Cisco APIC 管理/インストール/アップグレード/ダウングレード ガイド

初版：2016 年 7 月 1 日

最終更新：2018 年 6 月 25 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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 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.

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/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016–2018 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに vii

対象読者 vii

表記法 vii

関連資料 ix

マニュアルに関するフィードバック x

マニュアルの入手方法およびテクニカル サポート x

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

Cisco APIC イメージのインストールまたは回復 3

設置上の注意事項 3

使用上のガイドライン 5

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 7

PXE サーバを使用した Cisco APIC ソフトウェアのインストール 8

インストール Cisco APIC 仮想メディアを使用してソフトウェア 10

KVM コンソールで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 10

1 つのクリーン インストール Cisco APIC Debug CLI を使用して 12

Debug CLI を使用して Cisco APIC クラスタ全体に明確にインストールして Cisco ACI ファブリックを消去する 13

ステートフルにインストールする Cisco APIC Debug CLI を使用してクラスタ化 14

第 3 章

Cisco APIC およびスイッチ ソフトウェアのアップグレードとダウングレード 15

ファームウェア管理について 16

ファームウェアのアップグレード モード 17
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 18
Cisco APIC およびスイッチ ソフトウェアのアップグレードについて 21
Cisco APIC およびスイッチ ソフトウェアのサポートされているアップグレード パス 23
Cisco APIC 長期リリース 73
Cisco APIC およびスイッチ ソフトウェアのダウングレードについて 74
ステートレス ダウングレード手順 76
Cisco APIC およびスイッチ ソフトウェアのサポートされているダウングレード パス 76
スケジューラによるアップグレードについて 90
アップグレードする前に LLDP に接続を無効にする方法 91
GUI を使用したソフトウェアのアップグレード 92
Upgrading the Cisco APIC Software Version Using the GUI 92
GUI を使用した、リーフおよびスパイン スイッチ ソフトウェアの バージョン アップグレード 94
GUI 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 96
変更、互換性を無視する設定を確認 97
REST API を使用したソフトウェアのアップグレード 98
REST API を使用した Cisco APIC ソフトウェアのアップグレード 98
REST API を使用したスイッチ ソフトウェアのアップグレード 99
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 100
CLI による ソフトウェアのアップグレード 100
NX-OS を使用した Cisco APIC ソフトウェアのアップグレード 101
NX-OS スタイル CLI を使用したスイッチのアップグレード 102
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 103
デバッグ CLI を使用したコントローラのアップグレード 104
3 つの手順でデバッグ CLI を使用してコントローラをアップグレードする 104
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 104
SSD インストール ステータスの確認 105
アップグレード プロセス中にフォールトのトラブルシューティング 105
ダウンロード障害の一般的な原因 106
クラスタの収束の確認 106

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 107
GUI を使用してコントローラのアップグレード スケジューラ一時停止しているかどうかを確認するには 107
REST API を使用してコントローラのアップグレード スケジューラ一時停止しているかどうかを確認するには 108
スイッチのアップグレードの一時停止確認 108
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 108
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 109
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 110
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 110
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 110
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 111
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 111
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 111
クリーン再起動の実行 112
共有レイヤ 3 アウトでアップグレードする 112
アップグレード、 Cisco APIC リーフ スイッチの前に 113
リーフをアップグレードする前にスイッチ、Cisco APIC 113
後に、 Cisco APIC リーフ スイッチをアップグレードと 114
共有レイヤ 3 アウトでダウングレードする 114
ダウン グレード、 Cisco APIC リーフ スイッチの前に 114
Cisco APIC 前にリーフ スイッチをダウンロードする 114
推奨されるダウングレード 114
ネットワーク設定機能と混合 OS 動作中の変更 115
Cisco Nexus 9300 プラットフォーム スイッチから Cisco Nexus 9300 EX プラットフォーム スイッチへの移行 119
アップグレードの例 121

コントローラ アップグレードの例 121
スイッチのアップグレード例 122

はじめに

この前書きは、次の項で構成されています。

- 対象読者 （vii ページ）
- 表記法 （vii ページ）
- 関連資料 （ix ページ）
- マニュアルに関するフィードバック （x ページ）
- マニュアルの入手方法およびテクニカル サポート （x ページ）

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- 仮想マシンのインストールと管理
- サーバ管理
- スイッチおよびネットワークの管理

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。

表記法	説明
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体のスクリーンフォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注）	「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

これらの注意事項を保存しておいてください

関連資料

Application Policy Infrastructure Controller（APIC）のマニュアル

次のガイドでは、APIC のドキュメントを提供します。

- 『*Cisco APIC Getting Started Guide*』
- 『*Cisco APIC Basic Configuration Guide*』
- *Cisco ACI* の基礎
- *Cisco APIC* レイヤ *2* ネットワーク設定ガイド
- *Cisco APIC Layer 3* ネットワーキング設定ガイド
- 『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』
- *Cisco APIC REST API* 設定ガイド
- 『*Cisco APIC* レイヤ *4* ～ レイヤ *7* サービス導入ガイド』
- 『*Cisco ACI Virtualization Guide*』
- *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：ベスト プラクティス ガイド

これらすべてのドキュメントは、次の URL で入手できます。 http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）のマニュアル

ACI の各種マニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ アプリケーションセントリック インフラストラクチャ（ACI）シミュレータのマニュアル

Cisco ACI Simulator のマニュアルは、次の URL から入手できます：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html

Cisco Nexus 9000 シリーズ スイッチのマニュアル

Cisco Nexus 9000 シリーズ スイッチのマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Cisco Application Virtual Switch のマニュアル

Cisco Application Virtual Switch（AVS）のマニュアルは、次の URL で入手できます。http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）と OpenStack の統合に関するマニュアル

Cisco ACI と OpenStack の統合に関するマニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。

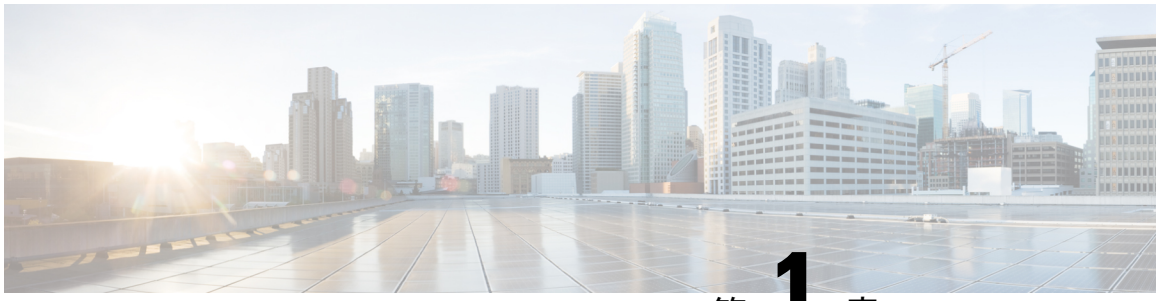
マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、Cisco バグ検索ツール（BST）の使用法、テクニカル サポートの依頼方法、および追加情報の収集方法については、『*What's New in Cisco Product Documentation*』（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダー アプリケーションを使用し

て、コンテンツをデスクトップに直接配信することもできます。RSS フィードは無料のサービスです。

はじめに



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 （1 ページ）

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。

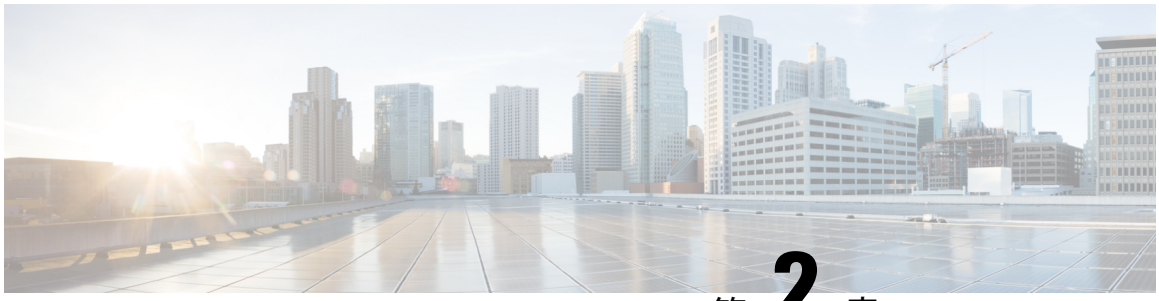
次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。ただし、このリリースに関するガイドの変更点や新機能の中には、一部、この表に記載されていないものもあります。

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	機能	説明	参照先
リリース 3.2(1m)	Cisco APIC 長寿命リリース		Cisco APIC 長期リリース （73 ページ）
リリース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。	ネットワーク設定機能と混合 OS 動作中の変更 （115 ページ）
リリース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。	ネットワーク設定機能と混合 OS 動作中の変更 （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	機能	説明	参照先
リリース2.2(2e)	--	このガイドの内容が再編成されました。このガイドの以前のリリースではCisco APIC クラスタ コンテンツのハイアベイラビリティは「*Cisco APIC Getting* 開始ガイド、リリース *2.x*」に以降されています。	--
リリース2.2(1n)	APIC クラスタのハイアベイラビリティ	APIC クラスタのハイアベイラビリティ機能では、Active/Standby モードのクラスタでAPIC を操作できます。	このコンテンツは「*Cisco APIC* 開始、*2.x* のリリース」で確認できます。
リリース 1.3(1g)	このドキュメントのタイトルは変更されています。	以前の名前は、Cisco APIC ファームウェア管理ガイドでした。	



第 2 章

Cisco APIC イメージのインストールまたは回復

- 設置上の注意事項 （3 ページ）
- 使用上のガイドライン （5 ページ）
- 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 （7 ページ）
- PXE サーバを使用した Cisco APIC ソフトウェアのインストール （8 ページ）
- インストール Cisco APIC 仮想メディアを使用してソフトウェア （10 ページ）
- KVM コンソールで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 （10 ページ）
- 1 つのクリーン インストール Cisco APIC Debug CLI を使用して （12 ページ）
- Debug CLI を使用して Cisco APIC クラスタ全体に明確にインストールして Cisco ACI ファブリックを消去する （13 ページ）
- ステートフルにインストールする Cisco APIC Debug CLI を使用してクラスタ化 （14 ページ）

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 epg ファイルがパッケージに含まれます（下記のリリース表を参照してください）。

  acicobra-2.1_1*X*-py2.7.egg

  "*X*" is the letter of the release. 例：「2.1_1h」

（注） 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。

（注） 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。

表 *2:* リリース表

リリース バージョン	SDK epg ファイル名
リリース 3.2(1m)	acicobra-3.2_1m-py2.7.egg
リリース 3.1(2m)	acicobra-3.1_2m-py2.7.egg
リリース 3.1(1i)	acicobra-3.1_1i-py2.7.egg
リリース3.0(2h)	acicobra-3.0_2h-py2.7.egg
リリース3.0(1k)	acicobra-3.0_1k-py2.7.egg
リリース2.3(1e)	acicobra-2.3_1e-py2.7.egg
リリース2.2(2e)	acicobra-2.2_2e-py2.7.egg
リリース2.2(1n)	acicobra-2.2_1n-py2.7.egg
リリース2.1(1h)	acicobra-2.1_1h-py2.7.egg
リリース 2.0(2f)	acicobra-2.0_2f-py2.7.egg
リリース 2.0(1m)	acicobra-2.0_1m-py2.7.egg
リリース 1.3(2f)	acicobra-1.3_2f-py2.7.egg

リリース バージョン	SDK epg ファイル名
リリース 1.3(1i)	acicobra-1.3_1i-py2.7.egg
リリース1.3(1h)	acicobra-1.3_1h-py2.7.egg
リリース 1.3(1g)	acicobra-1.3_1g-py2.7.egg

以前のリリースについての詳細は、「Cisco Application Policy Infrastructure Controller (APIC) Release Notes」を参照してください。

使用上のガイドライン

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

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

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

- リーフおとびスパイン 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、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 基礎ガイドおよび KB を参照してください：ドメインの作成、エンティティ プロファイルの接続、特定のポートの EPG を展開する VLAN 記事。

（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 は独自のテナントのコントラクト インターフェイスにのみ関連付けられます。
- ユーザー 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 文字です
  - 最大文字数は 64 文字です
  - 連続して繰り返される文字は 3 文字未満です
  - 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
  - ユーザー名やユーザー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ー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 ドメインにユーザー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 グループは、最大 80 ノードを含める必要があります。
- 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 ファブリックに NTP サーバとしてリーフ スイッチを使用することをお勧めします。

CiscoAPICソフトウェアイメージの回復またはインストールの条件

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

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

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

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

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

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

- PXE サーバの使用
- 仮想メディアの使用

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

PXE サーバを使用した Cisco APIC ソフトウェアのインストール

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

手順

ステップ 1 次のように PXE サーバを設定します。

a) Linux の標準構成で PXE サーバを設定します。
b) ISO イメージをマウントします。

例：

```
$ mount -t iso9660 -o loop aci-apic-dk9.1.0.0.200v.iso myisomount
```

c) ファイルの内容を検査します。

例：

```
$ ls -n myisomount
…
drwxrwxr-x 6 76989 2000  4096 May 30 14:56 insieme
drwxrwxr-x 3 76989 2000  4096 May 30 14:56 images
…

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

d) PXE メニュー エントリ：<pxe-dir>/tftpboot/boot_msg

e) PXE メニュー エントリのイメージ：<pxe-dir>/tftpboot/pxelinux.cfg/default

例：

```
$ cat tftpboot/pxelinux.cfg/default
…
label 10
 kernel ifcimages/vmlinuz
 append initrd=ifcimages/initrd.img ks=http://172.21.157.10/kickstart/ifc-stable
ksdevice=eth0 loglevel=0 console=tty9
…

