Cisco APIC 開始ガイド、リリース 5.3(x)

最終更新：2025 年 11 月 5 日

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

Trademarks

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

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

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

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

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

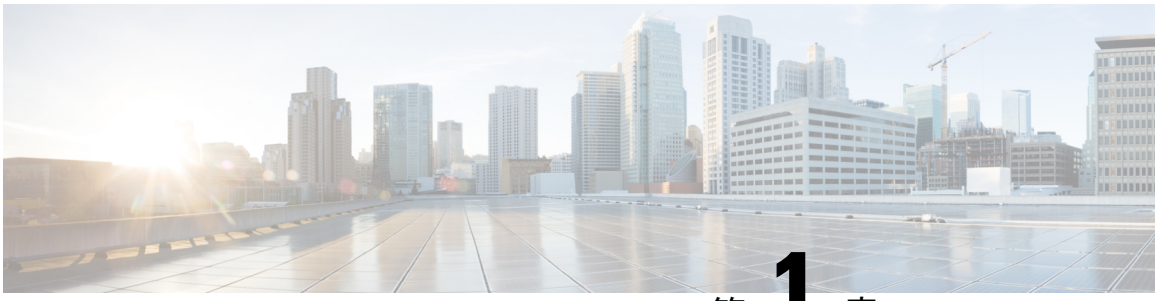
The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality.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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

Trademarks

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

目 次



第 1 章

新機能および変更された機能に関する情報

この章で説明する内容は、次のとおりです。

新機能および変更された機能に関する情報

次の表に、本リリースに関するこのガイドでの重要な変更点の概要を示します。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *5.2(4)* の新機能と変更情報

特長	説明	参照先
Cisco NX-OSから Cisco ACI POAP への自動変換 IPN サポート	IPN デバイスのみを介して Cisco APIC クラスタに到達する Cisco ACI スイッチを追加または交換できるようになりました。	Cisco NX-OS から Cisco ACI POAP への自動変換の注意事項と制限事項 （84 ページ）

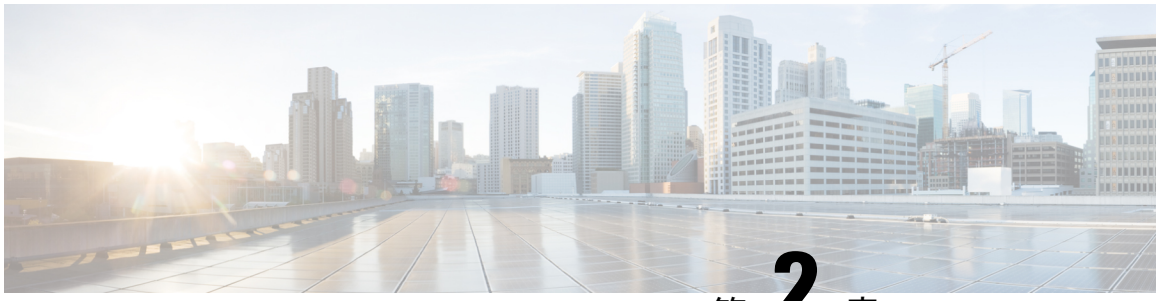
表 *2 : Cisco APIC* リリース *5.2(3)* の新機能と変更情報

特長	説明	参照先
Cisco NX-OS からCisco ACI Cisco ACI POAP への自動変換	Cisco NX-OS から Cisco ACIPower On Auto Provisioning（POAP）への自動変換によって、最初にネットワークに導入されたノードでソフトウェア イメージをアップグレードし、スイッチ上に構成ファイルをインストールするプロセスを自動化できます。	Cisco NX-OSからCisco ACI POAPへの自動変換について （83 ページ）

新機能および変更された機能に関する情報

表 *3 : Cisco APIC* リリース *5.2(1)* の新機能と変更情報

特長	説明	参照先
レイヤ3ネットワークを介したファブリックへのAPICクラスタ接続	APICクラスタのサポートはファブリックに直接接続されていませんが、レイヤ3ポッド間ネットワーク（IPN）によって接続されています。クラスタの初期設定で「スタンドアロンAPICクラスタ」を有効にします。	• アクティブAPICとスタンバイAPICのセットアップ（9 ページ） • 「*Deploying APIC Cluster Connectivity to the Fabric Over a Layer 3 Network*」ナレッジベースの記事も参照してください。



第 2 章

初期設定

この章で説明する内容は、次のとおりです。

次の手順については、以下を参照してください

このテーブルは、『*Cisco APIC Getting Started Guide*』とともに使用するのに役に立つ、参照情報を提供する付加的なドキュメントの一覧です。これらの Cisco APIC のドキュメントおよびその他は、APIC ドキュメント ランディング ページから入手できます。

ヒント 特定の Cisco APIC 機能のドキュメントを検索するには、**APIC ドキュメントランディング ページ**の [トピックの選択（Choose a Topic）] ボックスに機能名を入力します。

ドキュメント
『Application Centric Infrastructure Fabric Hardware Installation Guide』
Cisco APIC インストール、アップグレード、ダウングレード ガイド
Cisco APIC ベーシック コンフィギュレーション ガイド
Cisco APIC レイヤ 2 ネットワーク設定ガイド

ドキュメント
Cisco APIC Layer 3 ネットワーキング設定ガイド
Cisco APIC Security セキュリティ設定ガイド
Cisco Fabric Manager システム管理設定ガイド
『Cisco ACI Virtualization Guide』
『Cisco Application Centric Infrastructure Fundamentals』
『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』

これらのリンクのほとんどは、指定されたドキュメントを含むドキュメントランディングページのセクションに移動します。セクションタイトルの右端にある矢印をクリックしてそのセクションのドキュメント リストを展開し、ご使用のリリースのドキュメントを見つけます。

リリースのドキュメントが存在しない場合は、以前のリリースのドキュメントが適用されます。たとえば、*Cisco Fabric Manager* システム管理設定ガイド は 4.2 リリースからの変更がないため、5.0 リリースでは再公開されませんでした。したがって、4.2 リリースのドキュメントを使用する必要があります。

Cisco APIC での設定のための簡略化されたアプローチ

Cisco APIC追加の NX-OS スタイル CLI インターフェイスで、ACI の設定を簡略化したアプローチをサポートしています。REST API と GUI を使用する既存の設定方法もサポートします。

ネットワーク管理者やその他の NX-OS スタイル CLI のユーザが使用できるシンプルなアプローチに加えて、GUI や REST API と比較できるインテリジェンスな機能も組み込まれています。ある状況では、NX-OS スタイル CLI と GUI は、ユーザの利便性のために ACI モデルの構造を暗黙的に作成し、設定の一貫性を確保するための検証も提供します。この機能によって障害の減少や防止が図れます。

設定とタスクに関する詳細については、『*Cisco APIC Basic Configuration Guide*』と『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』を参照してください。

BIOS のデフォルト パスワードの変更

Cisco Application Policy Infrastructure Controller（APIC）には、デフォルト BIOS パスワードが付属しています。デフォルトのパスワードは「password」です。起動プロセスが開始されると、ブート画面にコンソール サーバの BIOS 情報が表示されます。

（注） 6.0(2) 以降のリリースでは、APIC-L4 および APIC-M4 サーバーがサポートされています。これらのサーバーのデフォルトパスワードは「password」または「Insieme123」です。

デフォルトの BIOS パスワードを変更するには、次のタスクを実行します。

手順

ステップ 1 BIOS の起動プロセス中に、画面に **Press <F2> Setup** と表示されたら、**F2** キーを押します。**Entering Setup** メッセージが表示され、セットアップ メニューにアクセスします。

ステップ 2 **[Enter Password]** ダイアログボックスに、現在のパスワードを入力します。

（注）
デフォルトは、「password」です。

6.0(2) 以降のリリースでは、APIC-L4 および APIC-M4 サーバーがサポートされています。これらのサーバーのデフォルトパスワードは「password」または「Insieme123」です。

ステップ 3 **[Setup Utility]** で、**[Security]** タブを選択し、**[Set Administrator Password]** を選択します。

ステップ 4 **[Enter Current Password]** ダイアログボックスに、現在のパスワードを入力します。

ステップ 5 **[Create New Password]** ダイアログボックスに、新しいパスワードを入力します。

ステップ 6 **[Confirm New Password]** ダイアログボックスに、新しいパスワードを再入力します。

ステップ 7 **[Save & Exit]** タブを選択します。

ステップ 8 **[Save & Exit Setup]** ダイアログボックスで、**[Yes]** を選択します。

ステップ 9 再起動プロセスが完了するまで待機します。
更新された BIOS パスワードが有効になります。

APIC について

Cisco Application Centric Infrastructure（ACI）は、外部エンドポイントの接続性がアプリケーション セントリック ポリシーを通じて制御およびグループ化される、分散型のスケーラブルなマルチテナント インフラストラクチャです。Application Policy Infrastructure Controller（APIC）は、ACI の自動化、管理、モニタリングおよびプログラマビリティの統合ポイントです。APIC は、インフラストラクチャの物理コンポーネントと仮想コンポーネントの統合運用モデルを使用して、場所を問わずアプリケーションの展開、管理、およびモニタリングに対応します。APIC は、アプリケーションの要件とポリシーに基づき、ネットワークのプロビジョニングおよび制御をプログラムで自動化します。また、これは幅広いクラウド ネットワークに対する中央制御エンジンなので、管理が簡単になり、アプリケーション ネットワークの定義および自動化の方法に柔軟性が得られます。また、ノースバウンド Representational State Transfer (REST) API が提供されます。APIC は、多くのコントローラ インスタンスのクラスタとして実装される分散システムです。

Cisco APIC のセットアップ

このセクションでは、Cisco APIC サーバへのローカル シリアル接続を確立して初期基本設定を開始する方法について説明します。セットアップのためにサーバにリモートで接続する手順など、追加の接続情報については、『*Cisco APIC M3 / L3* サーバ インストールおよびサーバ セットアップ』の「初期サーバ セットアップ」を参照してください。

初期接続

Cisco APIC M3 / L3 サーバは、Cisco Integrated Management Controller (CIMC) プラットフォームで動作します。次のいずれかの方法を使用して、CIMC プラットフォームへの初期接続を確立できます。

- サーバの前面パネルの KVM コネクタにキーボードとモニタを接続するには、KVM ケーブル (Cisco PID N20-BKVM) を使用します。
- USB キーボードと VGA モニタをサーバの背面パネルの対応するコネクタに接続します。

（注） 前面パネルの VGA と背面パネルの VGA は同時に使用できません。

次のいずれかの方法を使用して、シリアル接続を確立できます。次の 2 つの方法では、CIMC で設定を変更する必要があります。

（注） これらの方法を同時に複数使用することはできません。

- KVM ケーブルの DB9 コネクタを使用する
- 背面パネルの RJ-45 コンソール ポートを使用します (CIMC で有効にした後)。
- Serial-over-LAN (SoL) による接続 (CIMC で有効にした後)

工場出荷時のデフォルトの接続設定は次のとおりです。

- シリアル ポートのボー レートは 115200 です
- 背面パネルにある RJ-45 コンソール ポートは、CIMIC では無効です
- CIMCでSoLが無効になっています

シリアル アクセスに関するその他の注意事項を次に示します。

- セットアップに Cisco Integrated Management Controller (CIMC) を設定に使用している場合は、まず CIMC をセットアップしてから、CIMC KVM を介して Cisco APIC にアクセスするか、または背面パネルのUSB / VGAポートを介してローカルで Cisco APIC にアクセスし

ます。CIMC KVM アクセスを選択すると、操作中に必要なリモート アクセスが後で使用可能になります。

- RJ-45 コンソール ポートを使用している場合は、SSH を使用して CIMC に接続し、次のコマンドを使用して、SoL ポートを有効化します。

```
scope sol
  set enabled yes
  set baud-rate 115200
  commit
  exit
```

SoL を有効にしたら、 **connect host** コマンドを入力して、APIC コンソールにアクセスします。

（注） SoL を使用する場合は、背面パネルの RJ-45 コンソール ポートを物理的に取り外します。

Cisco APIC の初期設定

Cisco Application Policy Infrastructure Controller (Cisco APIC) を初めて起動すると、 Cisco APIC コンソールに一連の初期化設定オプションが表示されます。多くのオプションでは、**Enter** キーを押すことで角カッコで囲まれて表示されているデフォルト設定を選択できます。設定ダイアログの任意の時点で、**Ctrl+C** を押すことでダイアログを最初から再開できます。

特記事項

- UNIX のユーザ ID が、リモート認証サーバからの応答で明示的に指定されていない場合、一部の Cisco APIC ソフトウェア リリースでは、すべてのユーザに 23999 のデフォルト ID が割り当てられます。リモート認証サーバからの応答で UNIX ID の指定に失敗すると、すべてのユーザが 23999 という同じ ID を共有することになり、ユーザには、Cisco APIC の RBAC ポリシーで設定されている権限より上または下の権限が付与されることになります。

- Cisco では、（SSH、Telnet または Serial/KVM のコンソールを使用して） bash シェルでユーザに割り当てられる AV ペアには、16000 ～ 23999 の範囲で固有の UNIX ユーザ ID を割り当てることを推奨します。Cisco AV ペアが UNIX ユーザ ID を提供しない状況が発生すると、そのユーザにはユーザ ID 23999 または範囲内の類似した番号が割り当てられます。これにより、そのユーザのホームディレクトリ、ファイル、およびプロセスに UNIX ID 23999 を持つリモート ユーザがアクセスできるようになってしまいます。

  リモート認証サーバが **cisco-av-pair** 応答で明示的に UNIX ID を割り当てているかどうかを確認するには、Cisco APIC への SSH セッションを開いて、(リモート ユーザ アカウントを使用し) 管理者としてログインします。ログインしたら、次のコマンドを実行します (**userid** は、ログインで使用したユーザー名に置き換えます)。

  - **admin@apic1: remoteuser-userid> cd /mit/uni/userext/remoteuser-userid**

- **admin@apic1: remoteuser-userid> cat summary**

- CIMCを使用してパラメータを変更しないことを推奨します。問題がある場合には、CIMC管理ノードのデフォルト設定が **Dedicated Mode** であること (**Shared** ではないこと) を確認してください。**Dedicated Mode** を使用していない場合には、ファブリック ノードの検出が妨げられる場合があります。
- 変更されたプロパティとソフトウェアまたはファームウェアのバージョンがユーザの特定の Cisco APIC バージョンでサポートされている場合を除き、CIMC ユーザ インターフェイス、XML、または SSH インターフェイスを使用してソフトウェアまたはファームウェアをアップグレードしないでください。
- CIMC 設定ユーティリティで、CIMC を設定する際に、NIC モードを **Dedicated** に設定します。CIMC GUI で CIMC を設定後、以下のパラメータが設定されていることを確認します。

パラメータ（Parameters）	Settings
LLDP	VIC で無効
TPM Support	BIOS でイネーブル
TPM Enabled Status	イネーブル
TPM Ownership	所有する

- リリース 5.0(2) 以降、https を使用して Cisco APIC にログインし、https ウィンドウで Cisco APIC からログアウトせずに、同じブラウザ ウィンドウで http を使用して同じ Cisco APIC にログインしようとすると、次のエラー メッセージが表示されることがあります。

  `有効な webtoken Cookie (APIC-Cookieという名前) またはCookieに署名された署名付き要求が必要です。`

  この場合は、次のいずれかの方法を使用して問題を解決します。

  - https ウィンドウで Cisco APIC からログアウトする
  - ブラウザウィンドウで Cookie を削除する

  上記のいずれかの方法で問題を解決した後、http を使用してCisco APIC に正常にログインできるはずです。

- 初期セットアップ時に IPv4 または IPv6、またはデュアル スタック構成の選択を求められます。デュアル スタックを選択すると、Cisco APIC と、IPv4 または IPv6 アドレスでの Cisco Application Centric Infrastructure (Cisco ACI) ファブリック アウトオブバウンド管理インターフェイスへのアクセスが有効になります。次のテーブルの例では IPv4 アドレスを使用していますが、初期設定時に有効にすることを選択したどの IP アドレス設定のオプションでも使用できます。
- サブネットマスクには最低でも /19 を推奨します。

- Cisco APIC を Cisco ACI ファブリックに接続する場合には、ACI モード リーフ スイッチに 10 G インターフェイスが必要です。Cisco APIC は、40G -10G コンバータ (部品番号 CVR-QSFP-SFP10G) を使用しない限り、Cisco Nexus 9332PQ、Cisco Nexus 93180LC、または Cisco Nexus 9336C-FX2 ACI モード リーフ スイッチに直接接続することはできません。その場合、リーフ スイッチのポートは、手動での設定を行わなくても、自動ネゴシエートで 10G に切り替わります。

（注） Cisco APIC 2.2(1n) 以降では、Cisco Nexus 93180LC リーフ スイッチがサポートされています。

- ファブリック ID は、Cisco APIC のセットアップ中に設定されます。これは、ファブリックのクリーン リロードを行わない限り変更できません。ファブリック ID を変更するには、Cisco APIC 設定をエクスポートし、sam.config ファイルを変更し、Cisco APIC とリーフ スイッチ上でクリーン リロードを実行します。Cisco APIC を起動した後、Cisco APIC に設定をインポートする前に、エクスポートした設定から「fvFabricExtConnP」設定を削除します。クラスタ内のすべての Cisco APIC は同じファブリック ID を持つ必要があります。
- デフォルトでは、ロギングは有効です。
- ログインおよびクラスタ操作の場合、デフォルト以外の HTTPS ポート（デフォルトは 443）は、レイヤ 3 物理およびレイヤ 3 仮想 APIC（ESXi および AWS）ではサポートされません。ESXi/AWS の仮想 APIC は、リリース 6.0(2) からサポートされています。

Cold Standby について (Cisco APIC クラスタ用)

Cold Standby 機能 (Cisco APIC クラスタ用) を使用すれば、クラスタ内の Cisco APIC をアクティブ/スタンバイモードで運用できます。Cisco APIC クラスタでは、指定されたアクティブ状態の Cisco APIC は負荷を共有し、指定されたスタンバイ状態の Cisco APIC はアクティブなクラスタ内の任意の Cisco APIC の置き換えとして動作することができます。

管理者ユーザは Cold Standby の機能をセットアップできます。これは Cisco APIC を初めて起動するときに行います。クラスタ内には少なくとも 3 基のアクティブ状態の Cisco APIC があり、1 基以上のスタンバイ状態の Cisco APIC があるようにすることを推奨します。アクティブな Cisco APIC をスタンバイ状態の Cisco APIC で置き換えるには、管理者ユーザーが切り替えを開始する必要があります。詳細については、『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』を参照してください。

アクティブ APIC とスタンバイ APIC のセットアップ

Cisco Application Policy Infrastructure Controller（APIC）リリース 6.0(2) 以降では、初期設定とクラスタの呼び出し GUI を使用します詳細については、GUI を使用した Cisco APIC クラスタの呼び出し （16 ページ） の手順を参照してください。

表 *4:* アクティブな *APIC* のセットアップ

名前	説明	デフォルト値
ファブリック名	ファブリック ドメイン名	ACI Fabric1
ファブリック ID	ファブリック ID	1
アクティブなコントローラの数	クラスタ サイズ	3 （注） アクティブ スタンバイ モードで Cisco APICを設定する場合には、クラスタ内に少なくとも 3 つのアクティブな Cisco APIC が必要です。
ポッド ID	ポッド ID	1
スタンバイ コントローラ	スタンバイ コントローラのセットアップ	NO
コントローラ ID	アクティブな Cisco APIC インスタンスに対する一意の ID 番号です。	有効な範囲は 1 ～ 132 です。
スタンドアロン APIC クラスタ	クラスタはファブリックに直接接続されていませんが、レイヤ3ポッド間ネットワーク（IPN）によって接続されています。Cisco APICこの機能は、Cisco APIC リリース 5.2（1）以降でのみ使用できます。	いいえ 追加の設定手順については、ナレッジベースの記事 「*Deploying APIC Cluster Connectivity to the Fabric Over a Layer 3 Network*」 を参照してください。
コントローラ名	アクティブなコントローラの名前	apic1

名前	説明	デフォルト値
トンネル エンドポイント アドレス用の IP アドレス プール	トンネル エンドポイント アドレス プール	10.0.0.0/16 この値は、インフラストラクチャ仮想ルーティングおよび転送（VRF）専用です。 このサブネットは、ネットワークの他のルートのサブネットと重複させることはできません。このサブネットが別のサブネットと重複した場合、このサブネットを他の /16 のサブネットに変更します。3 Cisco APIC クラスタについて最小のサポートされているサブネットは /23 です。リリース 2.0(1) を使用している場合には、最小は/22 です。 172.17.0.0/16サブネットは、docker0 インターフェイスとのアドレス空間の競合のため、インフラ TEP プールではサポートされません。インフラ TEP プールに172.17.0.0/16サブネットを使用する必要がある場合は、Cisco APICs をクラスタに配置する前に、docker0 の IP アドレスをそれぞれの異なる Cisco APIC アドレス空間に手動で設定する必要があります。
インフラストラクチャ ネットワークの VLAN ID [1]	仮想スイッチを含む Cisco APIC/スイッチ間の通信用のインフラストラクチャ VLAN （注） Cisco APIC での使用専用にこの VLAN を予約します。 インフラストラクチャ VLAN ID は、現在の環境外では使用できません。また他のプラットフォーム上の他の予約された VLAN と重複できません。	

