次のシナリオ例では、この問題が発生します。

- Cisco APICが 5.2（4）、6.0（1）、またはそれ以降のリリースを実行しており、vPCスイッチは -Cisco ACIモード スイッチ 14.2（7u）以前のリリースを実行しています。
- Cisco APICが 5.2（4）、6.0（1）、またはそれ以降のリリースを実行しており、vPCスイッチはCisco ACI モード スイッチ 15.2（3）以前のリリースを実行しています。

次のシナリオ例では、この問題は発生しません。

- Cisco APICが 5.2（4）、6.0（1）、またはそれ以降のリリースを実行しており、vPCスイッチでCisco ACIモード スイッチ 14.2（7v）、15.2（4）、16.0（1）、またはそれ以降のリリースを実行している。
- Cisco APIC 5.2（3）以前のリリースを実行している。



第 6 章

アップグレード / ダウン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または、ダウン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 （82 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

アップグレードまたは、ダウン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

Cisco Application Centric Infrastructure （ACI）のアップグレード前の検証を実行するための 3 つの異なるツールがあります。

- **アップグレード前検証ツール（APIC）**：Cisco Application Policy Infrastructure Controller（APIC）アップグレード構成に組み込まれている検証ツール。これは、Cisco 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 Cisco APIC にインストールできる検証ツール。ACI リリース 6.1.2 で App Center（dcappcenter.cisco.com）が廃止されたため、このオプションは廃止と見なされます。すべての ACI バージョンで他のオプションを活用。
- **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、アップグレード前にスタンドアロン スクリプトを Cisco APIC に直接実行して、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。

  問題にアドレスするための十分な時間を確保するために、メンテナンスウィンドウの少なくとも 2 週間前に検証を実行してください。

  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。

スクリプトでサポートされている検証のリストについては、https://datacenter.github.io/ACI-Pre-Upgrade-Validation-Script/validations/ を参照してください。

32 ビットと 64 ビットの両方の ACI モードスイッチイメージをダウンロードする（6.0(2) 以降）

Cisco APIC リリース 6.0（2）内以降では、32 ビットと 64 ビット Cisco ACI モード スイッチ イメージを Cisco APIC にダウンロードします。一つのイメージしかダウンロードしない場合、アップグレード中にエラーが生じることがあります。詳細については、「アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）」を参照してください。

廃止された管理対象のオブジェクト

Cisco APIC は、実行中のバージョンのソフトウェアに以下の廃止された管理対象のオブジェクトが存在するかどうかを確認し、構成に存在する場合はアップグレードをブロックします。構成を更新する必要があります。

- **Class: config:RsExportDestination**
- **Class: config:RsImportSource**
- **Class: fabric:RsResMonFabricPol**
- **Class: infra:RsResMonInfraPol**
- **Class: fabric:RsResMonCommonPol**
- **Class: trig:Triggered**
- **Class: trig:Triggered**
- **Class: fv:CCg**
- **Class: fv:RsToCtrct**
- **Class: mgmt:RsOobEpg**
- **Class: mgmt:RsInbEpg**
- **Class: vns:RsCIfAtt**
- **Class: fault:RsHealthCtrlrRetP**
- **Class: fv:PndgCtrctCont**
- **Class: vz:RsAnyToCtrct**
- **Class: fv:PndgCtrctEpgCont**
- **Class: fv:AREpPUpd**
- **Class: vns:Chkr**
- **Class: aaa:RsFabricSetup**
- **Class: ap:PluginPol**
- **Class: tag:ExtMngdInst**
- **Class: telemetry:Server**
- **Class: telemetry:FltPolGrp**
- **Class: telemetry:FilterPolicy**
- **Class: telemetry:Server**
- **Class: pol:RsFabricSelfCAEp**
- **Class: fabric:PodDhcpServer**

- **Class: fabric:SetupAllocP**
- **Class: fabric:AssociatedSetupP**
- **Class: cloud:AEPgSelector**
- **Class: fv:VmmSelCont**

アップグレードのチェックリスト

次のリストには、参照用の項目が含まれています。他のチェック ルールの詳細については、「ACIアップグレード前検証スクリプト」を参照してください。

- Cisco APICリリース 4.2（6o）、4.2（7l）、5.2（1g）以降にアップグレードする場合は、リーフ スイッチのフロントパネルのVLANプログラミングに明示的に使用しているVLANカプセル化ブロックがすべて「外部（ワイヤー）。」これらの VLAN カプセル化ブロックが代わりに「内部」に設定されている場合、アップグレードによって前面パネルのポート VLAN が削除され、データパスが停止する可能性があります。
- Cisco APIC が Cisco APIC 4.0 以前から 5.1(1) 以降にアップグレードされると、サービス グラフが再レンダリングされます。これにより、サービス グラフとの vzAny-to-vzAny コントラクト、そしてサービス グラフとの別のコントラクトが同じサービス EPG を使用する場合、再レンダリングが完了するまでトラフィックが中断されます。
- APIC バージョン 5.0 より前では、次の設定がある場合、プロバイダーからコンシューマへの方向のトラフィックが **誤って**許可されていました。これは APIC 5.0 以降で修正されました。その結果、誤って許可されたトラフィックは、5.0 より前のバージョンから 5.0 以降のバージョンへのアップグレード後に動作を停止します。プロバイダーからコンシューマへの方向をドロップしない場合は、それに応じてその方向のコントラクトフィルタ処理を設定します。
  - 単方向コントラクト（「両方向の適用（Apply Both Direction）」フラグなしのコンシューマからプロバイダーへのフィルタ処理のみ）
  - 共有サービス（コントラクト プロバイダーとコンシューマが異なる VRF にある）
  - L3Out EPG はプロバイダー
  - L3Out EPG には「共有されたセキュリティ インポート サブネット（ Security Import Subnet）」を持つ 0.0.0.0/0 があります。
  - トラフィックのプロバイダーIP は、L3Outサブネット0.0.0.0/0 に分類されます。
  - コンシューマ VRF で優先グループ（PG）が有効になっています。
  - コンシューマ EPG は PG に含まれています。
  - プロバイダー VRF はコンシューマ リーフ上にあります。

- APIC バージョン 5.0 より前では、次の設定がある場合、設定が無効であっても、プロバイダーからコンシューマへの方向のトラフィックが **誤っ** て許可されていました。「共有されたセキュリティ インポート サブネット（Shared Security Import Subnet）」範囲は必須の構成です。これは APIC 5.0 以降で修正されました。その結果、誤って許可されたトラフィックは、5.0 より前のバージョンから 5.0 以降のバージョンへのアップグレード後に動作を停止します。
  - 共有サービス（コントラクト プロバイダーとコンシューマが異なる VRF にある）
  - L3Out EPG はプロバイダー
  - L3Out EPG のすべての非 0.0.0.0/0 サブネットで「共有されたセキュリティ インポート サブネット（Shared Security Import Subnet）」範囲がありません。
  - これらの 0.0.0.0/0 以外のサブネットには、「外部 EPG の外部サブネット」範囲があります。
  - トラフィックのプロバイダー IP は、L3Out EPG の 0.0.0.0/0 以外のサブネットのいずれかに分類されます。
- APICリリース 6.1(2) 以降にアップグレードするには、グローバル AES 暗号化を有効にする必要があります。

ダウングレードのチェックリスト

一般に、古いバージョンにダウングレードする場合は、アップグレードチェックリストと同じチェックリストを適用する必要があります。また、古いバージョンではまだサポートされていない可能性のある新しいハードウェアまたはソフトウェアの機能にも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、古いバージョンにダウングレードした後に一部の機能が動作しなくなる可能性があります。これはすべてのリリースに適用されます

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 6.2 以降のリリースから 6.2(1) 以前のリリースへのダウングレードはサポートされていません。この制限はスイッチには適用されません。このようなダウングレードが必要な場合は、ファブリックを初期化して、古い APIC イメージを新規インストールとしてインストールできます。それ以外の場合は、ターゲットの古いリリースで収集した構成バックアップで Cisco TAC に連絡して、Cisco TAC がリカバリ プロセスを実行できるようにする必要があります。
- Cisco Application Policy Infrastructure Controller（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。

- Cisco APICのコンテナブリッジ IP アドレスの変更は、Cisco APICリリース 4.2（1）以降でのみサポートされます。AppCenter の Cisco 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、Cisco 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。

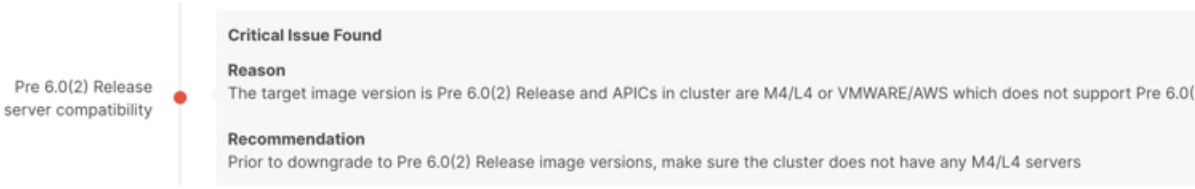
- Cisco APIC リリース 4.0(1) 以降からリリース 3.2(x) 以前のものにダウングレードする場合、リリース間でサポートされる QoS クラスの違いにより、ファブリックで小規模のトラフィックドロップが発生する可能性があります。詳細については、CSCwa32037 を参照してください。
- リモートリーフスイッチを展開している場合、Cisco APIC ソフトウェアをリリース 3.1(1) またはそれ以降からリモートリーフスイッチ機能をサポートしていない前のリリースにダウングレードする場合は、ダウングレードする前にノードの使用を停止する必要があります。リモートリーフスイッチのダ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。
- Transport Layer Security (TLS) バージョン 1.3 をサポートする Cisco APICリリースからダウングレードし、管理アクセス ポリシーで TLS 1.3 を有効にしていて、ターゲットの Cisco APIC リリースが TLS 1.3 をサポートしていない場合は、TLS 1.3 を無効化して、代わりに TLS 1.2 を有効にする必要があります。
- 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。
- Cisco APIC6.0（2）リリース以降で、クラスタの検出モードが「strict」に設定されていて、4.2 以前のリリースにダウングレードする場合は、最初に検出モードを「permissive」に変更する必要があります。
- APIC-M4/L4 サーバは、 Cisco APIC 6.0(2) リリース以降および 5.3(1) リリース以降でサポートされています。ただし、6.0(2) または 6.0(3) リリースから 5.3 リリースにダウングレー