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

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。

f) キックスタート ファイルの追加：<pxe-dir>/kickstart/<mykickstartfile>

例：

```
$ cat kickstart/ifc-stable

# IFC Kickstart script for UCS C200
install
url --url=http://172.21.157.10/myisomount
lang en_US.UTF-8
keyboard us
network --onboot yes --device eth0 --bootproto dhcp --noipv6
network --onboot no --device eth1 --bootproto dhcp --noipv6
network --onboot no --device eth2 --bootproto dhcp --noipv6
network --onboot no --device eth3 --bootproto dhcp -noipv6
```

ステップ 2 Cisco APIC を再起動し、F12 キーを押してネットワークを起動します。

ステップ 3 PXE サーバで設定されたオプションを選択して、Cisco APIC イメージを起動します。

インストール Cisco APIC 仮想メディアを使用してソフトウェア

インストールまたはアップグレード、 Cisco APIC vMedia を使用してソフトウェアは、次の高度なプロセスが必要です。

- 取得、関連する Cisco APIC CCO から .iso イメージ。
- コントローラの Cisco 統合管理コントローラ (IMC) Web インターフェイスにアクセスします。

（注） IMC へのアクセスと、仮想メディアを管理の詳細については、対応するを参照してくださいの IMC 設定ガイド IMC 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。

- 統合管理コントローラ vMedia 機能を使用して、.iso イメージをマウントします。
- ブートまたは電源の再投入は、コントローラをします。
- 起動プロセス中を押して **F6** を選択、 **Cisco vKVM マッピング vDVD** ワンタイム ブートデバイスとして。BIOS パスワードを入力する必要があります。デフォルトのパスワードは「password」です。
- インストールする画面の指示に従って、 Cisco APIC ソフトウェア。

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

KVM コンソールで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

この手順を実行し、KVM コンソールで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またはアップグレードします。

手順

ステップ 1 Java セキュリティを更新します。

a) [Java] コントロール パネルを開きます。
b) **[セキュリティ]** タブで、**[高度なセキュリティ]** ラジオ ボタンをクリックします。
c) **[除外サイト リスト]** に IMC の IP アドレスを追加します。
d) [OK] をクリックします。

ステップ 2 IMC クレデンシャルを使用して Cisco Integrated Management Controller（IMC）にログインします。

IMC 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ります。

ステップ 3 KVM コンソールにアクセスします。

a) **[サーバ（Server）]** > **[概要（Summary）]** > **[KVM コンソールの起動（Launch KVM Console）]** の順に選択します。
b) **[Java Web Start ランチャ]** を使用してダウンロードしたファイルを開きます。
c) `C:/user/Program Files/Java/bin/`*`name of the java viewer`* にあるビューアにファイルをマップします。

（注） ダウンロード済みファイルの拡張子が `.jnlp` であることを確認します。

ステップ 4 Cisco APIC `.Iso` イメージをマップします。

a) Cisco.com から Cisco APIC `.iso` イメージをダウンロードします。
b) KVM コンソールで、**[仮想メディア]** > **[仮想デバイスの有効化]** を選択し、**[仮想メディア]** > **[CD/DVD のマップ]** を選択します。
c) **[参照]** をクリックして、Cisco APIC `.iso` イメージを選択します。
d) [Map Device] をクリックします。

ステップ 5 コントローラを起動し電源を再投入します。

a) IMC ページで、**[サーバ]** > **[サーバ サマリ]** > **[電源サイクル サーバ]** の順に選択します。
b) **[F6]** を押して起動デバイスを選択します。
c) 必要に応じて BIOS 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。
d) **[Cisco vKVM マッピング vDVD1.22]** を選択して、イメージをロードします。

このプロセスが完了した後、 Cisco APIC セットアップ スクリプトが表示されます。

e) 確認のため、**[KVM コンソール]** > **[ツール]** > **[統計情報]** を選択します。

ステップ 6 Cisco APIC コンソールで、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 など初期セットアップのオプションを入力します。

（注） Active-standby モードで Cisco APIC をセットアップする場合、クラスタのすべての Cisco APIC の Cisco APIC 情報は同じです。

1 つのクリーン インストール Cisco APIC Debug CLI を使用して

この手順を使用して 1 つのインストールを Cisco APIC ; 全体のクラスタはインストールされません。

手順

ステップ 1 使用停止、 Cisco APIC 、GUI または REST API を使用します。

ステップ 2 Root としてログイン、 Cisco APIC 。

ステップ 3 次の手順のいずれかの手順で使用するイメージを取得します。

a) リポジトリで既存のイメージを探します。

例：

```
root@apic1:~ > ls/firmware/fwrepos/fwrepo
```

b) 外部から自分のイメージにコピーする必要があります探しているイメージがすでに存在、リポジトリに存在しない場合、 Cisco APIC 。リポジトリに (/ファームウェア/fwrepos/fwrepo)、イメージをコピーする必要があることに注意してください。代わりに、/firmware にコピーします。

例：

```
root@apic1:~ > scp
<username>@<external-server-ip-address>:/<path-to-image>/firmware/</path-to-image>
</external-server-ip-address> </username>
```

ステップ 4 Statelessly コピーしたイメージをインストールします。

例：

```
/mgmt/support/insieme/installer.py フル
f/firmware/<image-name></image-name>
```

ステップ 5 追加するイメージを削除します。
rm-f/firmware<image-you-added></image-you-added>

ステップ 6 リブート。

例：

```
root@apic1:~ > 同期 && 再起動
```

ステップ 7 Recommission、 Cisco APIC GUI または REST API を使用します。

Debug CLI を使用して Cisco APIC クラスタ全体に明確にインストールして Cisco ACI ファブリックを消去する

手順

ステップ 1 設定をエクスポートします（設定のエクスポート）。

ステップ 2 Cisco APIC クラスタの各 Cisco APIC については、次の手順を実行します。

a) root としてログインします。

b) 次の手順のいずれかを完了して、使用するイメージを取得します。

- リポジトリで既存のイメージを検索します。

```
root@apic1:~>ls /firmware/fwrepos/fwrepo
```

- リポジトリの外部に固有のイメージをコピーします。

```
root@apic1:~> scp
<username>@<external-server-ip-address>:/<path-to-image>/firmware/
```

c) クリーン インストールを実行します。

例：

```
root@apic1:~>/mgmt/support/insieme/installer.py full -f /firmware/<image-name>
```

d) リブート。

例：

```
root@apic1:~> sync && reboot
```

ステップ 3 Cisco ACI ファブリックの各スイッチで、次の手順を実行します。

a) root としてログインします。

b) クリーン データのマーク

例：

```
root@apic1:~> touch/mnt/pss/.clean
```

c) リブート。

例：

```
root@apic1:~> vsh -c reload
```

ステップ 4 手順 1 でエクスポートした設定をインポートします。

ステートフルにインストールする Cisco APIC Debug CLI を使用してクラスタ化

クラスタ内の Cisco APIC ごとに、この手順を繰り返します。

手順

ステップ 1 Root としてログイン、 Cisco APIC 。

ステップ 2 次の手順のいずれかの手順で使用するイメージを取得します。

a) リポジトリで既存のイメージを探します。

例：

```
root@apic1:~>ls /firmware/fwrepos/fwrepo
```

b) リポジトリの外部独自のイメージをコピーします。

例：

```
root@apic1:~> scp <username>@<external-server-ip-address>:/<path-to-image>/firmware/
```

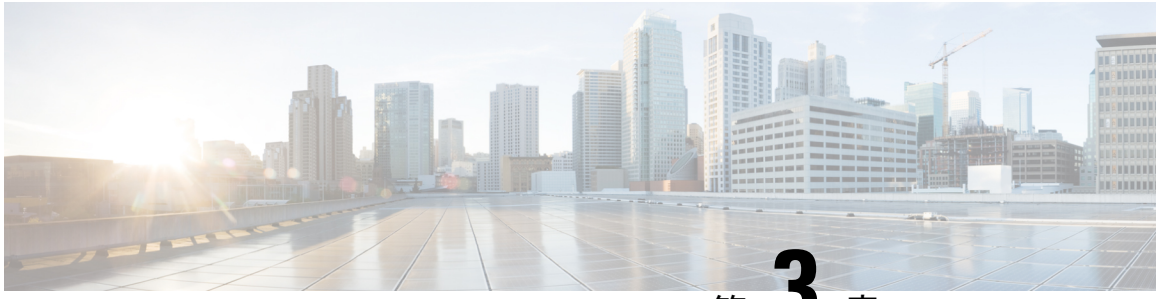
ステップ 3 ステートフルのインストールを実行、 Cisco APIC 。

例：

```
root@apic1:~>/mgmt/support/insieme/installer.py full -f /firmware/<image-name>
--dataconvertandreboot
```

ステップ 4 待機、 Cisco APIC 処理し、クラスタが収束するを再開します。

ステップ 5 次の手順を繰り返します Cisco APIC 。



第 3 章

Cisco APIC およびスイッチ ソフトウェアのアップグレードとダウングレード

- ファームウェア管理について （16 ページ）
- 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 （18 ページ）
- Cisco APIC およびスイッチ ソフトウェアのアップグレードについて （21 ページ）
- Cisco APIC およびスイッチ ソフトウェアのサポートされているアップグレード パス （23 ページ）
- Cisco APIC 長期リリース （73 ページ）
- Cisco APIC およびスイッチ ソフトウェアのダウングレードについて （74 ページ）
- ステートレス ダウングレード手順 （76 ページ）
- Cisco APIC およびスイッチ ソフトウェアのサポートされているダウングレード パス （76 ページ）
- スケジューラによるアップグレードについて （90 ページ）
- アップグレードする前に LLDP に接続を無効にする方法 （91 ページ）
- GUI を使用したソフトウェアのアップグレード （92 ページ）
- REST API を使用したソフトウェアのアップグレード （98 ページ）
- CLI による ソフトウェアのアップグレード （100 ページ）
- デバッグ CLI を使用したコントローラのアップグレード （104 ページ）
- 3 つの手順でデバッグ CLI を使用してコントローラをアップグレードする （104 ページ）
- 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 （104 ページ）
- SSD インストール ステータスの確認 （105 ページ）
- アップグレード プロセス中にフォールトのトラブルシューティング （105 ページ）
- 共有レイヤ 3 アウトでアップグレードする （112 ページ）
- 共有レイヤ 3 アウトでダウングレードする （114 ページ）
- ネットワーク設定機能と混合 OS 動作中の変更 （115 ページ）
- Cisco Nexus 9300 プラットフォーム スイッチから Cisco Nexus 9300 EX プラットフォーム スイッチへの移行 （119 ページ）
- アップグレードの例 （121 ページ）

ファームウェア管理について

このガイドで使用されている「ファームウェア」を指します、 Cisco APIC アプライアンス ファームウェアにアップグレードすることできますが、 Cisco APIC の GUI で、メニュー バーで **ADMIN > ファームウェア** とナビゲーション ペイン [にも **コントローラ ファームウェア** . この用語は、混同しないようにする必要があります、 Cisco APIC の CIMC、BIOS、LOM、および RAID コントローラ、および NIC/VIC PCI アダプタなどのコンポーネントのファームウェアです。

バージョン名称

次の情報は、ファームウェアを管理する必要があります。

- ファームウェア リポジトリ: ファームウェア リポジトリがアップグレードに必要なファームウェア イメージを保存する分散ストア Cisco ACI ファブリック。ファームウェア リポジトリは、クラスタ内のすべてのコントローラに同期されます。ファームウェア ソース ポリシーを設定した場合、ファームウェア イメージは、外部サーバ（HTTP または（SCP）からファームウェア リポジトリにダウンロードされます。リポジトリに保存可能なファームウェア イメージの 3 つの種類があります。
  - Cisco APICイメージ: このイメージは、Cisco Application Policy Infrastructure コントローラ上で実行されるソフトウェアで構成されています (Cisco APIC s)。
  - スイッチ イメージ: このイメージは、上で実行されるソフトウェア Cisco ACI スイッチ。
  - カタログ イメージ: このイメージは、Cisco によって作成された内部ポリシーで構成されています。これらの内部ポリシーには、ハードウェアの各モデルの機能、ソフトウェアの異なるバージョン間の互換性、およびハードウェアと診断テストに関する情報が含まれます。このイメージは、通常、バンドルし、コントローラのイメージとアップグレードします。特定のリリースのリリース ノートの指示具体的には、限り、管理者はカタログ イメージを個別にアップグレードする必要があることはありません。
- コントローラのファームウェアのポリシーおよびコントローラのメンテナンス ポリシー:、コントローラのファームウェアのポリシーがコントローラの適切なバージョンを指定します。コントローラのメンテナンス ポリシーでは、コントローラのアップグレードが開始する必要がありますを指定します。コントローラのファームウェア ポリシーとコントローラのメンテナンス ポリシー、クラスタ内のすべてのコントローラに適用されます。
- ファームウェア グループ、およびファームウェア ポリシー — A ファームウェア グループは、スイッチのグループのファームウェア ポリシーを設定します。ファームウェア ポリシーは、グループのスイッチでは、目的のファームウェアバージョンを指定します。
- メンテナンス グループおよびメンテナンス ポリシー — A メンテナンス グループは、スイッチのグループがでは、メンテナンス ポリシーを設定します。メンテナンス ポリシーは、アップグレードのスケジュールを指定します。