名前	説明	デフォルト値
ブリッジ ドメイン マルチキャスト アドレス (GIPO) の IP アドレス プール	ファブリック マルチキャストで使用する IP アドレスです。 Cisco APIC (Cisco ACI マルチサイト 内のもの) のトポロジでは、この GIPo アドレスをサイト全体で同じものにすることができます。	225.0.0.0/15 有効な範囲：225.0.0.0/15 ～ 231.254.0.0/15、prefixlen は 15（128k IP）でなければなりません。
アウトオブバンド管理用の IPv4/IPv6 アドレス	GUI、CLI、または API を通じて Cisco APIC にアクセスするためにユーザが使用する IP アドレス。 このアドレスは、カスタマーの VRF からの予約アドレスである必要があります。	—
デフォルト ゲートウェイの IPv4/IPv6 アドレス	アウトオブバンド管理を使用した外部ネットワークへの通信用のゲートウェイ アドレス	—
管理インターフェイスの速度/デュプレックス モード	アウトオブバンド管理インターフェイスのインターフェイス速度とデュプレックス モード	auto 有効な値は、次のとおりです。 • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full
強力なパスワードの確認	強力なパスワードをチェックします。	[Y]

名前	説明	デフォルト値
パスワード	システム管理者のパスワード このパスワードは、1つの特殊文字を含む 8 文字以上にする必要があります。	—

[1] 最初の APIC セットアップ後に VLAN ID を変更するには、設定をエクスポートし、新しいインフラストラクチャ VLAN ID でファブリックを再構築して、ファブリックが古いインフラストラクチャ VLAN ID に戻らないように構成をインポートします。「エクスポートおよびインポートを使用して設定状態を復元する」の KB 記事を参照してください。

表 *5:* スタンバイ *APIC* のセットアップ

名前	説明	デフォルト値
ファブリック名	ファブリック ドメイン名	ACI Fabric1
ファブリック ID	ファブリック ID	1
アクティブなコントローラの数	クラスタ サイズ	3 （注） アクティブ スタンバイ モードで Cisco APICを設定する場合には、クラスタ内に少なくとも 3 つのアクティブな Cisco APIC が必要です。
ポッド ID	ポッドの ID	1
スタンバイ コントローラ	スタンバイ コントローラのセットアップ	Yes
スタンバイ コントローラ ID	スタンバイ状態の Cisco APIC インスタンスに対する一意の ID 番号です。	推奨範囲: > 20
コントローラ名	スタンバイ状態のコントローラの名前	該当なし

名前	説明	デフォルト値
トンネル エンドポイント アドレス用の IP アドレス プール	トンネル エンドポイント アドレス プール	10.0.0.0/16 この値は、インフラストラクチャ仮想ルーティングおよび転送（VRF）専用です。 このサブネットは、ネットワークの他のルートのサブネットと重複させることはできません。このサブネットが別のサブネットと重複した場合、このサブネットを他の /16 のサブネットに変更します。3 Cisco APIC クラスタについて最小のサポートされているサブネットは /23 です。リリース 2.0(1) を使用している場合には、最小は/22 です。
インフラストラクチャ ネットワークの VLAN ID [2]	仮想スイッチを含む Cisco APIC/スイッチ間の通信用のインフラストラクチャ VLAN （注） Cisco APIC での使用専用にこの VLAN を予約します。 インフラストラクチャ VLAN ID は、現在の環境外では使用できません。また他のプラットフォーム上の他の予約された VLAN と重複できません。	
アウトオブバンド管理用の IPv4/IPv6 アドレス	GUI、CLI、または API を通じて Cisco APIC にアクセスするためにユーザが使用する IP アドレス。 このアドレスは、カスタマーの VRF からの予約アドレスである必要があります。	—
デフォルト ゲートウェイの IPv4/IPv6 アドレス	アウトオブバンド管理を使用した外部ネットワークへの通信用のゲートウェイ アドレス	—

名前	説明	デフォルト値
管理インターフェイスの速度/デュプレックス モード	アウトオブバンド管理インターフェイスのインターフェイス速度とデュプレックス モード	auto 有効な値は、次のとおりです。 • auto • 10baseT/Half • 10baseT/Full • 100baseT/Half • 100baseT/Full • 1000baseT/Full
強力なパスワードの確認	強力なパスワードをチェックします。	[Y]
パスワード	システム管理者のパスワード このパスワードは、1つの特殊文字を含む 8 文字以上にする必要があります。	—

[2] 最初の APIC セットアップ後に VLAN ID を変更するには、設定をエクスポートし、新しいインフラストラクチャ VLAN ID でファブリックを再構築して、ファブリックが古いインフラストラクチャ VLAN ID に戻らないように構成をインポートします。「エクスポートおよびインポートを使用して設定状態を復元する」の KB 記事を参照してください。

例

次は、コンソールに表示される初期設定ダイアログの出力例です。

（注） **APIC クラスタの呼び出し** GUI を使用する代わりに、REST API を使用してクラスタをブートストラップおよび起動できます。詳細については、*Cisco APIC REST API* 設定ガイドを参照してください。

Cisco APIC リリース 6.0(2) 以降では、出力例の質問は含まれていません。Cisco APIC クラスタをブートストラップして起動するには、GUI を使用します。詳細については、「GUI を使用した Cisco APIC クラスタの呼び出し （16 ページ）」の手順を参照してください。

```
Cluster configuration ...
  Enter the fabric name [ACI Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-9) [1]:
  Is this a standby controller? [NO]:
```

```
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: apic-1
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (2-4094): 3914
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]:
  Enter the IPv4 address [192.168.10.1/24]: 172.31.1.2/24
  Enter the IPv4 address of the default gateway [None]: 172.31.1.1
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:

Cluster configuration ...
  Fabric name: ACI Fabric1
  Fabric ID: 1
  Number of controllers: 3
  Controller name: apic-1
  POD ID: 1
  Controller ID: 1
  TEP address pool: 10.0.0.0/16
  Infra VLAN ID: 3914
  Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
  Management IP address: 172.31.1.2/24
  Default gateway: 172.31.1.1
  Interface speed/duplex mode: auto

admin user configuration ...
  Strong Passwords: Y
  User name: admin
  Password: ********

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool
         cannot be changed later, these are permanent until the
         fabric is wiped.

Would you like to edit the configuration? (y/n) [n]:
```

GUI を使用した Cisco APIC クラスタの呼び出し

Cisco APIC リリース 6.0(2) 以降、クラスタの初期セットアップとブートストラップ手順が簡素化され、クラスタ起動用の GUI 画面が追加されました。**APIC クラスタの呼び出し** GUI は、仮想と物理 APIC プラットフォームをサポートします。仮想 APIC（ESXi または AWS を使用して展開）と物理 APIC は、リーフ スイッチに直接 ACI ファブリックに接続することも、レイヤ 3 ネットワークを介してリモート接続することもできます。GUI は両方のシナリオをサポートしています。**APIC クラスタ呼び出し** GUI を使用する主な利点は、クラスタ内のすべての APIC のパラメータを入力する必要がないことです。1 つの APIC は、クラスタの他の APIC に情報をリレーできます。

または、REST API を使用して初期設定とクラスタの起動を実行できます。『APIC REST API Configuration Procedures』ガイドの「*Getting Started*」セクションを参照してください。

始める前に

- ESXi 上の仮想 APIC の場合は、VMware vCenter GUI で OVF テンプレートを使用して Cisco APIC VM の展開を完了してください。3 ノード クラスタの場合は、管理 IP アドレス、ゲートウェイ、および管理者パスワードを使用して 3 つの VM を設定します。VM の数は、Cisco APIC クラスタのサイズによって異なります。
- AWS での仮想 APIC の場合は、AWS GUI でクラウド形成テンプレート（CFT）を使用して Cisco APIC VM の展開を完了してください。AWS は、仮想の APIC EC2 インスタンスのネットワークアダプタに対応するように、アウトオブバンド（OOB）/インフラ/インバンドサブネットから IP アドレスを動的に割り当てます。
- 仮想 APIC の場合（AWS/ESXi を使用して展開）、管理者パスワードがクラスタ内のすべての Cisco APIC で同じであることを確認します。
- 物理 APIC クラスタの場合、APIC1 の OOB アドレスを構成します。APIC の CIMC アドレス 2 ～ *N*（N はクラスタ サイズ）が APIC 1 の OOB アドレスを介して到達可能であることを確認します。
- アウトオブバンドと CIMC 間の接続は必須です。

制限事項

- AWS を使用して展開された仮想 APIC では IPv6 アドレスはサポートされません。
- ログインおよびクラスタ操作の場合、デフォルト以外の HTTPS ポート（デフォルトは 443）は、リモート接続された Cisco APIC（物理および仮想）ではサポートされません。

手順

ステップ 1 *https://APIC1-IP* を使用して APIC 1 にログインします。

a) 仮想 APICの場合：

ESXi（OVF テンプレート）またはリモート AWS（CFT）を使用した仮想 APIC の展開が完了している場合は、次の例のような出力が VM コンソールに表示されます。

```
System pre-configured successfully.
Use: https://172.31.1.2 to complete the bootstrapping.
```

ブートストラップ GUI にアクセスするための IP アドレス（**[APIC Cluster Bringup]**）は、例に示すように明示的に示されます。ステップ 2 に進むことができます。

AWS に Cisco APIC を展開した後、OOBMgmt IP アドレスを手元に置いて、**クラスタの起動** GUI にアクセスします。OOB 管理 IP アドレスは、AWS GUI の **[スタック出力（Stacks Outputs）]** タブから取得できます。

b) 物理 APIC：

CIMC を使用して APIC 1 KVM コンソールにログインします。次のような画面が表示されます。

```
APIC Version: 6.0(2a)
Welcome to Cisco APIC Setup Utility
Press Enter Or Input JSON string to bootstrap your APIC node.
```

KVM に黒い画面しか表示されない場合は、SSH を使用して CIMC に接続し、Serial over LAN（SoL）（「connect host」）を使用してコンソールに接続します。

APIC 1 で **Enter** を押し、要求された情報を入力します。ブートストラップ GUI（**APIC Cluster Bringup**）にアクセスするための IP アドレスが明示的に示されます。

```
admin user configuration ...
  Enter the password for admin [None]:
  Reenter the password for admin [None]:
Out-of-band management configuration ...
  Enter the IP Address [192.168.10.1/24]: 172.20.7.79/23
  Enter the IP Address of default gateway [192.168.10.254]: 172.20.6.1
Would you like to edit the configuration? (y/n) [n]:
System pre-configured successfully.
Use: https://172.20.7.79 to complete the bootstrapping
```

上記の IP アドレスは例です。IP アドレスは、展開環境によって異なる場合があります。

ステップ 2 OOB アドレスを使用して、**APIC クラスタの呼び出し** GUI にログインします。

ステップ 3 **[ワークフローの選択（Select Workflow）]** 画面で、**[新しいクラスタ（New cluster）]** を選択し、**[次へ（Next）]**をクリックします。

（注）
ワークフローの選択は、リリース 6.1（3）以降からのみです。

GUI 画面には 4 つの部分があります。以下の画面の詳細を入力します。

- Connection Type
- クラスタの詳細
- コントローラ登録
- サマリー

上記の各画面については、以降の手順で詳しく説明します。画面は、1、2、3、4 の連続番号でステップとしてマークされます。これらの各画面で必要な詳細を入力して保存すると、番号がチェックマークに置き換えられます。

ステップ 4 最初のステップは、**接続タイプ**情報を入力することです。**[接続タイプ（Connection Type）]** 画面で、APIC とファブリック間の接続のタイプを選択します。

次のオプションがあります。

- リーフ スイッチ（ACI ファブリック）に直接接続されます
- レイヤ 3 ネットワーク経由でリモート接続

AWS を使用した仮想化 APIC の場合、システムは APIC がレイヤ 3 ネットワークを介してリモート接続されていることを検出し、**[クラスタの詳細（Cluster Details）]** 画面に直接進みます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 2 番目のステップでは、**[クラスタの詳細（Cluster Details）]** を入力します。**[クラスタの詳細（Cluster Details）]** 画面にファブリックレベルの詳細を入力します。

- [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。
- [クラスタ サイズ（Cluster Size）]：表示されるデフォルトのクラスタサイズは、推奨される最小クラスタサイズである「3」です。この値は、クラスタ サイズに基づいて変更できます。サポートされる値は、1、3、4、5、6、7、8、および 9 です。
- GiPo プール：ファブリック マルチキャストで使用する IP アドレスを入力します。デフォルトのアドレスは 225.0.0.0/15 です。範囲は 225.0.0.0/15 ～ 231.254.0.0/15 です。prefixlen は 15（128k の IP アドレス）である必要があります。

  構成の完了後にこの値を変更することはできません。この値を変更する必要がある場合は、ファブリックのワイプが必要です。
- [ポッド ID（Pod ID）]：（直接接続された APIC（仮想および物理）にのみ適用）ポッド ID が表示されます。初めての APIC 場合は、「1」が自動的に入力されます。クラスタの後続の APIC は、任意のポッド番号に関連付けることができます。

  リモート接続された APIC の場合、ポッドは 0 です。
- [TEP プール（TEP Pool）]：（直接接続された APIC（ESXi 仮想 APIC および物理APIC）にのみ適用）は、内部ファブリック通信に使用されるアドレスのサブネットを入力します。使用されるサブネットのサイズは、ポッドのスケールに影響します。

  構成の完了後にこの値を変更することはできません。この値を変更する必要がある場合は、ファブリックのワイプが必要です。
- [インフラストラクチャ VLAN（Infrastructure VLAN）]：ファブリック接続用の VLAN ID（インフラ VLAN）を入力します。この VLAN ID は、ACI にのみ割り当てられ、ネットワーク内の他のレガシー デバイスでは使用されませんデフォルト値は 3914 です。範囲は 0 ー 4093 です。

  構成の完了後にこの値を変更することはできません。この値を変更する必要がある場合は、ファブリックのワイプが必要です。
- [Enable IPv6 on APICs]（AWS の仮想 APIC には適用されません）：アウトオブバンド管理の IPv6 アドレスを有効にする場合は、このチェックボックスをオンにします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 3 番目のステップでは、**コントローラ登録**の詳細を入力します。**[コントローラの追加（Add Controller）]** をクリックして、（クラスタの）最初の APIC を追加します。次の詳細を入力します。

- [コントローラ タイプ（Controller Type）]：ブートストラップ手順は、構成が実行されている展開を自動検出します。それに基づいて、**[仮想（Virtual）]**または**[物理（Physical）]**が選択されます。仮想コントローラ タイプと物理コントローラ タイプに表示されるオプションについては、それぞれサブステップ（a）と（b）で説明します。コントローラのタイプに基づいて、次のサブステップのいずれかを実行します。

a) コントローラタイプが **仮想（Virtual）** の場合：

- [仮想インスタンス（Virtual Instance）]：APIC クラスタ呼び出し GUI へのアクセスに使用される管理 IP。最初の場合にのみ、この IP アドレスは自動入力されます。APIC その後クラスタに追加するノードについては、管理 IP アドレスを入力して **[検証（Validate）]** をクリックする必要があります。

  管理 IP アドレスは、ESXi/AWS を使用した VM の展開時に定義されます。前提条件で説明したように、クラスタを起動している間は、必要なすべての IP アドレスを手元に置いておいてください。

- [一般（General）] ペイン
  - [名前（Name）]：コントローラのユーザー定義名。
  - [コントローラ ID（Controller ID）]：ID は自動入力されます。これがクラスタの最初の APIC の場合、ID は「1」です。クラスタの 2 番目のコントローラを追加する場合は、「2」が自動的に入力されます（以下同様）。
  - [ポッド ID（Pod ID）]：（ESXi で直接接続された仮想 APIC にのみ適用されます）ポッド ID は、クラスタの APIC 1 に自動入力されます。クラスタの後続のコントローラの場合は、値を入力します。有効な範囲は 1 ～ 128 です。
  - [シリアル番号（Serial Number）]：仮想マシンのシリアル番号は自動入力されます。

- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4 アドレス（IPv4 Address）]：IP アドレスが表示されます（展開時に定義）。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：IP アドレスが表示されます（展開時に定義されます）。

  すでに（ステップ 5）で OOB 管理用に IPv6 アドレスを有効にしている場合は、IPv6 アドレスとゲートウェイを入力します。

- [インフラストラクチャ L3 ネットワーク（Infra L3 Network）]ペイン（このペインは、以前に選択した **[接続タイプ（Connection Type）]** が *[L3* ネットワークを介してリモート接続（*Remotely attach*）*]* である場合にのみ表示されます。
  - [IPv4 アドレス（IPv4 Address）]：インフラ ネットワーク アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイの IP アドレスを入力します。
  - [VLAN]：（リモート接続された仮想APIC - ESXi にのみ適用）使用するインターフェイス VLAN ID を入力します。

AWS を使用して仮想 APIC を展開する場合、[インフラ L3 ネットワーク（Infra L3 Network）] ペインは表示されません。

最初の APIC 詳細を入力して保存したら、**[コントローラの登録（Controller Registration）]** 画面で **[コントローラの追加（Add Controller）]** をクリックして、クラスタに別の APIC を追加します。

b) コントローラタイプが **[物理（Physical）]** の場合：

- CIMCの詳細ペイン
  - [IPアドレス（IP Address）]：CIMC の IP アドレス。最初の Cisco APIC の場合にのみ、この IP アドレスは自動入力されます。クラスタにコントローラを追加する場合は、CIMC IP アドレスを入力する必要があります。
  - [ユーザー名（Username）]：CIMC にアクセスするためのユーザー名。ユーザー名は自動的に入力されます（最初のコントローラと後続のコントローラの場合）。
  - [パスワード（Password）]：CIMC にアクセスするためのパスワードを入力します。最初のコントローラの場合、パスワードは自動的に入力されます。後続のコントローラの場合は、パスワードを入力します。
  - [**Validate**] をクリックします。認証が成功すると、検証成功が表示されます。

    CIMC NIC モード設定が原因で Cisco APIC アウトオブバンド管理 IP アドレスから CIMC に到達できない場合は、NIC モードを変更するか、JSON 文字列を入力してブートストラップを実行します。

- [一般（General）] ペイン
  - [名前（Name）]：コントローラの名前を入力します。
  - [コントローラ ID（Controller ID）]：クラスタの最初のコントローラの場合、「1」が自動入力されます。2 番目のコントローラの場合は、「2」が自動的に入力され、以降も同様です（昇順）。
  - [ポッド ID（Pod ID）]：（APIC に直接接続されたにのみ適用）クラスタの APIC1 にポッド ID が自動入力されます。クラスタの後続のコントローラの場合は、値を入力します。有効な範囲は 1 ～ 128 です。
  - [シリアル番号（Serial Number）]：シリアル番号は、CIMC 検証後に自動入力されます（APIC が 1 ～ N の場合、N はクラスタ サイズです）。

    APIC 1 は、CIMC IP アドレスの到達可能性を確認し、新しい APICのシリアル番号もキャプチャします。

- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4アドレス（IPv4 Address）]：APIC 1 の場合、アドレスは自動入力されます。後続の APIC では、IP アドレス（展開時に定義）を入力します。

- [IPv4 ゲートウェイ（IPv4 Gateway）]：APIC 1 の場合、ゲートウェイ アドレスは自動入力されます。後続の APIC では、IP アドレス（展開時に定義）を入力します。

すでに（ステップ 5）で OOB 管理用に IPv6 アドレスを有効にしている場合は、IPv6 アドレスとゲートウェイを入力します。

- [インフラストラクチャ L3 ネットワーク（Infra L3 Network）]ペイン（このペインは、以前に選択した **[接続タイプ（Connection Type）]** が [レイヤ 3 ネットワークを介してリモート接続（Remotely attach）] である場合にのみ表示されます。
  - [IPv4 アドレス（IPv4 Address）]：インフラ ネットワークの IP アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイのインフラ ネットワーク IP アドレスを入力します。
  - [VLAN ID]：VLAN ID を入力します。

[コントローラの登録（Controller Registration）] 画面で、最初の APIC の詳細を入力して保存した後、**[コントローラの追加（Add Controller）]** をクリックして、クラスタに別の APIC コントローラを追加します。

（オプション、仮想 APIC にのみ適用）**[コントローラ登録（Controller Registration）]** 画面で、**[既存のセキュリティ証明書のインポート（Import existing security certificates）]** チェックボックスをオンにして、仮想 APIC のファブリック リカバリ用に既存のセキュリティ証明書をインポートします。チェックボックスをオンにした後、次のフィールドに必要な詳細を入力します。

- 構成ファイルを含む**リモート サーバーの IP アドレス**。
- 構成ファイルを含む**リモート パス**。
- 構成**ファイル名**。
- 構成のバックアップ中に以前に使用された**AES暗号化パスフレーズ**。バックアップ構成ファイルは、このキー（パスフレーズ）にリンクされます。
- **プロトコル** を選択します。選択できる基準は、次のとおりです。
  - **FTP**
  - **SFTP**
  - **SCP**
- **[リモート ポート（Remote Port）]**
- （SFTP および SCP **プロトコル**にのみ適用）**[認証タイプ（Authentication Type）]** を選択します。選択できる基準は、次のとおりです。
  - **パスワードを使用**

- **SSH 秘密キー ファイルの使用**

  - **username**：リモート サーバーへのアクセスに必要なユーザー名です。
  - リモート サーバーへの認証を受ける **パスワード（Password）** 。
  - （[SSH 秘密キー ファイルを使用する**認証タイプ**（Use SSH Private Key Files Authentication Type）] にのみ適用）ここに **SSH キーの内容**を入力します。
  - （[SSH 秘密キー ファイルを使用する**認証タイプ**（Use SSH Private Key Files Authentication Type）] にのみ適用）秘密キーの暗号化に使用する **SSH キー パスフレーズ**を指定します。