ドすると、APIC-M4/L4 サーバがサポートされていないことを示すアップグレード前の検証警告が表示されます。この場合、警告は無視してかまいません。

次のスクリーンショットは、このアップグレード前の検証警告の例を示しています。

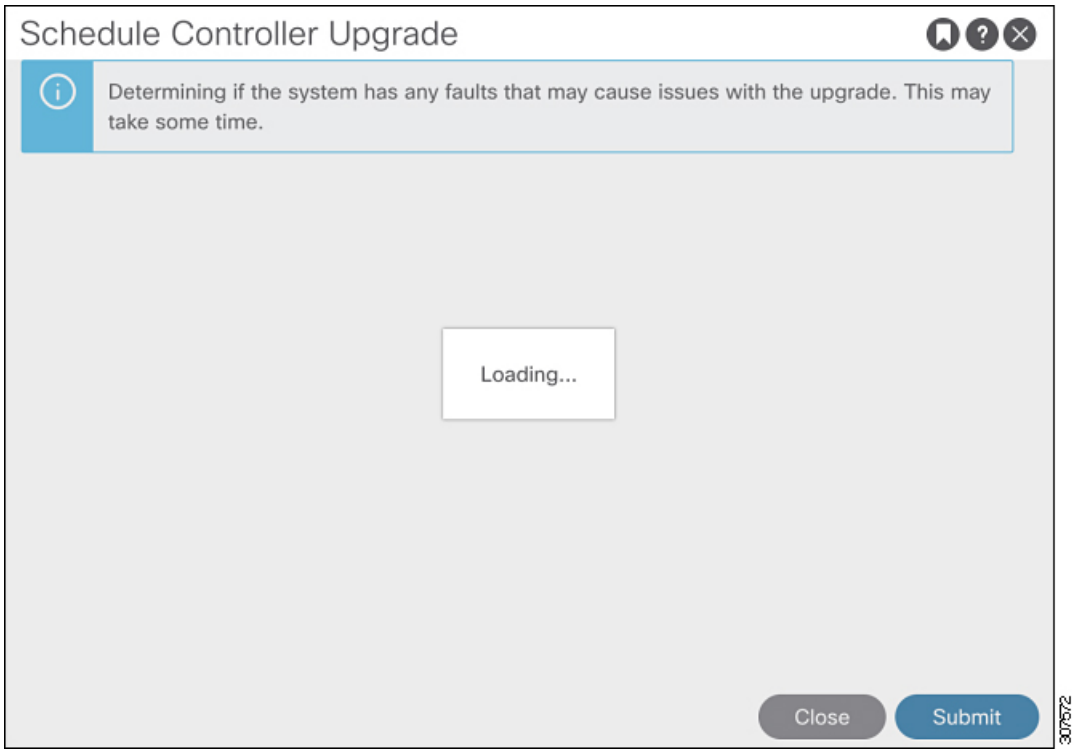


アップグレード前検証の例（APIC）

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

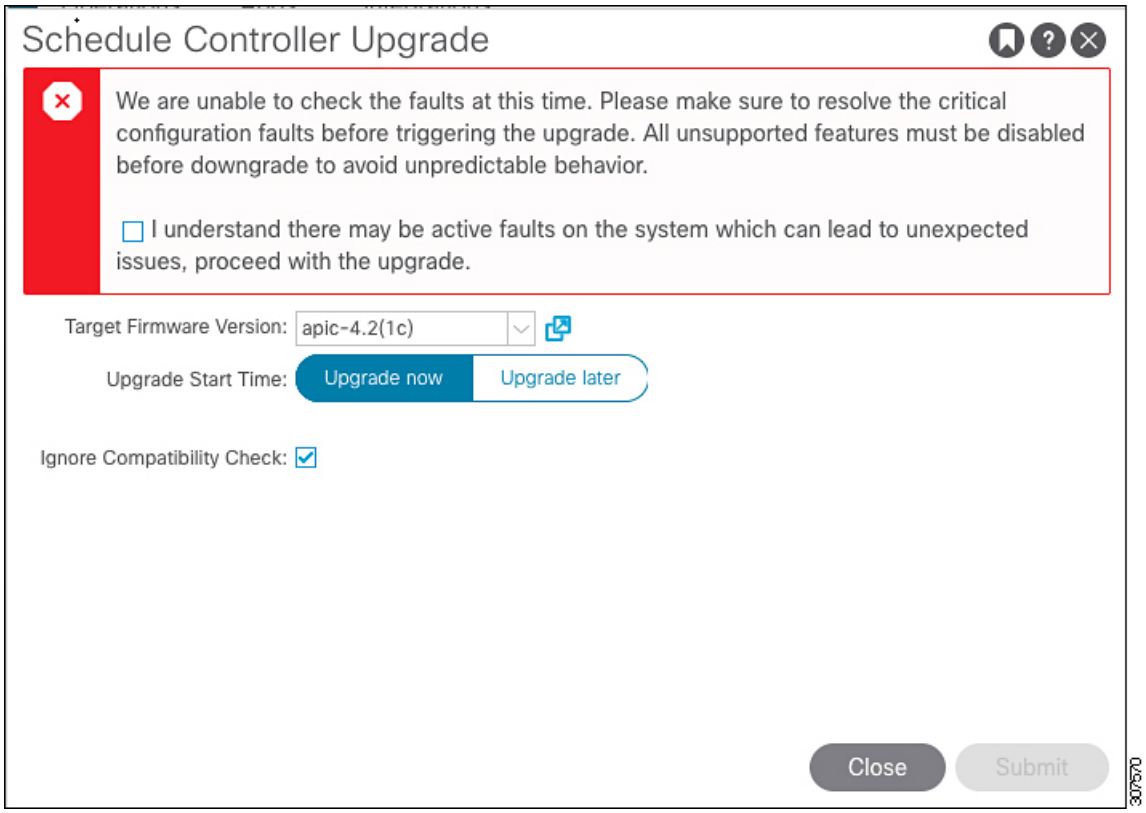
警告メッセージが GUI で表示される場合は、次の 3 つの状況が考えられます。

- 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。

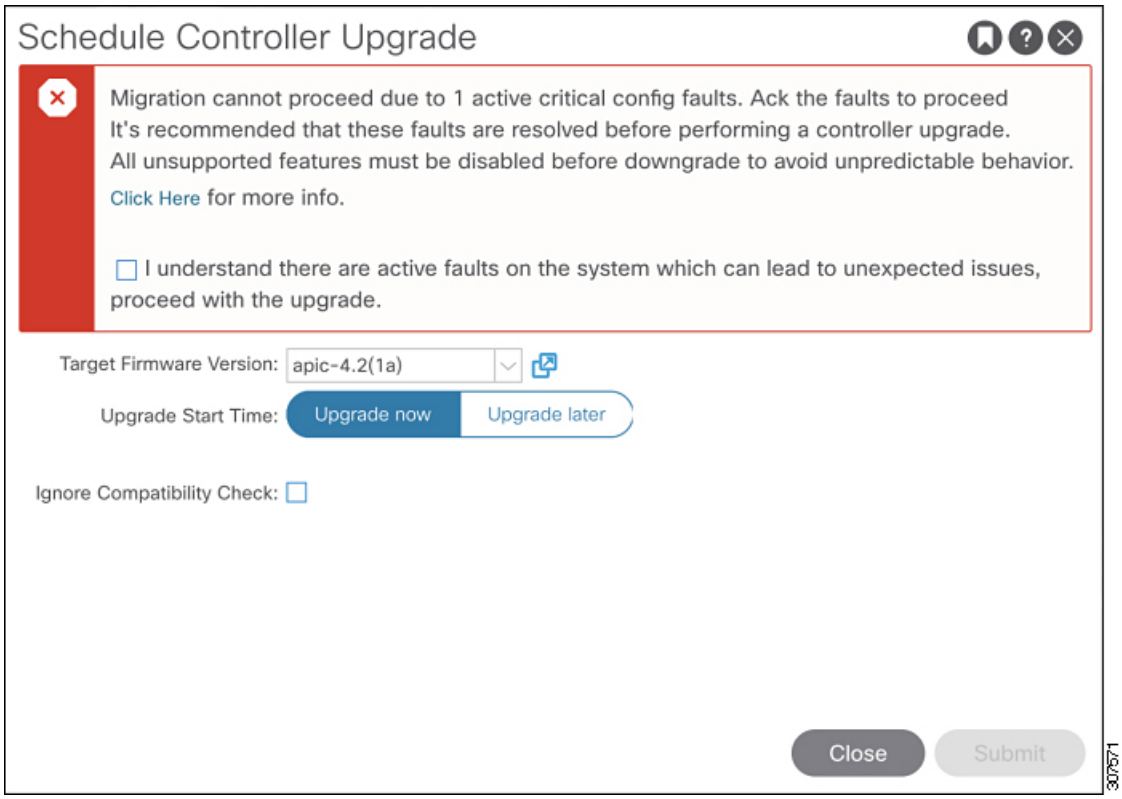
- 何らかの理由でクエリが失敗した場合は、次のようなメッセージが表示されることがあります。



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：



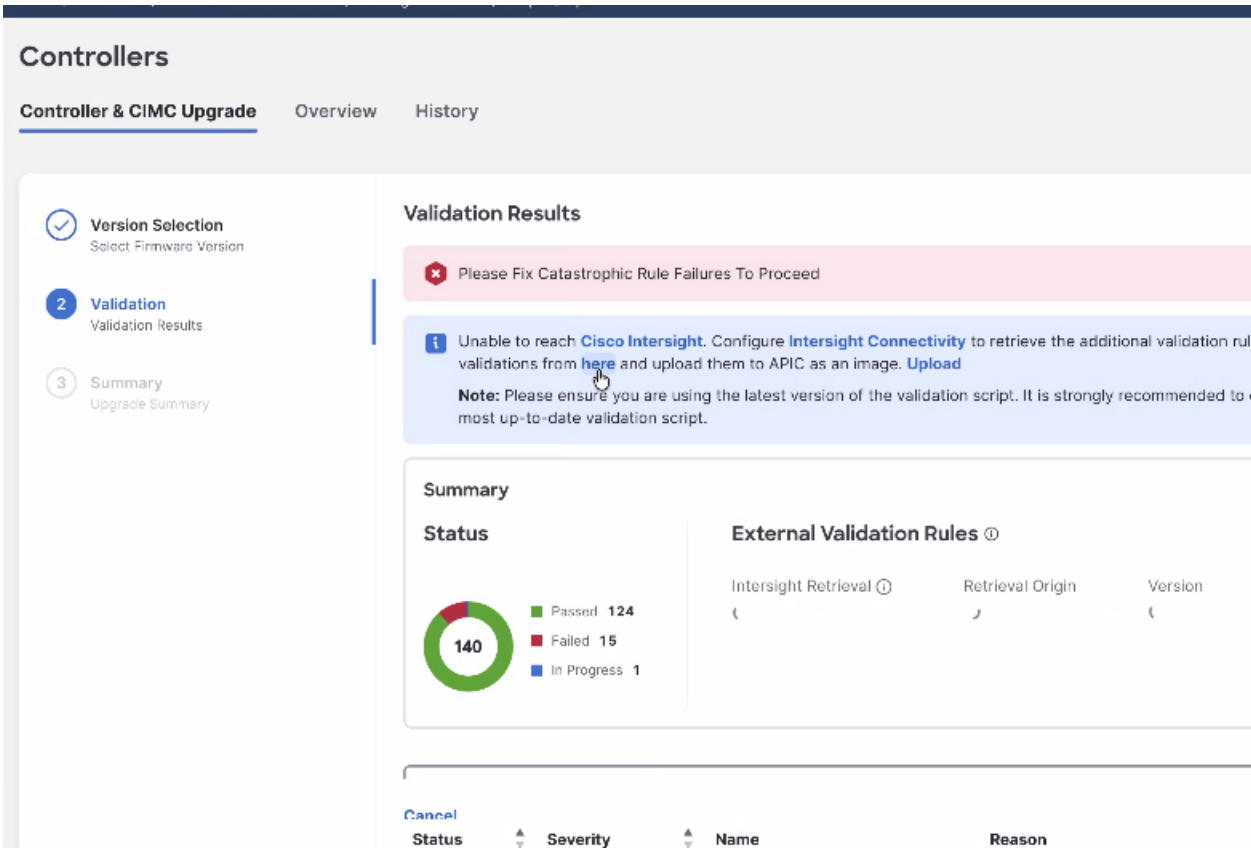
この警告メッセージは、障害クエリが完了して、システムが 1 つ以上の障害を検出したときに表示されます。この状況では、**[ここをクリック (Click Here)]** リンクをクリックして、システムが検出した障害の詳細情報を取得してください。

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。

APIC リリース 6.2(1) の GUI を使用したエラー メッセージの例

[コントローラと CIMC（Controller & CIMC）] ウィンドウで外部検証ルールを検証しているときに、アップグレードで Cisco Intersight からルールを取得できない場合、 GUI に警告メッセージが表示される場合があります。



追加の検証ルールを取得するには、Intersight接続を構成するか、外部検証ルールをダウンロードして、イメージとしてAPICにアップロードします。検証スクリプトの最新バージョンを使用していることを確認してください。Cisco Intersightに接続して、最新の検証スクリプトを取得することを強くお勧めします。

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
```

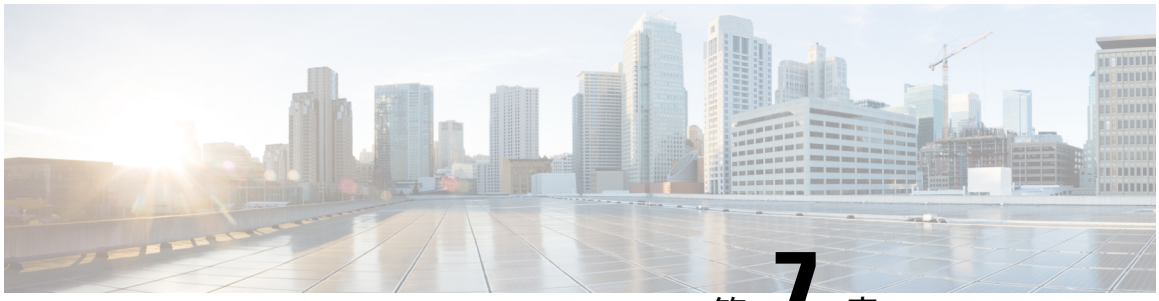
ファブリックの障害が検出された場合は、次のようなエラーメッセージが表示されることがあります。

```
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 7 章

GUI を使用した 4.x 以前の APIC でのアップグレードまたは、ダウングレード

（注） 次の注意事項を確認し、それに従ってください。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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または、ダウン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 のアップグレードまたは、ダウングレード

（注） リリース 4.0 以降にアップグレードする場合は、 Cisco Application Policy Infrastructure Controller (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、アップグレード / ダウングレード前のチェックリスト （81 ページ） を参照してください。

ファブリック内の Cisco APIC の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には、次の GUI ベースの手順を使用します。

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 Cisco APIC のソフトウェアをアップグレードまたはダウン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 Cisco 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）、Cisco 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 Cisco 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、仮想メディアを使用する Cisco APIC ソフトウェアのインストール （20 ページ） を参照してください。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）

手順

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。

a) **[ターゲット 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、アップグレードまたはダウングレードするイメージ バージョンを選択します。

b) **[ポリシー追加 (Apply Policy)]** フィールドで、**[今すぐ適用 (Apply Now)]** のオプション ボタンをクリックします。**[送信 (Submit)]** をクリックします。

[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、アップグレードまたはダウングレードプロセスが開始されます。コントロールクラスタがアップグレードまたは、ダウングレードの際に使用可能にするためCisco APICは、シリアルにアップグレードまたは、ダウングレードされます。

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、アップグレードまたはダウングレードの状態を **[作業（Work）]** ペインで確認します。

コントローラのアップグレードまたはダウングレードはランダムに行われます。コントローラのイメージがアップグレードまたはダウングレードされた後で、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。コントローラをリブートした後で、クラスタに再び加わります。その後、クラスタが収束し、次のコントローライメージがアップグレードまたはダウングレードを開始します。クラスタがすぐに収束せず、完全に適合しない場合は、クラスタが収束して完全に当てはまるまでアップグレードまたはダウングレードは待機状態になります。この間、アップグレードまたはダウングレードされる各 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。

ブラウザが接続されている Cisco APIC がアップグレードまたはダウン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またはダウングレード済みの 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または、ダウングレード

（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または、ダウングレード手順です。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。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