特記事項

- Application Policy Infrastructure Controller (Cisco APIC) の登場させアップグレードの-接続されている Cisco APIC リーフ スイッチがアップグレードされた 1 つずつを取得するなど、さまざまなメンテナンス グループに接続されているリーフ スイッチを配置する必要があります。
- 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。詳細については、「ファームウェアのアップグレード モード （17 ページ）」を参照してください。
- シリアル コンソール アクセスのアップグレードまたはスイッチのイーサネット、インバンド アクセスせぬダウン グレードするときにする必要があります。 またはアウトオブバンド アクセスは不要です。
- ファームウェアを使用してをアップロードすると、 Cisco APIC GUI の [転送時間が web トークンのタイムアウト値を超えると、web トークンがタイムアウトし、アップロードが失敗します。ファームウェアを使用して、アップロードする前に、Cisco APIC GUI、予想されるアップロード時刻よりも後の時刻に web トークンのタイムアウト値を大きく必要があります。

ファームウェアのアップグレード モード

Cisco APIC を使用してファームウェアをアップグレードするには、2 つのモードがあります。

Cisco APIC GUI で、**[管理]** > **[ファームウェア]** > **[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]** に移動してファームウェアをアップグレードできます。メンテナンス グループを選択し、[アクション] メニューから **[ワンタイム ウィンドウ トリガの作成]** または **[定期的なウィンドウ トリガの作成]** を選択して、アップグレードをスケジュール設定します。

- すぐにアップグレード：このモードでは、ファームウェアのアップグレードプロセスを即時に開始します。
- アップグレードのスケジュール：このモードでは、後の日時にファームウェアのアップグレードをスケジュールすることができます。アップグレードのスケジュール設定するには、次のパラメータを指定してください。
  - **名前** ：名前を指定します。
  - **日付** ：アップグレードを開始する日時を指定します。
  - **最大同時ノード** ：同時にアップグレードするノードを指定します。Cisco APIC のデフォルト値は 1 です。スイッチのデフォルト値は 20 です。
  - **最長実行時間**：アップグレードの期間ウィンドウを指定します。デフォルト値は *[*無制限*]* です。

ファームウェアのアップグレードをスケジュール設定するときに、次のシナリオが発生する可能性があります。

- シナリオ 1：**[最長実行時間]** が設定され、**[日付]** が現在の日付と時刻より後に設定されています。このシナリオでは、アップグレードはスケジュール設定された開始日に開始されます。
- シナリオ 2：**[最長実行時間]** が設定されていないと、**[日付]** が現在の日付と時刻より後に設定されます。このシナリオでは、アップグレードはスケジュール設定された開始日に開始されます。
- シナリオ3：アップグレードが現在の日付と時刻より前の **[日付]** に設定されており、**[最長実行時間]** も現在の時刻よりも前に設定されています。このシナリオでは、アップグレードは開始されません。
- シナリオ 4：アップグレードが現在の日付と時刻より前の **[日付]** にスケジュール設定されており、**[最長実行時間]** も現在の時刻より後の時刻に設定されています。このシナリオでは、アップグレードがすぐに開始されます。
- シナリオ 5：アップグレーが現在の日付と時刻よりも前の **[日付]** にスケジュール設定されており、**[最長実行時間]** が設定されていません。このシナリオでは、アップグレードがすぐに開始されます。

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

高レベルは、アップグレードまたはダウン グレードする手順は Cisco ACI ファブリックは、次のとおり。

- プロシージャまたはの手順を実行、アップグレードし、特定のリリースのリリース ノートに限りは、同じのダウン グレードします。
- 必要な必要な CIMC バージョンがあることを確認 Cisco APIC アップグレードします。参照してください、 Cisco APIC のリリース ノート のサポートされている CIMC バージョン。
- Cisco ACI コントローラ イメージ（Cisco APIC イメージ）をリポジトリにダウンロードします。
- リポジトリに Cisco ACI スイッチ イメージをダウンロードします。
- Application Policy Infrastructure コントローラのクラスタのアップグレード (Cisco APIC s)。
- ファブリックが動作していることを確認します。
- スイッチを複数のグループに分割します。たとえば、2 つのグループ – 赤色と青色に分割します。
- 赤のグループのスイッチをアップグレードします。
- ファブリックが動作していることを確認します。

- 青のグループのスイッチをアップグレードします。
- ファブリックが動作していることを確認します。

（注） 場合、 Cisco ACI ファブリックの導入環境に Cisco AV が含まれて、Cisco AV との互換性のバージョンにアップグレードする Cisco APIC 。Cisco AV をアップグレードするには、セクションを参照してください。 **のアップグレード シーケンスの推奨 Cisco APIC 、ファブリックのスイッチと Cisco AV** で、 Cisco Application Virtual Switch Installation guide』 。

ガイドライン

また、一部の一般的なガイドラインを次のとおりですす Cisco ACI ファブリック アップグレードまたはダウン グレード。

- スイッチを 2 つまたは複数のグループに分割します。一度に 1 つの グループをアップグレードします。その方法、アップグレードの] ウィンドウの中にまったくファブリック帯域幅をしない失われます。
- 無効にされた設定ゾーンに属するノードは、アップグレードまたはダウングレードしないでください。
- 特定のリリースのリリース ノートで指定しない限り、アップグレード(したり、ダウン グレード)コントローラのスイッチの前に、その逆(コントローラの前にスイッチ)できます。
- **特定のリリースでは、またはのリリースの組み合わせは、いくつかの制限およびアップグレードまたはダウン グレード手順の推奨事項があります。見直し、リリース ノートがリリースにアップグレードまたはダウン グレードする前に、 Cisco ACI ファブリック。If no such limitations or recommendations are specified in the release notes, the steps mentioned above should be followed to upgrade or downgrade your Cisco ACI fabric.**
- 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、前に、ファブリックに何らかの調査および解決済みの必要があります。未使用または未完了の設定を含めることがありますアップグレードは影響しません無害の障害がファブリックの可能性があります。アップグレードまたはダウン グレード操作の前にすべての障害を評価する必要があります。ディスク使用率は関連の障害は、設備新しいソフトウェアを開梱中に問題が発生することができます、アップグレードする前に対処する必要があります。
- アップグレードまたはダウン グレード操作をトリガーする前にする必要がファブリックがで構成されている、 **十分に適合** 状態。すべて Cisco APIC s にあります **十分に適合** 間を移動する前に状態 Cisco APIC イメージ バージョンのスイッチを開始する前にアップグレードまたはダウン グレードします。アップグレードまたはコントローラに追加されていない中にダウン グレード コントローラまたはスイッチを開始する **十分に適合** 動作状態が予期しない結果につながることができます。

  複数のバージョンのアップグレードまたはダウン グレード操作を実行するときに、ファブリックがあることを確認する必要があります、 **十分に適合** 状態。たとえば、A から B へのアップグレード後に、バージョン A、C に B をからアップグレードするかどうかを待つ

必要がありますすべてのコントローラとスイッチでは、 **十分に適合** およびCにBのバージョンからアップグレードを開始する前にバージョン B の動作の状態

- アップグレードまたはダウン グレード ファブリックする前に構成のバックアップを収集することをお勧めします。

（注） 2つまたは複数のグループのアップグレードまたはダウン グレードをスイッチに分割することをお勧めします。2 つのグループ、および 4 つのグループにスイッチを得られると、それぞれの例を次にします。

Two-group method:

1. 2つのグループに、スイッチを分割:赤いグループと青色グループ。赤色のグループと青のグループにその他の半分で、スパイン スイッチの半分いずれかを配置します。赤色のグループと青のグループにその他の半分でも、リーフ スイッチの半分いずれかを配置します。
2. 赤色のグループをアップグレードします。
3. 赤のグループのアップグレードが完了した後は、ファブリックが正常な状態を確認します。
4. 青色のグループをアップグレードします。

Four-group method:

1. 4 つのグループをスイッチに分割: 赤いスパイン スイッチ グループ、青色スパイン スイッチ グループ、赤色のリーフ スイッチ グループ、および青色リーフ スイッチ グループ。いずれかを配置赤色スパイン スイッチでスパイン スイッチの半分グループ、およびその他の半分スパイン スイッチの青色スパイン スイッチのグループにします。次に、赤色のリーフ スイッチ グループ、および青のリーフ スイッチのグループ内の他の半半のリーフ スイッチを配置します。
2. 赤のリーフ スイッチのグループをアップグレードします。
3. 赤のリーフ スイッチのグループのアップグレードが完了した後は、ファブリックが正常な状態を確認します。
4. 青のリーフ スイッチのグループをアップグレードします。
5. 青のリーフ スイッチのグループのアップグレードが完了した後は、ファブリックが正常な状態を確認します。
6. 赤のスパイン スイッチのグループをアップグレードします。
7. 赤のスパイン スイッチのグループのアップグレードが完了した後は、ファブリックが正常な状態を確認します。

8. 青のスパイン スイッチのグループをアップグレードします。

Cisco APIC およびスイッチ ソフトウェアのアップグレードについて

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。

特記事項

- Cisco APIC リリース 1.2(2) 以降では、アウトオブバンド管理ノード EPG でコントラクトが提供されると、アウトオブバンド ノード管理アドレスで設定されるローカル サブネットが、デフォルトの Cisco APIC アウトオブバンド コントラクト送信元アドレスになります。以前は、任意のアドレスをデフォルトの Cisco APIC アウトオブバンド コントラクト送信元アドレスにすることが可能でした。
- アップグレードの前に、適切に設定された OOB EPG の下で契約が行われることを確認します。1.2(2) リリースにアップグレードするとき、アウトオブバンド ノード管理エンドポイント グループに適用されるデフォルト以外のアウトオブ バンド契約は、Cisco APIC に対して予期しない接続の問題が発生する可能性があります。Cisco APIC リリース以前には影響がない誤って設定されているアウトオブ バンド契約が存在する場合、1.2(2) リリースにアップグレードすると、そのような誤った設定のアウトオブバンド契約を使用するアウト オブ バンド管理 EPG により、Cisco APIC のクラスタへアクセスできなくなる可能性があります。
- 最低でも /19 のサブネット マスクを推奨します。
- アップグレードのリリース制限事項
  - Cisco APIC リリース 1.3 への直接アップグレードに必要な最小バージョンは 1.1 です。
  - Cisco APIC リリース 2.0 への直接アップグレードに必要な最小バージョンは 1.2(3) です
  - Cisco APIC リリース 2.1 への直接アップグレードに必要な最小バージョンは 1.2(3) です
  - Cisco APIC リリース 2.2 への直接アップグレードに必要な最小バージョンは 2.0(2) です
  - Cisco APIC リリース 2.3 への直接アップグレードに必要な最小バージョンは 2.1(1) です
  - Cisco APIC リリース 3.0 への直接アップグレードに必要な最小バージョンは 2.2(1) です
  - Cisco APIC リリース 3.1(1) への直接アップグレードに必要な最小バージョンは 2.2(2) です

- Cisco APIC リリース 3.1(2) への直接アップグレードに必要な最小バージョンは 2.2(3) です
- Cisco APIC リリース 3.2(1) への直接アップグレードに必要な最小バージョンは 2.2(2) です

（注） Cisco APIC リリース 1.x から Cisco APIC リリース 2.x にアップグレードするとき、すべての Cisco APIC は同時にリロードされます。

- Cisco ACI マルチポッド導入には、PIM BIDIR 範囲としてポッド内ネットワークで設定されている 239.255.255.240 システム GIP が必要です。IPN デバイスのこの 239.255.255.240 PIM BIDIR 範囲の設定は、**システム GIPo として GIPo インフラ** 機能を使用して回避できます。**システム GIPo として GIPo インフラ** 機能は、リーフ スイッチやスパイン スイッチを含む Cisco ACI ファブリックのすべてのスイッチを、最新の Cisco APIC リリースにアップグレードした後でのみ有効にする必要があります。
- 2.2(1) 以降のリリースから、 Cisco APIC には SSD 1 および 2 HDD が必須となり、このリリースにアップグレードする前に両方の RAID ボリュームが正常な状態になっている必要があります。
- 2.2(1) リリースから、Cisco APIC には SSD のインストールが必須です。SSD は Cisco APIC の起動にひつようであり、Cisco APIC は SSD がインストールされていない場合は起動しません。SSD インストール ステータスの確認 （105 ページ）を参照してください。
- Cisco APIC リリース 3.0 (1) から、スイッチのアップグレードがトリガーされると Cisco APIC アップグレード中、すべての Cisco APIC が正常にアップグレードされた後でスイッチがアップグレードされます。Cisco APIC アップグレード プロセス中、スイッチは **IN キュー** 状態になります。
- マルチ ステップのアップグレードを実行中は、サポートされている場合 Cisco APIC リリース 2.1 かそれ以降の中間バージョンを使用して、「CSCvb94260」に関連する問題を防止することをお勧めします。
- Apic では、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。「互換性チェックを無視」の設定がありますが、デフォルトでは **[オフ]** に設定されているため、デフォルトで可能なアップグレードの互換性をシステムが自動チェックします。いずれかの理由で互換性チェック機能が無効になるように、「互換性チェックを無視」設定を **[オン]** に変更する場合は、変更、互換性を無視する設定を確認 （97 ページ） の手順に従います。

次の表では、Cisco APIC をアップグレードする際に従う必要がある、サポートされているアップグレードパスを一覧にしています。目的のアップグレード元または**アップグレード先**パスが表に記載されていない場合は、初めにサポート対象の中間バージョンにアップグレードしたう