    インポート/エクスポート手順の詳細については、『Cisco ACI Configuration Files：Import and Export』を参照してください。

[既存のセキュリティ証明書のインポート（Import existing security certificates）] は、仮想 APIC（AWS/ESXi を使用して展開）にのみ適用されます。物理 APIC には組み込みの証明書があります。ただし、仮想 APIC の場合、ファブリックを回復するためにバックアップ設定を使用して復元する場合、既存のセキュリティ証明書を再利用できます。

ステップ 9 **[次へ (Next)]** をクリックします。

[次へ（Next）] ボタンは、クラスタのすべてのコントローラが追加されるまで無効になります。これは、**[クラスタの詳細（Cluster Details）]** 画面の **[クラスタ サイズ（Cluster Size）]** に入力した値によって定義されます。

[戻る（Back）] ボタンを使用して、前の画面に移動できます。APIC を追加したら、**[詳細の編集（Edit Details）]** をクリックして APIC の情報を編集します。最初の APIC を除き、必要に応じて、削除アイコンをクリックして他のコントローラを削除できます。

ステップ 10 **[概要（Summary）]** 画面で更新を確認し、**[展開（Deploy）]** をクリックします。

ステップ 11 **[クラスタ ステータス（Cluster Status）]** ページが表示され、クラスタ形成の現在のステータスが示されます。数分待つと、標準 Cisco APIC GUI に自動的にリダイレクトされます。

APIC の IPv6 管理アドレスのプロビジョニング

IPv6 管理アドレスは、セットアップ時や、Cisco APIC が動作中になった際にポリシーによって、Cisco Application Policy Infrastructure Controller（APIC）にプロビジョニングできます。純粋な IPv4、純粋な IPv6、またはデュアル スタック（つまり IPv6 と IPv4 アドレス両方）がサポートされます。セットアップ中に帯域外管理インターフェイスのデュアル スタック（IPv6 および IPv4）アドレスをセットアップする方法を説明する一般的なセットアップ画面のスニペットを以下に示します。ただし、次の質問事項は、6.0(2) より前のリリースに適用されます。Cisco APIC リリース 6.0(2) から、クラスタの起動は上記の GUI を使用します。

```
Cluster configuration …

  Enter the fabric name [ACI Fabric1]:
  Enter the number of controllers in the fabric (1-9) [3]:
```

```
  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: infraipv6-ifc1
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
        and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (1-4094): 3914
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]: Y (Enter Y to Configure IPv6 Address
 for Out of Band Management Address)
  Enter the IPv6 address [0:0:0:0:0:ffff:c0a8:a01/40]:
2001:420:28e:2020:0:ffff:ac1f:88e4/64 (IPv6 Address)
  Enter the IPv6 address of the default gateway  [None]:
2001:420:28e:2020:acc:68ff:fe28:b540 (IPv6 Gateway)
  Enable IPv4 also for Out of Band Mgmt Interface? [Y]: (Enter Y to Configure IPv4 Address
 for Out of Band Management Address)
  Enter the IPv4 address [192.168.10.1/24]: 172.31.136.228/21 (IPv4 Address)
  Enter the IPv4 address of the default gateway [None]: 172.31.136.1 (IPv4 Gateway)
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Reenter the password for admin:
```

（注） **APIC クラスタ呼び出し** GUI の使用中に、**[IPv6 の有効化（Enable IPv6）]** オプションを選択して IPv6 アドレスを使用できます。

GUI へのアクセス

手順

ステップ 1 サポートされているブラウザの 1 つを開きます。

- Chrome バージョン 59（またはそれ以後）
- Firefox バージョン 54（またはそれ以後）
- Internet Explorer バージョン 11（またはそれ以後）
- Safari バージョン 10（またはそれ以後）

（注）
既知の問題が Safari ブラウザおよび未署名の証明書に存在します。WebSockets で使用するために未署名の証明書を受け入れる前に、ここで示す情報をお読みください。HTTPS のサイトにアクセスすると、次のメッセージが表示されます。

“Safari can’t verify the identity of the website APIC. The certificate for this website is invalid. You might be connecting to a website that is pretending to be an APIC, which could put your confidential information at risk. Would you like to connect to the website anyway?”

WebSockets が接続できることを保証するには、次の手順を実行します。

[Show Certificate] をクリックします。

表示される 3 つのドロップダウン リストで [Always Trust] を選択します。

これらの手順に従わないと、WebSockets は接続できません。

ステップ 2 URL を入力します。**https://***mgmt_ip-address*

初期設定時に設定したアウトオブバンド管理 IP アドレスを使用します。たとえば、https://192.168.10.1 などがこれに該当します。

（注）
https だけがデフォルトでイネーブルになっています。デフォルトでは、http および http から https へのリダイレクションがディセーブルになっています。

（注）
Cisco APIC にログインするときに次のエラー メッセージが表示される場合：

```
Need a valid webtoken cookie (named APIC-Cookie) or a signed request with signature in
the cookie.
```

これは、https と http の両方を使用して Cisco APIC にログインするときに発生する既知の問題が原因です。この問題と回避策の詳細については、Cisco APIC のセットアップ （6 ページ）の「重要事項」を参照してください。

ステップ 3 ログイン画面が表示されたら、初期設定時に設定した管理者名とパスワードを入力します。

ステップ 4 [Domain] フィールドで、ドロップダウン リストから、定義した適切なドメインを選択します。

複数のログイン ドメインが定義されている場合、[Domain] フィールドが表示されます。ユーザがドメインを選択しないと、デフォルトで DefaultAuth のログイン ドメインが認証に使用されます。この場合、DefaultAuth のログイン ドメインにユーザ名がないとログインに失敗する可能性があります。

次のタスク

アプリケーション セントリック インフラストラクチャ ファブリック および Application Policy Infrastructure Controller の機能および処理については、ホワイト ペーパーや、『*Cisco Application Centric Infrastructure Fundamentals Guide*』を参照してください。

REST API へのアクセス

手順

スクリプトまたはブラウザベースの REST クライアントを使用して、次の形式の API POST または GET メッセージを送信できます。**https://***apic-ip-address*/**api/***api-message-url*

初期設定時に設定したアウトオブバンド管理 IP アドレスを使用します。

（注）
- https だけがデフォルトでイネーブルになっています。デフォルトでは、http および http から https へのリダイレクションがディセーブルになっています。
- API セッションを開始するために認証メッセージを送信する必要があります。初期設定時に設定した管理者ログイン名とパスワードを使用します。

NX-OS スタイル CLI へのアクセス

端末から直接または APIC GUI で、APIC NX-OS スタイル CLI にアクセスできます。

NX-OS スタイルの CLI コマンドを使用する方法の詳細についてを参照してください、 *Cisco APIC NX-OS* スタイル コマンド ライン インターフェイス コンフィギュレーション ガイド 、および *Cisco APIC NX-OS* スタイル *CLI* コマンド リファレンス 。

ガイドラインと、APIC NX-OS スタイル CLI の制限事項

- CLI は、管理者としてログイン権限を持つユーザに対してのみサポートされます。
- APIC NX-OS スタイルの CLI は、Cisco NX-OS CLI と類似したシンタックスや他の規則を使用しますが、APIC オペレーティング システムは Cisco NX-OS ソフトウェアの 1 バージョンでというわけではありません。Cisco NX-OS CLI コマンドが APIC CLI で動作するわけでも、同じ機能を使用できるわけでもありませんので注意してください。
- Cisco ACI 設定では、FIPS が有効である場合 SHA256 サポートは、SSH クライアントに必須です。さらに、SHA256 サポートを表示するには、openssh クライアントする必要が稼働しているバージョン 6.6.1 以降。
- Cisco APIC リリース 1.2 以前のリリースでは、デフォルト CLI は管理対象オブジェクト（MO）および管理情報モデルのプロパティから上で直接動作するコマンドの Bash シェルでした。Cisco APIC リリース 1.2 以降のデフォルト CLI は NX-OS スタイル CLI です。オブジェクト モデル CLI は、最初の CLI プロンプトで **bash** コマンドを入力することにより使用できます。

端末から NX-OS スタイル CLI へのアクセス

手順

ステップ 1 セキュア シェル（SSH）クライアントから、*username*@ip-address の APIC への SSH 接続を開きます。

初期設定時に設定した管理者のログイン名とアウトオブバンド管理 IP アドレスを使用します。たとえば、admin@192.168.10.1 などがこれに該当します。

ステップ 2 プロンプトが表示されたら、管理者パスワードを入力します。

次のタスク

NX-OS スタイル CLI を入力する場合、最初のコマンド レベルは EXEC レベルになります。EXEC モードのままにするか、**configure** を入力して、グローバル コンフィギュレーション モードに入ります。どのモードでも、**?** を入力すれば、使用可能なコマンドを参照できます。

NX-OS スタイルの CLI コマンドを使用する方法の詳細については、「*Cisco APIC NX-OS* スタイル コマンド ライン インターフェイス設定ガイド」および「*Cisco APIC NX-OS* スタイル *CLI* コマンド リファレンス」を参照してください。

GUI から NX-OS スタイル CLI へのアクセス

手順

ステップ 1 メニュー バーで、**System > Controllers** を選択します。

ステップ 2 ナビゲーション ペインで **Controllers** を選択します。

ステップ 3 対象とする APIC を右クリックして、**Launch SSH** を選択します。

ステップ 4 画面上に指示に従って、選択したコントローラへの SSH セッションを開きます。

次のタスク

NX-OS スタイル CLI を入力する場合、最初のコマンド レベルは EXEC レベルになります。EXEC モードのままにするか、**configure** を入力して、グローバル コンフィギュレーション モードに入ります。どのモードでも、**?** を入力すれば、使用可能なコマンドを参照できます。

NX-OS スタイルの CLI コマンドを使用する方法の詳細については、「*Cisco APIC NX-OS* スタイル コマンド ライン インターフェイス設定ガイド」および「*Cisco APIC NX-OS* スタイル *CLI* コマンド リファレンス」を参照してください。

オブジェクト モデル CLI へのアクセス

（注） Cisco APIC リリース 1.2 以前のリリースでは、デフォルト CLI は管理対象オブジェクト（MO）および管理情報モデルのプロパティから上で直接動作するコマンドの Bash シェルでした。Cisco APIC リリース 1.2 以降のデフォルト CLI は NX-OS スタイル CLI です。オブジェクト モデル CLI は、最初の CLI プロンプトで **bash** コマンドを入力することにより使用できます。

手順

ステップ 1 セキュア シェル (SSH) クライアントから、*username@ip-address* への SSH 接続を開きます。

初期設定時に設定した管理者のログイン名とアウトオブバンド管理 IP アドレスを使用します。たとえば、`ssh admin@192.168.10.1` と入力します。

ステップ 2 入力を求められた場合は、初期設定時に設定した管理者パスワードを入力します。

現在 APIC 用の NX-OS スタイル CLI です。

ステップ 3 オブジェクト モデル CLI を入力するには、**bash** と入力します。

ステップ 4 NX OS スタイル CLI に戻るには、**exit** と入力します。

次の例では、オブジェクト モデル CLI にする方法、および NX-OS スタイル CLI に戻す方法を示しています。

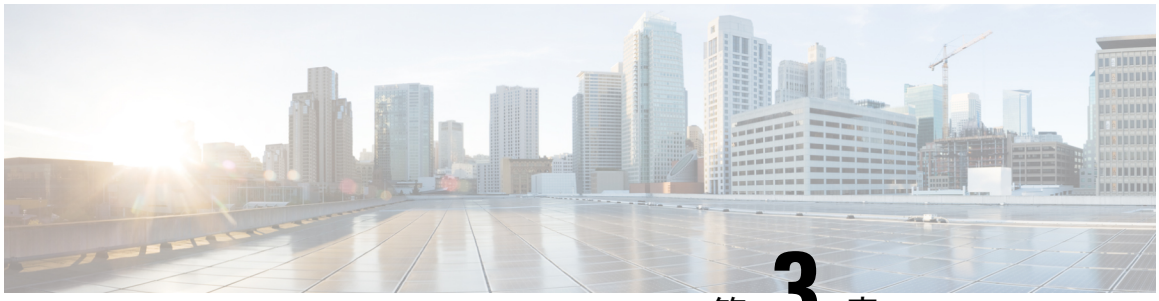
```
$ ssh admin@192.168.10.1
Application Policy Infrastructure Controller
admin@192.168.10.1's password: cisco123
apic#             <---- NX-OS style CLI prompt
apic# bash
admin@apic1:~>    <---- object model CLI prompt
admin@apic1:~> exit
apic#
```

次のタスク

すべてのユーザが /home と呼ばれる共有ディレクトリを使用する必要があります。このディレクトリでは、ディレクトリとファイルを作成する権限がユーザに与えられます。/home 内で作成されたファイルはデフォルトの umask 権限を継承し、ユーザおよび root としてアクセスできます。ユーザは、初めてのログイン時に、/home/jsmith などのファイルを保存するための /home/userid ディレクトリを作成することを推奨します。

BASH または VSH などの動作モードで ACI CLI を使用してスイッチにアクセスする方法については、『*Cisco APIC Command Line Interface User Guide*』および『*Cisco ACI Switch Command Reference*』を参照してください。

APIC CLI の設定の詳細については、『*Cisco APIC Object Model Command Line Interface User Guide*』を参照してください。



第 3 章

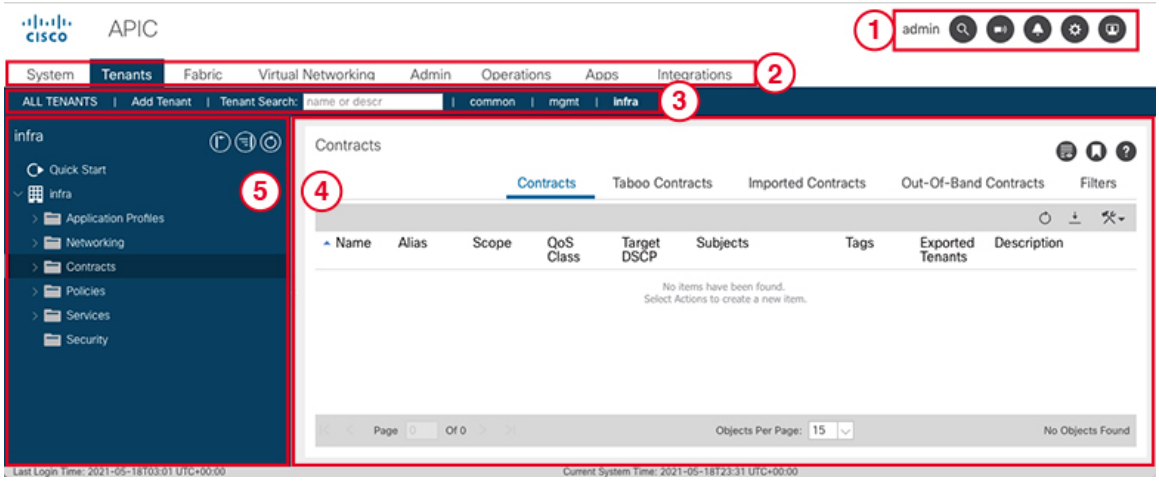
APIC GUI の概要

この章で説明する内容は、次のとおりです。

GUI の概要

APIC GUI は、ACI ファブリックの設定とモニタリングを行うための、ブラウザ ベースのグラフィカル インターフェイスです。GUI は、システム全体の論理および物理コンポーネントすべてに対し、階層的なナビゲーションを行えるように編成されています。GUI の主要なコントロール領域を次の図に示します。

図 *1 : APIC* の *GUI* 領域



これらの領域の機能は、次のリンクで説明されています:

1. メニューバーツール：を参照メニュー バーおよびサブメニュー バー （32 ページ）
2. メニューバー：を参照 メニュー バーおよびサブメニュー バー （32 ページ）
3. サブメニュー バー: メニュー バーおよびサブメニュー バー （32 ページ）
4. 作業ウィンドウ: [Work] ペイン （41 ページ）
5. ナビゲーション ウィンドウ: ナビゲーション ウィンドウ （40 ページ）

ナビゲーションウィンドウの下に最終ログインが表示され、現在のユーザが最後にログインした時の日時が表示されます。

GUI を操作して設定を変更したり情報を取得したりすると、GUI は、REST API メッセージを交換することによって、基盤であるオペレーティング システムと通信します。GUI 内の API 交換の表示 （46 ページ） で説明されている API インスペクタ ツールを使用すれば、これらの API メッセージを観察できます。

メニュー バーおよびサブメニュー バー

メニュー バーは、APIC GUI の上部に表示されます。メニュー バーでは、メインの構成タブや、検索、通知、および基本設定などのツールにアクセスできます。メニューバーのすぐ下にはサブメニュー バーがあり、各選択したメニュー バーのタブごとに、特定の構成エリアを表示します。サブメニュー バーのタブは、メニュー バーのタブごとに異なります。また特定の構成または権限レベルによっても変わります。

ヒント　APIC GUI での設定手順では、**Fabric > Fabric Policies** のような表記が用いられています。この例は、メニューバーの **Fabric** タブをクリックし、それからサブメニューバーの **Fabric Policies** タブをクリックすることを意味しています。

メニュー バーのずっと右には、次のメニュー バー ツールがあります:

メニュー バーのツール	説明
username	現在ログインしているローカル ユーザの名前。
	検索 （37 ページ）
	Multi-Site Manager の起動 （37 ページ）
	フィードバック （37 ページ）
	アラート （38 ページ）
	ツール （38 ページ）
	ヘルプ （39 ページ）
	マイ プロファイルの管理 （39 ページ）

個々のメニュー バーのタブとツールについては、続くセクションで説明します。

メニュー バーのタブ

[System] タブ

システム全体の状態のサマリー、その履歴、およびシステムレベルの障害のテーブルを収集および表示するには、**[システム]** タブを使用します。

さらに、**System** タブは次の機能を提供します。

- **System Settings** サブメニューでは、グローバル システム ポリシーを設定することができます。
- **Smart Licensing** サブメニューでは、ライセンスのステータスを表示することができます。
- **Active Sessions** サブメニューでは、ユーザ セッションを表示することができます。

[Tenants] タブ

メニュー バーの **Tenants** タブは、テナント管理を実行するために使用します。サブメニュー バーには、すべてのテナントのリスト、 **Add Tenant** リンク、および 3 つの組み込みテナントと最近使用されたテナント 2 つまでのリンクが表示されます。

- テナントには、承認されたユーザのドメインベースのアクセス コントロールをイネーブルにするポリシーが含まれます。承認されたユーザは、テナント管理やネットワーキング管理などの権限にアクセスできます。
- ユーザは、ドメイン内のポリシーにアクセスしたりポリシーを設定するには読み取り/書き込み権限が必要です。テナント ユーザは、1 つ以上のドメインに特定の権限を持つことができます。
- マルチテナント環境では、リソースがそれぞれ分離されるように、テナントによりグループ ユーザのアクセス権限が提供されます(エンドポイント グループやネットワーキングなどのため)。これらの権限では、異なるユーザが異なるテナントを管理することもできます。

組み込みのテナントは次のとおりです:

- **[common]** テナントは、ファブリックの全テナントの共通動作を指定するポリシーを定義するために事前に設定されたテナントです。共通テナントで定義されたポリシーはどのテナントでも使用可能です。
- **[infra]** テナントは、ファブリックのインフラストラクチャに関連した構成を行うための、事前に設定されたテナントです。
- **[mgmt]** テナントは、ホストとファブリック ノード(リーフ、スパイン、およびコントローラ) のインバウンドとアウトオブバウンドの接続に関連した構成を行うための、事前に設定されたテナントです。

（注） ポートのレイヤ2構成については、ポートのフィルタリングを行うために、ノードとパス フィールドに入力できます。

[Fabric] タブ

[ファブリック] タブには、サブメニュー バーに次のタブが含まれます。

- **[インベントリ]** タブ：ファブリックの個々のコンポーネントを表示します。

- **[ファブリック ポリシー]**タブ：モニタリングおよびトラブルシューティングのポリシーとファブリック プロトコルの設定またはファブリック最大伝送単位（MTU）の設定を表示します。
- [ACCESS POLICIES] タブ：システムのエッジ ポートに適用するアクセス ポリシーを表示します。これらのポートは、外部と通信するリーフ スイッチ上にあります。

[Virtual Networking] タブ

仮想マシン（VM）のさまざまなマネージャのインベントリを表示および設定するには、**[仮想ネットワーク]**タブを使用します。個別の管理システムへの接続(VMware vCenter または VMware vShield など) を設定できるさまざまな管理ドメインを設定し作成できます。これらの VM 管理システム（API のコントローラとも呼ばれます）によって管理されるハイパーバイザ および VM を表示するには、サブメニュー バーの **[インベントリ]** タブを使用します。

[Admin] タブ

認証、許可などの管理機能、アカウンティング機能、ポリシーのスケジューリング、レコードの保持と消去、ファームウェアのアップグレード、および syslog、Call Home、SNMP などの制御機能を実行するには、**[管理]** タブを使用します。