- 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または、ダウングレード （103 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または、ダウングレード （115 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または、ダウン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または、ダウングレードに進みます。
- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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）
互換性チェックを無視フィールドの隣の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設定することを選択する場合、システム内でサポートされていないアップグレードまたは、ダウングレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

d) **[ターゲット 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、スイッチをアップグレードまたは、ダウン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または、ダウングレードは、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) アップグレードまたは、ダウン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または、ダウン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または、ダウン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または、ダウングレードされ、その後また 20 台のスイッチの組がアップグレードまたは、ダウングレードされます。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、アップグレードまたは、ダウン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または、ダウングレードされます。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または、ダウングレードには約 10 分かかります。スイッチはアップグレードまたは、ダウン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後、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または、ダウン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または、ダウングレード

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または、ダウングレードされるとアップグレードまたは、ダウングレードされます。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または、ダウン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または、ダウン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。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされてい

るリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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。

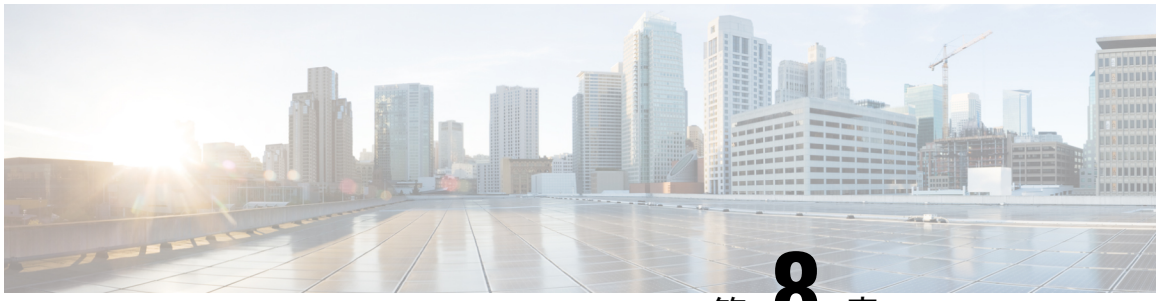
ステップ 2 [Work] ペインで、**[Actions]** > **[Change Catalog Firmware Policy]** を選択します。

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、**[ポリシーを適用（Apply Policy）]** フィールドの **[今すぐ適用（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、アップグレードまたは、ダウングレードされました。



第 8 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または、ダウングレード

（注） 次の注意事項を確認し、それに従ってください。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）
- イメージをアップグレードまたは、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。

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。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲット リリースは、現在インストールされてい

るリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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 （106 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 コピーのユーザー名を入力します。
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。

Cisco APIC のリリース 4.x または 5.0 からのアップグレードまたはダウングレード

これらの GUI ベースのアップグレードまたはダウングレード手順を使用して、ファブリック内の APIC 上のソフトウェアをアップグレードまたはダウングレードします。

何らかの理由で、これらの GUI ベースのアップグレードまたはダウングレード手順を使用してファブリック内の Cisco APIC のソフトウェアをアップグレードまたはダウン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 Cisco APIC を受け取った場合、GUI を使用してアップグレードまたはダウン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）、Cisco 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代わりに、CIMC を使用して Cisco 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、仮想メディアを使用する Cisco APIC ソフトウェアのインストール（20 ページ） を参照してください。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲット リリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ)
- アップグレード / ダウングレード前のチェックリスト （81 ページ)

- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）
- 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。
- ICisco APIC リリースを 5.0 より前のリリースから 5.0 以降のリリースにアップグレードしており、MP-BGP を使用して学習された IPv4 ホスト ルート (/32) または IPv6 ホスト ルート (/128) がある場合、それらのホスト ルートが L3Out SVI サブネットなど、ローカルに接続された非パーベイシブ サブネットの場合、転送情報ベース (FIB) プロセスは、それらのホストルートのハードウェア プログラミングをスキップします。この動作は意図的です。以下の回避策のいずれかを使用してこの情報を回避できます。
  - L3Out インターフェイス サブネットと重複する /32 または /128 ホスト ルートでアドバタイズしない。
  - /32 または /128 以外の任意のサブネットを使用してアドバタイズする。
  - 境界リーフ スイッチから、ピアリングが存在する元のノードと同じピアに直接ピアリングします。

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。

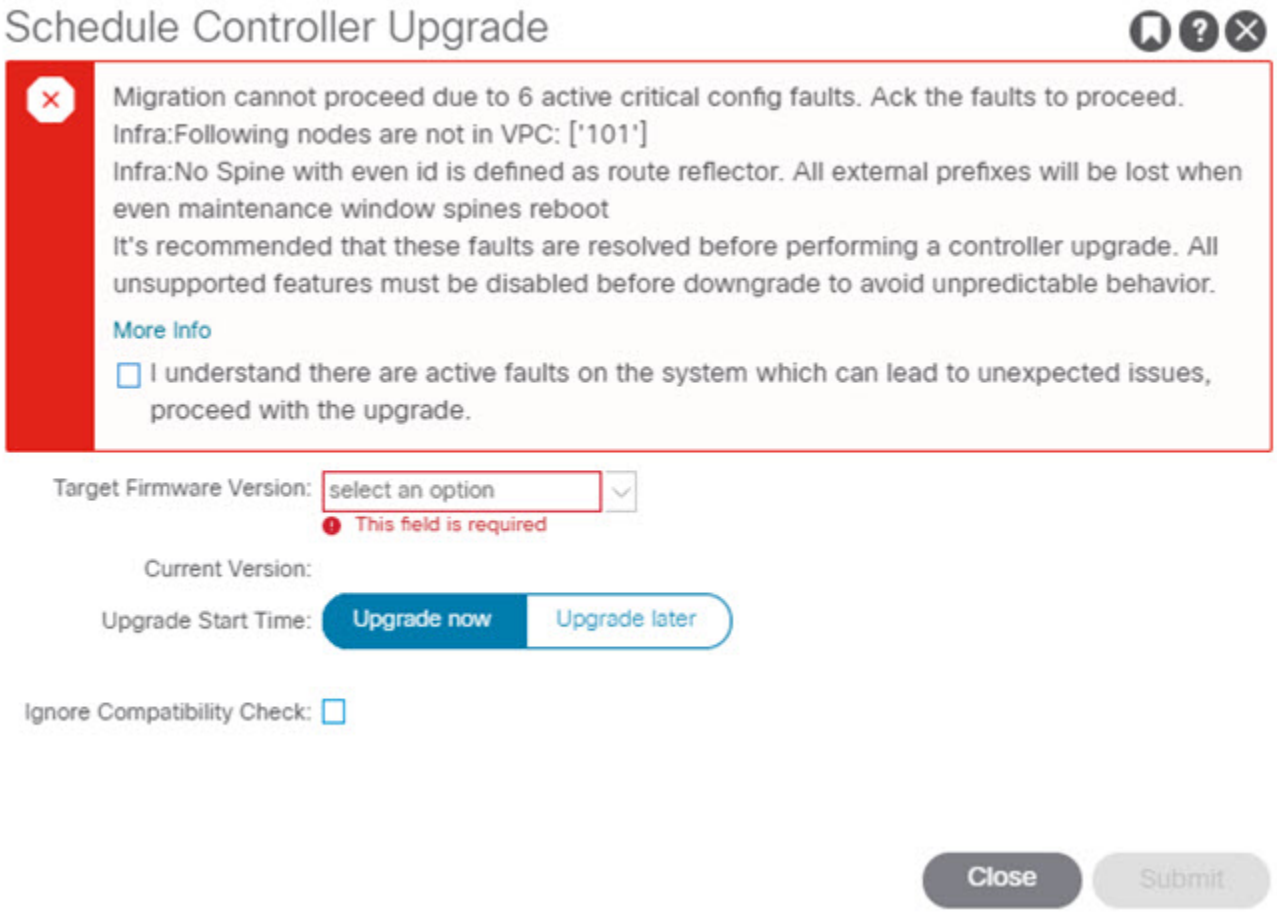
- **[ノード（Nodes）]**タイル：物理ノードで使用されているファームウェア バージョンに関する情報を提供します。
- **[仮想ノード（Virtual Nodes）]** タイル：仮想ノードで使用されているファームウェア バージョンに関する情報を提供します。
- **[コントローラ（Controller）]** タイル：このコントローラで使用されているファームウェア バージョンに関する情報を提供します。カタログのバージョンに関する情報も提供します。
- **[コントローラ ストレージ（Controller Storage）]** タイル：各コントローラのストレージ容量に関する情報を提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

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 Cisco 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 / ダウングレード前のチェックリスト（81 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 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、アップグレードまたはダウン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**: アップグレードまたはダウン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**: アップグレードまたはダウングレードは、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）
互換性チェックを無視フィールドの隣の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設定することを選択する場合、システム内でサポートされていないアップグレードまたは、ダウングレードを発生させるリスクを生じ、これにより使用不能な状態を引き起こす可能性があります。

[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、アップグレードまたはダウングレードプロセスが開始されます。コントロールクラスタがアップグレードまたは、ダウングレードの際に使用可能にするためCisco APICは、シリアルにアップグレードまたは、ダウングレードされます。

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、アップグレードまたはダウン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またはダウングレードはランダムな順番で行われます。コントローラのイメージがアップグレードまたはダウングレードされた後で、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。コントローラをリブートした後で、クラスタに再び加わります。その後、クラスタが収束し、次のコントローライメージがアップグレードまたはダウングレードを開始します。クラスタがすぐに収束せず、完全に適合しない場合は、クラスタが収束して完全に適合するまでアップグレードまたはダウングレードは待機状態になります。この間、アップグレードまたはダウングレードされる各 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。Cisco APIC のアップグレードのさまざまな段階の詳細については、「**APIC のアップグレードおよびダウングレードの段階について**」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 Cisco 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または、ダウングレード

これは、リリース 4.x または 5.0 で実行されているCisco Application Policy Infrastructure Controller（APIC）GUI を使用したスイッチのアップグレードまたは、ダウングレード手順です。Cisco APICがすでにリリース 5.1 以降にアップグレードされている場合、スイッチが 14.x または 15.0 より前のリリース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または、ダウングレード（115 ページ） などの対応するセクションを確認します。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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 リリースにアップグレードまたは、ダウン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または、ダウングレードに進みます。
- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ)
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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 リリースにアップグレードまたは、ダウングレードされていることを確認します。
全コントローラが新しいファームウェア リリースにアップグレードまたは、ダウングレードされるまでスイッチ ファームウェアをアップグレードまたは、ダウングレードしません。

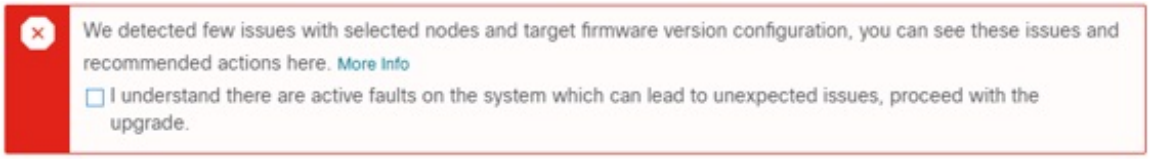
ステップ 2 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。
[サマリー（Summary）] ウィンドウが表示され、次の情報が表示されます。

- **[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 リリース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 リリース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 リリース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。



お使いのリリースの Cisco 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/ダウングレード前のチェックリスト（81 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 （183 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。

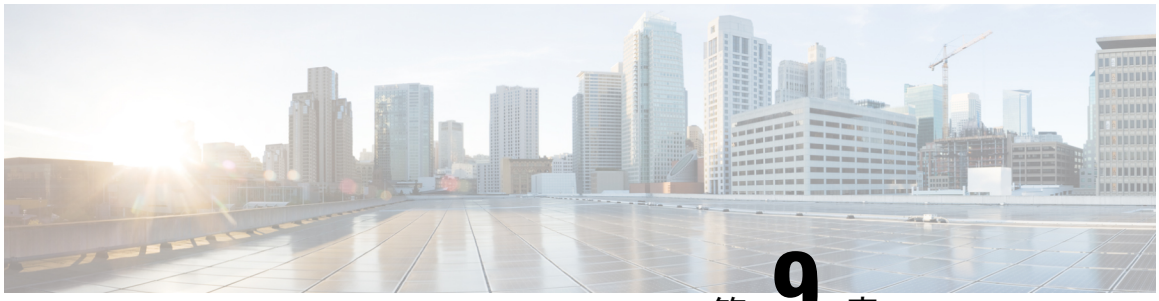
Admin > **Firmware** > **Infrastructure** > **Nodes** の下のテーブルには、各ノードが属しているアップグレードグループを示す **[アップグレードグループ（Upgrade Group）]**（以前はPODメンテナンスグループとして表示されていました）の列があります。特定のノードのこの列を右クリックすると、次のオプションが表示されます。

- 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) [Submit] をクリックします。



第 9 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または、ダウングレード

（注） 次の注意事項を確認し、それに従ってください。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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。
- リリース 5.2(5) ～ 5.3(2) からリリース 6.0 以降にアップグレードすると、すべてのユーザーは、次回ログイン時にパスワードを変更するように求められます。ユーザーがパスワードを変更する必要がないようにするには、アップグレードの前に、**パスワード強度チェック** と **パスワード強度プロファイル**の両方を有効または無効にします。

  [パスワード強度プロファイル（Password Strength Profile）] は、アップグレード後は常に有効になり、無効にすることはできません。すでにアップグレード済みの場合は、すべてのユーザーに対して **[パスワードの更新が必要（Password Update Required）]** ボックスを手動でオフにする必要があります。