えで、サポート対象の最終バージョンにアップグレードする必要があります。同じアップグレード パスが、スイッチ ソフトウェアにも同様に適用されます。

Cisco APIC およびスイッチ ソフトウェアのサポートされているアップグレード パス

表 *3 : Cisco APIC* でサポートされるアップグレード パス

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.1(2)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、 2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.1(1)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、 2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.1(1)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.0(2)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.0(2)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.0(2)	Cisco APIC 3.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.0(1)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.0(1)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.0(1)	Cisco APIC 3.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 3.0(1)	Cisco APIC 3.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.3(1)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題がある場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザー ログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.3(1)	Cisco APIC 3.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、 2 個以上のメンテナンスグループを使用してスイッチをアップグレードします。
APIC 2.3(1)	APIC 3.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. Cisco APIC をアップグレードします。 2. Cisco APIC が正常にアップグレードされた後、 2 個以上のメンテナンスグループを使用してスイッチをアップグレードします。
Cisco APIC 2.3(1)	Cisco APIC 3.0(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(4)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(4)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(3)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(3)	Cisco APIC 3.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(3)	Cisco APIC 3.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(3)	Cisco APIC 3.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(3)	Cisco APIC 2.3(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(3)	Cisco APIC 2.2(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(2)	Cisco APIC 3.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(2)	Cisco APIC 3.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(2)	Cisco APIC 3.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(2)	Cisco APIC 3.0(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(2)	Cisco APIC 2.3(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(2)	Cisco APIC 2.2(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(2)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(1)	Cisco APIC 3.0(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(1)	Cisco APIC 2.3(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.2(1)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(1)	Cisco APIC 2.2(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(4)	Cisco APIC 2.2(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(3)	Cisco APIC 2.2(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。 このアップグレードは公式にはサポートされていますが、互換性チェック機能が公式にサポートされているアップグレードパスとして認識しない既知の問題があります。変更、互換性を無視する設定を確認 （97 ページ） の手順に従い、[互換性チェックを無視] 機能を一時的に有効にすることで、システムはこの特定のアップグレードの互換性をチェックしません。 この特定のアップグレードが完了した後に、[互換性チェックを無視] 機能に戻り無効にすることで、今後のアップグレードの互換性をシステムがチェックします。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(3)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。 このアップグレードは公式にはサポートされていますが、互換性チェック機能が公式にサポートされているアップグレードパスとして認識しない既知の問題があります。変更、互換性を無視する設定を確認 （97 ページ） の手順に従い、[互換性チェックを無視] 機能を一時的に有効にすることで、システムはこの特定のアップグレードの互換性をチェックしません。 この特定のアップグレードが完了した後に、[互換性チェックを無視] 機能に戻り無効にすることで、今後のアップグレードの互換性をシステムがチェックします。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(3)	Cisco APIC 2.1(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。 このアップグレードは公式にはサポートされていますが、互換性チェック機能が公式にサポートされているアップグレードパスとして認識しない既知の問題があります。変更、互換性を無視する設定を確認 （97 ページ） の手順に従い、[互換性チェックを無視] 機能を一時的に有効にすることで、システムはこの特定のアップグレードの互換性をチェックしません。 この特定のアップグレードが完了した後に、[互換性チェックを無視] 機能に戻り無効にすることで、今後のアップグレードの互換性をシステムがチェックします。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(2)	Cisco APIC 2.3(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(2)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(2)	Cisco APIC 2.2(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(2)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(1)	Cisco APIC 2.3(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(1)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(1)	Cisco APIC 2.2(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(1)	Cisco APIC 2.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.1(1)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(1)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(2)	Cisco APIC 2.2(4)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(2)	Cisco APIC 2.2(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.0(2)	Cisco APIC 2.2(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(2)	Cisco APIC 2.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(2)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.0(2)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(2)	Cisco APIC 2.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(1)	Cisco APIC 2.2(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.0(1)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(1)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 2.0(1)	Cisco APIC 2.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.0(1)	Cisco APIC 2.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 （注） 複数の手順があるアップグレードを実行する際、サポートされている場合 APIC リリース 2.1 の即時バージョンまたはそれ以降を使用し、CSCvb94260 に関連する問題を防止することを推奨します。
Cisco APIC 1.3(2)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(2)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.3(2)	Cisco APIC 2.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.3(2)	Cisco APIC 2.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(2)	Cisco APIC 2.0(1)		1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
		Cisco ACI に連携する Microsoft サーバは、APIC を 2.0(1) リリースにアップグレードする前に、KB2919355 と KB3000850 更新ロールアップを更新する必要があります。KB2919355 更新ロールアップには 2929781 パッチを含み、新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 の暗号スイート優先順位を変更します。 次の Microsoft サーバにパッチを適用する必要があります: • Microsoft Windows Azure パック リソース プロバイダ サーバ • Microsoft Windows Azure パック テナント サイト サーバ • Microsoft Windows Azure パック管理サイト サーバ • Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ • Microsoft System Center 2012 R2 サーバ • Microsoft HyperV	

遷移元	目的	制限事項	推奨される手順
		2012 R2 サーバ	
Cisco APIC 1.3(1)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.3(1)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.3(1)	Cisco APIC 2.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(1)	Cisco APIC 2.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 （注） 複数の手順があるアップグレードを実行する際、サポートされている場合 APIC リリース 2.1 の即時バージョンまたはそれ以降を使用し、CSCvb94260 に関連する問題を防止することを推奨します。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(1)	Cisco APIC 2.0(1)		1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 （注） 複数の手順があるアップグレードを実行する際、サポートされている場合 APIC リリース 2.1 の即時バージョンまたはそれ以降を使用し、CSCvb94260 に関連する問題を防止することを推奨します。

遷移元	目的	制限事項	推奨される手順
		Cisco ACI に連携する Microsoft サーバは、APIC を 2.0(1) リリースにアップグレードする前に、KB2919355 と KB3000850 更新ロールアップを更新する必要があります。KB2919355 更新ロールアップには 2929781 パッチを含み、新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 の暗号スイート優先順位を変更します。 次の Microsoft サーバにパッチを適用する必要があります: • Microsoft Windows Azure パック リソース プロバイダ サーバ • Microsoft Windows Azure パック テナント サイト サーバ • Microsoft Windows Azure パック管理サイト サーバ • Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ • Microsoft System Center 2012 R2 サーバ • Microsoft HyperV	

遷移元	目的	制限事項	推奨される手順
		2012 R2 サーバ	
Cisco APIC 1.2(3)	Cisco APIC 2.1(3)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(3)	Cisco APIC 2.1(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(3)	Cisco APIC 2.1(1)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(3)	Cisco APIC 2.0(2)	Cisco APIC のクラスタがアップグレードされる際、接続の問題が存在する場合 Cisco APIC クラスタが珍しいステータスになる可能性があります。この状況では、Cisco APIC の大半がアップグレードを完了しクラスタが少数になるまで、ユーザーログインは失敗します。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 （注） 複数の手順があるアップグレードを実行する際、サポートされている場合 APIC リリース 2.1 の即時バージョンまたはそれ以降を使用し、CSCvb94260 に関連する問題を防止することを推奨します。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(3)	Cisco APIC 2.0(1)		1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 （注） 複数の手順があるアップグレードを実行する際、サポートされている場合 APIC リリース 2.1 の即時バージョンまたはそれ以降を使用し、CSCvb94260 に関連する問題を防止することを推奨します。

遷移元	目的	制限事項	推奨される手順
		Cisco ACI に連携する Microsoft サーバは、APIC を 2.0(1) リリースにアップグレードする前に、KB2919355 と KB3000850 更新ロールアップを更新する必要があります。KB2919355 更新ロールアップには 2929781 パッチを含み、新しい TLS 暗号スイートを追加し、Windows 8.1 および Windows サーバ 2012 R2 の暗号スイート優先順位を変更します。 次の Microsoft サーバにパッチを適用する必要があります: • Microsoft Windows Azure パック リソース プロバイダ サーバ • Microsoft Windows Azure パック テナント サイト サーバ • Microsoft Windows Azure パック管理サイト サーバ • Microsoft System Center のサービス プロバイダの基盤/オーケストレーション サーバ • Microsoft System Center 2012 R2 サーバ • Microsoft HyperV	

遷移元	目的	制限事項	推奨される手順
		2012 R2 サーバ	
Cisco APIC 1.2(2)	Cisco APIC 2.0(2)	1,2(2) リリースから 2.0(2) リリースに直接アップグレードすることはできません。 1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(2) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。
Cisco APIC 1.2(2)	Cisco APIC 2.0(1)	1,2(2) リリースから 2.0(1) リリースに直接アップグレードすることはできません。 1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(1) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。
Cisco APIC 1.2(2)	Cisco APIC 1.3(2)	TEP サブネットマスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	**1.** APIC をアップグレードします。 **2.** APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(2)	Cisco APIC 1.3(1)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(2)	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(1)	Cisco APIC 2.0(2)	1,2(1) リリースから 2.0(2) リリースに直接アップグレードすることはできません。1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(2) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(1)	Cisco APIC 2.0(1)	1,2(1) リリースから 2.0(1) リリースに直接アップグレードすることはできません。1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(1) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。
Cisco APIC 1.2(1)	Cisco APIC 1.3(2)	TEP サブネットマスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(1)	Cisco APIC 1.3(1)	TEP サブネットマスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.2(1)	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(1)	Cisco APIC 1.2(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(4)	Cisco APIC 2.0(2)	1,1(4) リリースから 2.0(2) リリースに直接アップグレードすることはできません。 1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(2) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。
Cisco APIC 1.1(4)	Cisco APIC 2.0(1)	1,1(4) リリースから 2.0(1) リリースに直接アップグレードすることはできません。 1.2(3) リリースまたは 1.3 リリースのいずれかに最初にアップグレードして、それから 2.0(1) リリースにアップグレードする必要があります。	選択したパスの適切なアップグレード手順を参照してください。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(4)	Cisco APIC 1.3(2)	TEP サブネットマスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。 Bug CSCux40954 、1.2(1) のリリースで解決されたが、Cisco APIC ファームウェアの処理を使用して、**アップロード** GUI から、ボタンが機能しません。アップロードが正常に完了したように見えますが、ファームウェアはリポジトリで更新されていません。代わりに、サーバから APIC に SCP または HTTP を使用してイメージをダウンロードする必要があります。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(4)	Cisco APIC 1.3(1)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。 Bug CSCux40954 、1.2(1) のリリースで解決されたが、Cisco APIC ファームウェアの処理を使用して、**アップロード** GUI から、ボタンが機能しません。アップロードが正常に完了したように見えますが、ファームウェアはリポジトリで更新されていません。代わりに、サーバから APIC に SCP または HTTP を使用してイメージをダウンロードする必要があります。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(4)	Cisco APIC 1.2(3)	Bug CSCux40954 、1.2(1) のリリースで解決されたが、Cisco APIC ファームウェアの処理を使用して、**アップロード** GUI から、ボタンが機能しません。アップロードが正常に完了したように見えますが、ファームウェアはリポジトリで更新されていません。代わりに、サーバから APIC に SCP または HTTP を使用してイメージをダウンロードする必要があります。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(4)	Cisco APIC 1.2(2)	Bug CSCux40954 、1.2(1) リリースで解決されましたが、Cisco APIC ファームウェアの処理を使用して、**アップロード** GUI から、ボタンが機能しません。アップロードが正常に完了したように見えますが、ファームウェアはリポジトリで更新されていません。代わりに、サーバから APIC に SCP または HTTP を使用してイメージをダウンロードする必要があります。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(4)	Cisco APIC 1.2(1)	Bug CSCux40954 、1.2(1) リリースで解決されましたが、Cisco APIC ファームウェアの処理を使用して、**アップロード** GUI から、ボタンが機能しません。アップロードが正常に完了したように見えますが、ファームウェアはリポジトリで更新されていません。代わりに、サーバから APIC に SCP または HTTP を使用してイメージをダウンロードする必要があります。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 レイヤ 3 アウトでアップグレードには、共有レイヤ 3 アウトでアップグレードする （112 ページ） を参照してください。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(3)	Cisco APIC 1.3(2)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(3)	Cisco APIC 1.3(1)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(3)	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(3)	Cisco APIC 1.2(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(3)	Cisco APIC 1.2(1)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 レイヤ 3 アウトでアップグレードには、共有レイヤ 3 アウトでアップグレードする （112 ページ） を参照してください。
Cisco APIC 1.1(3)	Cisco APIC 1.1(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(2)	Cisco APIC 1.3(2)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(2)	Cisco APIC 1.3(1)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(2)	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(2)	Cisco APIC 1.2(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(2)	Cisco APIC 1.2(1)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 レイヤ 3 アウトでアップグレードには、共有レイヤ 3 アウトでアップグレードする （112 ページ） を参照してください。
Cisco APIC 1.1(2)	Cisco APIC 1.1(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(2)	Cisco APIC 1.1(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(1)	Cisco APIC 1.3(2)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(1)	Cisco APIC 1.3(1)	TEP サブネット マスクは、/8 ～ /22 の範囲である必要があります。推奨される最小マスクで /19 です。	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(1)	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(1)	Cisco APIC 1.2(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(1)	Cisco APIC 1.2(1)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 レイヤ 3 アウトでアップグレードには、共有レイヤ 3 アウトでアップグレードする （112 ページ） を参照してください。
Cisco APIC 1.1(1)	Cisco APIC 1.1(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.1(1)	Cisco APIC 1.1(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(1)	Cisco APIC 1.1(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(4Q) 以降	Cisco APIC 1.2(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(4q) 以降	Cisco APIC 1.2(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.0(4o) 以降	Cisco APIC 1.2(1k)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。 レイヤ 3 アウトでアップグレードには、共有レイヤ 3 アウトでアップグレードする （112 ページ） を参照してください。
Cisco APIC 1.0(4)	Cisco APIC 1.1(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(4)	Cisco APIC 1.1(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.0(4)	Cisco APIC 1.1(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(4)	Cisco APIC 1.1(1)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(3)	Cisco APIC 1.1(2)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(3)	Cisco APIC 1.1(1)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.0(3)	Cisco APIC 1.0(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(2)	Cisco APIC 1.0(4)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。
Cisco APIC 1.0(2)	Cisco APIC 1.0(3)	なし	1. APIC をアップグレードします。 2. APIC が正常にアップグレードされた後、2 個以上のメンテナンス グループを使用してスイッチをアップグレードします。