[Operations] タブ

[操作]タブには、ファブリック リソースの計画とモニタリングのためにの次の内蔵ツールが用意されています。

- **可視性 & トラブルシューティング**：ファブリックの指定されたエンドポイントの場所を示し、L4 L7 デバイスを含むトラフィック パスが表示されます。
- **容量ダッシュボード**：エンド ポイント、ブリッジ ドメイン、テナント、コンテキストなどの設定可能なリソースの使用可能な容量が表示されます。
- **EP トラッカー**：リーフ スイッチおよび FEXes に仮想およびベア メタルのエンドポイントの接続および切断を表示できます。
- **可視化**：トラフィック マップの可視化を提供します。

キャパシティ ダッシュボード

キャパシティ ダッシュボードは、エンド ポイント、ブリッジ ドメイン、テナント、コンテキストなどの設定可能なリソースの使用可能なキャパシティが表示されます。ダッシュボードには、次のタブが含まれています。

- **[ファブリック キャパシティ（Fabric Capacity）]**：ファブリック内の管理対象オブジェクトのキャパシティを表示します。各タイルには、各オブジェクトの現在のキャパシティと最大キャパシティ、および使用されている最大キャパシティのパーセンテージが表示されます。一部のタイルにカーソルを合わせると、詳細情報を表示できます。

- **[リーフ キャパシティ（Leaf Capacity）]**：Cisco Application Policy Infrastructure Controller（APIC）が管理する各リーフ スイッチの管理対象オブジェクトのキャパシティを表示します。
  - すべてのオブジェクトについて、GUIには現在のリソース使用率と最大リソースキャパシティ、および使用されている最大リソースキャパシティのパーセンテージが表示されます。
  - 一部のオブジェクトのデータは、ESG MAC アドレスのローカルとリモートなどのサブカテゴリに分割されます。
  - MAC、IPv4、およびIPv6アドレスのデータは、ローカル アドレスとリモート アドレスの合計数を示します。
  - /32 ルートおよび /128 ルートのデータは、次の情報を提供します。
    - **UC**：IPv4 /32 または /128 ユニキャスト ルートの合計。この値は、ゼロにリセットされることなく、各間隔で保持されます。
    - **EP**：IPv4 /32 または /128 エンドポイントの合計。この値は、ゼロにリセットされることなく、各間隔で保持されます。
    - **MCast**：IPv4 /32 または /128 マルチキャストルートの合計。この値は、ゼロにリセットされることなく、各間隔で保持されます。
  - **[スイッチ（Switch）]** 列の **[プロファイルの構成（Configure Profile）]** ボタンをクリックすると、そのスイッチの転送スケール プロファイルを構成できます。
  - 行の他の部分をクリックすると、そのスイッチの詳細なキャパシティ使用状況情報を表示できます。**絶対**エントリを持つリソースの場合、これは現在のリソース使用率です。/32 および /128 ルートの場合、**[絶対（Absolute）]** は、使用されているユニキャスト ルート、エンドポイント、およびマルチキャスト ルートの合計です。**パーセント** は、使用される最大のリソース キャパシティのパーセンテージです。

APIC リリース 6.1（4）以降、[容量ダッシュボード（Capacity Dashboard）] タブのパフォーマンスが大幅に向上し、ここに表示されるさまざまな要素の表示時間が短縮されました。次には、他の重大な機能の拡張されています：

- 各リソースのステータス表示は、**[リソース使用状況（Resource Usage）]**に応じて異なります。**[リソース使用状況（Resource Usage）]** 列にカーソルを合わせると、リソースの使用状況のステータスを確認できます。使用可能なステータスインジケータは次のとおりです：
  - 適合
  - アプローチ制限
  - アプローチ上限
  - 違反制限

- Opflex エージェントと Opflex レイヤ 2 エンドポイントは、**[リーフスイッチ容量（Leaf Switch Capacity）]** タブの 2 つの新しいエントリです。**[リソース使用率（Resource Usage）]** 列の下に表示されている数字をクリックすると、選択したリーフのエントリのリストが表示されます。
- [リダイレクト先モニタリング（Redirect Destination Monitoring）] は、**[ファブリック キャパシティ（Fabric Capacity）]** タブの新しいエントリです。テナント、ESG などの他の標準規格メトリックは、引き続き表示されます。

[Apps] タブ

[アプリ] タブは、APIC にインストールまたはアップロードされたすべてのアプリケーションを表示します。タブでは、APIC 管理者が APIC のパッケージ化されたアプリケーションをアップロード、アップグレード、インストール、アンインストールできます。

[インテグレーション (Integrations)] タブ

すべてのサードパーティ インテグレーションを表示するには、**[インテグレーション (Integrations)]** タブを使用します。

メニュー バーのツール

検索

検索フィールドを表示するには、[Search] アイコンをクリックします。検索フィールドでは、名前またはその他の固有フィールドによってオブジェクトを検索できます。

図 *2 :* 検索

検索機能では、ワイルドカード (*) を使用できます。

Multi-Site Manager の起動

Multi-Site Manager のアイコンをクリックして、Multi-Site Manager を起動します。Multi-Site Manager を使用すると、サイト APIC を起動できます。

図 *3 : Multi-Site Manager* の起動

フィードバック

フィードバックメニューバーアイコンをクリックして、Cisco にコメントを送信します。

図 *4 : Feedback*

アラート

アクティブなアラートのリストを表示するには、アラート メニュー バー アイコンをクリックします。システム アラートがある場合は、アラートのアイコンに数字バッジが表示され、アクティブなアラートの数を示します。重大なシステム通知がある場合は、アラートのアイコンは赤色で点滅します。アラートを表示するには、次のアイコンをクリックします。

図 *5 : [アラート（Alerts）]*

アラートのアイコンの点滅を止めるには、アラートのリストからすべての重大アラートを削除します。重大アラートの **Close** ボタンが無効になっている場合には、アラートをクリアする前に、原因となっている問題を解決する必要があることを示しています。

ツール

システム ツールにアクセスするには、次のメニュー バー アイコンをクリックし、ドロップダウンリストから項目を選択します。

図 *6 : ツール*

以下の選択項目を使用できます:

- **ACI ファブリック セットアップ（ACI Fabric Setup）** : ACI ファブリック セットアップを開きます。このパネルは、基本的な APIC インフラストラクチャをセットアップするのに役立ちます。
- **Show API Inspector** — API インスペクタを表示します。これは APIC の組み込みツールで、タスクを実行するためにやりとりされる、GUI と APIC オペレーティング システムの間の内部 API メッセージを表示できるようにします。詳細については、GUI 内の API 交換の表示 （46 ページ）を参照してください。
- **Start Remote Logging** — ロギング 情報をリモート URL に転送します。
- **Object Store Browser** — 管理対象オブジェクト ブラウザ (バイザー) を開きます。これは APIC に組み込まれているユーティリティで、管理対象オブジェクトを (MO) をブラウザによりグラフィカルに表示します。

- **Show Debug Info** — GUI の下部にステータス バーを表示します。現在の管理対象オブジェクト (MO) やシステム時刻などの情報を表示します。ステータス バーが表示されているときには、この選択項目は **Hide Debug Info** に変わります。
- **Config Sync Issues** — [設定オブジェクトの保留中の解決（Configuration Objects Pending Resolution）]パネルを開きます。このパネルは、APICでまだ有効になっていないユーザ設定可能なオブジェクトに関連するトランザクションがあるかどうかを示します。パネルの情報を使用して、デバッグに役立てることができます。

（注） グローバル システム設定は **System > System Settings** で構成できます。

ヘルプ

ヘルプ ツールにアクセスするには、次のメニュー バー アイコンをクリックし、ドロップダウンリストから項目を選択します。

図 *7:* ヘルプ

以下の選択項目を使用できます:

- **[ヘルプ（Help）]**：API ドキュメントおよび APIC へのリンクを表示します。
- **[新機能（What's New）]**：最新の機能を示すスプラッシュ画面を表示します。
- **About** — APIC のバージョンを表示します。

マイ プロファイルの管理

設定とログイン ユーザの設定 (preferences) を設定するには、次のメニュー バー アイコンをクリックしをドロップダウンリストから項目を選択します。

図 *8:* マイ プロファイルの管理

以下の選択項目を使用できます:

- **[ブックマーク（Bookmarks）]**：ユーザーが設定できるブックマーク メニューへのリンクが表示されます。

  お気に入りアイコンが表示されるメニュー ( )] アイコンをクリックしてブックマークことができます。

- **自分のパスワードを変更** : 現在ログイン中のローカルユーザのパスワードを変更します。
- **My SSH キーを変更** : 証明書ベースのログインに使用されるユーザの公開 SSH キーを変更します。
- **変更 My X509 証明書** : ログインのユーザの X.509 形式の証明書を変更します。
- **My アクセス許可を表示**]: ユーザのロール ベースの読み取りを表示し、ドメインとアクセス可能なオブジェクトの権限を記述します。
- **設定** : 全般的な GUI 設定を変更します。
  - **ツリーの選択に注意してください** : ナビゲーション ツリーを保持する GUI 拡張ウィンドウに戻るときに有効化します。たとえば、このプロパティを有効にして、テナント] タブのナビゲーション ツリーを展開すると、ファブリック] タブをクリックし、タブに戻り、テナント、ツリーが拡張されたまましょう。
  - **ツリーの区切り線の位置を保持する** : ツリー区切り線を目的の位置にドラッグすた後ツリー区切り線の位置を保持する GUI を有効にします。
  - **成功した場合に通知を無効に** : 成功ダイアログボックス通知を非表示します。
  - **ログイン時の導入警告を無効に** : 無効にする、導入警告ダイアログ ボックス ログインするときにします。導入の警告とポリシーの利用情報 （44 ページ） を参照してください。
  - **デフォルトのテーブルのページ サイズ** : GUI table size(テーブル サイズ、テーブルのサイズ) を設定します。
  - **UI のすべてのセクションを表示する** : 非表示の UI 設定オプションが表示されます。
  - **ログイン時の新表示** : 最新の機能を示す、ログイン時スプラッシュ画面を表示します。
  - **Single-Browser Session (SBS) の有効化** : APIC GUI にログインし、それぞれの新しいタブまたはウィンドウからログインすることなく、追加のブラウザ タブやウィンドウを開くことができます。「単一ブラウザ セッション管理 （44 ページ）」を参照してください。
- **展開の設定を変更する**]: 有効にし、導入通知の範囲を設定します。導入の警告とポリシーの利用情報 （44 ページ） を参照してください。
- **ログアウト** : APIC 設定 GUI を終了します。

ナビゲーション ウィンドウ

サブメニュー バーの下にある APIC GUI の左側にある **[ナビゲーション (Navigation)]** ペインを使用して、サブメニュー カテゴリのすべての要素に移動できます。

各サブメニューカテゴリのアラーム、 **ナビゲーション** ペインは、そのカテゴリに関連するオブジェクトは、論理および物理の階層ツリーとして構成されています。通常、これらのオブジェクトは、ポート、ポリシー、またはその他のオブジェクトのグループを表します。**Navigation** ウィンドウでオブジェクトを選択すると、オブジェクトの詳細が **Work** ウィンドウに表示されます。

内のオブジェクトを右クリックしたとき、 **ナビゲーション**] ペインで、する可能性がありますが表示など、次のアクションの1つ以上のオブジェクトに関連する実行可能なアクションのメニュー。

- **削除** ：オブジェクトを削除します。
- **Create <type of="" object="">** ：新しいオブジェクトを作成します</type>。
- **名前を付けて保存...** JSON または XML 形式でオブジェクトとプロパティをローカル ファイルにダウンロードします。
- **Post...** オブジェクトとそのプロパティを既存のローカルファイルにエクスポートします。
- **Share**— オブジェクトの URL を表示します。URL をコピーし、他のユーザに送信できます。
- **オープンでオブジェクト ストア ブラウザ** : Visore、オブジェクトとそのプロパティを表示する組み込みユーティリティでオブジェクトを開きます。この情報は、またはAPIツールを開発するためのトラブルシューティングに役立つ可能性があります。
- **クローン** : オブジェクトのコピーを作成します。このアクションは、新しい契約または既存の契約またはポリシーに基づいてポリシーを取得するために役立ちます。

（注） [Navigation] ペインの任意のコンテナ、たとえば [Tenant] の下の [Application Profiles] に 40 以上のプロファイルがある場合、プロファイルをクリックして [Navigation] ペインでそれを展開することはできません。[Work] ペインから使用するプロファイルを選択して展開する必要があります。

[Work] ペイン

[Navigation] ペインで選択したコンポーネントに関する詳細を表示するには、APIC GUI の右側にある [Work] ペインを使用します。

[Work] ペインは、次の要素で構成されます。

- タブが表示されるコンテンツ領域。これらのタブを使用して、[Navigation] ペインで選択したコンポーネントに関連する情報にアクセスすることができます。コンテンツ領域に表示されるタブは、選択されたコンポーネントにより異なります。

- 一部のコンポーネントでは、コンポーネントに関連した概念的な情報へのリンクが、右上隅のリストのアイコンで表されています。 
- ほとんどのページをブックマーク可能で、ブックマークのリストからブックマークを選択して、簡単にページに戻ることができます。

  ブックマーク リンクは、メニュー バーの **[ユーザー プロファイルおよび基本設定 (User Profile and Preferences)]** アイコンからアクセスできます。
- ページでは「お気に入り」としてタブをマークできます。ページに移動するたびに、表示されているデフォルト タブになります。この機能は、**[作業 (Work)]** ペインのタブでのみ有効です。お気に入りとしてメニュー バーをマークできません。

作業ウィンドウの共通ページ

作業ペインには、特定のタスクのためのメニューだけでなく、このセクションで説明する、何種類かの専用メニューも表示されます。

[Quick Start] ページ

最初の [Quick Start] ページには、多くの APIC メニューとサブメニューが表示されます。タブの目的をまとめており、ステップバイステップでの方法と一般的に用いられる手順のビデオへのリンクを提供し、タブ内のよく用いられるサブセクションへのショートカット リンクを用意しています。**System > QuickStart** からアクセスできる、全体の [Quick Start] ページは、よく用いられる基本的な手順を実行する点で助けとなり、ステップバイステップの手順、利用可能な概念についての情報、そして GUI の主要な機能エリアへのリンクを提供しています。

[Dashboard] ページ

[Dashboard] ページは、ACI システムと主要なシステム コンポーネントのステータスを一目で理解できるようにまとめて表示します。これには健全性スコアの傾向、健全性スコアがしきい値を下回っているコンポーネント、および障害の回数が含まれます。健全性スコアのしきい値を設定すれば、コンポーネントがいつダッシュボードに表示されるかを調整できます。**System > Dashboard** で表示されるシステム ダッシュボード ページには、ACI システム全体の健全性がまとめられています。一方、 **Fabric > Inventory > Pod n > component > Dashboard** で表示されるスイッチ ダッシュボード ページには、スパインおよびリーフ スイッチごとの健全性と障害がまとめられています。

[Summary] ページ

[ナビゲーション (Navigation)] ウィンドウの多くのトップレベル フォルダは、サブフォルダにリンクしている、[Work] ウインドウのタイルベースのサマリ ページに表示されます。**[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ポッド n (Pod n)]** で表示されるもののような一部のサマリ ページには、主要なコンポーネントと、コンポーネントごとの簡潔な健全性および障害情報をまとめているタイルが含まれています。**[ファブリック (Fabric)] > [ファブリック ポ**

リシー (Fabric Policies)] > [ポリシー (Policies)] で表示されるような他のサマリ ページには、収められているフォルダが提供している設定エリアについて記述するタイルが含まれています。

インターフェイスのカスタマイズ

APIC GUI の命名

ACI コントローラ クラスタは、3 個以上の APIC で構成されます。場合によっては、APIC を表示する際に役立つ場合があります。次の手順で APIC GUI の見出しに独自の名前を追加します。

手順

ステップ 1 APIC メニュー バーで、**[システム (System)]** > **[システム設定 (System Settings)]** を選択します。

ステップ 2 **[ナビゲーション (Navigation)]** ペインで、**[APIC ID 基本設定 (APIC id Preferences)]** をクリックします。

ステップ 3 [作業 (Work)] ペインで、**[GUI エイリアス (GUI Alias)]** ボックスに目的の APIC 名を入力します。

ステップ 4 [Submit] をクリックします。`
GUI の左上にある括弧内に APIC 名が表示されます。

CLI または GUI へのログイン バナーを追加する

ユーザが CLI または GUI にログインするときに表示されるバナーを定義することができます。CLI バナーは、パスワードのプロンプトの前に端末に出力される、シンプルなテキスト文字列です。APIC CLI のバナーと、それとは別のスイッチ CLI のバナーを定義できます。GUI のバナーは、APIC の URL にアクセスしたとき、ユーザのログイン認証の前に表示されます。GUI のバナーは、目的の HTML をホストしているサイトの URL として定義されます。

手順

ステップ 1 APIC メニュー バーで、**[システム (System)]** > **[システム設定 (System Settings)]** を選択します。

ステップ 2 **[ナビゲーション (Navigation)]** ペインで、**[APIC ID 基本設定 (APIC id Preferences)]** をクリックします。

ステップ 3 [作業 (Work)] ペインで、次のフィールドに値を入力します。

a) APIC CLI バナーを設定するには、**Controller CLI Banner** テキストボックスにバナーのテキストを入力します。

b) スイッチ CLI バナーを設定するには、**Switch CLI Banner** テキストボックスにバナーのテキストを入力します。
c) APIC GUI バナーを設定するには、**GUI Banner (URL)** テキストボックスに、必要な HTML をホストしているサイトの URL を入力します。

（注）
URL のサイトの所有者は、情報提供のバナーを表示する iFrame を配置できるようサイトで許可を設定する必要があります。サイトの所有者が `x-frame-option` を `deny` または `sameorigin` に設定すると、URL がポイントしているサイトは表示されません。

ステップ 4 [送信（Submit）] をクリックします。

単一ブラウザ セッション管理

Cisco APIC リリース 4.0(1) から、APIC GUI にログインし、それぞれの新しいタブまたはウィンドウからログインすることなく、追加のブラウザ タブやウィンドウを開くことができます。この動作はデフォルトでは無効になっており、メイン メニュー バー ツールの**[ユーザー プロファイルおよび基本設定 (User Profile and Preferences)] > [設定 (Settings)]** にある **[単一ブラウザセッション (SBS) を有効にする (SBS) (Enable Single-Browser Session (SBS))]** チェック ボックスをオンにして有効にできます。

別のクレデンシャルを使用して別のタブまたはブラウザのウィンドウから APIC にログインする場合、単一ブラウザ セッション機能が無効になっていることを確認します。

導入の警告とポリシーの利用情報

Deployment Warning Settings を構成することにより、他のリソースやポリシーに影響を及ぼす可能性のあるポリシーを変更または削除した際に、ポリシーの使用情報が自動的に表示されるようにすることができます。ポリシーの利用情報では、ユーザが現在変更または削除しているポリシーがどのリソースおよびポリシーを使用しているかをユーザが確認することができます。テーブルには、特定のポリシーを使用するノード、およびこのポリシーを使用するほかのポリシーが表示されます。デフォルトでは、利用情報は、ユーザがポリシーを変更しようとするたびにダイアログ ボックス内に表示されます。また、いつでも画面下部の **Show Usage** ボタンをクリックして同じ情報を表示できます。

Deployment Warning Settings ダイアログ ボックスでは、ポリシーの使用情報を表示する導入の通知の範囲を有効にし、変更することができます。このダイアログ ボックスには、**Change Deployment Settings** を選択して表示できます。これは、メニュー バー ツールの **User Settings and Preferences** ドロップダウンリストからアクセスできます。または **Policy Usage Information** ダイアログ ボックスのボタンで表示できます。

Policy タブ (**Deployment Warning Settings** ダイアログ ボックスの右上) を選択しているときには、次のポリシー オプションを設定できます:

- **(グローバル) [Show Deployment Warning on Delete/Modify]:** APIC 全体にわたり、すべてのポリシーの削除または修正に対して、**[Deployment Warning]** の通知を有効にします。
- **(ローカル) [Show Deployment Warning on Delete/Modify]:** 特定のポリシー構成に対して、**[Deployment Warning]** 通知のためのルールを設定します。
  - **[Use Global Settings]**: **[(Global) Show Deployment Warning on Delete/Modify]** で選択した設定を使用します。
  - **[Yes]**: ポリシーの構成の変更を送信する前に、**[Deployment Warning]** の通知を表示します。このブラウザセッションでのみ有効です。
  - **[No]**: ポリシーの構成の変更を送信する前に、**[Deployment Warning]** の通知を表示しません。このブラウザセッションでのみ有効です。

History タブ (**Deployment Warning Settings** ダイアログ ボックスの右上) を選択しているときには、以前の導入の警告の**イベント**のテーブルと、**監査ログ**のエントリを表示できます。

ポートのグラフィカル設定

APIC GUI は、ファブリックのリーフスイッチ上でポート、ポート チャネル、および仮想ポート チャネルを設定し、ダイナミック ブレークアウト用のポートを設定し、FEX スイッチのインターフェイスをリンクするためのグラフィカルな方法を提供します。この設定機能は、GUI の次の場所に存在します。

- **Fabric > Inventory > Topology**
- **Fabric > Inventory > Pod**
- **Fabric > Inventory > Pod > Leaf**
- **Fabric > Inventory > Pod > Spine**

作業ウィンドウの **Interface** タブで、+ ボタン (左上) をクリックし、設定する 1 つ以上のスイッチを選択し、**Add Selected** をクリックします。複数のスイッチを選択するには、**Ctrl キーを押しながらクリック**または**Shift キーを押しながらクリック**してください。。

スイッチは、ポートおよびリンクとともに、グラフィカルに表示されます。ブレークアウト ポートを設定した場合には、サブ ポートを含むブロックがリーフ図の下に表示されます。