- ダッシュボードへのアクセス （116 ページ）
- APIC で APIC とスイッチ イメージをダウンロードする （116 ページ）

- リリース 5.1x 以降からの Cisco APIC のアップグレードまたは、ダウングレード（118 ページ）
- 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または、ダウングレード（121 ページ）
- アプリケーションのインストール動作について（126 ページ）

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、Cisco Application Policy Infrastructure Controller（APIC）および Cisco Application Centric Infrastructure（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、Cisco APICのファームウェア レポジトリにダウンローします。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲット リリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

（注） Cisco APIC リリース 6.0（2）内以降では、32 ビットと 64 ビット Cisco ACI モード スイッチ イメージを Cisco APIC にダウンロードします。一つのイメージしかダウンロードしない場合、アップグレード中にエラーが生じることがあります。詳細については、アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項（68ページ）を参照してください。

Cisco ACI モード スイッチ 16.x リリースでは、64 ビット スイッチ ソフトウェアは、スイッチにインストールされている場合、32 ビット ソフトウェアと同じイメージ名を持ちます。スイッチで実行されているバージョンを確認するには、スイッチのイメージファイルに対して **md5sum** コマンドを使用します。この md5sumハッシュを、Cisco APIC の `/firmware/fwrepos/fwrepo` ディレクトリに含まれるスイッチ イメージと比較します。その後のアップグレードでは、64 ビットと 32 ビットのイメージ名がスイッチ上で区別されます。

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、ドロップダウン 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（118 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 コピーのユーザー名を入力します。
    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、Cisco 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 サーバー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、Cisco 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 Cisco 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。

Cisco APICは、構成された送信元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 のアップグレードまたは、ダウングレード

ファブリック内の Cisco 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または、ダウン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Cisco 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Cisco 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）、Cisco 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 Cisco 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。それらの手順の仮想メディアを使用する Cisco APIC ソフトウェアのインストールを参照します。または、Cisco APICクラスタが Cisco APIC 6.0(2) リリース以降を実行している場合、新しい Cisco APICは、APIC ディスカバリの自動ファームウェア アップデートを介して、既存のクラスタの同じバージョンに自動的にアップグレードまたはダウングレードされます。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）
- ICisco APIC リリースを 5.0 より前のリリースから 5.0 以降のリリースにアップグレードしており、MP-BGP を使用して学習された IPv4 ホスト ルート (/32) または IPv6 ホスト ルート (/128) がある場合、それらのホストルートが L3Out SVI サブネットなど、ローカルに接続された非パーベイシブ サブネットの場合、転送情報ベース (FIB) プロセスは、それらのホストルートのハードウェアプログラミングをスキップします。この動作は意図的です。以下の回避策のいずれかを使用してこの情報を回避できます。
  - L3Out インターフェイス サブネットと重複する /32 または /128 ホスト ルートでアドバタイズしない。
  - /32 または /128 以外の任意のサブネットを使用してアドバタイズする。
  - 境界リーフ スイッチから、ピアリングが存在する元のノードと同じピアに直接ピアリングします。

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。
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（116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、アップグレードまたは、ダウングレードのステータスが表示されます。

コントロール クラスタがアップグレードまたは、ダウングレードの際に使用可能にするため Cisco APIC は、シリアルにアップグレードまたは、ダウングレードされます。 コントローラのイメージがアップグレードまたはダウングレードされた後で、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 イメージがアップグレードまたはダウングレードを開始します。クラスタがすぐに収束せず、完全に適合しない場合は、クラスタが収束して完全に適合するまでアップグレードまたはダウングレードは待機状態になります。この間、アップグレードまたはダウングレードされる各 Cisco APIC の **[アップデート ステータス（Update 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。

ブラウザが接続されている Cisco APIC がアップグレードまたは、ダウン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 Cisco 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 Cisco APIC にログインして、アップグレード または、ダウングレード 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。Cisco APIC のアップグレードまたは、ダウングレードのさまざまな段階の詳細については、「**APIC のアップグレードおよびダウングレードの段階について**」を参照してください。

（注）
実際のアップグレードまたは、ダウン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、アップグレードまたは、ダウングレード 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 Cisco APIC がアップグレードまたは、ダウングレードを完了し、**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または、ダウングレード

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）または、ダウングレードを開始せずに、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。

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。

（注） あるリリースから次のリリースにスイッチをアップグレードすると、ブートフラッシュ メモリが増加すると、障害コード F1821 が表示されます。この障害は、スイッチのアップグレード後に自動にクリアされるため、無視してください。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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または、ダウン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または、ダウングレードに進みます。
- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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、**[スイッチ（Switches）]**をクリックします。
[スイッチ（Switches）] 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 **[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**[更新グループの作成（Create Update Group）]**を選択します。

ステップ 4 **[スイッチ アップデート グループの設定（Setup Switch Update Group）]** ウィンドウが表示されたら、**[グループ名のアップグレード（Upgrade Group Name）]** の名前を入力します。

ステップ 5 **[スイッチの選択（Switch Selection）]** ステップで、**[スイッチの追加（Add Switches ）]** ボタンをクリックし、アップグレードまたはダウングレードする必要があるスイッチを選択して、**[OK]** をクリックし、**[次へ（Next）]** をクリックします。

ステップ 6 **[バージョンの選択（Version Selection）]** ステップで、**[ファームウェアの選択（Select Firmware ）]** セクションで **[アップデート タイプ（ Update Type）]** を選択し、アップグレード/ダウングレードするイメージを選択します。

ステップ 7 （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（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 **[適用（Enforced）]** 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、**[互換性の確認（Compatibility Check）]** フィールドの隣にあるボックスのチェック マークをオンにして互換性チェック機能を無効にするを選択すると、システムに対してサポートされていないアップグレードが実行されるリスクが発生し、システムが利用できない状態になる可能性があります。

- **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。デフォルトでは、この設定は **[適用しない（Unenforced）]**です。

  詳細については ACI スイッチのグレースフル アップグレードまたは、ダウングレード（45 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 アップグレードとダウングレードのガイドライン （41 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 8 **[バージョン選択（Version 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 9 **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。

詳細は、アップグレード / ダウングレード前のチェックリスト （81 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 10 **[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）
リリース 4.x または 5.0 を実行している Cisco 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または、ダウングレード（110 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 （125 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 11 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（166 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、スクリプトを使用します。これは、APIC に組み込まれているアップグレード前検証によってスイッチ イメージが再度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。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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 （121 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、**[アクション（Actions）]** をクリックし、それから **[インストールの開始（Begin Install）]** 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または、ダウングレードすると、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または、ダウン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 がアップグレードまたは、ダウン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または、ダウングレードされた後、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または、ダウングレードされます。
- 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。

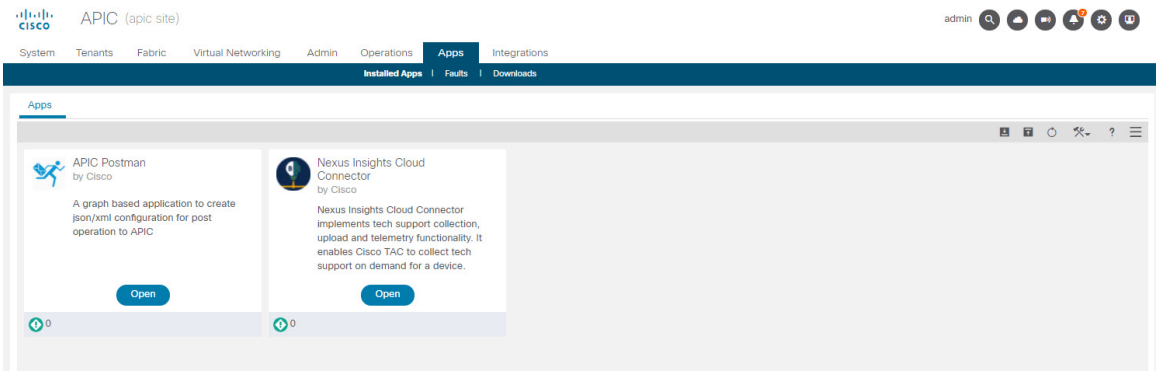
   [事前パッケージ化されたアプリケーション ポリシー（Prepackaged Apps Policy）] ページが表示されます。

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。

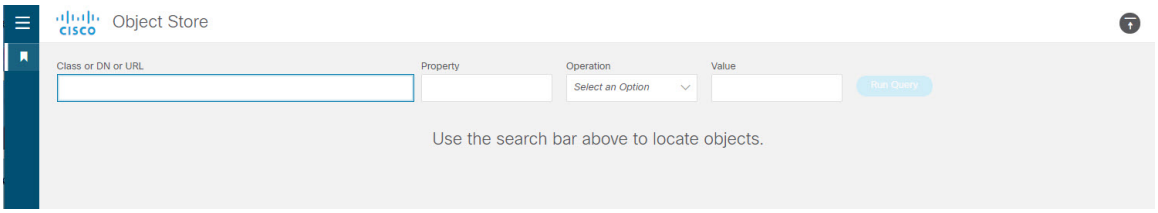
（注） リリース 5.2(1) で使用可能になった、事前にパッケージ化された ApicVision アプリは、App Store からダウンロードできません。そのため、ApicVision アプリを変更したり、削除したりしないでください。事前にパッケージ化された ApicVision アプリに問題や障害がある場合は、Cisco TAC サポートにお問い合わせください。