Cisco APIC 長期リリース

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

（注） 一部のリリースは、他のユーザはサポートされない可能性があります中に、長命リリースとしてサポート可能性があります。たとえば、ある可能性があります 3 2 。*x* リリース: 2.1、2.2、および 2.3。ただし、3.2 リリースでは、次の 3 つの 2 のいずれかに直接アップグレード パスで長命リリースの 。*x* リリースもサポートする長命リリース (2.2) として、他の 2 つのリリース (2.1 と 2.3) がサポートされていない可能性があります中に長命リリースとして。

長命リリースのライフ サイクル

- 長命のメジャー リリースのライフ サイクルは、マイナーの最初のリリースの first customer shipment（FCS; から始まります。
- メジャー リリースのは、製品の障害に対処する利用可能な行ったは複数のリリース、メンテナンス リリースの概要フェーズを開始します。
- 、その後で、メジャー リリースはが成熟メンテナンス フェーズに移行します。このフェーズでは、リリースは、重大度 1 および 2 の重大度の欠陥が、顧客が見つかりませんでしたのみの不具合修復を受け取ります。内部で発見された不具合で個別に対処します。
- すべての長命リリース サポートへのアップグレードまたはダウン グレード長命次または前のリリースの最後のメンテナンス バージョンをそれぞれ

Cisco では、新規または既存の Cisco Nexus 9000 ACI モードのスイッチと Application Policy Infrastructure Controller (APIC) の導入でお客様が次の長命リリースから選択することを推奨します。

表 *4 : Cisco APIC* 長期リリース

Cisco APIC リリース バージョン	Cisco APIC の長期リリース バージョン	長命の Cisco スイッチのリリース バージョン
3.2(1)	2.2(4)	12.2(4)

Cisco APIC およびスイッチ ソフトウェアのダウングレードについて

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。

特記事項

- Cisco APIC およびスイッチ ソフトウェアをダウングレードする場合、次の注意事項と制限事項が適用されます。

- インポートされた設定が、希望のバージョン設定が 1.0(1x) に設定されているファームウェア ポリシーで構成されている場合、スイッチは1.0(1x)バージョンにダウンロード可能です。
- 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F1371の policy-deployment-failed のような障害が発生します。
- 内部 EPG 拒否設定が設定された Cisco APIC を、1.2(2) リリースからそれ以前のリリースにダウングレードすることはサポートされていません。内部 EPG 拒否設定は、ダウングレードする前に手動で削除する必要があります。
- Cisco APIC ソフトウェアのダウングレードを行う際は、最初に Federal Information Processing Standards（FIPS）を無効にする必要があります。詳細は、「*Cisco APIC and Federal Information Processing Standards (FIPS)*」の資料を参照してください。

- Cisco APIC 1.2(1x) から 1.0(4q) 以前にダウングレードする、または 1.1(1x)、1.1(2x)、1.1(3x)、1.1(4x) から 1.0(4h) 以前にダウン グレードする場合、下記のステートレス ダウングレード手順に従ってください。この手順はファブリックを再構築するため、ファブリック停止を計画する必要があります。
- Cisco APIC 3.0(1) 以前のリリースにダウングレードする前に、Cisco N9K-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。
- 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以前のリリースダウン グレードする際、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 。
- Cisco ACI ファブリックで Federal Information Processing Standards（FIPS）を有効または無効にしている場合、変更を有効にするためファブリック内のスイッチをそれぞれリロードする必要があります。FIPS設定を変更した後に最初のリロードを発行すると、設定されているスケールプロファイル設定が失われます。スイッチは動作状態ですが、デフォルトのポート スケール プロファイルを使用します。FIPS 設定が変更されていない場合は、この問題は後続のリロードでは発生しません。FIPS は Cisco NX-OS リリース 13.1(1) またはそれ以降でさぽーとされています。

  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。

ステートレス ダウングレード手順

手順

ステップ 1 ファブリック設定をエクスポートします。

ステップ 2 Cisco APIC で **eraseconfig** コマンドを実行します。これで、コントローラが再起動されます。コントローラがステップ 3 移動する前にリブートされていることを確認します。

ステップ 3 ファブリックを再検索します。

ステップ 4 目的のリリースにファブリックのダウン グレードします。

ステップ 5 Cisco APIC で **eraseconfig setup** コマンドを実行します。この手順は、使用中のバージョンで必要になる可能性がある追加のコマンドをスクリプトから実行できるようにするために必要です。**eraseconfig setup** コマンドによって Cisco APIC がリロードされます。

ステップ 6 実行、 `セットアップ clean config.sh` スイッチのノードでスクリプトを作成し、それらをリロードします。

ステップ 7 Initial setup(初期セットアップ、初期設定) スクリプトを実行します、 Cisco APIC s。

ステップ 8 ファブリックをインポート「マージ」モードを使用して設定をインポートします。

Cisco APIC およびスイッチ ソフトウェアのサポートされているダウングレード パス

次の表では、Cisco APIC をダウングレードするときに従う必要があるサポートされているダウングレード パスを一覧にしています。

表 *5 : Cisco APIC* ソフトウェアのサポートされているダウングレード パス

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.2(1)	• Cisco APIC 3.1(2) • Cisco APIC 3.1(1) • Cisco APIC 3.0(2) • Cisco APIC 3.0(1) • Cisco APIC 2.2(4) • Cisco APIC 2.2(3) • Cisco APIC 2.2(2)	スイッチ モデル N9K-X9736C-FX、N9K C9508 FM E2、N9K-C9348GC-FXP および N9K C9364C がある場合、Cisco APIC 3.0 (1) 以前のバージョンにはダウングレードしないでください。これらのモデルは Cisco APIC 3.0 (1) 以前のバージョンではサポートされていません。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 3.1(2)	• Cisco APIC 3.1(1) • Cisco APIC 3.0(2) • Cisco APIC 3.0(1) • Cisco APIC 2.3(1) • Cisco APIC 2.2(4) • Cisco APIC 2.2(3)	スイッチ モデル N9K-X9736C-FX、N9K C9508 FM E2、N9K-C9348GC-FXP および N9K C9364C がある場合、Cisco APIC 3.0 (1) 以前のバージョンにはダウングレードしないでください。これらのモデルは Cisco APIC 3.0 (1) 以前のバージョンではサポートされていません。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 3.1(1)	• Cisco APIC 3.0(2) • Cisco APIC 3.0(1) • Cisco APIC 2.3(1) • Cisco APIC 2.2(3) • Cisco APIC 2.2(2)	スイッチ モデル N9K-X9736C-FX、N9K C9508 FM E2、N9K-C9348GC-FXP および N9K C9364C がある場合、Cisco APIC 3.0 (1) 以前のバージョンにはダウングレードしないでください。これらのモデルは Cisco APIC 3.0 (1) 以前のバージョンではサポートされていません。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 3.0(2)	• Cisco APIC 2.2(2) • Cisco APIC 2.2(3) • Cisco APIC 2.3(1) • Cisco APIC 3.0(1)	スイッチ モデル N9K-X9736C-FX、N9K C9508 FM E2、N9K-C9348GC-FXP および N9K C9364C がある場合、Cisco APIC 3.0 (1) 以前のバージョンにはダウングレードしないでください。これらのモデルは Cisco APIC 3.0 (1) 以前のバージョンではサポートされていません。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 3.0(1)	• Cisco APIC 2.2(1) • Cisco APIC 2.2(2) • Cisco APIC 2.3(1)	スイッチ モデル N9K-X9736C-FX、N9K C9508 FM E2、N9K-C9348GC-FXP および N9K C9364C がある場合、Cisco APIC 3.0 (1) 以前のバージョンにはダウングレードしないでください。これらのモデルは Cisco APIC 3.0 (1) 以前のバージョンではサポートされていません。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 2.3(1)	• Cisco APIC 2.1(1) • Cisco APIC 2.1(2) • Cisco APIC 2.2(1) • Cisco APIC 2.2(2) • Cisco APIC 2.2(3)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(4)	• Cisco APIC 2.0(2) • Cisco APIC 2.1(3) • Cisco APIC 2.1(4) • Cisco APIC 2.2(2) • Cisco APIC 2.2(3)	なし	**1.** Cisco APIC にダウングレードします。 **2.** Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 2.2(3)	• Cisco APIC 2.0(2) • Cisco APIC 2.1(1) • Cisco APIC 2.1(2) • Cisco APIC 2.1(3) • Cisco APIC 2.2(1) • Cisco APIC 2.2(2)	なし	**1.** Cisco APIC にダウングレードします。 **2.** Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 2.2(2)	• Cisco APIC 2.0(2) • Cisco APIC 2.1(1) • Cisco APIC 2.1(2) • Cisco APIC 2.2(1)	なし	**1.** Cisco APIC にダウングレードします。 **2.** Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.2(1)	• Cisco APIC 2.0(1r) 以降 • Cisco APIC 2.0(2) • Cisco APIC 2.1(1)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 2.1(4)	• Cisco APIC 2.1(3)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 2.1(3)	• Cisco APIC 1.3(1) • Cisco APIC 1.3(2) • Cisco APIC 2.0(1) • Cisco APIC 2.0(2) • Cisco APIC 2.1(1) • Cisco APIC 2.1(2)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.1(2)	• Cisco APIC 1.3(1) • Cisco APIC 1.3(2) • Cisco APIC 2.0(1) • Cisco APIC 2.0(2) • Cisco APIC 2.1(1)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 2.1(1)	• Cisco APIC 1.3(1i) 以降 • Cisco APIC 1.3(2) • Cisco APIC 2.0(1) • Cisco APIC 2.0(2)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 2.0(2)	• Cisco APIC 1.2(3) • Cisco APIC 1.3(1) • Cisco APIC 1.3(2) • Cisco APIC 2.0(1)	なし	1. ダウングレードする前に単一ポッドにマルチポッド セットアップを変換します。 2. Cisco APIC にダウングレードします。 3. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 2.0(1)	• Cisco APIC 1.2(3) • Cisco APIC 1.3(1) • Cisco APIC 1.3(2)	なし	1. ダウングレードする前に単一ポッドにマルチポッドセットアップを変換します。 2. N9K-C93108TC-EX ノードは、ダウングレード手順を開始する前にデコミッションする必要があります。 3. Cisco APIC にダウングレードします。 4. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 1.3(2)	Cisco APIC 1.3(1)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(2)	• Cisco APIC 1.1(2I) 以降 • Cisco APIC 1.1(3) • Cisco APIC 1.1(4) • Cisco APIC 1.2(1) • Cisco APIC 1.2(2) • Cisco APIC 1.2(3) • Cisco APIC 1.3(1)	なし	1. ダウングレードの手順を開始する前に、N9K-C93180YC-EX、N9K-X9732C-EX がデコミッションされていることを確認してください。 2. Cisco APIC にダウングレードします。 3. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 1.3(1)	• Cisco APIC 1.1(2I) 以降 • Cisco APIC 1.1(3) • Cisco APIC 1.1(4) • Cisco APIC 1.2(2) • Cisco APIC 1.2(1) • Cisco APIC 1.2(3)	なし	1. ダウングレードの手順を開始する前に、N9K-C93180YC-EX、N9K-X9732C-EX がデコミッションされていることを確認してください。 2. Cisco APIC にダウングレードします。 3. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.3(1)	• Cisco APIC 1.1(2I) 以降 • Cisco APIC 1.1(3) • Cisco APIC 1.1(4) • Cisco APIC 1.2(2) • Cisco APIC 1.2(1) • Cisco APIC 1.2(3)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 1.2(3)	• Cisco APIC 1.1(1o) 以降 • Cisco APIC 1.1(2) • Cisco APIC 1.1(3) • Cisco APIC 1.1(4) • Cisco APIC 1.2(1) • Cisco APIC 1.2(2)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。
Cisco APIC 1.2(2)	• Cisco APIC 1.1(1o) 以降 • Cisco APIC 1.1(2) • Cisco APIC 1.1(3) • Cisco APIC 1.1(4) • Cisco APIC 1.2(1)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンスグループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.2(1)	• Cisco APIC 1.1(1) • Cisco APIC 1.1(2) • Cisco APIC 1.1(3) • Cisco APIC 1.1(4)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。 共有レイヤ 3 アウトのダウングレードについては、共有レイヤ 3 アウトでダウングレードする （114 ページ） を参照してください。。
Cisco APIC 1.2(1)	Cisco APIC 1.0(4Q) 以前	1.2(1x) リリースは、1.0(4q) およびそれ以前のリリースへのステートフル ダウングレードをサポートしていません。1.2(1X) から 1.0(4q) 以前にダウングレードする場合は、ステートレス ダウングレードに従う必要があります。	ダウングレードマトリクス表の上に一覧になっているステートレス ダウングレードの手順を参照してください。 また、共有レイヤ 3 アウトのダウングレードについては、共有レイヤ 3 アウトでダウングレードする （114 ページ） を参照してください。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(4)	Cisco APIC 1.0(4o) 以降	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 1.1(4)	Cisco APIC 1.0(4h) 以前	1.1(4x) リリースは、1.0(4h) およびそれ以前のリリースへのステートフル ダウングレードをサポートしていません。1.1(4x) から 1.0(4h) 以前にダウングレードする場合は、ステートレス ダウングレードに従う必要があります。	ダウングレードマトリクス表の上に一覧になっているステートレス ダウングレードの手順を参照してください。
Cisco APIC 1.1(3)	Cisco APIC 1.0(4o) 以降	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(3)	Cisco APIC 1.0(4h) 以前	1.1(3x) リリースは、1.0(4h) およびそれ以前のリリースへのステートフルダウングレードをサポートしていません。1.1(3x) から 1.0(4h) 以前にダウングレードする場合は、ステートレス ダウングレードに従う必要があります。	ダウングレードマトリクス表の上に一覧になっているステートレス ダウングレードの手順を参照してください。
Cisco APIC 1.1(2)	Cisco APIC 1.0(4o) 以降	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 1.1(2)	Cisco APIC 1.0(4h) 以前	1.1(2x) リリースは、1.0(4h) およびそれ以前のリリースへのステートフルダウングレードをサポートしていません。1.1(2x) から 1.0(4h) 以前にダウングレードする場合は、ステートレス ダウングレードに従う必要があります。	ダウングレードマトリクス表の上に一覧になっているステートレス ダウングレードの手順を参照してください。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.1(1)	Cisco APIC 1.0(4o) 以降	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。
Cisco APIC 1.1(1)	Cisco APIC 1.0(4h) 以前	1.1(2x) リリースは、1.0(4h) およびそれ以前のリリースへのステートフル ダウングレードをサポートしていません。1.1(2x) から 1.0(4h) 以前にダウングレードする場合は、ステートレス ダウングレードに従う必要があります。	ダウングレードマトリクス表の上に一覧になっているステートレス ダウングレードの手順を参照してください。
Cisco APIC 1.0(4)	Cisco APIC 1.0(3)	なし	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.0(4)	Cisco APIC 1.0(2)	• スイッチ モデル N9K C9372PX、N9K C9332PQ、N9K C9372TX がある場合、1.0(2x) にダウングレードし内でください。これらのモデルはリリース 1.0(2x) ではサポートされていません。 • fvIP オブジェクトを使用したフローベースのアトミック カウンタ ポリシーのサポートは、リリース 1.0(2x) に追加されました。そのようなポリシーで設定されたファブリックが 1.0(2X) 以前のリリースにダウングレードされる場合、ポリシー設定は UI に正確に反映されません。ダウングレードする前に、既存の fxIP ベース アトミック カウンタ ポリシーを削除して、fvCEp ベースのポリシーに置き換えます。 • 可能であれば、1.0(3x) にダウングレードを考慮します。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