（注） リーフ スイッチから **Interface** タブをクリックすると、リーフスイッチが自動的に追加されます。

構成するインターフェイスを選択します。インターフェイスを選択すると、使用可能な設定ボタンが表示されます。選択したインターフェイスとその場所に応じて、ページの上部にある次のボタンのいずれかをクリックすることができます。

- **L2**— レイヤ 2。スイッチ図で 1 つ以上のリーフ インターフェイスをクリックすると表示されます。
- **PC**— ポート チャネル。スイッチ図で 1 つ以上のリーフ インターフェイスをクリックすると表示されます。
- **VPC**— 仮想ポートチャネル。2 つのスイッチ図で少なくとも 1 つのインターフェイスをクリックすると表示されます。
- **FEX**— ファブリック エクステンダ。スイッチ図で 1 つ以上のリーフ インターフェイスをクリックすると表示されます。
- **Breakout**— ブレイク アウト モード。スイッチ図で 1 つ以上のリーフ インターフェイスをクリックすると表示されます。
- **ファブリック**：ファブリック インターフェイスにポリシーを追加します。ファブリック ポートに適格なポートをクリックすると表示されます。
- **アップリンク**および**ダウンリンク**：適格なアップリンクをダウンリンクに変換します (逆も同じ)。
- **Spine**— スイッチ図で 1 つ以上のリーフ インターフェイスをクリックすると表示されます。

GUI 内の API 交換の表示

APIC グラフィカル ユーザー インターフェイス（GUI）でタスクを実行すると、GUI は内部 API メッセージを作成してタスクを実行するためのオペレーティング システムに送信します。APIC の組み込み型ツールである APIC インスペクタを使用して、これらの API メッセージを表示およびコピーできます。ネットワーク管理者は、主要操作を自動化するためにこれらのメッセージを複製したり、API を使用する外部アプリケーションを開発するためにこれらのメッセージを例として使用できます。

手順

ステップ 1 APIC GUI にログインします。

ステップ 2 APIC ウィンドウの右上隅で、システム ツール アイコンをクリックしてドロップダウン リストを表示します。

ステップ 3 ドロップダウン リストで、[Show API Inspector] を選択します。

[API Inspector] が新しいブラウザ ウィンドウで開きます。

ステップ 4 [API Inspector] ウィンドウの [Filters] ツールバーで、表示する API ログ メッセージのタイプを選択します。

表示されたメッセージは選択されたメッセージのタイプに応じて色分けされます。次のテーブルに、使用可能なメッセージ タイプを表示します。

名前	説明
trace	トレース メッセージを表示します。
debug	デバッグ メッセージを表示します。このタイプには、ほとんどの API コマンドと応答が含まれます。
info	情報メッセージを表示します。
warn	警告メッセージを表示します。
error	エラー メッセージを表示します。
fatal	重大メッセージを表示します。
all	このチェックボックスをオンにすると、他のチェックボックスすべてがオンになります。他のチェックボックスのいずれかをオフにすると、このチェックボックスもオフになります。

ステップ 5 [Search] ツールバーで、正確な文字列に対し表示されるメッセージまたは正規表現で表示されるメッセージを検索できます。

次の表に、検索のコントロールを示します。

名前	説明
検索	このテキスト ボックスに、直接検索の文字列を入力するか、または regex 検索の正規表現を入力します。入力に応じて、ログ リストの最初に一致したフィールドが強調表示されます。
Reset	[Search] テキスト ボックスの内容を削除するには、このボタンをクリックします。
Regex	[Search] テキスト ボックスの内容を検索の正規表現として使用するには、このチェックボックスをオンにします。
Match case	検索で大文字と小文字が区別されるようにするには、このチェックボックスをオンにします。
Disable	検索を無効にし、ログ リストの検索一致結果の強調表示をクリアするには、このチェックボックスをオンにします。
Next	ログ リストを次の一致したエントリまでスクロールするには、このボタンをクリックします。このボタンは、検索がアクティブである場合にのみ表示されます。
Previous	ログ リストを前の一致したエントリまでスクロールするには、このボタンをクリックします。このボタンは、検索がアクティブである場合にのみ表示されます。

名前	説明
Filter	一致しない行を非表示にするには、このチェックボックスをオンにします。このチェックボックスは、検索がアクティブである場合にのみ表示されます。
Highlight all	すべての一致したフィールドを強調表示するには、このチェックボックスをオンにします。このチェックボックスは、検索がアクティブである場合にのみ表示されます。

ステップ 6 [Options] ツールバーで、表示されるメッセージを並べ替えることができます。

次の表に、使用可能なオプションを示します。

名前	説明
Log	ロギングをイネーブルにするには、このチェックボックスをオンにします。
Wrap	ログ リストの水平スクロールを無効にするために行の折り返しをイネーブルにするには、このチェックボックスをオンにします。
Newest at the top	ログ エントリを逆の時系列で表示するには、このチェックボックスをオンにします。
Scroll to latest	最新のログ エントリに迅速にスクロールするには、このチェックボックスをオンにします。
Clear	ログ リストを削除するには、このボタンをクリックします。
Close	API インスペクタを閉じるには、このボタンをクリックします。

例

次の例では、APIC インスペクター ウィンドウの 2 つのデバッグ メッセージを示します。

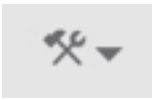
```
13:13:36 DEBUG - method: GET url: http://192.0.20.123/api/class/infraInfra.json
response: {"imdata":[{"infraInfra":{"attributes":{"instanceId":"0:0","childAction":"",
"dn":"uni/infra","lcOwn":"local","name":"","replTs":"never","status":""}}}]}

13:13:40 DEBUG - method: GET url: http://192.0.20.123/api/class/l3extDomP.json?
query-target=subtree&subscription=yes
response: {"subscriptionId":"72057598349672459","imdata":[]}
```

GUI アイコン

表 *6 : APIC GUI* に頻繁に表示されるアイコン

アイコン	説明
	検索 （37 ページ）
	アラート （38 ページ）
	マイ プロファイルの管理 （39 ページ）
	ツール （38 ページ）
	このページをブックマーク
	現在のメニュー ページに関連したコンセプトの情報を表示
	クイック スタート
	クイック スタートのビデオを再生
	クイック スタートの手順を表示
	関連するセクションへのリンク
	トポロジ
	ポッド

アイコン	説明
	ツリー ビューを折りたたむ
	ツリー ビューを展開する
	すべてのノードを折りたたむ
	アクションのドロップダウンリストを表示
	表示されている情報を更新
	ファイルをダウンロード
	ファイルをアップロード

障害、統計情報、およびヘルス レベルのアイコン

表 *7: APIC GUI* に表示される障害のシビラティ（重大度）レベル

アイコン	説明
	クリティカル：このアイコンは、シビラティ（重大度）がクリティカルな障害レベルを示します。
	メジャー：このアイコンは、シビラティ（重大度）がメジャーな障害レベルを示します。
	マイナー：このアイコンは、シビラティ（重大度）がマイナーな障害レベルを示します。
	警告：このアイコンは、警告を必要とする障害レベルを示します。

リリース 6.1(x) の次世代ユーザー インターフェイス

この Cisco Application Policy Infrastructure Controller (APIC) 6.1(x) リリースでは、最新の簡素化されたGUIを含む次世代ユーザーインターフェイス（UI）のプレビューが導入されています。このプレビューでは、GUI の今後の発展がどんなものになるか知ることができます。新しい

GUI でグレー表示されている選択肢は、このプレビューには存在しませんが、今後のリリースで追加される予定です。プレビューを使用して構成を変更することはできませんが、将来のリリースで新しい GUI が利用可能になったら、構成を変更できます。

図 9 : 新しい GUI （51 ページ） に、リリース 6.1.2 の GUI を示します。

図 *9* : 新しい *GUI*

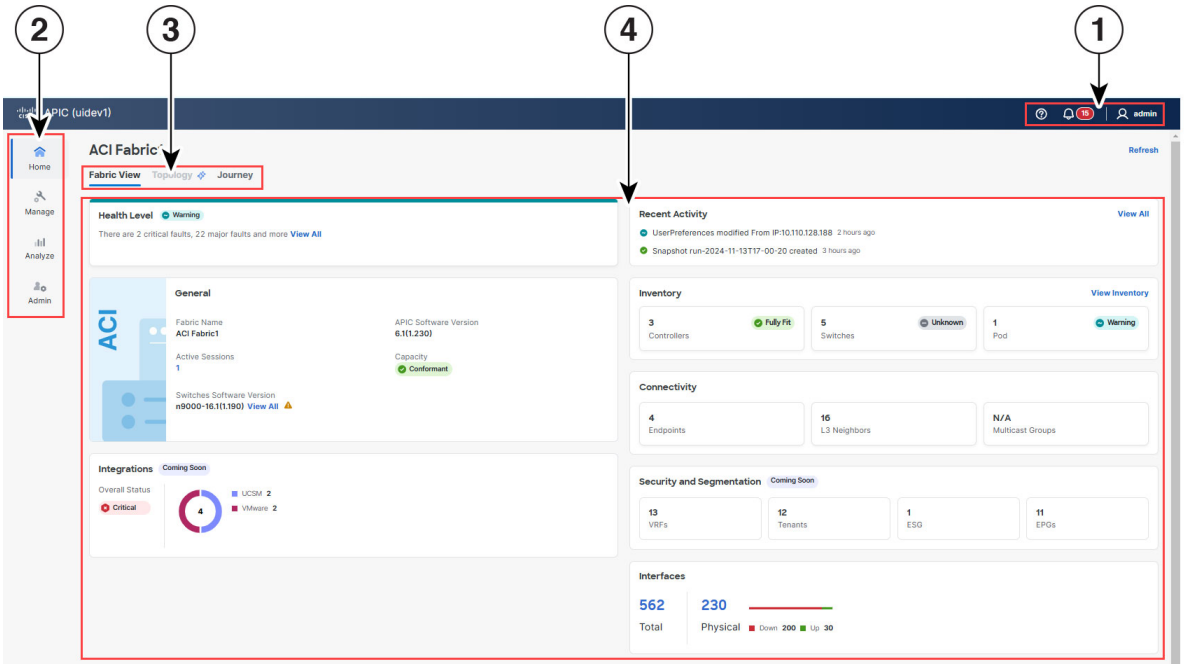


表 8 : 新しい GUI のエリア （51 ページ） では、新しい GUI のエリアについて説明します。

表 *8* : 新しい *GUI* のエリア

図表番号	説明
1	[ツール（Tools）] エリア
2	[ナビゲーション（Navigation）] エリア
3	[タブ（Tabs）] エリア
4	作業領域

[ツール（Tools）] エリア

このエリアには、GUI ページに関係なく表示される基本ツールが含まれています。

- **[ヘルプ（Help）]**：次の選択肢があるメニューを開きます。
  - **[バージョン情報（About）]**： Cisco APIC リリース、著作権の年、および現在のシステム時刻を表示します。

- **[APICファブリックのセットアップ（APIC Fabric Setup）]**：ファブリックでまだ構成していないものを判断するのに役立ちます。
- **[ヘルプ センター（Help Center）]**：より一般的に使用されるドキュメントの一部へのリンクを提供します。
- **[オブジェクト ストア ブラウザを開く（Open Object Store Browser）]**：管理対象オブジェクトブラウザ(バイザー)を開きます。これはCisco APICに組み込まれているユーティリティで、管理対象オブジェクト(MO)をブラウザによりグラフィカルに表示します。
- **Show API Inspector**: Opens the API Inspector, which is a built-in tool of the Cisco APIC that allows you to view the internal API messages between the GUI and the Cisco APIC operating system to execute tasks

- **[通知（Notifications）]**： Cisco APICに関する重要な問題に関する通知を表示します。ドロップダウンメニューを使用して、すべての通知を表示するか、特定の重大度の通知のみを表示するかを選択できます。メニューには、現在発生している障害の重大度のみが含まれます。**[すべて表示（View All）]**をクリックして、テーブル内のすべての障害を表示することもできます。
- **[プロファイル（Profile）]**：次の選択肢があるメニューを開きます。
  - **[既存の UI に切り替え（Switch to existing UI）]**：既存の（従来の）GUIに切り替えます。
  - **[ユーザー設定（User Preferences）]**：ユーザー設定を構成します。
  - **[パスワードの変更（Change Password）]**：パスワードを変更します。
  - **[ユーザー証明書の変更（Change User Certificate）]**：ユーザー証明書を変更します。
  - **[SSH キーの変更（Change SSH Key）]**: 証明書ベースのログインに使用されるユーザの公開 SSH キーを変更します。
  - **[ログアウト（Logout）]**： Cisco APICからログアウトします。

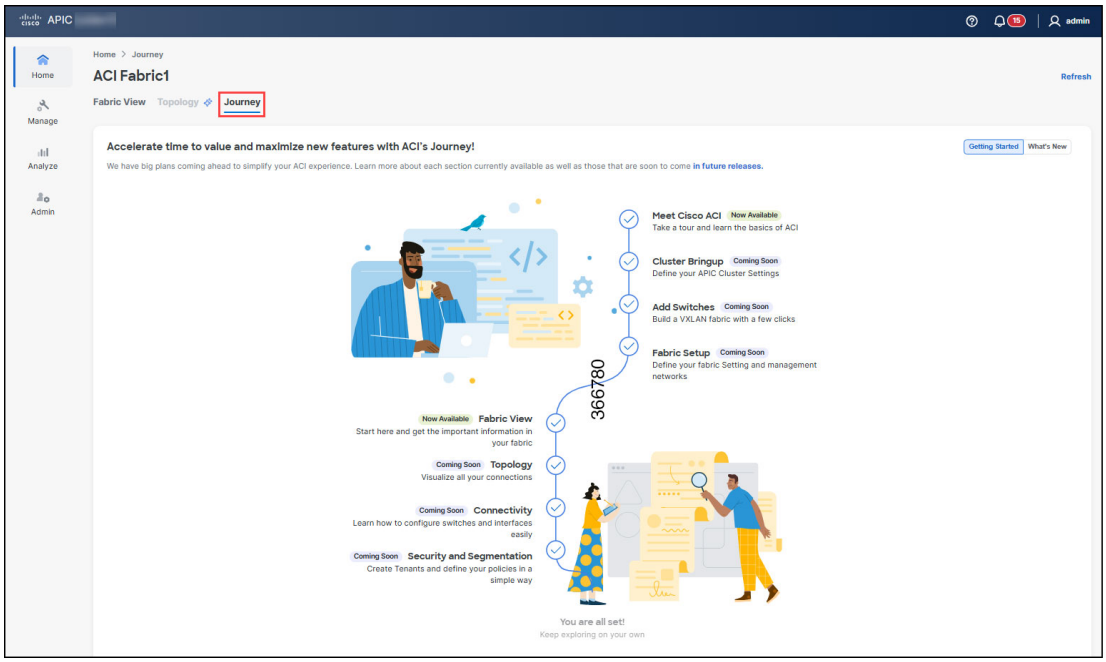
[ナビゲーション（Navigation）] エリア

これは、すべての GUI ページに存在する Cisco APICのコアナビゲーションです。

- **[ホーム（Home）]**：ファブリックに関する情報を表示できます。このエリアには、次のタブがあります。
  - **[ファブリック ビュー（Fabric View）]**：ファブリックに関するさまざまな情報を表示します。青色のテキストと**コントローラ**、**スイッチ**、および**ポッド**をクリックすると、それらに関する詳細情報を表示できます。
  - **[トポロジ（Topology）]**：ファブリックのトポロジをグラフィカルに表示します。
  - **[ジャーニー（Journey）]**： Cisco APICの主な機能を示し、新しい GUI の実行プランを表示し、今後の機能とその機能のプレビューを提供します。

ほとんどのステージには **[詳細情報（Tell Me More）]** ボタンがあります。ダイアログが開き、そのステージに関連付けられている GUI の部分に関する詳細情報（スクリーンショットなど）が表示されます。「近日公開」とラベル付けされたステージの場合、ダイアログにはGUIのその部分の今後の開発の概要が表示され、スクリーンショットには GUI がどのように表示されるかが示されます。

図 *10 : Cisco ACI*ジャーニー



- **[管理（Manage）]**：次の情報を表示および構成できます。
  - **[インベントリ（Inventory）]**：コントローラ、スイッチ、およびポッドに関する情報を表示します。
  - **[テナント（Tenants）]**：テナントに関する情報を表示します。
  - **[ポリシーグループ（Policy Groups）]**：ポリシーグループに関する情報を表示します。
  - **[ポリシー（Policies）]**：構成されたポリシーに関する情報を表示します。
  - **[ドメインとプール（Domains and Pools）]**：ドメインとプールに関する情報を表示します。
  - **[ソフトウェア管理（Software Management）]**：Cisco APICおよびスイッチのファームウェアをアップグレードできます。
  - **[モニタリングの宛先（Monitoring Destinations）]**：callhome、SNMP、TACACS などのモニタリングの宛先に関する情報を表示します。
  - **[スイッチとインターフェイス（Switches and Interfaces）]**：スイッチとインターフェイスに関する情報を表示します。

- **[分析（Analyze）]**：次の情報を表示できます。
  - **[障害（Faults）]**：ファブリックの問題が原因で Cisco APIC が発生させた障害を示します。
  - **[履歴とログ（History and Logs）]**：障害レコード、イベント レコード、監査ログなど、さまざまなレコードとログを表示します。
  - **[テクニカルサポート（Tech Support）]**：Cisco Technical Assistance Center（TAC）に連絡するときに提供するテクニカル サポート ログをエクスポートできます。
- **[管理（Admin）]**：次の項目を使用または構成できます。
  - **[バックアップと復元（Backup and Restore）]**： Cisco APIC 設定をバックアップおよび復元できます。
  - **[認証（Authentication）]**： Cisco APICにログインするためのユーザーの認証方法を構成できます。
  - **[アクティブなセッション（Active Sessions）]**： Cisco APICにログインしているユーザーを表示します。
  - **[統合（Integrations）]**：Cisco APICと統合したサードパーティ製品に関する情報を表示します。
  - **[ライセンス（Licensing）]**：Cisco APICとその機能を使用するためのアクティブなライセンスに関する情報を表示します。
  - **[システム設定（System Settings）]**：Cisco APICを構成できます。

[タブ（Tabs）] エリア

このエリアには、選択したコアナビゲーションに応じて変化するタブが含まれています。タブを使用すると、そのコア ナビゲーションのサブセクションに移動できます。

作業領域

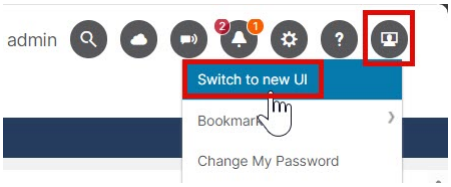
このエリアは、表示しているページに応じて変わります。作業エリアには、ステータスが表示され、設定されたオブジェクトなどを表示するためのリンクが含まれています。青色のテキストはリンクで、クリックすると詳細情報を表示したり、設定を変更したりできます。

次世代ユーザー インターフェイスのプレビュー

このリリースでは、次世代のユーザーインターフェイス（UI）のプレビューが導入されています。これには、最新の簡素化された Cisco Application Policy Infrastructure Controller （APIC）GUI が含まれています。次世代ユーザーインターフェイスをプレビューするには、次のステップを実行します。

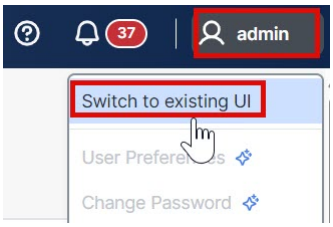
手順

ステップ 1 任意のページの右上にあるプロファイルアイコンをクリックし、**[新しい UI に切り替える（Switch to new UI）]**を選択します。



グレー表示されている新しい GUI では何も表示されません。これらのページは将来のリリースで追加される予定です。

ステップ 2 構成を変更できるように元の GUI に戻すには、任意のページの右上にあるプロファイル アイコンをクリックし、**[既存の UI に切り替える（Switch to existing UI）]**を選択します。



機能拡張と改善

ACI 6.1.2 リリースには、使いやすさの向上、より詳細な情報、より少ないクリックでの迅速なナビゲーションを実現するために、多数の UI の変更点が含まれています。

表 *9 : ACI* リリース *6.1.2* の *GUI* の更新

自宅	[ファブリックビュー（Fabric View）]	カラー コーディング、追加のカード、ピル型アイコン、詳細情報へのリンク： • **[正常性レベル（Health Level）] > [全般（General）]** 情報と **[概要（Overview）]**、**[障害（Faults）]**、および **[履歴（History）]** タブ • **監査ログ、イベントレコード、およびセッションログ** による**最近のアクティビティ**情報 • **コントローラ、スイッチ、およびポッド** の詳細を含む**インベントリ**情報 • **エンドポイント、L3 ネイバー、およびマルチキャストグループ**との**接続**情報 • **合計および物理の**詳細リスト、ダッシュレット、およびカードを含む**インターフェイス**情報 • ファブリック キャパシティまたはリーフ スイッチ キャパシティ情報への **キャパシティ** ハイパーリンク