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。

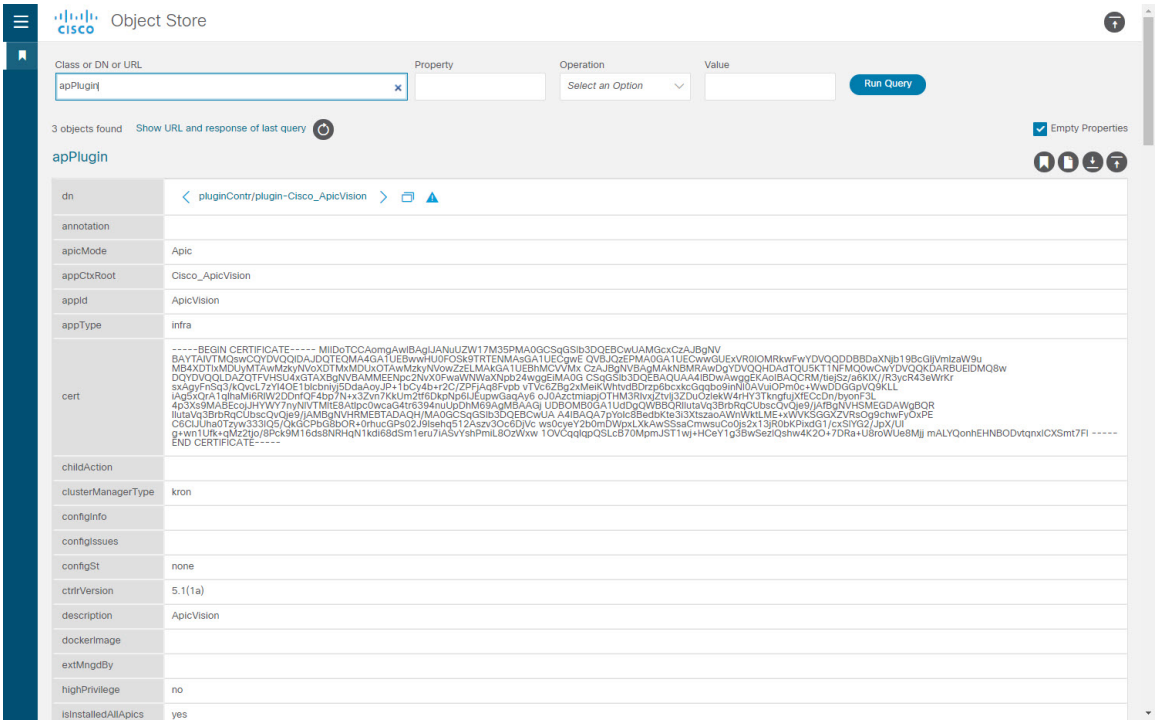
Visore にアクセスするには、APIC GUI へのログインに通常使用する URL に `/visore.html` を追加します。

```
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。



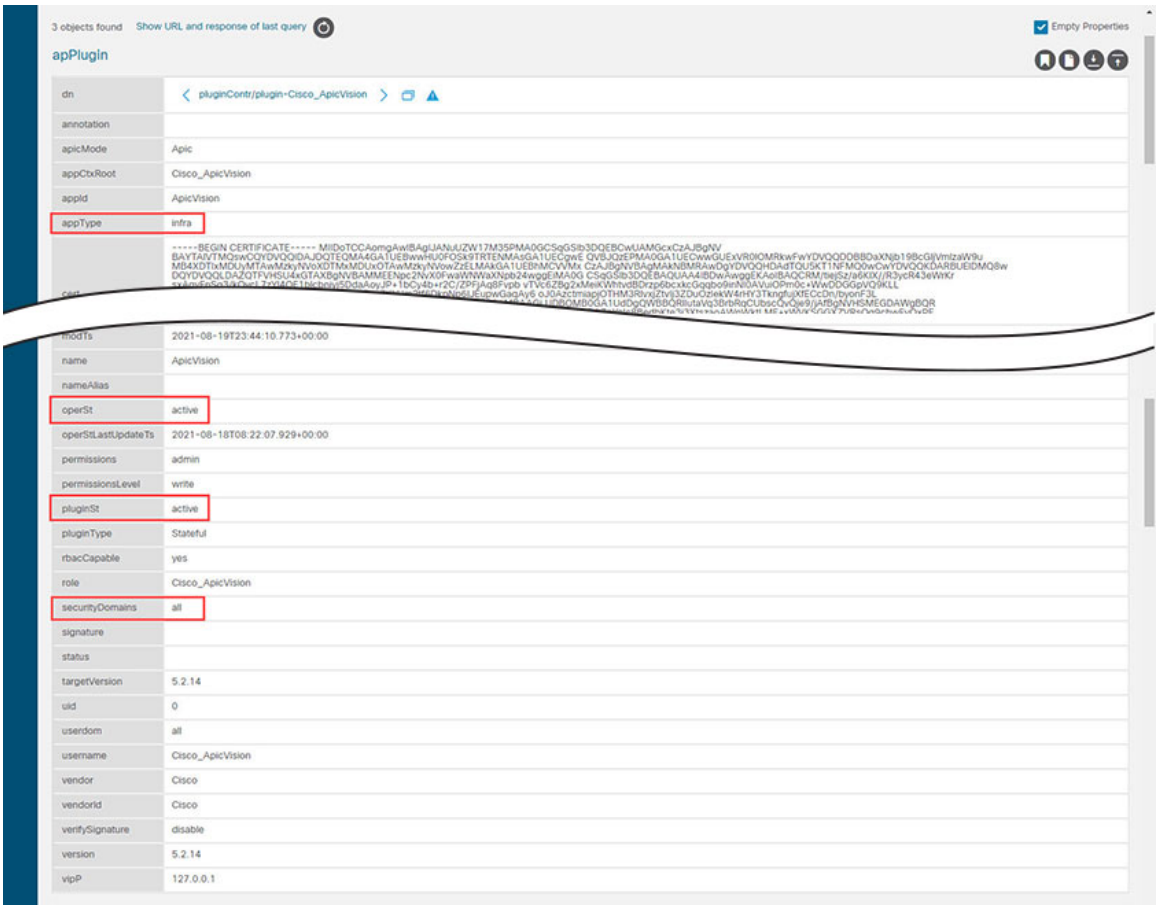
たとえば、上記の例の **[アプリケーション（Apps）]** ウィンドウに表示される情報には 2 つのアプリケーションがインストールされていますが、Visore の `apPlugin` クエリから返される情報には、アプリケーション MO で見つかった 3 つのオブジェクトが表示されます。アプリケーションの 2 つのリストを比較すると、ApicVision アプリは通常の APIC GUI の **[アプリ（Apps）]** ウィンドウには表示されず、Visore の出力に表示されるため、ApicVision アプリは事前にパッケージ化された非表示のアプリです。

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。

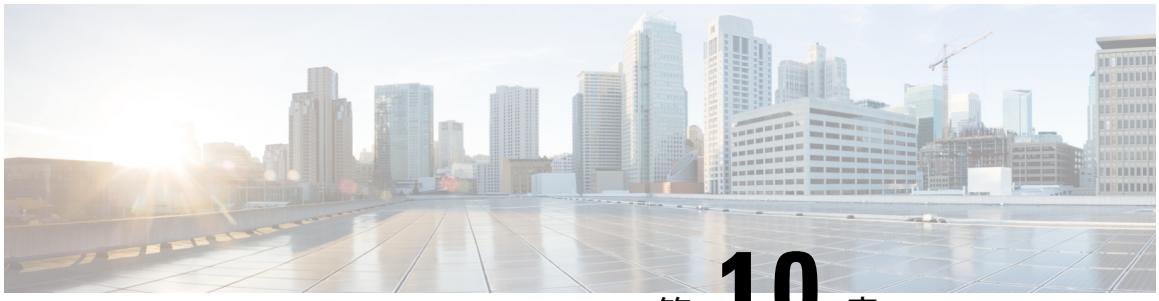
  - 非表示のアプリケーションを無効にする場合、セキュリティドメインは必要ありません。
  - 上記のいずれかの投稿のアプリケーションの appCtxRoot 値を検索するには、apPlugin MO のインスタンスを照会し、対象のアプリケーションに対応する apPlugin MO のインスタンスの appCtxRoot フィールドのエントリを使用します。

    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 10 章

GUI を使用した APIC リリース 6.2 以降でのアップグレードまたは、ダウングレード

（注） 次の注意事項を確認し、それに従ってください。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）

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のアップグレード前の検証のためのAPIC、APIC CIMC、スイッチ、および追加のルールのダウンロード

この手順では、外部ファイル サーバまたはローカル マシンから Cisco APIC ファームウェア リポジトリへイメージをダウンロードします。サポートされているイメージ タイプは次のとおりです。

- Cisco APIC ファームウェア イメージ
- Cisco ACI スイッチ ファームウェア イメージ
- APIC CIMC の Cisco CIMC HUU イメージ
- アップグレード前の検証のための外部の追加ルール

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲット リリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

（注） Cisco APIC リリース 6.0(2) 内以降では、32 ビットと 64 ビット Cisco ACI モード スイッチ イメージを Cisco APIC にダウンロードします。一つのイメージしかダウンロードしない場合、アップグレード中にエラーが生じることがあります。詳細については、アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項（68ページ）を参照してください。

Cisco APIC モード スイッチ 16.x リリースでは、64 ビット スイッチ ソフトウェアは、スイッチにインストールされている場合、32 ビット ソフトウェアと同じイメージ名を持ちます。スイッチで実行されているバージョンを確認するには、スイッチのイメージ ファイルに対して **md5sum** コマンドを使用します。この md5sumハッシュを、Cisco APIC の /firmware/fwrepos/fwrepo ディレクトリに含まれるスイッチ イメージと比較します。その後のアップグレードでは、64 ビットと 32 ビットのイメージ名がスイッチ上で区別されます。

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、ドロップダウン 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 （138 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-dk9.6.2.1a.iso` です。
    2. [Username] フィールドに、セキュア コピーのユーザー名を入力します。
    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、Cisco 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、Cisco 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 Cisco 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-dk9.6.2.1a.iso` です。

ステップ 6 [**送信 (Submit)**] をクリックします。

Cisco APIC は、構成された送信元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 6.2x 以降からの Cisco APIC CIMC のアップグレードまたは、ダウングレード

Cisco ACI リリース 6.2(1) 以降、システムには統合され、オーケストレーションされた CIMC アップグレードワークフローが含まれています。この機能により、APIC のユーザーインターフェイスからクラスタ内の APIC の CIMC を直接アップグレードできます。

Cisco ACI ファブリックの Cisco APIC ソフトウェアをアップグレードする前に、ファブリックで実行されている CIMC バージョンの更新が必要な場合もあります。互換性を確保するには、各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、Cisco APIC リリース ノートを参照してください。Cisco APIC のリリース ノートは、APIC のドキュメンテーション ページで見つけることができます。

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。

- 環境に関連するすべてのアップグレード前のチェックリストと注意事項を確認します。詳細については、「アップグレード / ダウングレード前のチェックリスト （81 ページ）」を参照してください。
- 「アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項（68 ページ）」を確認してください。
- APIC のアップグレード前の検証のための APIC、 APIC CIMC 、スイッチ、および追加のルールのダウンロード （136 ページ） セクションの説明に従って、必要なCIMC HUU イメージをAPICにダウンロードします。

（注） APIC によるCIMC のアップグレードは、カタログ オブジェクト **compatRsSuppHw**にリストされている特定の CIMC HUU バージョンでのみサポートされます。たとえば、 APIC モデルが APIC-G5（apicg5）で、 APIC バージョンが 6.2(1) の場合、 APIC CIMC アップグレード ワークフローでサポートされる唯一の CIMC HUU バージョンは C225M8 6.0（1.250131）です。カタログ オブジェクトの出力例を次に示します。APIC のリリース ノートには、サポートされる追加の CIMC HUU バージョンが記載されている場合があります。これらの他のバージョンのいずれかを使用する必要がある場合は、 CIMCユーザー インターフェイスを使用して CIMC をアップグレードする必要があります。