遷移元	目的	制限事項	推奨される手順
Cisco APIC 1.0(3)	Cisco APIC 1.0(2)	• スイッチ モデル N9K C9372PX、N9K C9332PQ、N9K C9372TX がある場合、1.0(2x) にダウングレードしないでください。これらのモデルはリリース 1.0(2x) ではサポートされていません。 • fvIP オブジェクトを使用したフローベースのアトミック カウンタ ポリシーのサポートは、リリース 1.0(2x) に追加されました。そのようなポリシーで設定されたファブリックが 1.0(2X) 以前のリリースにダウングレードされる場合、ポリシー設定は UI に正確に反映されません。ダウングレードする前に、既存の fxIP ベース アトミック カウンタ ポリシーを削除して、fvCEp ベースのポリシーに置き換えます。	1. Cisco APIC にダウングレードします。 2. Cisco APIC が正常にダウングレードされた後、2 個以上のメンテナンス グループを使用してスイッチをダウングレードします。

スケジューラによるアップグレードについて

スケジューラを使用すると、Cisco APIC クラスタやスイッチのアップグレードなど、操作の時間枠を指定します。これらの時間枠は、1-回だけ発生させるか、または毎週指定した日時に繰

り返し発生させることができます。このセクションでは、アップグレードのスケジューラの仕組みについて説明します。スケジューラに関する詳細情報については、『Ciscoアプリケーション セントリック インフラストラクチャの基礎』を参照してください。

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

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

  グループ内のスイッチに対して runningVersion != desiredVersion の場合、このアクティブな 1 日のウィンドウの間いつでもスイッチはアップグレードの対象となります。アップグレードの対象ノード間で、次の制約がアップグレードの候補の選択に適用されます。
  - 「concurCap」ノード以上には現在アップグレードできません。
  - 1 回で 1 個の VPC ペアのノードのみアップグレードされます。
  - 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。

アップグレードする前に LLDP に接続を無効にする方法

Cisco ACI ファブリックから Cisco APIC 2.x にアップグレードする前に、アップグレード対象が異なるインフラストラクチャ VLAN を持つ別の 2 つの Cisco ACI ファブリックが参加する、

バックツー バック リーフ スイッチの接続を介した LLDP を持つ場合、それらの LLDP 接続を最初に無効にする必要があります。

それらの接続で LLDP を無効にしない場合、アップグレードが Cisco ACI を上書きし、スパインとリーフ スイッチ間の接続を中断します。

- ターゲット接続で LLDP を無効にする方法の 1 つは、ポリシーを使用することです。共通のリーフ スイッチ インターフェイス プロファイルの関連付けられたインターフェイスを含み、共通のインターフェイス ポリシー グループとインターフェイス プロファイルを関連付けます。受信状態と送信状態が無効になる特別な LLDP インターフェイス ポリシーであるポリシー グループを含みます。
- lldp が受信および送信を行わない CLI NX-OS スタイル CLI コマンドの対象のインターフェイスにも適用できます。
- REST API POST で無効にすることもできます。

```
POST https://<apic>/api/node/mo/uni/infra/lldpIfP-LLDP-Disabled.json
{
  "lldpIfPol":{
    "attributes":{
      "dn":"uni/infra/lldpIfP-LLDP-Disabled",
      "name":"LLDP-Disabled",
      "adminRxSt":"disabled",
      "adminTxSt":"disabled",
      "status":"created"
    },"children":[]
  }
}
```

GUI を使用したソフトウェアのアップグレード

GUI を使用してソフトウェアをアップグレードできます。

Upgrading the Cisco APIC Software Version Using the GUI

（注） 参照してください Cisco APIC およびスイッチ ソフトウェアのアップグレードについて （21 ページ） およびを正しいアップグレードの順序を決定するためにアップグレードするバージョンのリリース ノート、 Cisco APIC と、スイッチ。

手順

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

[作業（Work）] ペインの Cisco APIC に、各コントローラにロードされた現在のファームウェアが表示されます。ファームウェアが最後にアップグレードされたときの状態も表示されます。

ステップ 2 [Navigation] ペインで、[Controller Firmware] をクリックします。
Cisco APIC の現在のファームウェア バージョンが、[作業（Work）] ペインの [現在のファームウェア（Current Firmware）] に表示されます。

ステップ 3 **[ADMIN]** > **[Firmware]** を選択して、[Navigation] ペインの [Download Tasks] をクリックします。

ステップ 4 [Work] ペインで、**[General]** > **[Actions]** を選択し、[Create Outside Firmware source] をクリックします。

ステップ 5 [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) [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) [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 が例 **10.67.82.87:/home/<username>/ACI/aci-apic-dk9.1.0.2j.iso** .</username>

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。[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 6 [Navigation] ペインで、[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。

[Navigation] ペインで、ダウンロードが 100% に達したら、[Firmware Repository] をクリックします。

[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。

ステップ 7 [Navigation] ペインで、[Controller Firmware] をクリックします。[Work] ペインで、**[Actions]** > **[Upgrade Controller Firmware Policy]** を選択します。[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) [Target Firmware Version] フィールドで、ドロップダウン リストから、アップグレードするイメージ バージョンを選択します。

b) [Apply Policy] フィールドで、[Apply Now] のオプション ボタンをクリックします。[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、アップグレードプロセスが開始されます。アップグレード中にコントローラ クラスタを使用できるように、Cisco APIC は順番にアップグレードされます。

ステップ 8 [Navigation] ペインの [Controller Firmware] をクリックして、アップグレードの状態を [Work] ペインで確認します。

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

（注） ブラウザが接続されている Cisco APIC がアップグレードされて再起動すると、ブラウザにエラー メッセージが表示されます。

ステップ 9 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 にサインインします。

GUI を使用した、リーフおよびスパインスイッチ ソフトウェアのバージョン アップグレード

始める前に

全コントローラが新しいファームウェア バージョンにアップグレードされるまで待機してから、スイッチのファームウェアのアップグレードに進みます。

手順

ステップ 1 メニュー バーで **[ADMIN]** > **[Firmware]** を選択し、[Navigation] ペインで [Fabric Node Firmware] を選択します。
[Work] ペインに、ファブリック内の全スイッチのリストが表示されます。ファームウェアが最後にアップグレードされたときの状態も表示されます。

ステップ 2 [Navigation] ペインで、[Download Tasks] をクリックします。

ステップ 3 [Work] ペインで、**[General]** > **[Actions]** を選択して、[Create Outside Firmware source] をクリックし、次の操作を実行します。

a) [Source Name] フィールドにスイッチ イメージの名前（*switch_image*）を入力します。
b) [Protocol] フィールドで、[Secure copy] オプション ボタンをクリックします。

（注） Http ソースまたは Secure Copy Protocol（SCP）のどちらからソフトウェア イメージをダウンロードするかに応じて、適切なラジオ ボタンを選択します。

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

e) [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。[Submit] をクリックします。`
スイッチ 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 4 [Navigation] ペインで、[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。

[Navigation] ペインで、ダウンロードが 100% に達したら、[Firmware Repository] をクリックします。

[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。

ステップ 5 **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 6 [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]** フィールドのチェック ボックスをチェックします。

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

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

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

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

g) **[メンテナンス グループ]** ダイアログ ボックスの **[グループ名]** 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) 確認、 **グレースフル メンテナンス** アップグレードを実行する前に、正常な挿入および削除 (登場させ) モードにノードが停止するチェック ボックス。参照してください、 *Cisco APIC Getting Started guide* 』、リリース *3.x* グレースフル挿入と削除 (登場させ) モードについて。

j) [Submit] をクリックします。`

k) [Finish] をクリックします。

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

ステップ 7 [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 8 [Navigation] ペインで、**[Fabric Node Firmware]** > **[Maintenance Groups]** 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 9 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 10 [Upgrade Now] ダイアログボックスで、「Do you want to upgrade the maintenance group policy now?」 に対する [Yes] をクリックします。[OK] をクリックします。

（注） [Work] ペインで、[Status] にグループ内の全スイッチが同時にアップグレードされていく状況が表示されます。グループ内のデフォルトの同時実行数は 20 に設定されます。したがって、20 台のスイッチが同時にアップグレードされ、その後また 20 台のスイッチの組がアップグレードされます。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。スイッチのアップグレードには、グループごとに最長で 12 分かかります。スイッチはアップグレードすると再起動し、接続が切断されて、クラスタ内のコントローラはグループ内のスイッチとしばらくの間、通信しません。スイッチが起動後にクラスタに再加入した場合、コントローラ ノードの下に全スイッチが一覧で表示されます。クラスタに VPC コンフィギュレーションがある場合、アップグレードプロセスは VPC ドメインの 2 台のスイッチのうち一度に 1 台のスイッチのみをアップグレードします。

ステップ 11 [Navigation] ペインで、[Fabric Node Firmware] をクリックします。
[Work] ペインで、一覧表示される全スイッチを確認します。[Current Firmware] 列に、アップグレードイメージの詳細が、各スイッチに対して表示されます。ファブリック内のスイッチが新しいイメージにアップグレードされることを確認します。

GUI を使用したカタログ ソフトウェア バージョンのアップグレード

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

手順

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

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

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

a) [Catalog Version] フィールドで、目的のカタログ ファームウェアの バージョンを選択します。
b) ファームウェアをただちにアップグレードするために、[Apply Policy] フィールドの [Apply Now] オプション ボタンをクリックします。[Submit] をクリックします。`
c) [Work] ペインで、[Target Firmware version] フィールドが [Current Firmware Version] フィールドのイメージ バージョンに一致する画像が表示されるまで待機します。
これでカタログのバージョンが、アップグレードされました。

変更、互換性を無視する設定を確認

、Apic内では、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。「互換性チェックを無視」の設定がありますが、デフォルトでは **[オフ]** に設定されているため、デフォルトで可能なアップグレードの互換性をシステムが自動チェックします。「互換性チェックを無視」設定を変更する場合は、次の手順をに従って **で** いずれかの理由で、互換性チェック機能が無効になるようにします。

（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。

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 互換性の確認を無視する機能が含まれている画面にアクセスします。次に例を示します。

- ファームウェア管理左側のパネルで、[選択 **ファブリック ノード ファームウェア** を右クリックし、 **ファームウェア グループ**] を選択します **ファームウェア グループの作成** します。
- 左側のパネル ファームウェア管理、下を右クリックして **コントローラ ファームウェア**] を選択します **コントローラのアップグレード** 。

ステップ 3 該当する項目を選択、 **互換性の確認を無視** ()] フィールド。

- ボックスにチェック マークを入力 を有効にする 、 **互換性の確認を無視** (機能を無効に互換性チェック、システムが可能なアップグレードの互換性をオンにしないように)] オプションをまたは

• (空のボックスをオンのままに)] ボックスから、チェック マークを削除 を無効にする 、**互換性の確認を無視** オプション(機能を有効に互換性チェック、システムで可能なアップグレードの互換性を確認するため)。

REST API を使用したソフトウェアのアップグレード

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

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

手順

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

例：

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

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

例：

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

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

例：

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

REST API を使用したスイッチ ソフトウェアのアップグレード

手順

ステップ 1 リポジトリにスイッチ イメージをダウンロードします。

例：

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

ステップ 2 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 すべてのスイッチのアップグレードをただちにトリガする次のポリシーを POST します。