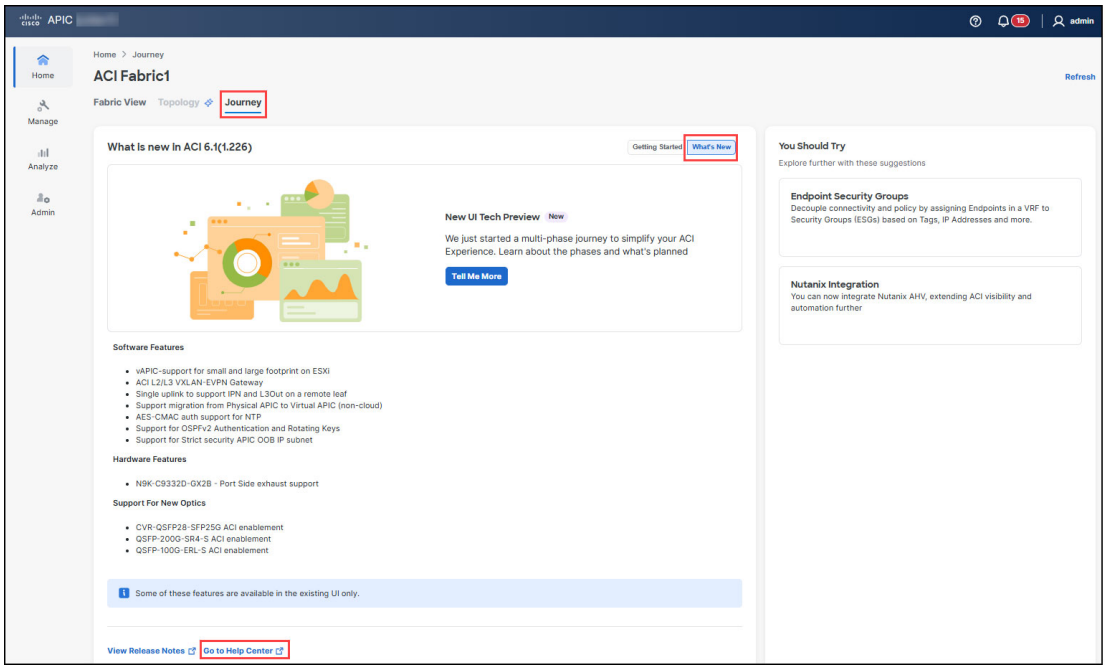
管理	> インベントリ	

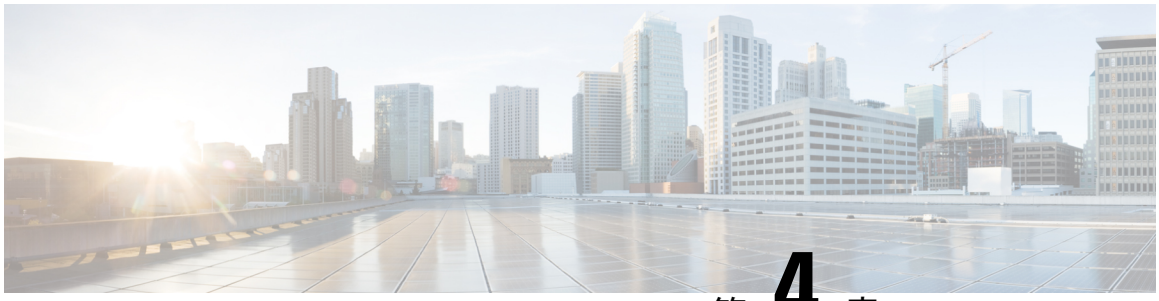
		> コントローラ[コントローラ（Controller）]画面には、テーブル内のコントローラのタイプ（物理または仮想）が表示されます。 [コントローラ（Controller）]を選択し、コントローラを選択します。 • **> [履歴（History）] > [履歴タイムライン（Historical Timeline）]**. 過去 1 時間または 1 日のすべての正常性スコアがグラフィカルに表示されます。 • **[インターフェイス（Interfaces）] > [物理インターフェイス（Physical Interfaces）] を選択し、**インターフェイス ID を選択します。インターフェイス ID や CDP/LLDP ネイバー情報など、物理インターフェイスの詳細が表示されます。 > [Switches（スイッチ）] > スイッチを選択します。 • スイッチ ビューのグラフィックが表示されます。コンポーネントにカーソルを合わせると、ポップアップウィンドウが表示されます。 • 下部の **[ラック（Rack）]** をクリックします。ルーム、フロア、ビルディング、スイッチのロール、ファブリックの状態、バージョン、および正常性を示すサマリーカードを示すラックの詳細が表示されます。

		• **> [履歴（History）] > [履歴タイムライン（Historical Timeline）]**. 過去 1 時間または 1 日のすべての正常性スコアがグラフィカルに表示されます。 > [Pods（ポッド）] > ポッドを選択します。 • 正常性レベル、一般情報、最近のアクティビティ、インベントリの詳細などの正常性の概要情報が表示されます。 • **> [履歴（History）] > [履歴タイムライン（Historical Timeline）]**. 過去 1 時間または 1 日のすべての正常性スコアがグラフィカルに表示されます。
テーブルの設定	歯車アイコン	• 歯車をクリックし、右からテーブルの [構成（Configuration）] ウィンドウのスライドをクリックします。 • 各インターフェイスのリストからカテゴリを選択します。 設定は、ユーザーが変更を加えたブラウザでのみ、ログアウト後も保持されます。
ヘルプ	疑問符のアイコン	ヘルプ センター

右上端の疑問符のアイコン以外にも、**[ヘルプ（Help）]** メニューにアクセスできる方法が用意されました。**[ホーム（Home）]** メニューから、**[ジャーニー（Journey）]> [新着情報（What's New）]** タブをクリックします。**[新着情報（What's new）]** ウィンドウが表示されます。下部にある **[ヘルプセンターに移動（Go to Help Center）]** をクリックします。

図 *11 : ACI 6.1.2* の新機能





第 4 章

ファブリックの初期化とスイッチの検出

この章で説明する内容は、次のとおりです。

ファブリックの初期化

ファブリックの初期化について

スイッチを APIC で管理されるように追加し、GUI、CLI、または API を使用して手順を検証することによってファブリックを構築できます。

（注） ファブリックを構築するには、アウトオブバンド ネットワーク経由で APIC クラスタを事前に作成する必要があります。

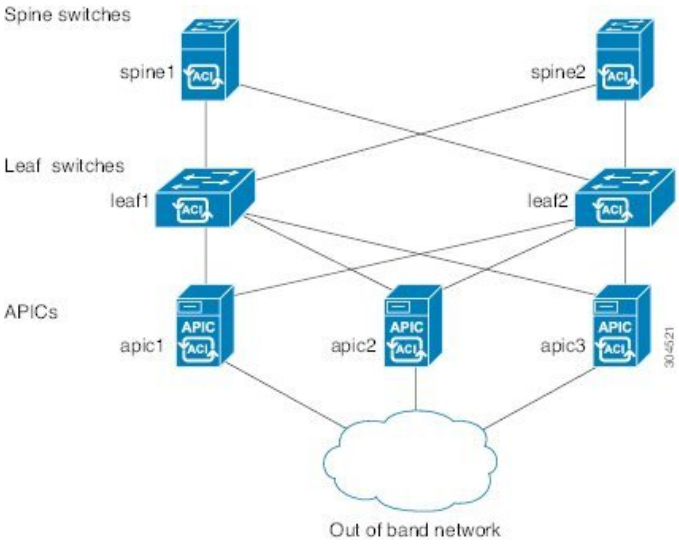
ファブリック トポロジ (例)

ファブリック トポロジの例は次のとおりです。

- 2 つのスパイン スイッチ（spine1、spine2）
- 2 つのリーフ スイッチ（leaf1、leaf2）
- APIC の 3 つのインスタンス（APIC1、APIC2、APIC3）

次の図は、ファブリック トポロジの例を示します。

図 *12 :* ファブリック トポロジ例



接続：ファブリック トポロジ

ファブリック トポロジの接続の詳細例は次のとおりです。

名前	Connection Details
leaf1	eth1/1 = apic1（eth2/1） eth1/2 = apic2（eth2/1） eth1/3 = apic3（eth2/1） eth1/49 = spine1（eth5/1） eth1/50 = spine2（eth5/2）
leaf2	eth1/1 = apic1（eth 2/2） eth1/2 = apic2（eth 2/2） eth1/3 = apic3（eth 2/2） eth1/49 = spine2（eth5/1） eth1/50 = spine1（eth5/2）
spine1	eth5/1 = leaf1（eth1/49） eth5/2 = leaf2（eth1/50）
spine2	eth5/1 = leaf2（eth1/49） eth5/2 = leaf1（eth1/50）

マルチ階層ファブリック トポロジ(例)

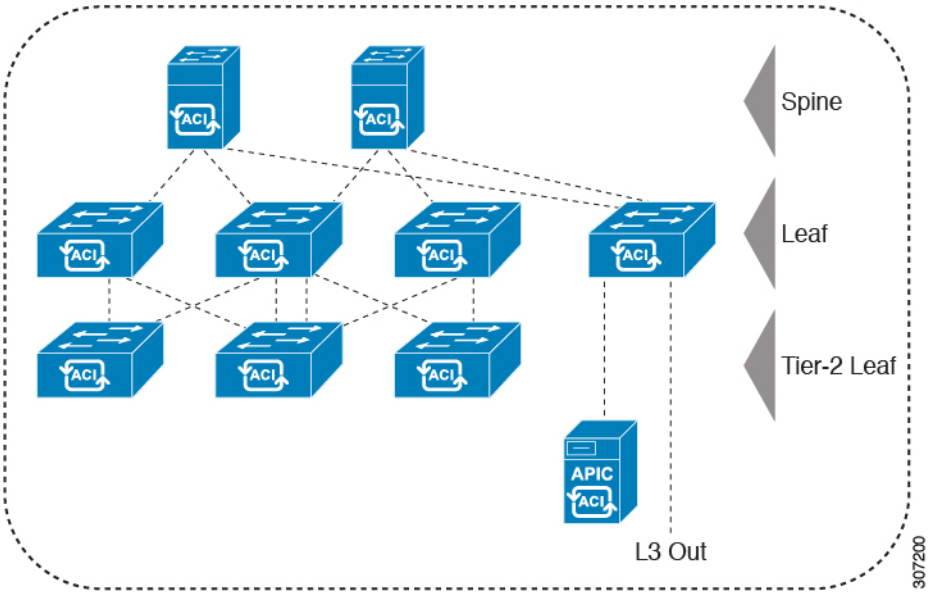
3 階層コア集約アクセス アーキテクチャは、データ センター ネットワーク トポロジで共通です。Cisco APIC リリース 4.1(1) 時点で、コア集約アクセス アーキテクチャに対応するマルチ階層 ACI ファブリック トポロジを作成するため、ラックスペースや配線などコストが高いコンポーネントのアップグレードの必要性を軽減できます。階層 2 リーフ レイヤーを追加することで、このトポロジが可能になります。階層 2 リーフ レイヤーは、ダウンリンク ポート上のホストまたはサーバへの接続、およびアップリンク ポート上のリーフ レイヤー (集約) への接続をサポートします。

マルチ階層トポロジでは、リーフ スイッチには最初にスパイン スイッチへのアップリンク接続と、階層 2 リーフ スイッチへのダウンリンク接続があります。トポロジ全体を ACI ファブリックにするには、階層 2 リーフ ファブリック ポートに接続されているリーフ スイッチ上のすべてのポートが、ファブリック ポートとして設定されている必要があります (まだデフォルトのファブリック ポートを使用していない場合)。APIC が階層 2 リーフ スイッチを検出した後、階層 2 リーフ上のダウンリンク ポートをファブリック ポートに変更し、中間レイヤ リーフ上のアップリンク ポートに接続できます。

（注） デフォルトのファブリック ポートを使用してリーフ スイッチを階層 2 リーフに接続していない場合、リーフ ポートをダウンリンクからアップリンクに変換する必要があります (リーフ スイッチのリロードが必要です)。ポート接続の変更についての詳細は、『*Cisco APIC* 階層 *2* ネットワーキング設定ガイド』の「アクセス インターフェイス」の章を参照してください。

次の図は、マルチ階層ファブリック トポロジの例を示します。

図 *13* : マルチ階層ファブリック トポロジ例



上の図のトポロジがリーフ集約レイヤに接続している Cisco APIC および L3Out/EPG を示しており、階層 2 リーフ アクセス レイヤは APIC および L3Out/EPG への接続もサポートしています。

（注） EX で終わるモデル番号の Cisco Nexus 9000 シリーズ スイッチは、階層 2 リーフ スイッチが接続されている場合、階層 2 リーフ スイッチおよびリーフ スイッチとしてサポートされます。次の表を参照してください。

リモート リーフ スイッチに接続されている階層 2 リーフ スイッチはサポートされていません。

表 *10 :* マルチ階層アーキテクチャでサポートされているスイッチおよびポート速度

スイッチ	サポートされている最大ダウンリンク ポート* (階層 2 リーフ)	サポートされている最大ファブリック ポート (階層 2 リーフ)	サポートされている最大ファブリック ポート (階層 1 リーフ)
Nexus 93180YC-EX	48x1/10/25 Gbps 4x40/100 Gbps	48 x 10/25-Gbps 6 x 40/100-Gbps	48 x 10/25-Gbps 6 x 40/100-Gbps
Nexus 93108TC-EX	48x100M/1/10G BASE-T 4x40/100-Gpbs	6 x 40/100-Gbps	6 x 40/100-Gbps
N9K-9348GC-FXP**	48 x 100M/1G BASE-T	4 x 10/25-Gbps 2 x 40/100-Gbps	4 x 10/25-Gbps 2 x 40/100-Gbps
N9K-93180YC-FX	48 x 1/10/25-Gbps 4x40/100 Gbps	48 x 10/25-Gbps 6 x 40/100-Gbps	48 x 10/25-Gbps 6 x 40/100-Gbps
N9K-93108TC-FX	48 x 100M/1/10G BASE-T 4x40/100 Gbps	6 x 40/100-Gbps	6 x 40/100-Gbps
N9K-93240YC-FX2	48x1/10/25 Gbps 10x40/100 Gbps	48x1/10/25 Gbps 12x40/100 Gbps	48x10/25-Gbps ファイバ ポート 12x40/100 Gbps
N9K-C9336C-FX2	34 x 40/100-Gbps	36 x 40/100-Gbps	36 x 40/100-Gbps
N9K-C93216TC-FX2***	96 x 10G BASE-T 10 x 40/100-Gbps	12 x 40/100-Gbps	12 x 40/100-Gbps
N9K-C93360YC-FX2***	96 x 10/25 Gbps 10 x 40/100-Gbps	52 x 10/25Gbps 12 x 40/100Gbps	52 x 10/25Gbps 12 x 40/100Gbps
N9K-C9364C-GX	62 x 40/100-Gbps	62 x 40/100-Gbps	62 x 40/100-Gbps

* 最後 2 個の元のファブリック ポートは、ダウンリンク ポートとして使用できません。

** 階層 2 リーフに多くの帯域幅が必要ない場合、ファイバ ポートが少なくても階層 1 として使用できます。銅ポートはファブリック ポートとして使用できません。

*** Cisco APIC リリース 4.1(1) 以降でサポートされます。

外部ロータブル サブネットの交換

次の手順では、これらの設定を行った後、サブネットまたは TEP テーブルの情報を変更する必要がある場合に、外部ロータブル サブネットを変更する方法について説明します。

（注） 複数のサブネットを使用した外部ロータブル サブネット設定の変更はサポートされていません。

手順

ステップ 1 外部ロータブル サブネットを最初に設定したエリアに移動します。

a) メニュー バーで、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** をクリックします。

b) [ナビゲーション (Navigation)] ウィンドウで、**[ポッド ファブリック セットアップ ポリシー (Pod Fabric Setup Policy)]** をクリックします。

c) **[ファブリック セットアップ ポリシー（Fabric Setup Policy）]** パネルで、外部ロータブル サブネットを最初に設定したポッドをダブルクリックします。

このポッドの **[ポッド向けファブリック セットアップ ポリシー（Fabric Setup Policy for a POD）]** ページが表示されます。

d) APIC ソフトウェアのリリースに応じて、サブネットまたは TEP テーブルの情報を検索します。

- 4.2(3) よりも前のリリースでは、**ロータブル サブネット** テーブルを検索します。
- 4.2(3) の場合のみ、**外部サブネット** テーブルを見つけます。
- 4.2(4) 以降では、**外部 TEP** テーブルを見つけます。

ステップ 2 テーブルで削除する外部ロータブルサブネットを検索し、そのサブネットの状態が**アクティブ**または**非アクティブ**に設定されているかどうかを確認します。

状態が**アクティブ**に設定されている場合は、状態を**非アクティブ**に変更します。

a) 削除する既存の外部ロータブル サブネットのサブネットまたは TEP テーブルのエントリをダブルクリックします。

b) サブネットの状態を**非アクティブ**に変更し、**[更新（Update）]** をクリックします。

ステップ 3 既存の外部ロータブル サブネットを削除します。

a) 削除する既存の外部ロータブル サブネットのサブネットまたは TE Pテーブルのエントリをクリックします。

b) テーブルの上部にあるゴミ箱アイコンをクリックし、ポップアップ確認ウィンドウで **[はい（Yes）]** をクリックして、外部ロータブル サブネットを削除します。

ステップ 4 30 秒以上待ってから、新しい外部ロータブル サブネットを設定します。

a) サブネットまたは TEP テーブルで **[+]** をクリックして、新しい外部ロータブル サブネットを設定します。

b) 必要に応じて IP アドレスと予約アドレスを入力し、状態を**アクティブ**または**非アクティブ**に設定します。

- IP アドレスは、ロータブル IP スペースとして設定するサブネット プレフィックスです。
- 予約アドレスは、スパイン スイッチおよびリモート リーフ スイッチに動的に割り当ててはいけないサブネット内のアドレスの数です。カウントは常にサブネットの最初の IP から始まり、順番に増加します。このプールからユニキャスト TEP を割り当てる場合は、予約する必要があります。

c) **[更新（Update）]** をクリックして、新しい外部ロータブル サブネットをサブネットまたは TEP テーブルに追加します。

d) **Fabric Setup Policy** パネルで、**Submit** をクリックします。

ステップ 5 新しいロータブル IP アドレスが正常に設定されていることを確認します。

CLI を使用して APIC コントローラにログインし、次のコマンドを入力します。

```
apic1# avread | grep routableAddress
```

以下のような出力が表示されます。

```
routableAddress   14.3.0.228              14.3.0.229              14.3.1.228
```

ステップ 6 スパイン スイッチで作成された NAT エントリを確認します。

CLI を使用してスパイン スイッチにログインし、次のコマンドを入力します。

```
spine1# show nattable
```

以下のような出力が表示されます。

```
-----NAT TABLE---------
Private Ip  Routable Ip
----------  -----------
10.0.0.2    14.3.0.229

10.0.0.1    14.3.0.228

10.0.0.3    14.3.1.228
```

スイッチの検出

APIC によるスイッチ検出

APIC は、ACI ファブリックの一部であるすべてのスイッチに対する自動プロビジョニングおよび管理の中心となるポイントです。単一のデータセンターには、複数の ACI ファブリックを組み込むことができます。各データセンターは、自身の APIC クラスタとファブリックの一部である Cisco Nexus 9000 シリーズ スイッチを持つことができます。スイッチが単一の APIC クラスタによってのみ管理されるようにするには、各スイッチがファブリックを管理するその特定の APIC クラスタに登録される必要があります。

APICは、現在管理している任意のスイッチに直接接続されている新規スイッチを検出します。クラスタ内の各 APIC インスタンスは、直接接続されているリーフ スイッチのみを最初に検出します。リーフ スイッチが APIC で登録されると、APIC はリーフ スイッチに直接接続されているすべてのスパイン スイッチを検出します。各スパイン スイッチが登録されると、その APIC はそのスパイン スイッチに接続されているすべてのリーフ スイッチを検出します。このカスケード化された検出により、APIC は簡単なわずかな手順でファブリック トポロジ全体を検出することができます。

APIC クラスタによるスイッチ登録

スイッチが Cisco Application Policy Infrastructure Controller（APIC）で登録されると、そのスイッチは Cisco APIC で管理されるファブリック インベントリの一部となります。Cisco Application Centric Infrastructure（ACI）ファブリックを使用すると、Cisco APIC はインフラストラクチャ内のスイッチのプロビジョニング、管理、およびモニタリングのシングル ポイントとなります。

次の注意事項および制約事項が適用されます。

- スイッチを登録する前に、ファブリック内のすべてのスイッチが物理的に接続され、適切な設定で起動されていることを確認します。シャーシの設置については、https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.htmlを参照してください。

  スイッチが APIC クラスタとは異なるバージョンを実行している場合は、スイッチ検出時の自動ファームウェア更新を使用して、検出フェーズ中にスイッチを自動的にアップグレードします。詳細については、「Cisco APIC インストールおよび ACI アップグレード、ダウングレード ガイド（Cisco APIC Installation and ACI Upgrade and Downgrade Guide）」の「**検出の自動ファームウェア更新（Auto Firmware Update on Discovery）**」を参照してください。

- 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 ACI 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。

- スイッチの電源の再投入またはアップグレードを行うと、外部デバイスがまだ準備ができていないスイッチにトラフィックを送信するのを防ぐために、スイッチが Cisco APIC から構成を再度ダウンロードできるまで、ダウンリンク インターフェイスは管理ダウン状態になります。Cisco APIC 接続のファブリック リンクとダウン リンクは、admin-down 状態に変更されません。この免除を実現するために、リーフ スイッチは、電源の再投入またはアップグレードの前に Cisco APIC に接続されていたダウンリンク インターフェイスを記憶します。このため、電源の再投入またはアップグレード後にスイッチが再度完全に動作するまで、Cisco APIC 接続を変更しないでください。