```
admin@apic1:~> moquery -d
'uni/fabric/compcat-default/ctlrfw-apic-6.2(1)/rssuppHw-[uni/fabric/compcat-default/ctlrhw-apicg5]'
 | egrep '#|cimc|dn'
# compat.RsSuppHw
cimcFamily   : C225M8
cimcVersion  : 6.0(1.250131)
dn           :
uni/fabric/compcat-default/ctlrfw-apic-6.2(1)/rssuppHw-[uni/fabric/compcat-default/ctlrhw-apicg5]
```

手順

ステップ 1 APIC ユーザー インターフェイスの **[管理（Admin）] > [ファームウェア（Firmware）]** セクションに移動します。

ステップ 2 ナビゲーション ペインから **[コントローラ（Controllers）]** を選択します。
[コントローラと CIMC のアップグレード（Controller & CIMC upgrade）] ウィンドウが表示され、選択に基づいてコンポーネントをアップグレードできます。

ステップ 3 **[アップグレード コンポーネント（Upgrade Component）]** 領域で、 **[CIMC]**を選択します。

ステップ 4 APIC ノードは、現在の **CIMC** バージョンとその **ステータス**とともに次の表に表示されます。対応する **CIMC** バージョンが APIC のファームウェア リポジトリで利用可能な場合、**[ステータス（Status）]** カラムには **[アップグレードを使用可能（Upgrade Available）]**と表示されま

す。 **アップグレードを利用可能な** ステータスを持つ各 APIC に対して、 **[検証（Validate）]** をクリックします。 **[CIMC ファームウェアの検証（Validate CIMC firmware）]** スライダが表示されます。

[CIMC ファームウェアの検証（Validate CIMC firmware）] スライダで、 CIMC **ユーザー名**、 **パスワード** 、 **IPアドレス** とターゲット **CIMC HUU** イメージ バージョンを入力し、 **[検証]**をクリックします。

これにより、 APIC が CIMC にアクセスして、指定されたイメージで CIMC アップグレードを実行できるかどうかが検証されます。

ステップ 5 **[ステータス（Status）]**列にすべての APIC ノードが **[検証済み（Validated）]** と表示されたら、 **[次へ（Next）]**をクリックします。

一部の APIC ノードが互換性のある CIMC バージョンをすでに実行している場合は、[ステータス（Status）] 列に **[アップグレード済み（Upgraded）]** と表示され、 **[次へ（Next）]**をクリックして検証する必要はありません。

ステップ 6 **[ステップ 2 - 検証結果（Step 2 - Validation Results）]** ステップが表示されます。クラスタのアップグレード前の検証の完了を待機します。

すべての検証に合格したことを確認します。重大度が「致命的」で失敗した検証がある場合は、修正して次の手順に進む必要があります。

ステップ 7 **[ステップ 3：概要（Step 3 - Summary）]** ビューが表示されます。選択内容を確認してから **[送信（Submit）]** をクリックし、 CIMC アップグレードを開始します。

ステップ 8 **[進捗状況（Progress）]** ビューが表示されます。ステータスをモニタし、すべてのステップで **[完了（Completed）]** と表示されるまで待ちます。

リリース 6.2x 以降からの Cisco APIC のアップグレードまたはダウングレード

Cisco ACI リリース 6.2(1) 以降、 APICアップグレード プロセスは、以前のアップグレード プロセスと比較して、合理化およびオーケストレーションされた処理により強化され、各 APIC ノードは中央のオーケストレーション ポイントなしで半個別にアップグレードされます。最適化された APIC 再起動プロセスにより、より高速なアップグレードが可能になります。

（注） Cisco APIC 6.2 以降のリリースから 6.2(1) 以前のリリースへのダウングレードはサポートされていません。詳細については、ダウングレードのチェックリスト （85 ページ）を参照してください。

アップグレード前の検証手順も強化され、個別にインポートできる追加のルールが追加されました。これにより、常に最新かつ最大のルール セットが提供されます。

新しいプロセスでは、APIC 1 はアップグレードのためにクラスタ全体の中央のオーケストレーション ポイントとして機能します。このため、APIC クラスタのアップグレードを実行するには、APIC1 のユーザー インターフェイスを使用している必要があります。

水面下でのアップグレード プロセスの詳細については、ACI アップグレード/ダウングレード アーキテクチャ （61 ページ） セクションを参照してください。

外部機関による検証

ACI リリース 6.2(1) より前は、[ACI アップグレード 前検証スクリプト（ACI Pre-Upgrade Validation Script）]から Python スクリプトを手動でダウンロードして実行することが推奨されていました。このスクリプトは、 APIC GUIのアップグレード ワークフロー中に実行される組み込みの検証とは別に、これとは別に使用する必要があります。

ACI リリース 6.2(1) 以降、 APIC GUIのアップグレード ワークフローは、ACI アップグレード前の検証スクリプトに相当する追加の外部ルールをロードし、組み込みルールとともに実行できます。

外部ルールをロードするためのオプションが 2 つあります。

- APIC のアップグレード前の検証のための APIC、 APIC CIMC 、スイッチ、および追加のルールのダウンロード （136 ページ） セクションの手順に従って、cisco.com からルール バンドルのイメージ（tarball ファイル）を手動でダウンロードし、アップロードします。APIC は、アップグレード ワークフロー中にイメージを検索します。
- スクリプトを Intersight から直接統合して取得します。

  APIC が Cisco Intersight によって要求され、 IP に到達可能性である場合、アップグレード ワークフロー中、 APIC はCisco Intersight からルール バンドル イメージ（tarball ファイル）をダウンロードしようとします。Cisco Intersight への接続の詳細については、「Cisco APIC および Intersight デバイス コネクタ」を 参照してください。

  実際のアップグレードを続行するには、いずれかのオプションの外部ルール バンドル イメージが必要です。

APICアップグレード ワークフローのアップグレード前の検証手順中に、 APIC は常に Cisco Intersight オプションを最初に使用しようとします。外部ルールをダウンロードできる場合、ローカル ファームウェア リポジトリ内の他のすべての外部ルールとバージョンを比較し、最新バージョンを使用します。cisco.com を手動でチェックすることなく、 APIC に常に最新のルールを適用できるため、 Cisco Intersight の使用を強くお勧めします。

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。

- 「アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）」を確認してください。
- 環境に関連するすべてのアップグレード前のチェックリストと注意事項を確認します。詳細については、「アップグレード / ダウングレード前のチェックリスト （81 ページ）」を参照してください。

- 「アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項（68 ページ）」を確認してください。

手順

ステップ 1 APIC ユーザー インターフェイスの **[管理（Admin）] > [ファームウェア（Firmware）]** セクションに移動します。

ステップ 2 ナビゲーション ペインから **[コントローラ（Controllers）]** を選択します。
[コントローラと CIMC のアップグレード（Controller & CIMC upgrade）] ウィンドウが表示され、選択に基づいてコンポーネントをアップグレードできます。

ステップ 3 **[アップグレードコンポーネント（Upgrade Component）]** 領域で、**[コントローラ（Controller）]** のいずれかを選択します。

ステップ 4 メイン ファームウェアをアップグレードまたはダウングレードには、**[通常アップグレード（Regular Upgrade）]** を選択し、**[ファームウェア イメージ（Firmware Image）]** ドロップダウンから目的のファームウェア イメージを選択します。

ステップ 5 **[ステップ 2 - 検証（Step 2 - Validation）]** ステップが表示されます。

APIC は、外部検証ルールとともに、組み込みの事前アップグレード検証を実行します。すべての検証に合格したことを確認するか、失敗した検証に対して適切なアクションが実行されたことを確認します。重大度が「致命的」で失敗した検証がある場合は、修正して次の手順に進む必要があります。

「外部検証ルール」のセクションで説明したように、 APIC は Cisco Intersight またはローカル ファームウェア リポジトリから外部ルールを取得できます。

（注）
次のステップに進むには、APIC に Cisco Intersight またはローカル ファームウェア リポジトリのいずれかからの外部ルールが必要です。

ステップ 6 **ステップ 2**：**検証**で失敗したすべての検証に対処したら、**[次へ（Next）]** をクリックします。

ステップ 7 **[ステップ3 ：アップグレード（Step 3 - Upgrade）]** ビューで、選択内容を確認してから **[送信（Submit）]** をクリックします。

ステップ 8 コントローラとクラスターのアップグレード/ダウングレードステータスをモニタします。

- コントローラは、クラスターの可用性を維持するために、一度に 1 つずつアップグレードまたはダウングレードします。
- APIC1 の再起動中に、APIC2 のモニタリング ビューに移動します。この特定の期間を除いて、進行状況をモニタするには常に APIC1 上にいる必要があります。

  進捗バーには次の 3 種類があります。

  - **アップグレード** ：全体のアップグレードの進行状況
  - **クラスター全体** ：クラスター レベルの操作の手順と進行状況
  - **ノード X**：個々の APIC ノードの手順と進行状況

[クラスタ全体（Cluster Wide）] と **[ノードの 進行状況（Node progress）]** を展開すると、詳細を確認できます。

- すべてのコントローラが完了し、**[Fully Fit（完全に適合）]** ステータスを報告するまで待ちます。

ステップ 9 以前のアップグレードのアップグレードの詳細を表示するには、**[履歴（History）]** タブを選択します。

a) ドロップダウンから **[インスタンスのアップグレード（Upgrade instance）]** を選択、コントローラの以前のアップグレードを選択します。コントローラの **[アップグレード タイプ（Upgrade Type）]**、**[From Version]**、**[To Version]**、**[Start Time]**、**[Updated Time]** など、以前のアップグレードの詳細を確認できます。

また、以前のアップグレードのノード レベルおよびクラスタ全体の段階/手順の数を確認することもできます。番号をクリックすると、各段階の詳細と開始時刻、更新（終了時刻）が表示されます。

（注）
Cisco ACI 6.2(1) リリース以降のリリースからのアップグレードまたはダウングレードの履歴のみを表示できます。

クラスター内のすべてのコントローラが、ターゲットのファームウェア バージョンにアップグレードまたはダウングレードされます。APIC クラスターは、新しいリリースで完全に適合して動作可能になります。

次のタスク

完了後、クラスターの正常性を確認し、アップグレードログまたは監査証跡で追加のアクションや検証を確認します。

リリース 6.2x 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または、ダウングレード

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）または、ダウングレードを開始せずに、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。

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。

（注） あるリリースから次のリリースにスイッチをアップグレードすると、ブートフラッシュ メモリが増加すると、障害コードF1821が表示されます。この障害は、スイッチのアップグレード後に自動にクリアされるため、無視してください。

Cisco APIC 上のソフトウェアをダウングレードする場合、プロセスは、ソフトウェアをアップグレードのプロセスと同じです。しかし、ターゲットリリースは、現在インストールされているリリースより以前のものを選択します。ソフトウェアをダウングレードしている場合でもダイアログ、フィールド、ボタンとその他の Cisco APIC GUI 内のコントロールのテキストは、「アップグレード」を指定します。

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または、ダウン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または、ダウングレードに進みます。
- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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、**[スイッチ（Switches）]**をクリックします。
[スイッチ（Switches）] 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 **[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**[更新グループの作成（Create Update Group）]**を選択します。

ステップ 4 **[スイッチ アップデート グループの設定（Setup Switch Update Group）]** ウィンドウが表示されたら、**[グループ名のアップグレード（Upgrade Group Name）]** の名前を入力します。

ステップ 5 **[スイッチの選択（Switch Selection）]** ステップで、**[スイッチの追加（Add Switches ）]** ボタンをクリックし、アップグレードまたはダウングレードする必要があるスイッチを選択して、**[OK]** をクリックし、**[次へ（Next）]** をクリックします。

ステップ 6 **[バージョンの選択（Version Selection）]** ステップで、**[ファームウェアの選択（Select Firmware）]** セクションで **[アップデート タイプ（Update Type）]** を選択し、アップグレード/ダウングレードするイメージを選択します。

ステップ 7 （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（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 **[適用（Enforced）]** 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、**[互換性の確認（Compatibility Check）]** フィールドの隣にあるボックスのチェック マークをオンにして互換性チェック機能を無効にするを選択すると、システムに対してサポートされていないアップグレードが実行されるリスクが発生し、システムが利用できない状態になる可能性があります。

- **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。デフォルトでは、この設定は **[適用しない（Unenforced）]** です。

  詳細については ACI スイッチのグレースフル アップグレードまたは、ダウングレード（45 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 アップグレードとダウングレードのガイドライン（41 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 8 **[バージョン選択（Version 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 9 **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。

詳細は、アップグレード / ダウングレード前のチェックリスト （81 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 10 **[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）
リリース 4.x または 5.0 を実行している Cisco 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または、ダウングレード（110 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 （125 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 11 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 （166 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、スクリプトを使用します。これは、APIC に組み込まれているアップグレード前検証によってスイッチ イメージが再度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。

- アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 ページ）
- アップグレード / ダウングレード前のチェックリスト （81 ページ）
- アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 ページ）

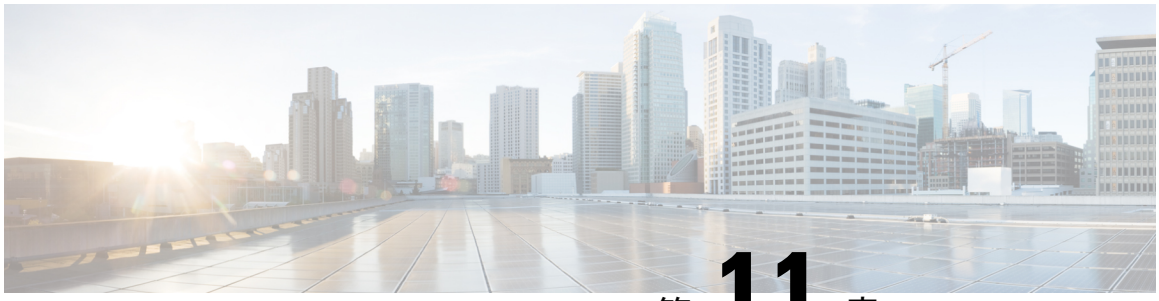
最初に、リーフおよびスパイン スイッチへのイメージの事前ダウンロード（121 ページ） で事前ダウンロード手順を完了する必要があります。

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、**[アクション（Actions）]** をクリックし、それから **[インストールの開始（Begin Install）]** 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。



第 11 章

REST API を使用するソフトウェアのアップグレードまたは、ダウングレード

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 を使用するCisco 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

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 を使用してスイッチをソフトウェアのアップグレードまたは、ダウングレード

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>
```

- リリース 5.1(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。

  - アップグレード前の検証ツール（APIC）

    APIC 事前検証の場合

    ```
    GET URL - https://<ip
    address>/mqapi2/deployment.query.json?mode=validateCtrlrMaintP&targetVersion=6.1.(4h)
    b.
    ```

    （注）
    targetVersion パラメータは **6.1.(4h)**に設定されます。これは、この API コールで受け入れられる唯一の形式です。

    スイッチの事前検証用

    ```
    POST URL - https://<ip
    address>/mqapi2/deployment.query.xml?mode=validateSwitchMaintPAsync
    <syntheticMaintPSwitchDetails maintPName="POD2_LEAF_ODD" />
    ```

  - 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

    ```
    POST URL - https://<ip address>/api/node/mo/uni/fabric.xml
                        <fabricInst>
                    <maintMaintP downloadSt="triggered" name="
                    </maintMaintP>
                    <maintMaintGrp name="
                           <fabricNodeBlk name="blk102" from_="102" to_="102">
                           </fabricNodeBlk>
                           <maintRsMgrpp  tnMaintMaintPName="
                           </maintRsMgrpp>
                    </maintMaintGrp>
            </fabricInst>
    ```

    （注）
    downloadSt 属性で **トリガとして使用する** 値または **使用しない** 値を指定すると、これらの値は無視されます。

  - グレースフルアップグレード

    ```
    POST URL - https://<ip address>/api/node/mo/uni/fabric.xml
                        <fabricInst>
                    <maintMaintP downloadSt="triggered" name="
                    </maintMaintP>
                    <maintMaintGrp name="
                           <fabricNodeBlk name="blk102" from_="102" to_="102">
                           </fabricNodeBlk>
                           <maintRsMgrpp  tnMaintMaintPName="
                           </maintRsMgrpp>
                    </maintMaintGrp>
            </fabricInst>
    ```

（注）
downloadSt 属性で **トリガとして使用する** 値または **使用しない** 値を指定すると、これらの値は無視されます。

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または、ダウングレード

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または、ダウングレード時にアップグレードまたは、ダウングレードされます。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

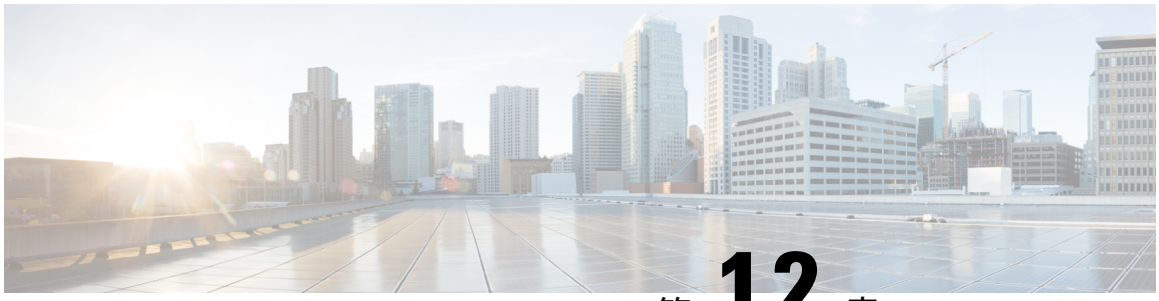
```
POST URL: http://trunk6-ifc1/api/node/mo/uni/fabric.xml
<maintMaintP name="AllswitchesMaintP" adminSt="triggered">
</maintMaintP>
```

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 を使用したソフトウェアのアップグレードまたは、ダウングレード

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。
  - アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック（38 ページ）
  - アップグレード / ダウングレード前のチェックリスト （81 ページ）
  - アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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 スタイル CLI を使用したCisco 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

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：

```
apic1# scp <username>@<Host IP address that has the image>:/<absolute path to the image
 including image file name>  .
apic1# pwd
/home/admin
apic1# 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 アップグレードまたはダウングレード用に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またはダウングレードします。

例：

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

コントロール クラスタがアップグレードまたは、ダウングレードの際に使用可能にするため Cisco APICは、シリアルにアップグレードまたは、ダウングレードされます。 アップグレードまたは、ダウン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または、ダウン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または、ダウングレード

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：

```
apic1# scp <username>@<image_host_IP>:/<filename_and_image_absolute_path>  .
apic1# pwd
/home/admin
apic1# 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
```

（注）
CLI モードを使用してファームウェアをアップグレードして 6.0（2）に移行すると、メンテナンス グループに 2 つのターゲット ファームウェア バージョンが表示されます。基本バージョ

ンが同じであるため、これらの画像は両方とも表示されます。両方のファームウェアバージョンは同じリリースに属しており、次に示すように、一方のバージョンには 64 ビットの拡張機能があり、もう一方のバージョンには 64 ビットの拡張機能がありません。