例：

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

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

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

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

手順

カタログ イメージをアップグレードします。

例：

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

CLI による ソフトウェアのアップグレード

CLI を使用して、ソフトウェアをアップグレードできます。

NX-OS を使用した Cisco APIC ソフトウェアのアップグレード

手順

ステップ 1 送信元からコントローラにイメージをダウンロードします。

例：

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

ステップ 2 リポジトリ情報を表示します。

例：

```
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。

例：

```
firmware repository add <name of the image file>
firmware repository add aci-apic-dk9.2.0.1r.iso
```

ステップ 4 アップグレードするコントローラを設定します。

例：

```
apic1(config)# firmware
apic1(config-firmware)# controller-group
apic1(config-firmware-controller)# firmware-version <name of the image file>
apic1(config-firmware-controller)# firmware-version aci-apic-dk9.2.2.2e.bin
```

ステップ 5 コントローラをアップグレードします。

例：

```
apic1# firmware upgrade controller-group
```

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

ステップ 6 コントローラのアップグレードを確認します。

例：

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

```
 1            101          n9000-12.3(0.102)      n9000-12.3(0.102)      success
         100
 1            102          n9000-12.3(0.102)      n9000-12.3(0.102)      success
         100
 1            103         n9000-12.3(0.100)      n9000-12.3(0.102)      upgrade in progress
        5
 1            104          n9000-12.3(0.102)      n9000-12.3(0.102)      success
         100
 1            201          n9000-12.3(0.102)      n9000-12.3(0.102)      success
         100
 1            202         n9000-12.3(0.100)      n9000-12.3(0.102)      upgrade in progress
        5
apic1#
```

NX-OS スタイル CLI を使用したスイッチのアップグレード

手順

ステップ 1 送信元からコントローラにイメージをダウンロードします。

例：

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

ステップ 2 リポジトリ情報を表示します。

例：

```
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。

例：

```
firmware repository add <name of the image file>
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。

例：

```
apic1(config)# firmware
apic1(config-firmware)# switch-group <name of the switch group>
apic1(config-firmware-switch)# switch 101-104,201,202
apic1(config-firmware-switch)# firmware-version aci-n9000-dk9.12.2.2e.bin
```

ステップ 5 スイッチのグループをアップグレードします。

例：

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

ステップ 6 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。

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 を使用したカタログ ソフトウェア バージョンのアップグレード

デフォルトで、コントローラをアップグレードすると、自動的に対応するカタログ コントローラのバージョンにアップグレードされます。つまり、リポジトリにコントローラのイメージを追加すると、リポジトリにもカタログ イメージが追加されます。

別のカタログ イメージをコピーし、リポジトリに追加することもできます。

手順

ステップ 1 カタログ イメージをリポジトリに追加します。

例：

```
apic1(config)# firmware
apic1(config-firmware)# catalog-version aci-catalog-dk9.2.2.2e.bin
```

ステップ 2 カタログ アップグレード ステータスを確認します。

例：

```
apic1# show catalog
Catalog-version : 2.2(2e)
apic1#
```

デバッグ CLI を使用したコントローラのアップグレード

実行中のファームウェア イメージと互換性がない新しい Cisco APIC ファームウェア イメージをインストールする場合は、デバッグ CLI を使用してアップグレードできます。

（注） これらの手順で、この Cisco APIC から以前のすべてのユーザ データを削除します。クラスタが一部の場合、コントローラはクラスタの他のコントローラからデータを取得できます。

3つの手順でデバッグCLIを使用してコントローラをアップグレードする

手順

ステップ 1 管理者として Cisco APIC にログインします。

ステップ 2 Cisco APIC からユーザのデータを消去します。

例：

```
admin@apic1:~> acidiag touch clean
```

ステップ 3 Cisco APIC のイメージをインストールします。

例：

```
admin@apic1:~> acidiag install http://<ip>/<ver-no>
```

ステップ 4 Cisco APIC をリブートします。

例：

```
admin@apic1:~> acidiag reboot
```

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

確認内容	URL の例
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

SSD インストール ステータスの確認

この手順を使用して、Cisco APIC に SSD がインストールされているか確認します。

手順

ステップ 1 管理者ユーザとして Cisco APIC にログインします。

ステップ 2 コマンド **acidiag hwcheck | grep -A 6 "Physical Disk /dev devices"** を入力します。

```
admin@APIC1:~> acidiag hwcheck | grep -A 6 "Physical Disk /dev devices".
====================== Physical Disk /dev devices

Disk /dev/sda: 999.0 GB, 998999326720 bytes, 1951170560 sectors
Disk /dev/sdb: 119.5 GB, 119453777920 bytes, 233308160 sectors
Disk /dev/sdc: 4009 MB, 4009754624 bytes, 7831552 sectors
Disk /dev/mapper/vg_ifc0_ssd-data: 113.8 GB, 113816633344 bytes, 222298112 sectors

admin@APIC1:~>
```

ステップ 3 CIMC にログインします。

ステップ 4 **[ストレージ]** > **[物理ドライブ情報]** を選択します。

ステップ 5 SSD がインストールされているかどうかを確認します。

アップグレードプロセス中にフォールトのトラブルシューティング

メンテナンス ポリシーごとに1つのスケジューラが存在します。デフォルトでアップグレードフォールトが検出されると、スケジューラを停止し、そのグループのノードはアップグレードを開始しません。スケジューラは、アップグレードフォールトの場合に手動介入によるデバッグを必要とします。手動介入が完了したら、一時停止されたスケジューラを再開させる必要があります。

スイッチのステータスが「queued」になっている場合は、以下を確認します。

- コントローラのクラスタが正常かどうか。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。

スイッチについて API で「waitingForClusterHealth = no」と表示されるまで、または GUI で [クラスタ コンバージェンスの待機（Waiting for Cluster Convergence）] に [いいえ（No）] が表示されるまで約 60 分以上かかる場合は、スケジューラの一時停止を確認するステップを完了します。

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。

- 不十分な許可
- ディレクトリまたはファイルが見つからない
- 宛先のディレクトリに空きがない
- 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

ダウンロードを再開するには手順のいずれかを実行します。

クラスタの収束の確認

GUI を使用して、クラスタ コンバージェンスを確認します。

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。

（注） 成功するため、アップグレードの2つのグループに、スイッチを分割必須です。デフォルトでは、システムは、一度に; 20 スイッチをアップグレードします。この番号を変更することができます。

コントローラとスイッチのアップグレードの進行に伴い、キューに入っているノードの数とアップグレード中のノードの数、および成功したアップグレードの数に関するメッセージが表示されます。

表示されるノードのアップグレード ステータスは次のとおりです。

- NotScheduled：現在、ノードに対してアップグレードはスケジュールされていません。
- Scheduled：ノードに対してアップグレードがスケジュールされています。
- Queued：現在アクティブな時間枠（スケジュール）があり、ノードがアップグレードの認可を要求しています。
- Inprogress：現在、ノードに対してアップグレードが進行中です。
- CompleteOK：アップグレードが正常に完了しました。
- CompleteNOK：ノードでのアップグレードが失敗しました。
- Inretryqueue：アップグレードを再試行するためにノードがキューに入っています（5 回試行した後に、失敗が宣言されます）。

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。

コントローラのアップグレードを一時停止することの確認

コントローラのアップグレードは、GUI または REST API のいずれかを使用して一時停止を確認することができます。

GUI を使用してコントローラのアップグレード スケジューラー時停止しているかどうかを確認するには

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[Firmware]** を選択します。

ステップ 2 [Navigation] ペインで、**[Fabric Node Firmware]** > **[Controller Firmware]** を展開します。

ステップ 3 スケジュールされたメンテナンス ポリシーが一時停止して かどうかが表示されます **アップグレードに失敗しました** で、 **ステータス** 内の列、 **作業** ペインで、特定の Cisco APIC 。

ものが正しく進行していることが表示されます **ファームウェア アップグレード queued、クラスタ コンバージェンスを待機中** で [Status] カラムで、 **作業** ペインで、特定の Cisco APIC 。

ステップ 4 問題を特定して、この問題を修正します。

ステップ 5 をクリックします **アクション**] タブをクリックします **コントローラ ファームウェア ポリシーのアップグレード** 。

REST API を使用してコントローラのアップグレード スケジューラー時停止しているかどうかを確認するには

手順

コントローラ メンテナンス ポリシーのためにスケジューラが一時停止されていることを確認するには、次の API を POST 送信します。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

次のような返品が表示されます。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/fabric/
maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00" polName="
ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="local"
maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status="" uid="0"
waitOnClusterHealth="no" windowName=""/>
</imdata>
```

スイッチのアップグレードの一時停止確認

GUI または REST API のいずれかを使用して、スイッチのアップグレードの一時停止を確認できます。

GUI を使用してスイッチ アップグレード スケジューラの一時停止を確認する

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。

ステップ 2 [ナビゲーション] ペインで、**[ファブリック ノード ファームウェア]** > **[メンテナンス グループ]** を展開します。

ステップ 3 **[メンテナンス グループ]** を展開して、**[すべてのスイッチ]** をクリックします。

ステップ 4 **[作業]** ペインで、**[スケジューラのステータス]** が **[一時停止]** を読み取っているか確認します。

（注） **[スケジューラのステータス]** が **[実行中]** を読み取り、グループ内のノードがアップグレードを続行または完了している場合、デバイスが実行されアップグレードが続行または完了します。

ステップ 5 デバイスに移動し、手順 1 ～ 4 を繰り返します。

この時点で、**[スケジューラのステータス]** は **[実行中]** を読み取ります。

ステップ 6 右上の **[アクション]** ドロップダウンリストを使用して、**[アップグレード スケジューラの再開]** を選択します。

ステップ 7 右上の **[アクション]** ドロップダウン リストを使用して、**[今すぐアップグレード]** を選択します。

REST API を使用してスイッチのアップグレード スケジューラが時停止しているか確認する

手順

スイッチ メンテナンス ポリシーのためにスケジューラが一時停止されていることを確認するには、次の API を POST 送信します。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml
```

次のような返品が表示されます。

例：

```
https://<ip address>/api/node/class/maintUpgStatus.xml

ConstCtrlrMaintP ==> controller group
Nowgrp ===> A switch group

<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="2">
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-ConstCtrlrMaintP"
 faultDelegateKey="uni/
fabric/maintpol-ConstCtrlrMaintP" lcOwn="local" maxConcurrent="0"
modTs="2014-08-28T14:45:24.232-07:00"
polName="ConstCtrlrMaintP" runStatus="paused" status="" uid="0" waitOnClusterHealth="no"
 windowName=""/>
    <maintUpgStatus childAction="" dn="maintupgstatuscont/maintupgstatus-nowgrp"
faultDelegateKey="" lcOwn="
local" maxConcurrent="0" modTs="2014-08-28T08:05:15.148-07:00" polName="nowgrp"
runStatus="running" status=""
uid="0" waitOnClusterHealth="no" windowName=""/>
</imdata>
```

スコントローラのメンテナンス ポリシーのために一時停止したスケジューラの再開

GUI または REST API のいずれかを使用してコントローラ メンテナンス ポリシーの一時停止スケジューラを再開することができます。

コントローラのアップグレード スケジューラ Resume を GUI を使用して一時停止しています

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[Firmware]** を選択します。

ステップ 2 [Navigation] ペインで、**[Fabric Node Firmware]** > **[Controller Firmware]** を展開します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

ステップ 4 [Controller Maintenance Policy] 領域で、[Running Status] フィールドの表示が [Paused] であることを確認します。

ステップ 5 [Actions] タブをクリックし、[Resume Upgrade Scheduler] をクリックします。

ステップ 6 をクリックします **アクション**] タブを選択します **コントローラ ファームウェア ポリシーのアップグレード** ドロップダウンリストから。

ステップ 7 [アクション（Actions）] タブをクリックし、ドロップダウン リストから [今すぐ適用（Apply Now）] を選択します。

REST API を使用して一時停止したコントローラのアップグレード スケジューラを再開する

手順

ステップ 1 コントローラ メンテナンス ポリシーのために一時停止されたスケジューラを再開するには、次の API をPOST 送信します。

この例では、メンテナンス ポリシーは ConstCtrlrMaintP です。

例：

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="ConstCtrlrMaintP" status="deleted" />
</maintUpgStatusCont>
```

ステップ 2 Cisco APIC コントローラ ソフトウェアをアップグレードするために最初に使用される REST API を使用します。

スイッチのメンテナンスポリシーのために一時停止したスケジューラの再開

一時停止したスイッチのアップグレード スケジューラを再開するために GUI を使用する

手順

ステップ 1 メニュー バーで、**[管理]** > **[ファームウェア]** を選択します。

ステップ 2 **[ナビゲーション]** ペインで、**[ファブリック ノード ファームウェア]** > **[メンテナンス グループ]** > ***[maintenance_group_name]*** を展開します。

ステップ 3 [Work] ペインで、[Policy] タブをクリックします。

ステップ 4 [Maintenance Policy] 領域で、[Running Status] フィールドの表示が [Paused] であることを確認します。

ステップ 5 **[メンテナンス ポリシー]** 領域で、**[スケジューラのステータス]** フィールドに **[一時停止]** が表示され、**[クラスタ コンバージェンスの待機]** フィールドに **[いいえ]** が表示されていることを確認します。

ステップ 6 [Actions] タブをクリックし、[Resume Upgrade Scheduler] をクリックします。

ステップ 7 **[アクション]** タブをクリックして、ドロップダウン リストから **[今すぐアップグレード]** を選択します。

REST API を使用して一時停止したスイッチ アップグレード スケジューラを再開する

手順

ステップ 1 スイッチ メンテナンス ポリシーのために一時停止されたスケジューラを再開するには、次の API をPOST 送信します。

この例では、メンテナンス ポリシーは swmaintp です。

例：

```
URL: https://<ip address>/api/node/mo.xml
<maintUpgStatusCont>
<maintUpgStatus polName="swmaintp" status="deleted" />
</maintUpgStatusCont>
```