スイッチ ロールの考慮事項

- デフォルトのファブリック リンクは、別のスイッチからの最初のスイッチ検出に使用する必要があります。
- デフォルトのスパイン スイッチが Cisco Application Policy Infrastructure Controller（APIC）に直接接続されている場合、スイッチは自動的にリーフ スイッチに変換されます。変換期間中は、Cisco APICに障害が発生しますが、これは正常な動作です。スイッチの変換が完了すると、障害は解消されます。
- リーフ スイッチの場合、ポートが Cisco APIC に登録された後、ポートをダウンリンクまたはファブリック リンクに変換するようにポート プロファイルを設定できます。詳細については、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』を参照してください：

  https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html#Configuration_Guides

この表に、ロールを変更できるスイッチのデフォルト ロールを示します。

表 *11* : デフォルト ロール

スイッチ製品 ID	デフォルト ロール	ロール変更をサポートする最初のリリース[1]
N9K-C93600CD-GX	リーフ	5.2(1)
N9K-C9316D-GX	スパイン	5.1(4)
N9K-C9364C-GX	リーフ	5.1(3)
N9K-C9332D-GX2B	リーフ	5.2(3)
N9K-C9364D-GX2A	スパイン	5.2(3)
N9K-C9348D-GX2A	スパイン	5.2(3)
N9K-C9408	スパイン	6.0(2)

[1]指定されたスイッチのロール変更をサポートする最初のリリースを示します。そのスイッチのロール変更は、以降のすべてのリリースでサポートされます。

ハイブリッド スイッチはロールを変更できます。ハイブリッド スイッチのデフォルトのロールは、モデルごとに異なります。リリース 6.1(2) では、スイッチが検出される前に CLI コマンドを使用してスイッチのロールを変更できます。これらのスイッチのデフォルト ロールによって、検出フェーズでのインターフェイスのロールが決まります。これにより、スイッチがデフォルト以外のロールで使用されている場合に問題が発生する可能性があります。たとえば、デフォルトのロールがリーフであるスイッチは、スパイン スイッチとしてケーブル接続されたとします。スイッチが検出されると、そのロールは自動的にスパインに変換されます。ただし、デフォルトでは、リーフ スイッチとして起動し、そのインターフェイスのほとんどは、スパイン検出に使用できるファブリック リンクとして設定されません。その結果、スイッチを確実に検出するためのケーブル接続オプションが制限される場合があります。

別の例：デフォルトのロールがスパインであるスイッチがリーフ スイッチとしてケーブル接続され、APIC に直接接続されることになっている場合。ただし、スパイン スイッチのすべてのインターフェイスは、APIC への接続に使用できないファブリック リンクです。その結果、スイッチは、APIC に接続できるリーフ スイッチに変換できるように、別の APIC に接続されている別のスイッチを介して検出される必要があります。

これらの問題に対処するには、新しい 未検出の スイッチで次の CLI コマンドを使用して、検出される **前に** ロールを変更します。

```
(none)# acidiag setrole <leaf/spine>
This command will reboot the switch, Proceed? [y/N]
```

（注） スイッチが検出されている場合、 `acidiag setrole <leaf/spine>` コマンドは機能しません。次の場合はエラー メッセージが表示されます。

GUI を使用した未登録スイッチの登録

（注） 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 ACI 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。

始める前に

ファブリック内のすべてのスイッチが物理的に接続され、起動されていることを確認します。

手順

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

ステップ 2 [Navigation] ペインで、[Fabric Membership] を選択します。

ステップ 3 [作業（Work）] ペインで、**[登録保留中のノード（Nodes Pending Registration）]** タブをクリックします。

[登録保留中のノード (Nodes Pending Registration)] タブ表のスイッチには、次の条件が存在する可能性があります。

- 新しく検出され、未登録のノードに、0 のノード ID があり、IP アドレスがありません。
- 手動で入力し（Cisco Application Policy Infrastructure Controller（APIC））未登録のスイッチは、ネットワークに物理的に接続されるまで、元のステータスは**[未検出 (Undiscovered）]** になります。接続されると、ステータスが **[検出済み (Discovered)]** になります。

ステップ 4 **[登録保留中のノード (Nodes Pending Registration)]** 表で、0 の ID を持つスイッチまたは登録するシリアル番号を持つ新しく接続されたスイッチを検索します。

ステップ 5 （任意）ノードに関する詳細情報を表示するには、そのノードの行をダブルクリックします。

ACI-mode スイッチのリリースや LLDP ネイバーに関する情報など、さまざまなノード プロパティを示すダイアログが表示されます。

ステップ 6 そのスイッチ行を右クリックして、**[登録（Register）]** を選択し、次のアクションを実行します。

a) 表示されているシリアル番号を確認し、どのスイッチを追加するか決定します。

b) 次の設定を実行または編集します。

フィールド	設定
ポッド ID	ノードが存在するポッドの ID。
ノード ID（Node ID）	100 以上の数字。最初の 100 ID は、Cisco APIC アプライアンス ノードのために予約されています。 （注） リーフ ノードとスパイン ノードには異なる数字をつけることをお勧めします。たとえば、100 の範囲の番号スパイン (例：101、102) と 200 の範囲の番号リーフ (例：201、202)。 ノード ID が割り当てられた後は、更新できません。ノードが **[登録済みノード (Registered Nodes)]** タブ表に追加された後、表の行を右クリックし、**[ノードとラック名の編集 (Edit Node and Rack Name)]** を選択してノードを更新できます。
RL TEP プール	n ノードのトンネル エンドポイント (TEP) プール ID。
ノード名	leaf1 または spine3 などのノード名。

フィールド	設定
ロール（**Role**）	割り当てられたノードの役割。次のオプションがあります。 • **spine** • **leaf** • **virtualleaf** • **virtualspine** • リモート リーフ • 層-2-leaf ノードにデフォルト ロール以外のロールを選択する場合、ロール変更のための登録中にノードは自動的に再起動します。
ラック名	ノードがインストールされているラック名。**[デフォルト (Default)]** を選択するか、**[ラックの作成（Create Rack）]** を選択して、名前と説明を追加します。

c) [Register] をクリックします。

Cisco APIC は IP アドレスをノードに割り当て、ノードが **[登録済みノード（Registered Nodes（]**タブ表に追加されます。次に適切な場合、ノードに接続されている他のノードが検出され、**[登録保留中のノード (Nodes Pending Registration)]** タブ表に表示されます。

ステップ 7 引き続き **[登録保留中のノード (Nodes Pending Registration)]** タブ表をモニタします。ノードが表示されたら、これらの手順を繰り返して、インストールされているノードが登録されるまで新しいノードをそれぞれ登録します。

GUI を使用したディスカバリ前のスイッチの追加

これらの手順に従いスイッチがネットワークに物理的に接続される前に、スイッチの説明を追加できます。

始める前に

スイッチのシリアル番号を把握するようにしてください。

手順

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

ステップ 2 [Navigation] ペインで、[Fabric Membership] を選択します。

ステップ 3 **[登録済みノード (Registered Nodes)]** または **[登録保留中のノード (Nodes Pending Registration)]** 作業ウィンドウで、[アクション (Actions)] アイコンをクリックし、**[ファブリック ノード番号の作成 (Create Fabric Node Member)]** をクリックします。

[ファブリック ノード番号の作成 (Create Fabric Node Member)] ダイアログが表示されます。

ステップ 4 次を設定します。

フィールド	設定
ポッド ID	ノードが存在するポッドを特定します。
シリアル番号（Serial Number）	必須：新しいスイッチのシリアル番号を入力します。
ノード ID（Node ID）	必須：100 以上の数字を入力します。最初の 100 ID は、Cisco Application Policy Infrastructure Controller（APIC）アプライアンス ノードのために予約されています。 （注） リーフ ノードとスパイン ノードには異なる数字をつけることをお勧めします。たとえば、100 の範囲の番号リーフ ノード（例：101、102）と 200 の範囲の番号スパイン ノード（例：201、202）。 ノード ID が割り当てられた後は、更新できません。ノードが **[登録済みノード (Registered Nodes)]** タブ表に追加された後、表の行を右クリックし、**[ノードとラック名の編集 (Edit Node and Rack Name)]** を選択してノードを更新できます。
Switch Name	leaf1 または spine3 などのノード名。

フィールド	設定
ノードタイプ（Node Type）	ノードのタイプ（ロール）を選択します。次のオプションがあります。 • **leaf** 必要に応じて、次のボックスのいずれかをオンにします。 • **Is Remote**：ノードがリモート リーフ スイッチであることを指定します。 • **Is Virtual**：ノードが仮想であることを指定します。 • **Tier-2 Leaf**：作成されるファブリック ノード メンバー（リーフ スイッチ）は、多層アーキテクチャの Tier-2 リーフ スイッチの特性を引き継ぎます。 • **spine** 必要に応じて、次のボックスのいずれかをオンにします。 • **Is Virtual**：ノードが仮想であることを指定します。 • **unknown** ノードにデフォルト ロール以外のロールを選択する場合、ロール変更のための登録中にノードは自動的に再起動します。
VPC ペア	これはオプションです。ノードが vPC ペアの一部である場合は、このノードとペアリングするノードの ID を選択します。
vPC ドメイン ID	vPC ペアの vPC ドメイン ID を入力します。範囲は 1 ～ 1000 です。このフィールドは、**VPC ペア**の値を入力した場合にのみ表示され、その場合は必須です。

Cisco APIC は新しいノードを **[登録保留中のノード (Nodes Pending Registration)]** タブの表に追加します。

次のタスク

物理スイッチをネットワークに接続します。接続されると、Cisco APIC は物理スイッチのシリアル番号と新しいエントリに一致します。新しいスイッチの **[ステータス (Status)](** が **[未検出 (Undiscovered)]** から**[検出済み (Discovered)]** に変更されるまで、**[登録保留中のノード (Nodes Pending Registration)]** をモニタします。Follow the steps in the GUI を使用した未登録スイッチの登録 （69 ページ） セクションの手順に従い、ファブリックの初期化と新しいスイッチのディスカバリ プロセスを完了します。

APIC からのスイッチ検出の検証とスイッチ管理

スイッチが APIC で登録された後、APIC はファブリック トポロジ ディスカバリを自動的に実行し、ネットワーク全体のビューを取得し、ファブリック トポロジ内のすべてのスイッチを管理します。

各スイッチは、個々にアクセスせずに、APIC から設定、モニタ、およびアップグレードできます。

GUI を使用した登録スイッチの検証

手順

ステップ 1 メニュー バーで、**[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ファブリック メンバーシップ (Fabric Membership)]** に移動します。

ステップ 2 **[ファブリック メンバーシップ (Fabric Membership)]** 作業ペインで、**[登録済みノード (Registered Nodes)]** タブをクリックします。
ファブリック内のスイッチがノード ID とともに **[登録済みノード (Registered Nodes)]** タブに表示されます。表に、登録されているすべてのスイッチが割り当てられた IP アドレスとともに表示されます。

ファブリック トポロジの検証

すべてのスイッチが APIC クラスタに登録された後、APIC はファブリック内のすべてのリンクおよび接続を自動的に検出し、その結果トポロジ全体を検出します。

GUI を使用したファブリック トポロジの検証

手順

ステップ 1 メニュー バーで、**[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ポッド番号 (Pod *number*)]** に移動します。

ステップ 2 [Work] ペインで、[Topology] タブをクリックします。
表示された図は、すべての接続されたスイッチ、APICインスタンスおよびリンクを示します。

ステップ 3 （任意） ヘルス、ステータス、インベントリ情報を表示するには、コンポーネント上にカーソルを移動します。

ステップ 4 （任意） リーフ スイッチまたはスパイン スイッチのポートレベルの接続を表示するには、トポロジ図のアイコンをダブルクリックします。

ステップ 5 （任意）トポロジ図を更新するには、**[作業]** ペインの左上隅にある アイコンをクリックします。

VM 管理でのアンマネージド スイッチの接続

VM コントローラ（vCenter など）で管理されているホストはレイヤ 2 スイッチを介してリーフ ポートに接続できます。必要な唯一の前提条件は、レイヤ2スイッチを管理アドレスで設定することです。この管理アドレスは、スイッチに接続されているポート上でLink Layer Discovery Protocol（LLDP）によってアドバタイズされる必要があります。レイヤ 2 スイッチは、APIC によって自動的に検出され、管理アドレスで識別されます。APIC で管理されていないスイッチを表示するには、**[ファブリック (Fabric)] > [インベントリ (Inventory)] > [ファブリック メンバーシップ (Fabric Membership)]** に移動し、**[管理されていないファブリック ノード (Unmanaged Fabric Nodes)]** タブをクリックします。

スイッチ検出の問題のトラブルシューティング

ACI モード スイッチ ソフトウェアには、包括的なリーフおよびスパイン スイッチの検出検証プログラムが含まれています。スイッチが検出モードでスタックした場合には、検証プログラムをスイッチの CLI コマンドで起動してください。

検証プログラムは、次のテストを実行します。

1. システム状態：`topSystem` 管理対象オブジェクト (MO) の状態を確認します。
    1. 状態が「サービス停止中（out-of-service）」の場合、スケジュールされたアップグレードがないかどうかを確認します。
    2. 状態が「ブートスクリプトのダウンロード中（downloading bootscript）」の場合、ブートスクリプトのダウンロードに失敗しています。失敗が報告されます。スイッチが L3out スパインの場合、プログラムはさらにブートストラップ ダウンロードの状態をチェックし、障害があれば報告します。
2. DHCP ステータス：TEP IP、ノード ID、`dhcpResp` MO から割り当てられた名前などの DHCP ステータスと情報を確認します。
3. AV の詳細：APIC が登録されているかどうか、および APIC に有効な IP アドレスがあるかどうかを確認します。
4. IP 到達可能性：**iping** コマンドを使用して、アドレス割り当て元 APIC への IP 到達可能性を確認します。この状態を再テストするには、**show discoveryissues apic***ipaddress* コマンドを使用します。
5. インフラ VLAN の受信：`lldpInst` MO にインフラ VLAN の詳細が存在するかどうかを確認します。このスイッチが APIC のないポッドに属している場合、インフラ VLAN の詳細は存在しないため、テスト結果のこのセクションは無視できます。

6. LLDP 隣接関係：LLDP 隣接関係の存在と、ワイヤリングの不一致の問題をチェックします。LLDP の問題により、インフラ VLAN の不一致、シャーシ ID の不一致、フロントエンド ポートへの接続がないなどの障害レポートが生成される可能性があります。
7. スイッチ バージョン：スイッチの実行中のファームウェア バージョンを報告します。APIC のバージョンも報告します（利用可能な場合）。
8. FPGA/BIOS：スイッチの FPGA/BIOS バージョンの不一致をチェックします。
9. SSL 検証：**acidiag verifyssl -s***serialNumber* コマンドを使用して、SSL 証明書の詳細の有効性を確認します。
10. ポリシーのダウンロード：`pconsBootStrap` MO をチェックして、APIC (PM シャード) への登録が完了しているかどうか、およびすべてのポリシーが正常にダウンロードされたかどうかを確認します。
11. 時間：スイッチの現在の時刻を報告します。
12. ハードウェア ステータス：`eqptCh`、`eqptFan`、`eqptPsu`、`eqptFt`および `eqptLC` MO からモジュール、電源、およびファンのステータスを確認します。

テストの手動実行

スイッチ検出検証プログラムを実行するには、スパインまたはリーフ スイッチの CLI コンソールにログインし、次のコマンドを実行します。

show discoveryissues [apic *ipaddress***]**

テストの成功例

次の例は、テストが成功した場合のスイッチ検出検証プログラムの出力を示しています。

```
spine1# show discoveryissues

Checking the platform type.................SPINE!
Check01 - System state - in-service                [ok]
Check02 - DHCP status                [ok]
    TEP IP: 10.0.40.65 Node Id: 106 Name: spine1
Check03 - AV details check                [ok]
Check04 - IP rechability to apic                [ok]
    Ping from switch to 10.0.0.1 passed
Check05 - infra VLAN received                [ok]
    infra vLAN:1093
Check06 - LLDP Adjacency                [ok]
    Found adjacency with LEAF
Check07 - Switch version                [ok]
    version: n9000-14.2(0.167)  and apic version: 5.0(0.25)
Check08 - FPGA/BIOS out of sync test                [ok]
Check09 - SSL check                [check]
    SSL certificate details are valid
Check10 - Downloading policies                [ok]
Check11 - Checking time                [ok]
    2019-08-21 17:15:45
Check12 - Checking modules, power and fans                [ok]
```

テストの失敗例

次の例は、検出機能に問題があるスイッチのスイッチ検出検証プログラムの出力を示しています。

```
spine1# show discoveryissues

Checking the platform type.................SPINE!
Check01 - System state - out-of-service                [FAIL]
    Upgrade status is notscheduled
    Node upgrade is notscheduled state
Check02 - DHCP status                 [FAIL]
    ERROR: discover not being sent by switch
    Ignore this, if the IP is already known by switch
    ERROR: node Id not configured
    ERROR: Ip not assigned by dhcp server
    ERROR: Address assigner's IP not populated
    TEP IP: unknown Node Id: unknown Name: unknown
Check03 - AV details check                [ok]
Check04 - IP reachability to apic                [FAIL]
    please rerun the CLI with argument apic Ip
    (show discoveryissues apic <ip>) to check its reachability from switch
Check05 - infra VLAN received                [FAIL]
    Please ignore if this switch is part of a pod with no apic
Check06 - LLDP Adjacency                [FAIL]
    Error: spine not connected to any leaf
Check07 - Switch version                [ok]
    version: n9000-14.2(0.146)  and apic version: unknown
Check08 - FPGA/BIOS out of sync test                [ok]
Check09 - SSL check                [ok]
    SSL certificate details are valid
Check10 - Downloading policies                [FAIL]
    Registration to all PM shards is not complete
    Policy download is not complete
    Pcons booststrap is in triggered state
Check11 - Checking time                [ok]
    2019-07-17 19:26:29
Check12 - Checking modules, power and fans                [FAIL]
    Line card state is testing
```

GUI を使用してスイッチ インベントリを検索する

このセクションでは、Cisco APIC GUI を使用してスイッチのモデルとシリアル番号を検索する方法について説明します。

始める前に

Cisco APIC GUI にアクセスできる必要があります。

手順

ステップ 1 メニュー バーで **[ファブリック（Fabric）] > [インベントリ（Inventory）]** を選択します。
ステップ 2 ナビゲーション ペインで **[ポッド（Pod）]** アイコンをクリックします。

ナビゲーション ペインにスイッチ アイコンが表示されます。

ステップ 3 ナビゲーション ペインでスイッチ アイコンをクリックします。
作業ウィンドウの上部にタブのリストが表示されます。

ステップ 4 [General] タブをクリックします。
作業ペインにスイッチ情報が表示されます。

スイッチ検出の問題のトラブルシューティング

ACI モード スイッチ ソフトウェアには、包括的なリーフおよびスパイン スイッチの検出検証プログラムが含まれています。スイッチが検出モードでスタックした場合には、検証プログラムをスイッチの CLI コマンドで起動してください。

検証プログラムは、次のテストを実行します。

1. システム状態：`topSystem` 管理対象オブジェクト (MO) の状態を確認します。
    1. 状態が「サービス停止中（out-of-service）」の場合、スケジュールされたアップグレードがないかどうかを確認します。
    2. 状態が「ブートスクリプトのダウンロード中（downloading bootscript）」の場合、ブートスクリプトのダウンロードに失敗しています。失敗が報告されます。スイッチが L3out スパインの場合、プログラムはさらにブートストラップ ダウンロードの状態をチェックし、障害があれば報告します。
2. DHCP ステータス：TEP IP、ノード ID、`dhcpResp` MO から割り当てられた名前などの DHCP ステータスと情報を確認します。
3. AV の詳細：APIC が登録されているかどうか、および APIC に有効な IP アドレスがあるかどうかを確認します。
4. IP 到達可能性：**iping** コマンドを使用して、アドレス割り当て元 APIC への IP 到達可能性を確認します。この状態を再テストするには、**show discoveryissues apic***ipaddress* コマンドを使用します。
5. インフラ VLAN の受信：`lldpInst` MO にインフラ VLAN の詳細が存在するかどうかを確認します。このスイッチが APIC のないポッドに属している場合、インフラ VLAN の詳細は存在しないため、テスト結果のこのセクションは無視できます。
6. LLDP 隣接関係：LLDP 隣接関係の存在と、ワイヤリングの不一致の問題をチェックします。LLDP の問題により、インフラ VLAN の不一致、シャーシ ID の不一致、フロントエンド ポートへの接続がないなどの障害レポートが生成される可能性があります。
7. スイッチ バージョン：スイッチの実行中のファームウェア バージョンを報告します。APIC のバージョンも報告します（利用可能な場合）。
8. FPGA/BIOS：スイッチの FPGA/BIOS バージョンの不一致をチェックします。

9. SSL 検証：**acidiag verifyssl -s***serialNumber* コマンドを使用して、SSL 証明書の詳細の有効性を確認します。
10. ポリシーのダウンロード：`pconsBootStrap` MO をチェックして、APIC (PM シャード) への登録が完了しているかどうか、およびすべてのポリシーが正常にダウンロードされたかどうかを確認します。
11. 時間：スイッチの現在の時刻を報告します。
12. ハードウェア ステータス：`eqptCh`、`eqptFan`、`eqptPsu`、`eqptFt`および `eqptLC` MO からモジュール、電源、およびファンのステータスを確認します。