```
apic1(config-firmware-switch)# show running-config
# Command: show running-config firmware switch-group 64bit
# Time: Thu Jan 19 05:23:15 2023
  firmware
    switch-group 64bit
      switch 102
      switch 103
      switch 104
      switch 105
      switch 152
      firmware-version aci-n9000-dk9.16.0.2.bin
      firmware-version aci-n9000-dk9.16.0.2-cs_64.bin
      exit
    exit
```

上記の出力の `firmware-version aci-n9000-dk9.16.0.2.bin` と `firmware-version aci-n9000-dk9.16.0.2-cs_64.bin` ファームウェア ステートメントは、1 つが構成されているにもかかわらず、2 つのファームウェア バージョンが存在することを示しています。

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 <image_filename>
```

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 <switch_group>
apic1(config-firmware-switch)# switch <switches_to_add_to_group>
apic1(config-firmware-switch)# firmware-version <image_filename>
```

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
```

（注）
上記の **switch** コマンドで **no** 引数を使用して、グループからスイッチを削除することもできます：

例：

```
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、「スケジューラを使用してアップグレードまたは、ダウングレードすることについて （50 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 <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 <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。

```
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。

```
Pod   Node  Current-Firmware   Target-Firmware    Status              Upgrade-     Download-   Download-
                                                                     Progress(%)  Status      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または、ダウングレード

デフォルトで、コントローラをアップグレードまたは、ダウングレードすると、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または、ダウングレードされます。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。

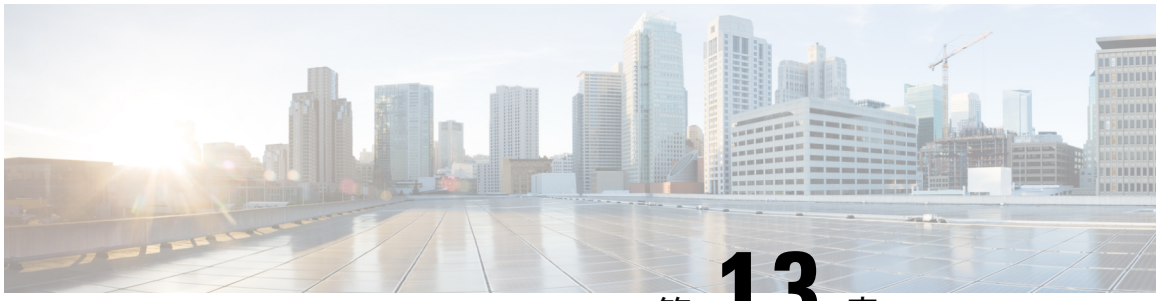
例：

```
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

アップグレードとダウングレード 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、アップグレードまたは、ダウングレードに関するガイドラインおよび制限事項 （68 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またはダウングレードの失敗が検出されると、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（165 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または、ダウングレードは、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または、ダウングレード 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または、ダウングレード 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または、ダウン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または、ダウン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

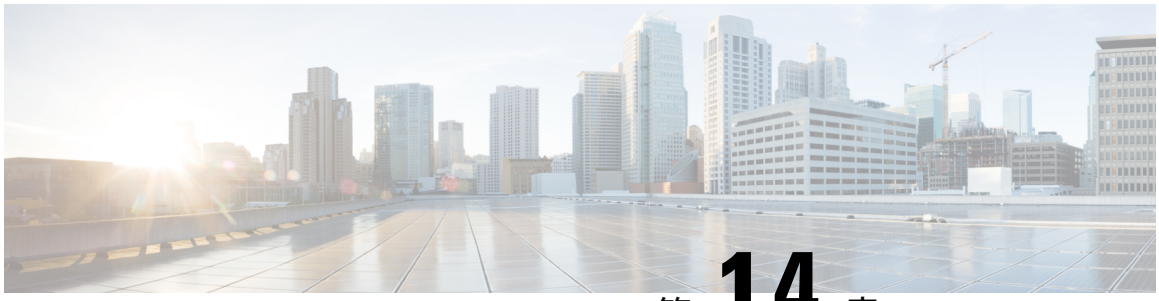
TPM 状態-所有

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

検出の自動ファームウェア更新

APIC 検出の自動ファームウェア更新

Cisco Application Policy Infrastructure Controller（APIC）6.0(2) リリース以降、製品の返品および交換（RMA）、クラスタ拡張、またはコミッションのいずれかによって新しい Cisco APIC をファブリックに追加するとき、Cisco APIC は既存のクラスタの同じリリースに自動的にアップグレードされます。新しいCisco APICがアップグレードプロセスを経るにつれて、 Cisco APICがアップグレードされてクラスタに参加するまでにさらに時間がかかる場合があります。自動アップグレードが失敗すると、Cisco APIC では障害が発生し、警告が表示されます。

検出機能の自動Cisco APICファームウェア アップデートの前提条件と条件：

- クラスタ内のコミッションされたすべての Cisco APIC は、同じリリース（6.2(1) 以外の 6.0(2) 以降）を実行している必要があります。
- クラスタ内のコミッションされた Cisco APIC と同じリリースの Cisco APIC イメージは、クラスタ内のコミッションされた Cisco APIC のファームウェア リポジトリで使用できる必要があります。
- 新しい Cisco APIC の CIMC IP アドレスが設定されていて、クラスタ内の委託された Cisco APIC から到達可能である必要があります。
- 新しい Cisco APIC が 6.0(2) 以前のリリースを実行している場合、新しい Cisco APIC でファブリック名、Cisco APIC ID などを設定する Cisco APIC コンソールを介して初期セットアップ ユーティリティを使用し完了する必要があります。新しい Cisco APIC でもリリース 6.0(2) 以降を実行している場合は、初期セットアップ ユーティリティを使用する必要はありません。
- APIC ディスカバリで自動ファームウェア更新は、更新する新しい APIC がCisco APIC リリース 4.2(1) 以降の場合でのみサポートされます。
- APIC クラスターが 6.1(2) または新しいバージョンを実行していて、6.0(2) よりも古いバージョンを実行している新しいスタンバイ APIC が APIC クラスターに追加された場合は、

新しいスタンバイ APIC で次のコマンドを実行する必要があります。 **APIC ディスカバリで自動ファームウェア更新が** 機能します。

1. 新しい APIC の CLI にログインします。

（注） 新しい APIC が ノード-1 でない場合は、「*rescue-user*」としてパスワードなしでログインします。これは、新しい APIC で **初期セットアップ ユーティリティ** が完了した後、管理者パスワード（またはその他の設定）がまだ同期されていないためです。

2. **acidiag vapicjoin -n <Active APIC OOB IP> -u admin -p <admin password>** を実行します。

   ここで **<Active APIC OOB IP>** は、クラスターにすでに存在する 1 つの APIC のアウトオブバンド IP アドレスです。

3. スタンバイ APIC が APIC クラスターの残りの APIC と同じバージョンに自動アップグレードされた場合は、アクティブな APIC を削除し、初期設定へのリセットを実行してから、アクティブな APIC をクラスターに戻す必要があります。

製品返品承認（RMA）を通じて新しい Cisco APIC をファブリックに追加する場合は、手順 1 と 2 を繰り返します。詳細については、「CLI を使用した、クラスタ内の Cisco APIC の交換」を参照してください。

- APIC の自動アップグレードは、Cisco ACI リリース 6.2.1 ではサポートされていません。

スイッチ検出の自動ファームウェア更新

[スイッチ検出で自動ファームウェア更新（Auto Firmware Update on Switch Discovery）] を有効にする場合、Cisco Application Policy Infrastructure Controller（APIC）では以下のシナリオで新しいスイッチのファームウェアを自動的に更新します。

- 新しいノード ID で新規スイッチ検出
- 既存のノード ID でスイッチ交換
- 既存のノードの初期化と再検出
- **reload** CLI コマンドを使用した、または電源の再投入によるスイッチのリロード

Cisco APIC リリース 5.1(1) 以前で、この機能は **[ブートスクリプト バージョン検証の強制（Enforce Bootscript Version Validation）]** と呼ばれ、**[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）]** に存在していました。リリース 5.1(1) で、この機能は名前が変更され、現在の場所に移動しました。

手順

ステップ 1 メニュー バーで、**[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ファブリック メンバーシップ (Fabric Membership)] > [自動ファームウェア更新 (Auto Firmware Update)]** に移動します。

ステップ 2 **[スイッチ検出で自動ファームウェア更新 (Auto Firmware Update on Switch Discovery)]** チェックボックスをオンにそて、この機能を有効にします。

ステップ 3 **[デフォルト ファームウェア バージョン (Default Firmware Version)]** ドロップダウン リストで新しいスイッチを更新するために、ターゲット ファームウェア バージョンを選択します。

（注）
交換シナリオなど新規スイッチのノード ID が **[管理 (Admin)] > [ファームウェア (Firmware)]** の下にあるファームウェア更新の一部である場合、新規スイッチは更新グループで指定されたターゲットバージョンに更新されます。もしくは、この手順で指定されたデフォルトのファームウェア バージョンに更新されます。

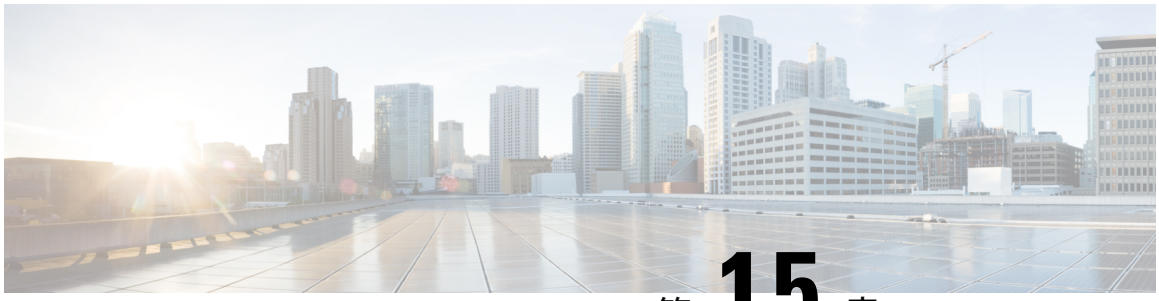
選択された **[デフォルトのファームウェア バージョン（Default Firmware Version）]** が「any」の場合、この機能ではファームウェア更新グループの一部ではない ID を持つ新規スイッチのファームウェアを更新しません。ファームウェア更新グループの一部であるノード ID を持つ新規スイッチは、更新グループで指定されたターゲット バージョンに更新されます。

ステップ 4 [Submit] をクリックします。

スイッチ検出制限の自動ファームウェア更新

スイッチ検出時の自動ファームウェア更新には、次の制限が適用されます。

- ターゲットスイッチのリリースが 16.0(3) 以降で、スイッチで実行されている現在のリリースが 15.2(7) 以前または 16.0(1) または 16.0(2) である場合、スイッチ検出時の自動ファームウェア更新はサポートされません。この状態でスイッチ検出の自動ファームウェア更新が試行された場合、スイッチが無期限にスタックする可能性があります。その状態からスイッチをファブリックに追加するには、 Cisco Application Policy Infrastructure Controller（APIC）でスイッチ検出時の自動ファームウェア更新を無効にした後、クリーンリブートを実行する必要があります。



第 15 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。

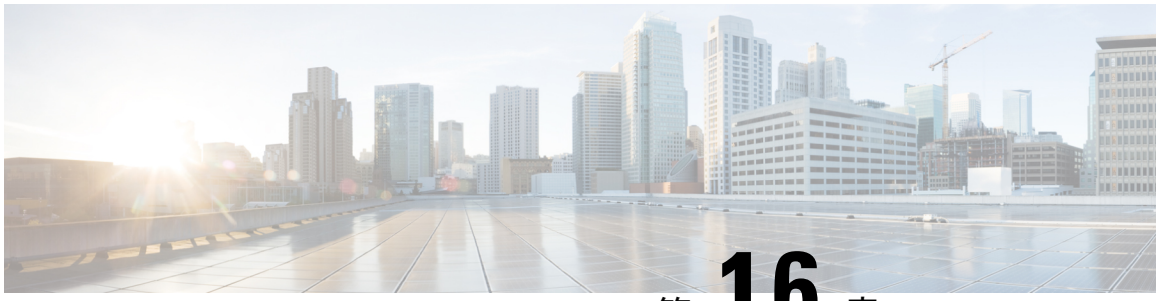
通常の起動シーケンス中のこれらの自動 FPGA / EPLD / BIOS アップグレードは、コンポーネントごとに実行されます。たとえば、新しいラインカードモジュールが挿入され、スーパーバイザモジュールからダウンロードされたベース ACI スイッチイメージを使用して起動すると、新しいラインカード モジュールのみの電源がオンになり、ベース ACI スイッチ イメージから FPGA / EPLD / BIOS が適用されます。他のモジュールは影響を受けません。

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 16 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または、ダウングレードについて

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

CLI APIC GUI 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または、ダウングレードの設定

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または、ダウン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（103 ページ）に記載されている手順を使用します)。
- 「アップグレードまたはダウン グレードするワークフローを Cisco ACI ファブリック （38 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) [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または、ダウングレードの設定

このセクションでは、SR パッケージのアップグレードまたは、ダウン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または、ダウングレードおよび 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または、ダウン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または、ダウン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または、ダウングレードについて （183 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または、ダウングレードの構成