ステップ 2 最初に使用した REST API を使用してスイッチ ソフトウェアをアップグレードします。

クリーン再起動の実行

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。

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。次のコマンドを使用して、スイッチをクリーン再起動します。

例：

```
/bin/setup-clean-config.sh
vsh-c reload
```

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
```

（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か、UI を使用してスイッチを登録できます。

共有レイヤ 3 アウトでアップグレードする

共有レイヤ3アウト機能は1.2(1i)リリースで導入されました。このセクションでは、サポートされていないリリースからアップグレードするときに発生する制限事項と動作を説明します。

アップグレード、 Cisco APIC リーフ スイッチの前に

共有レイヤ 3 Out 機能が有効になっていません自動的にアップグレードした後、アップグレードするため、 Cisco APIC は、無害で最初と動作の変更はされません。リーフ スイッチの古いイメージは引き続き動作しているためリーフ スイッチは、他の VRF の外部のプレフィクスをプログラムされません。共有レイヤ 3 Out リーフ スイッチが新しいイメージをアップグレードし、外部のプレフィックスが適切にマークしない限り、トラフィックは機能しない共有されます。

シナリオと予測される動作のリストを次に示します後に、リーフ スイッチをアップグレードすると、 Cisco APIC :

- シナリオでは、プロバイダー リーフ switche アプリケーション EPG あり、コンシューマ リーフ switche は、L3Out、リーフ スイッチをアップグレード順序は関係ありません。プレフィックスとしてマークされている L3Out 共有され、プロバイダーのプレフィックスのエントリが作成されていませんため、共有のレイヤ 3 Out 機能は動作しません VRF。両方のリーフ スイッチをアップグレードすると、適切な「スコープ」フラグと共有するプレフィックスのマークを付ける必要があります。プロバイダー VRF の外部のプレフィクスをリークをしも actrl:PfxEntry を作成します。共有レイヤ 3 Out 機能は、作業を開始する必要があります。
- ここでプロバイダー リーフ switche、L3Out はコンシューマ リーフ switche はアプリケーション EPG のシナリオでリーフ スイッチをアップグレード順序は関係ありません。プレフィックスとしてマークされている L3Out 共有され、プロバイダーのプレフィックスのエントリが作成されていませんため、共有のレイヤ 3 Out 機能は動作しません VRF。両方のリーフスイッチをアップグレードすると、適切な「スコープ」フラグと共有するプレフィックスのマークを付ける必要があります。プロバイダー VRF の外部のプレフィクスをリークをしも actrl:PfxEntry を作成します。共有レイヤ 3 Out 機能は、作業を開始する必要があります。
- ここでコンシューマとプロバイダーは、両方の L3Outs のシナリオでリーフ スイッチをアップグレード順序は関係ありません。プロバイダーまたはコンシューマ L3Outs のいずれかでプレフィックスとしてマークされている L3Out が共有ないために、共有レイヤ 3 Out 機能は動作しません。プロバイダーのプレフィックスのエントリが作成されていませんコンシューマの外部のプレフィックスとプレフィックス エントリがない VRF がコンシューマので作成されたプロバイダーの外部のプレフィックスの VRF。両方のリーフ スイッチをアップグレードすると、適切な「スコープ」フラグと共有するプレフィックスのマークを付ける必要があります。プロバイダー VRF の外部のプレフィクスをリークをしも actrl:PfxEntry を作成します。共有レイヤ 3 Out 機能は、作業を開始する必要があります。

リーフをアップグレードする前にスイッチ、Cisco APIC

共有レイヤ 3 Out 機能は最初は、無害でを動作で、変更が発生しないリーフ スイッチをアップグレードするためのアップグレード後に自動的に有効になっていません。

後に、 Cisco APIC リーフ スイッチをアップグレードと

すべてのリーフ スイッチおよび Cisco APIC レイヤ 3 外部と共有サービスに関与して s を共有レイヤ 3 Out 機能をサポートするリリースにアップグレードする必要があります。外部のサブネット (モデル クラス l3ext:Subnet で表されます) で次のフラグを配置のプライベート ネットワーク全体にわたって共有するサブネットのアップグレード後に、サブネットはします。

- その他のプライベート ネットワークのルートを漏出のサブネットの「スコープ」プロパティに「共有 rtctrl」ビットを追加します。
- 他のプライベートネットワーク内のルート上のセキュリティを有効にするには、サブネットの「スコープ」プロパティで、「セキュリティを共有」ビットを追加します。

共有レイヤ 3 アウトでダウングレードする

共有レイヤ3アウト機能は1.2(1i)リリースで導入されました。このセクションでは、サポートされていないリリースにダウン グレードときに発生する制限事項と動作を説明します。

ダウン グレード、 Cisco APIC リーフ スイッチの前に

ダウン グレード後に、 Cisco APIC 、システムには、外部のサブネットの「スコープ」プロパティから共有サービス有効にするために使用されるビットは自動的に削除します。リーフ スイッチが新しいイメージを実行しているは、この変更通知を取得し、これらのサブネットの共有を停止します。クロス VRF 契約の契約コンシューマとして動作する外部ネットワーク インスタンス プロファイル（モデル クラス l3ext:InstP により示される）は、ローカル クラス ID を取得します。これは、既存のコミュニケーションのトラフィック フラップになります。

Cisco APIC 前にリーフ スイッチをダウンロードする

スイッチがダウンロードされると、「shared-rtctr」または「shared-security」でのみマークされている外部サブネットの取得を停止します。スコープ プロパティにほかのビット設定がある場合、それらのビットに対応する以前の動作が応答します。クロス VRF 契約の契約コンシューマとして動作する外部ネットワーク インスタンス プロファイル（モデル クラス l3ext:InstP により示される）は、ローカル クラス ID を取得します。これは、既存のコミュニケーションのトラフィック フラップになります。

推奨されるダウングレード

共有レイヤ3アウト機能をサポートしていないイメージにリーフスイッチをダウングレードする前に、そのリーフスイッチで展開されている永続サブネットから、共有サービスに使用されたビットのチェックを外すことをお勧めします。ただし、この推奨される方法でも、通過VRFコントラクトのコントラクト コンシューマとして動作する外部インスタンス プロファイルに対して、トラフィックのフラップを回避することはできません。

ネットワーク設定機能と混合 OS 動作中の変更

リリース 2.2(1n) 以降、Cisco Application Policy Infrastructure Controller はネットワーク設定機能と混合 OS 動作中の変更に関する次の機能をサポートしています。

- エクスポート設定
- テクニカル サポート
- ネットワーク トリガ

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

表 *6 :* ネットワーク設定の機能および混合 *OS* の動作中の変でサポートされる機能

機能	オペレーション
契約	• 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 を作成および削除します。 • VMM、物理、外部、L2 外部、L3 外部ドメインの関連付けを追加および削除します。 • スタティック ポートの割り当ておよびノードへの静的リンクを追加、削除、更新します。 • 1 つの EPG から別の EPG にエンドポイントを移動します。 • uSeg EPG からベースに EPG にエンドポイントを移動します。
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。

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

機能	オペレーション
物理ネットワーク	• ポート ステータスを有効化および無効化します。 • 物理サーバのオンおよびオフ。 • リーフ スイッチおよびリーフ スイッチ間で物理サーバを移動します。 • スパイン スイッチとリーフ スイッチのリロード。 • スパイン スイッチ LC カード、FC カード、CS カードと SUP カードのリロード。 • スパイン スイッチとリーフ スイッチのデコミッション。 • VPC ドメインの追加と削除。 • プライマリ リンク、セカンダリ リンク、および VPC 内のすべてのリンクをフラップします。 • すべてのポート チャネル リンクをフラップし、ポート チャネルで 1 つのリンクをフラップして、FEX で NIF ポートをフラップし、ラック上部の全面パネル ポートをフラップします。
ファブリック ポリシー	• NTP サーバ、SNMP、BGP ルート リフレクタ、L2 MTU ポリシーを追加、更新、削除します。 • Cisco APIC 接続設定を更新します。

3.0 のリリース以前では、混合 OS 操作は、混合 OS がファブリックに存在することを知らせる赤いバナー警告が表示されます。3.0 のリリース後、この警告バナーが削除されています。

特記事項

- すべての Cisco APIC を最初に新しいバージョンにアップグレードする必要があり、アップグレードが完了したら、サポートされているネットワーク設定操作が実行可能です。Cisco APIC のアップグレード中に、サポートされているネットワーク設定操作を実行することはできません。
- アップグレード中のネットワーク設定機能と変更は、ノード レベルでのみサポートされています。仮想ポート チャネル（VPC）ペアについては、VPC に参加している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。

- ポート ステータスの変更などトリガに関連するすべての物理ネットワーク デバイスは、既存のファブリック スイッチにサーバを接続および切断するか、ファブリック上の Cisco APIC がサポートされています。
- リリース 2.3(1) 以降でサポートされているネットワーク トリガについては、表 6 : ネットワーク設定の機能および混合 OS の動作中の変でサポートされる機能 （115 ページ） を参照してください。

互換性に関する情報

表 7: 互換性に関する情報

説明	Cisco APIC リリース
リリース 2.2(1n) にアップグレード中の 特記事項 （117 ページ） に記載されているサポートされている変更は、次の Cisco APIC リリースでサポートされています。	• リリース2.1(1h) • リリース 2.0(2m)
リリース 2.2(1n) にアップグレード中の表 表 6 : ネットワーク設定の機能および混合 OS の動作中の変でサポートされる機能 （115 ページ） に記載されているサポートされている変更は、次の Cisco APIC リリースでサポートされています。 （注） 混合 OS 操作サポート中にのネットワーク設定機能と変更は、リリース 2.1(1h) まで利用可能です。	• リリース2.2(2k)
リリース 3.0(1) にアップグレード中の表 表 6 : ネットワーク設定の機能および混合 OS の動作中の変でサポートされる機能 （115 ページ） に記載されているサポートされている変更は、次の Cisco APIC リリースでサポートされています。 （注） 混合 OS 操作サポート中にのネットワーク設定機能と変更は、リリース 2.2(2k) まで利用可能です。	• リリース2.3(1f) • リリース2.2(2k)

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。

次の表は、アップグレード中にサポートされているネットワーク設定機能および変更を一覧にしています。

アップグレード パス	例	サポートされているネットワーク設定の機能および変更
1 個のメジャー リリースから別のメジャー リリースにアップグレードします。	リリース 2.0(1) ～ リリース 2.2(1)	• 物理ネットワークの設定変更がサポートされています。 • ポリシーの変更はサポートされていません。
1 個のメジャー リリースから別のマイナーまたはメンテナンス リリースにアップグレードします。	リリース 2.0(1) ～ リリース 2.0(2) リリース 2.1(1) ～ リリース 2.1(2)	• 物理ネットワークの設定変更がサポートされています。 • ポリシーの変更はサポートされていません。
1 個のメジャー リリースから別のメジャーパッチ リリースにアップグレードします。	リリース 2.0(1n) ～ リリース 2.0(1m)	• 物理ネットワークの設定変更がサポートされています。 • ポリシーの変更は、メジャー リリースの前に導入された機能をサポートします。

Cisco Nexus 9300 プラットフォーム スイッチから Cisco Nexus 9300 EX プラットフォーム スイッチへの移行

VPC の Cisco Nexus 9300 プラットフォームを Cisco Nexus 9300 EX プラットフォーム スイッチに移行するには、次の手順を実行します。

手順

ステップ 1 Cisco Nexus 9300 プラットフォーム スイッチからケーブルを取り外します。スイッチの電源を切ります。

ステップ 2 Cisco APIC にログインします。

ステップ 3 **Fabric** > **Inventory** > **Unreachable Nodes** を選択します。

ノードが到達不可能なことを確認します。**[ノード名]** と **[ノード ID]** のノードを作成します。

ステップ 4 ノードを選択します。**[アクション]** メニューから、**[コントローラから削除]** を選択します。

Cisco APIC からノードが削除されるまで 5 ～ 10 分間待機します。

ステップ 5 Cisco Nexus 9300 プラットフォーム スイッチ上のトラフィックをモニタします。すべてのトラフィックはその他の Cisco Nexus 9300 プラットフォーム スイッチによって処理されると、トラフィックへの影響が最小限になるか、影響を受けません。

ステップ 6 Cisco Nexus 9300 EX プラットフォームのスイッチと Cisco Nexus 9300 プラットフォーム スイッチを交換します。

ステップ 7 Cisco Nexus 9300 EX プラットフォーム スイッチの電源をオンにして、ケーブルを接続します。

ステップ 8 Cisco Nexus 9300 EX プラットフォームで Cisco APIC リリース 3.0 (1) ソフトウェアをロードします。スイッチを起動します。

ステップ 9 Cisco APIC にログインします。

ステップ 10 **Fabric** > **Inventory** > **Fabric Membership** を選択します。

スイッチが表示されていることを確認します。

ステップ 11 手順 3 から **[ノード名]** と **[ノード ID]** を Cisco Nexus 9300 EX プラットフォーム スイッチに割り当てます。

ステップ 12 すべての関連するポリシーが Cisco Nexus 9300-EX プラットフォーム スイッチにプッシュされ、エンドポイントの同期が完了するまで数分間待機します。確認のため、**[操作]**>**[容量ダッシュボード]** を選択します。このスイッチのポート チャネルは有効になっていません。

ステップ 13 その他の Cisco Nexus 9300 プラットフォーム スイッチからケーブルを取り外します。スイッチの電源を切ります。

ステップ 14 その他の Cisco Nexus 9300 プラットフォーム スイッチで手順 1-12 を繰り返します。

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
```