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または、ダウングレードを構成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または、ダウングレードについて （183 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 17 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。
- 5.2(8) より前のリリース、および 6.0(1) および 6.0(2) リリースでは、SMU パッチで Cisco Application Policy Infrastructure Controller （APIC）GUI を変更することはできません。5.2(8) および 6.0(3) リリース以降、SMU パッチは Cisco APIC GUI を変更できます。
- スイッチの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、そのスイッチに以前にインストールした SMU パッチが削除されます。

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または、ダウングレード （115 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または、ダウングレード （115 ページ）を参照してください。

リリース 6.2 以降から Cisco APIC ソフトウェア メンテナンス アップグレード パッチを GUI を使用してインストールする

Cisco Application Policy Infrastructure Controller（APIC）リリース 6.2(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 APIC ユーザー インターフェイスの **[管理（Admin）] > [ファームウェア（Firmware）]** セクションに移動します。

ステップ 2 ナビゲーション ペインから **[コントローラ（Controllers）]** を選択します。**[コントローラと CIMC のアップグレード（Controller & CIMC upgrade）]** ウィンドウが表示され、選択に基づいてコンポーネントをアップグレードできます。

ステップ 3 パッチをインストールするには、**[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 イメージ（Firmware Image）]** ドロップダウンから適切なパッチ イメージを選択します。

手順については、リリース 6.2x 以降からの Cisco APIC のアップグレードまたはダウングレード （140 ページ）を参照してください。

ステップ 4 **[次へ（Next）]** をクリックします。

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）。

Cisco APIC リリース 6.0（2）内以降では、32 ビットと 64 ビット SMU イメージを Cisco APIC にダウンロードします。一つのイメージしかダウンロードしない場合、アップグレード中にエラーが生じることがあります。

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または、ダウングレード （115 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または、ダウングレード （115 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）]** をクリックします。

6.0(2) リリースより前あるいは、6.0(2) リリース以降で**[スイッチ再起動タイプ（Switch Restart Type）]** プロパティが **[リロード（Reload）]** に設定されている場合は、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（Install and Reload）]**：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（Install and Skip Reload）]**：SMU パッチのインストール後、スイッチは再起動されません。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 Reload）]** 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、**[インストールおよびリロードのスキップ（Install and Skip Reload）]** を選択するか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。

6.0（2）リリース以降で、**[スイッチの再起動タイプ（Switch Reboot Type）]** というプロパティが **[再起動（Restart）]** に設定されている場合、**[インストール（Install）]** を選択します。スイッチを再起動せずにスイッチに適用できる SMU の場合、**[インストール（Install）]** を選択すると、スイッチが動作している間に SMU がインストールされます。SMU のインストールがスイッチを通過するトラフィックに影響を与えるかどうかは、SMU が適用する修正によって異なります。

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または、ダウングレード（115 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。

リリース 6.2 以降から Cisco APIC ソフトウェア メンテナンス アップグレード パッチを GUI を使用してアンインストールする

Cisco Application Policy Infrastructure Controller（APIC）6.2(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

ステップ 1 APIC ユーザー インターフェイスの **[管理（Admin）] > [ファームウェア（Firmware）]** セクションに移動します。

ステップ 2 ナビゲーション ペインから **[コントローラ（Controllers）]** を選択します。
[コントローラと CIMC のアップグレード（Controller & CIMC upgrade）] ウィンドウが表示され、選択に基づいてコンポーネントをアップグレードできます。

ステップ 3 パッチをインストールするには、**[ソフトウェアメンテナンス アップグレード（アンインストール）（Software Maintenance Upgrade (Uninstall）]**を選択し、**[ファームウェア イメージ（Firmware Image）]** ドロップダウンから適切なパッチ イメージを選択します。

手順については、リリース 6.2x 以降からの Cisco APIC のアップグレードまたはダウングレード（140 ページ）を参照してください。

ステップ 4 **[次へ（Next）]** をクリックします。

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または、ダウングレード（115 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>
```

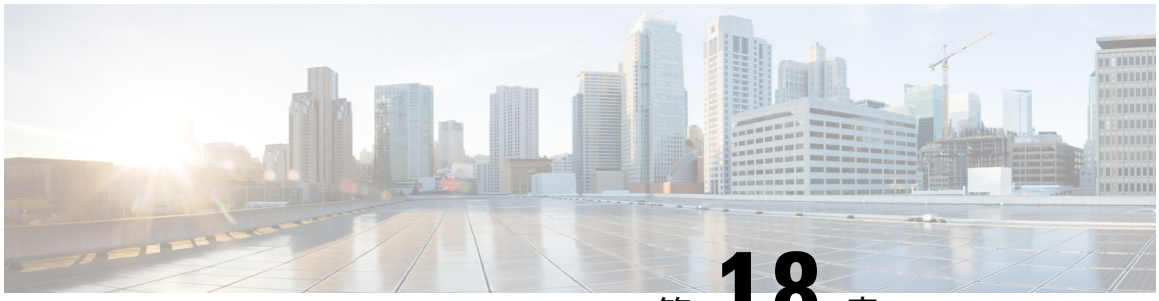
次のテーブルでは、SMU パッチ固有の要素とパラメータを説明します。

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 18 章

スイッチ ハードウェアのアップグレード

はじめに

ACI ファブリックのスイッチハードウェアをアップグレードする場合は、次の複数のシナリオを考慮する必要があります。

- **シナリオ 1** ：スパイン スイッチのハードウェアをアップグレードします。
- **シナリオ 2** ：vPC を使用せずにリーフ スイッチのハードウェアをアップグレードします。
- **シナリオ 3** ：vPC を使用してリーフ スイッチのハードウェアをアップグレードします。

各シナリオには、新旧のスイッチ ハードウェアのサポートされているソフトウェア バージョンに応じて 2 つのバリエーションがあります。

バリエーション 1 ：古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できます。

バリエーション 2 ：古いスイッチと新しいスイッチで同じ ACI ソフトウェア バージョンを実行することはできません。

可能な限り、古いスイッチと新しいスイッチの両方で同じソフトウェアバージョンを実行することをお勧めします（バリエーション 1）。バリエーション 2 は、古いスイッチ ハードウェアが新しいスイッチ ハードウェアをサポートするソフトウェア バージョンでサポートされなくなった特定の状況向けです。

「バリエーション 2：新旧のスイッチで同じ ACI ソフトウェアバージョンを実行できない」の例。

前述のように、バリエーション2は、古いスイッチハードウェアが新しいスイッチハードウェアをサポートするソフトウェア バージョンでサポートされなくなった特定の状況向けです。

最も一般的なシナリオは、第 1 世代のCisco Nexus 9000 シリーズ スイッチから新世代の Cisco Nexus 9000 シリーズ スイッチに移行する場合です。第 1 世代のスイッチは、Cisco ACI スイッチ ソフトウェア 15.0(1) 以降のリリースではサポートされなくなりましたが、新しい世代のスイッチの一部は 15.0(1) 以降でのみサポートされます。

（注）

- 第 1 世代のCisco Nexus 9000 スイッチには、Cisco Application Leaf Engine（ALE）ASIC が搭載されています。これらのスイッチの製品識別子には、-EX、-FX、または -GX が含まれていません。たとえば、N9K-C9372PX、N9K-C9372PX-E などです。
- 新世代の Cisco Nexus 9000 スイッチには、 Cisco Cloud Scale ASIC が搭載されています。これらのスイッチの製品識別子には、-EX、-FX、-GX 以降のサフィックスが付いています。例としては、N9K-C93180YC-EX、N9K-C93180YC-FX、N9K-C93180YC-FX3 などがあります。

一般的なガイドライン

- 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 Transceiver Modules Installation Guides』を参照してください。
- トラフィック損失の可能性があるため、メンテナンス ウィンドウ中にハードウェア置換を実行することをお勧めします。
- 交換するスイッチに接続されている Cisco Application Policy Infrastructure Controller（APIC）をファブリック内の他のスイッチに移動し、Cisco APICクラスタが「完全に適合」するまで待機することをお勧めします。
- 自動ファームウェア アップデート機能を使用する場合は、[デフォルト ファームウェア バージョン（Default Firmware Version）] をターゲット バージョンに設定してください。ノード ID がアップグレード グループの一部である場合は、アップグレード グループがターゲットバージョンで設定されていることを確認するか、アップグレードグループを削除しするようにしてください。詳細については、「自動ファームウェアの更新」を参照してください。
- 新しいスイッチのポート数とポートタイプは、交換する古いスイッチと一致している必要があります。番号が一致しない場合は、新しいポートまたはポートタイプに対応するように構成を変更する必要があります。

スパインスイッチ

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できません

1. APIC クラスタを、新しいスイッチ ハードウェアを実行できるソフトウェア バージョンにアップグレードします。
2. 交換しないスイッチを APIC クラスタと同じバージョンにアップグレードします。
3. 古いバージョンを実行している既存のスイッチと新しいバージョンを実行している新しいスイッチを使用して、RMA と同じ手順に従います。

   詳細については、「ACIファブリック検出のトラブルシューティング - デバイス交換」の「手順と検証」を参照してください。

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できます

手順は返品許可（RMA）と同じです。

詳細については、「ACIファブリック検出のトラブルシューティング - デバイス交換」の「手順と検証」を参照してください。

vPC を使用しないリーフ スイッチ

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できません

上記の スパイン スイッチ と同じです。

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できます

上記の スパイン スイッチ と同じです。

vPC を使用したリーフ スイッチ

『Cisco APIC レイヤ 2 ネットワーキング構成ガイド』に記載されているように、同じ vPC ペア内での第1世代スイッチと新世代スイッチの混在はサポートされていません。ただし、セカンダリ vPCスイッチがvPCレッグをダウン状態に保つという制限付きで、移行中に一時的にサポートされます。

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できません

始める前に

次の手順を実行します。

- 自動ファームウェア更新ポリシーを無効にする必要があります。
- クラスタが古いリリースを実行している場合は、Cisco APIC クラスタを 4.2（7v）リリースにアップグレードします。また、すべてのスイッチを 14.2（7v）リリースにアップグレードします。ファブリックが統合されるまで待ちます。
- Cisco APIC クラスタを 5.2（7f）リリースにアップグレードし、クラスタが「完全に適合」するのを待ちます。
- 交換しないスイッチを 15.2(7f) にアップグレードします。
- 新しいスイッチがプリロードされ、Cisco APIC と同等のリリース、つまり 15.2(7f) リリースが実行されていることを確認します。ソース バージョンとターゲット バージョンのソフトウェア リリース 4.2(7v)/14.2(7v) および 5.2(7f)/15.2(7f) 以外のソフトウェア リリースは、この移行手順でサポートされていません。

（注） 新しいスイッチの最小ソフトウェア バージョン要件が 15.2(7f) よりも新しい場合、次の手順はサポートされません。このような場合は、vPCペアの両方の古いスイッチを一度に削除し、新しいスイッチを一度に追加する必要があります。

手順

ステップ 1 Cisco APIC GUI から、動作中のセカンダリ vPC スイッチ ノードに対して**コントローラからの削除**操作を実行します。

Cisco APIC クリーンにより、スイッチが再起動します。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。

（注）
コントローラからの削除操作を実行すると、動作可能なセカンダリ vPC のトラフィックが数秒間失われます。

ステップ 2 取り外した第 2 世代のスイッチからケーブルを接続解除します。

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』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、古いスイッチを取り外します。

ステップ 4 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、新しいスイッチを取り付けます。

ステップ 5 古いスイッチから取り外したゆるんだケーブルを、新しいスイッチの同じポートに接続します。

ステップ 6 第 2 世代スイッチを Cisco 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。Cisco APIC では新しいスイッチにポリシーをプッシュし、スイッチ世代の不一致があるため vPC レッグが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 7 ステップ 8 （205 ページ） に進む前に、新しいスイッチが構成をダウンロードするまで 10 ～ 15 分待ちます。

ステップ 8 Cisco 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。Cisco APIC クリーンにより、スイッチが再起動します。

操作が完了するまで約 10 分待ちます。Cisco APIC によりダウン状態になっていた新しいスイッチの vPC レッグが起動します。このアクションにより、すべてのトラフィックが新しいスイッチに移動するように求められます。新しいスイッチの vPC ポートが起動するまでに数分かかる場合があり、その間にトラフィックがドロップします。トラフィック ドロップの期間は、ファブリック内のスケールとフローによって異なります。

ステップ 9 第 1 世代スイッチからケーブルを接続解除します。

ステップ 10 ステップ 3 （205 ページ） で行ったように、第 1 世代のスイッチを取り外します。

ステップ 11 で行ったように、第 2 世代スイッチを取り付けます。ステップ 4 （205 ページ）

ステップ 12 ステップ 5 （205 ページ） で行ったように、緩んだケーブルを接続します。

ステップ 13 第 2 世代スイッチを Cisco 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。Cisco APIC ではポリシーを新しいスイッチにプッシュし、vPC レッグが起動し、トラフィックの通過を開始します。

古いスイッチおよび新しいスイッチで、同じ ACI ソフトウェア バージョンを実行できます

次の「vPC を搭載したリーフ スイッチ」の「古いスイッチと新しいスイッチでは同じ ACI ソフトウェア バージョンを実行できない」セクションと同じ手順を実行します。これは、「古いスイッチと新しいスイッチでは同じ ACI ソフトウェア バージョンを実行できない」の「セクションを開始する前に」に記載されている特定の送信元とターゲットのバージョン要件などの追加要件のない同じ手順です。

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。