テストの手動実行

スイッチ検出検証プログラムを実行するには、スパインまたはリーフ スイッチの CLI コンソールにログインし、次のコマンドを実行します。

show discoveryissues [apic *ipaddress***]**

テストの成功例

次の例は、テストが成功した場合のスイッチ検出検証プログラムの出力を示しています。

```
spine1# show discoveryissues

Checking the platform type.................SPINE!
Check01 - System state - in-service                [ok]
Check02 - DHCP status                 [ok]
    TEP IP: 10.0.40.65 Node Id: 106 Name: spine1
Check03 - AV details check                [ok]
Check04 - IP rechability to apic                [ok]
    Ping from switch to 10.0.0.1 passed
Check05 - infra VLAN received                [ok]
    infra vLAN:1093
Check06 - LLDP Adjacency                [ok]
    Found adjacency with LEAF
Check07 - Switch version                [ok]
    version: n9000-14.2(0.167)  and apic version: 5.0(0.25)
Check08 - FPGA/BIOS out of sync test                [ok]
Check09 - SSL check                [check]
    SSL certificate details are valid
Check10 - Downloading policies                [ok]
Check11 - Checking time                [ok]
    2019-08-21 17:15:45
Check12 - Checking modules, power and fans                [ok]
```

テストの失敗例

次の例は、検出機能に問題があるスイッチのスイッチ検出検証プログラムの出力を示しています。

```
spine1# show discoveryissues

Checking the platform type.................SPINE!
Check01 - System state - out-of-service                [FAIL]
```

```
    Upgrade status is notscheduled
    Node upgrade is notscheduled state
Check02 - DHCP status                [FAIL]
    ERROR: discover not being sent by switch
    Ignore this, if the IP is already known by switch
    ERROR: node Id not configured
    ERROR: Ip not assigned by dhcp server
    ERROR: Address assigner's IP not populated
    TEP IP: unknown Node Id: unknown Name: unknown
Check03 - AV details check                [ok]
Check04 - IP reachability to apic                [FAIL]
    please rerun the CLI with argument apic Ip
    (show discoveryissues apic <ip>) to check its reachability from switch
Check05 - infra VLAN received                [FAIL]
    Please ignore if this switch is part of a pod with no apic
Check06 - LLDP Adjacency                [FAIL]
    Error: spine not connected to any leaf
Check07 - Switch version                [ok]
    version: n9000-14.2(0.146)  and apic version: unknown
Check08 - FPGA/BIOS out of sync test                [ok]
Check09 - SSL check                [ok]
    SSL certificate details are valid
Check10 - Downloading policies                [FAIL]
    Registration to all PM shards is not complete
    Policy download is not complete
    Pcons booststrap is in triggered state
Check11 - Checking time                [ok]
    2019-07-17 19:26:29
Check12 - Checking modules, power and fans                [FAIL]
    Line card state is testing
```

メンテナンス モード

メンテナンス モード

メンテナンス モードを使用する際に理解に役立つ用語を紹介します。

- **メンテナンス モード**：デバッグ目的でユーザー トラフィックからスイッチを分離するために使用されます。**ファブリック**インベントリ ファブリック メンバーシップ**にある APIC GUI の** [ファブリック メンバーシップ（Fabric Membership）] **ページの** > **[メンテナンス（GIR）（Maintenance（GIR））]**> **フィールドを有効にすることで、スイッチを** > **メンテナンス モード** > **にできます**（スイッチを右クリックして **[メンテナンス（GIR）Maintenance（GIR）]** を選択します）。

  スイッチを**メンテナンス モード**にすると、そのスイッチは動作可能な ACI ファブリック インフラストラクチャの一部とは見なされず、通常の APIC 通信は受け入れられません。

メンテナンスモード使用してスイッチを正常に取り出し、そのスイッチをネットワークから分離して、デバッグ操作を実行することができます。スイッチは、最小限のトラフィックの中断だけで、通常の転送パスから取り外されます。

正常に削除、外部のすべてのプロトコルが適切に電源を切るファブリック プロトコル (IS-IS) を除くと、スイッチは、ネットワークから切り離します。メンテナンスモード時に、最大メト

リックは IS-IS 内でアドバタイズ、 Cisco Application Centric Infrastructure (Cisco ACI) ファブリックおよびそのため、メンテナンス モードがスパイン スイッチからのトラフィックをひく点されません。さらに、スイッチの前面パネルのすべてのインターフェイスが、スイッチ ファブリック インターフェイスを除いてシャット ダウンされます。デバッグ操作後にスイッチを完全動作（通常）モードに戻すには、スイッチをリコミッショニングさせる必要があります。この操作により、スイッチのステートレス リロードがトリガーされます。

グレースフルの挿入で、スイッチは自動的にデコミッショニング、再起動、およびリコミッショニングされます。リコミッショニングが完了したら、外部のすべてのプロトコルを復元し、IS-IS で最大のメトリックは 10 分後にリセットされます。

次のプロトコルがサポートされています。

- Border Gateway Protocol（BGP）
- Enhanced Interior Gateway Routing Protocol（EIGRP）
- Intermediate System-to-Intermediate System（IS-IS）
- Open Shortest Path First（OSPF）
- リンク集約制御プロトコル（LACP）

プロトコルに依存しないマルチキャスト (PIM) はサポートされていません。

特記事項

- 境界リーフ スイッチに静的ルートがあり、メンテナンス モードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。

  この問題を回避するには、次のいずれかを実行します。

  - その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、
  - 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します

- イーサネット ポート モジュールでは、インターフェイスを増殖停止、スイッチは、メンテナンス モードでは、通知に関連します。その結果、リモート スイッチを再起動するか、またはこの時間中にファブリック リンクかを調べますは、ファブリック リンクはありません確立した後で、スイッチがリブート手動でない限り (を使用して、 **acidiag タッチ クリーン** コマンド)、廃棄、および recommissioned。
- スイッチがメンテナンス モード中の場合、スイッチの CLI「show」コマンドでは、前面パネル ポートがアップ状態であり、BGP プロトコルがアップ状態かつ実行中であることを示します。インターフェイスは実際にシャットダウンされ、BGP のその他すべての隣接関係がダウンしますが、表示されているアクティブ状態でデバッグが可能です。
- マルチポッド/マルチサイトの場合、ノードをファブリックに戻すときのトラフィックの中断を最小限に抑えるために、 **再配布されるルートの IS-IS メトリックを** 63 未満に設定する必要があります。**再配布されるルートの IS-IS メトリック**を設定するには、**[ファブ**

リック（**Fabric**）**]** > **[** ファブリック ポリシー（**Fabric Policies**）**]** > **[**ポッド ポリシー（**Pod Policies**）**]** > **[IS-IS** ポリシー（**IS-IS Policy**）**]**を選択します。

- スパインまたはリーフを再起動し、 IS-IS 隣接関係がアップした後、 **再配布されたルートの IS-IS メトリックが** 高くアドバタイズされます。これは 34 であり、 ECMP ネクストホップとして使用できません。
- 既存の登場させには、すべてのレイヤ3トラフィック迂回がサポートされています。LACP でレイヤ 2 のすべてのトラフィックは、冗長ノードを迂回も。ノードは、メンテナンスモードに入ります、されるとすぐに、ノードで実行されているLACPは、不要になった集約できるようにポートチャネルの一部としてネイバーを通知します。すべてのトラフィックは vPC ピア ノードを迂回します。
- メンテナンス モードでは、次の操作は許可されません。
  - **アップグレード**：ネットワークを新しいバージョンにアップグレードすること
  - **ステートフル リロード**：GIR ノードまたはその接続されたピアの再起動
  - **ステートレス リロード**：GIR ノードまたはその接続されたピアのクリーン設定または電源再投入による再起動
  - **リンク操作**：GIR ノードまたはそのピアノードでのシャットダウン/非シャットダウンまたは光ファイバの OIR（オンラインでの挿入または取り外し）
  - **構成変更**：設定変更（クリーン構成、インポート、スナップショット ロールバックなど）
  - **ハードウェアの変更**：ハードウェアの変更（FRU または RMA の追加、交換、削除など）

GUI を使用してスイッチをメンテナンス モードに移行する

GUI を使用してスイッチをメンテナンス モードに移行するには、次の手順を使用します。スイッチがメンテナンスモードに移行していても、アウトオブバンド管理インターフェイスは以前動作しており、アクセスが可能です。

手順

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

ステップ 2 ナビゲーション ウィンドウで、**Fabric Membership** をクリックします。

ステップ 3 作業ウィンドウで、**[**アクション（**Actions**）**]** > **[**メンテナンス（**Maintenance (GIR)**）**]** をクリックします。

ステップ 4 [OK] をクリックします。

安全に移行したスイッチでは、**Debug Mode** というメッセージが **Status** コラムに表示されます。

GUI を使用してスイッチを挿入し、動作モードにする

GUI を使用してスイッチを挿入し、動作モードにするには、次の手順に従います。

手順

ステップ 1 メニュー バーで、 **Fabric** > **Inventory** を選択します。
ステップ 2 ナビゲーション ウィンドウで、**Fabric Membership** をクリックします。
ステップ 3 作業ペインの **[登録済みノード (Registered Nodes)]** テーブルで、操作モードに対して挿入するスイッチの行を右クリックして、**[コミッション (Commision)]** を選択します。
ステップ 4 [はい（Yes）] をクリックします。

Cisco NX-OS から Cisco ACI POAP への自動変換

Cisco NX-OSからCisco ACI POAPへの自動変換について

5.2(3) リリースより、Cisco NX-OS から Cisco Application Centric Infrastructure（ACI）Power On Auto Provisioning（POAP）への自動変換によって、最初にネットワークに展開されたノードでソフトウェアイメージをアップグレードし、スイッチ上に構成ファイルをインストールするプロセスを自動化できます。POAP 自動変換機能を備えた Cisco NX-OSノードが起動し、スタートアップ構成が見つからない場合、ノードは POAP モードに入り、すべてのポートで DHCP ディスカバリを開始します。ノードは DHCP サーバーを見つけ、インターフェイス IP アドレス、ゲートウェイ、DNS サーバー IP アドレスを使用して自らをブートストラップします。また、TFTP サーバの IP アドレスを取得し、構成スクリプトをダウンロードします。このスクリプトはノード上で有効化され、適切なソフトウェアイメージと構成ファイルをダウンロードしてインストールします。このプロセスは、Cisco NX-OSノードをスタンドアロンモードからCisco ACI -mode に変換します。

Cisco NX-OS ノードを POAP を使用するCisco ACIノードに自動変換するには、自動変換が必要な Cisco NX-OS ノードに接続されているCisco ACIスイッチノードのインターフェイスを指定する必要があります。Cisco ACIスイッチで指定されたインターフェイスにより、POAP の処理が有効になり、Cisco NX-OS ノードが自動変換用の DHCP サーバとしてCisco Application Policy Infrastructure Controller（APIC）を使用できるようになります。Cisco ACIスイッチノードはすでにCisco ACIファブリックに登録されており、アクティブである必要があります。つまり、ノードはCisco APICクラスタから到達可能である必要があります。この自動変換は、ファブ

リックに新しいスイッチを追加するとき、または既存のCisco ACIスイッチを置き換えるときに使用できます。

Cisco NX-OS から Cisco ACI POAP への自動変換の注意事項と制限事項

Cisco NX-OS を使用してCisco Application Centric Infrastructure（ACI）電源投入時自動プロビジョニング（POAP）自動変換を行う場合は、次の注意事項と制約事項が適用されます。

- 変換中の Cisco NX-OS ノードは、管理を含むすべてのインターフェイスで検出パケットの送信を開始するため、Cisco Application Policy Infrastructure Controller（APIC）のサーバを除くすべての外部 DHCP サーバは、POAP 検出パケットをインターセプトし、変換を中断します。
- Cisco NX-OS から Cisco ACIPOAPへの自動変換は、変換対象の NX-OS デバイスが Cisco APIC クラスタに到達可能な既存の Cisco ACIスイッチ ノードに接続されている場合にサポートされます。このため、次のシナリオはサポートされていません。
  - APIC 1 から最初の Cisco ACI スイッチを検出する場合。
  - Cisco APIC がリーフ ノードにシングル ホーム接続されているときに Cisco ACIリーフ ノードを交換する場合。
  - IPN デバイスのみを介して Cisco APIC クラスタに到達する Cisco ACI スイッチを追加または交換する場合。つまり、Cisco NX-OS ノードを新しいリモート リーフ ノードとして追加する場合、Cisco NX-OS ノードを新しいポッドの最初のスパイン ノードとして追加する場合、リモート リーフ ノードを置き換える場合、または Cisco ACI マルチポッド セットアップでスパイン ノードをポッド内の唯一のスパイン ノードで置き換える場合です。このシナリオは、IPN デバイスで必要な構成を備えた Cisco APIC 5.2(4) リリースからサポートされています。
- モジュラー スパイン ノード スーパーバイザの交換はサポートされていません。
- POAP は、製品 ID（PID）に -EX、-FX、-GX、またはそれ以降のサフィックスを持つスイッチ、および Cisco N9K-C9364C および N9K-C9332C スイッチをサポートします。
- スパインまたはリーフ ノードを自動変換した後、**show system reset-reason** CLI コマンドは変換に関する情報を表示しません。出力には次の情報のみが表示されます。

  ```
  reset-requested-by-cli-command-reload
  ```

- Cisco ACI スイッチと Cisco NX-OS スイッチの間には光ケーブルを使用する必要があります。この場合、銅ケーブルは使用できません。
- 自動変換に使用する必要がある Cisco ACI スイッチ イメージは、Cisco APICクラスタのファームウェア リポジトリに存在する必要があります。**[Admin]** > **[Firmware]** > **[Images]** に移動して、GUI を使用してイメージが存在することを確認できます。
- POAP を使用した Cisco NX-OS から Cisco ACI への自動変換は、ターゲット スイッチのリリースが 16.0(3) 以降で、スイッチで実行されている現在のリリースが Cisco NX-OS 9.3(12) 以前の場合はサポートされません。この状態で POAP を使用して Cisco NX-OS を ACI 自

動変換に使用しようとすると、スイッチが無期限にスタックする可能性があります。これらの条件で Cisco NX-OS を Cisco ACI に変換するには、アップグレードを手動で行う必要があります

GUI を使用した POAP 自動変換を使用した Cisco NX-OS ノードから ACI への変換

次の手順では、既存の Cisco NX-OS ノードをスタンドアロンモードから電源投入時自動プロビジョニング（POAP）自動変換を使用するCisco ACIモードに変換します。このプロセスでは、ノードは解放されません。

始める前に

ターゲットCisco ACIファームウェアバージョンを使用して、**スイッチ検出時の自動ファームウェア更新**を有効にしておく必要があります。詳細については、『*Cisco APIC Getting Started Guide*』を参照してください。

手順

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

ステップ 2 [Navigation] ペインで、[Fabric Membership] を選択します。

ステップ 3 作業ペインで、**[登録済みノード (Registered Nodes)]** タブをクリックします。

ステップ 4 （任意） 既存のCisco ACIスイッチノードをNX-OSを実行している新しいスイッチと交換する場合は、交換するノードを右クリックし、通常の交換シナリオと同様に**[コントローラから削除（Remove From Controller）]**を選択します。

ステップ 5 テーブルの右上にあるアクションメニューで、 **[Add with NXOS to ACI Conversion]** を選択します。

交換シナリオでは、交換するスイッチノードが停止または非アクティブになっている場合は、ノードを右クリックして **[Replace with NXOS to ACI Conversion]** を選択することもできます。これにより、ステップ 4 の**[コントローラからの削除（Remove From Controller）]**とステップ 5 の **[NXOSからACIへの変換（Add with NXOS to ACI Conversion）]** が同時に実行されます。

ステップ 6 ダイアログで、次のようにフィールドを入力します。

- **ノードID**：変換するノードに接続されているノードのIDを選択します。ゴミ箱をクリックしてノードを削除するか、+ をクリックして別のノードを追加できます。少なくとも 1 つのノードを指定してください。追加のノードを設定するときにGUIでさらにスペースが必要な場合は、**[インターフェイスの非表示（Hide Interfaces）]**をクリックしてインターフェイス情報を非表示にできます。
- **インターフェイス ID** ：変換するノードに接続されているノードのインターフェイスのIDを選択します。ゴミ箱をクリックしてインターフェイスを削除するか、+をクリックして

別のインターフェイスを追加できます。POAP自動変換のPOAPを処理するように、各ノードで 1 つのインターフェイスのみを設定します。

ステップ 7 **[送信（Submit）]** をクリックします。`

ステップ 8 **[登録保留中のノード（ Nodes Pending Registration ）]** タブを選択します。

ノードがこのタブに現れた後のノード登録手順は、通常の Cisco ACI スイッチの場合と同じです。

ステップ 9 （任意）スイッチが登録され、アクティブステータスのファブリックに参加した後、ステップ6で設定したインターフェイスのPOAP自動変換設定を削除できます。変換が完了したら、接続されているノードからPOAP設定を削除してください。

a) **[登録済みノード（Registered Nodes）]**タブを選択します。
b) POAP 設定を削除するノードの行をダブルクリックします。
c) ダイアログで、**[NXOS変換ポリシー（NXOS Conversion Policy ）]**タブを選択します。
d) 削除したいパス名を選択し、削除アイコン（ゴミ箱）をクリックします。

Cisco Nexus 9000 スイッチの安全な消去

Cisco Nexus 9000 スイッチの安全な消去について

Cisco Nexus 9000 スイッチは、永続的なストレージを利用して、システム ソフトウェア イメージ、スイッチ構成、ソフトウェア ログ、および動作履歴を維持します。これらの各エリアには、ネットワーク アーキテクチャや設計の詳細など、ユーザ固有の情報と、潜在的な攻撃者からの目標ベクトルが含まれている可能性があります。安全な消去機能を使用すると、この情報を包括的に消去できます。これは、返品許可（RMA）を使用してスイッチを返品するとき、スイッチをアップグレードまたは交換するとき、または寿命に達したシステムを廃止するときに実行できます。

セキュア消去は、Cisco APIC リリース 6.0(x) からサポートされています。ファブリック内のすべてのリーフおよびスパイン スイッチは、APIC リリース 6.0(x) 以降である必要があります。

この機能は、次のストレージ デバイスのユーザ データを消去します。

- SSD
- EMMC
- MTD
- CMOS
- NVRAM

（注） すべてのスイッチ モデルにこれらすべてのストレージ デバイスがあるわけではありません。

GUI を使用した Cisco Nexus 9000 スイッチのユーザー データの安全な消去

GUI を使用して Cisco Nexus 9000 スイッチのユーザー データを安全に消去するには、次の手順に従います。

手順

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

ステップ 2 [Navigation] ペインで、[Fabric Membership] を選択します。

ステップ 3 [作業（Work）]ペインで、安全に消去するスイッチ（ノード）を右クリックし、**[デコミッション（Decommission）]** を選択します。

ステップ 4 **[デコミッション（Decommission）]**ダイアログで、**[デコミッションと安全な削除（Decommission & Secure Remove）]** を選択します。

ステップ 5 [OK] をクリックします。

デコミッション プロセスには、スイッチと SSD のタイプに応じて 2 ～ 8 時間かかります。このプロセスにより、スイッチが安全に消去され、スイッチ設定が Cisco Application Policy Infrastructure Controller（APIC ）から削除されます。安全な消去プロセスでは、ブートフラッシュから NX-OS イメージは削除されません。スイッチを手動で再登録するまで、スイッチはファブリックに参加できません。

安全な消去操作が完了すると、スイッチが再起動します。IPアドレスに到達できないため、スイッチに接続するには、端末コンソールを使用する必要があります。

GUI を使用して Cisco Nexus 9000 モジュラ スイッチ ラインカードのモジュールからユーザー データを安全に消去する

GUI を使用して Cisco Nexus 9000 モジュラ スイッチ ラインカードのモジュールからユーザー データを安全に消去するには、次の手順に従います。

手順

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

ステップ 2 [ナビゲーション（Navigation pane）] ペインで、***[pod_id]*** > ***[node_id]*** > **[シャーシ（Chassis）]** > **[ライン モジュール（Line Modules）]** > ***[slot_id]*** を選択します。

ステップ 3 スロット ID を右クリックし、**[無効化（Disable）]** を選択します。

ステップ 4 **[無効化（Disable）]** ダイアログで、**[安全な消去（Secure Erase）]** をクリックします。

デコミッション プロセスには、スイッチと SSD のタイプに応じて 30 分 ～ 2 時間かかります。このプロセスにより、スイッチのモジュールからデータが安全に消去され、モジュールの設定が Cisco Application Policy Infrastructure Controller（APIC）から削除されます。このプロセスでは、ブートフラッシュから NX-OS イメージは削除されません。

安全な消去操作が完了すると、モジュールはパワーダウン状態になります。IP アドレスに到達できないため、スイッチに接続するには、端末コンソールを使用する必要があります。

スイッチの CLI を使用して Cisco Nexus 9000 スイッチからユーザー データを安全に消去する

スイッチの CLI を使用して Cisco Nexus 9000 スイッチからユーザー データを安全に消去するには、次の手順を使用します。この手順では、Cisco Application Policy Infrastructure Controller（APIC）の CLI を使用することはできません。

始める前に

CLI を使用して安全な消去操作を実行する前に、スイッチをデコミッションするか、スイッチをファブリックから物理的に切断します。スイッチをデコミッションしないか、スイッチをファブリックから物理的に切断しないと、安全な消去プロセスが完了した後に、Cisco APIC から構成がスイッチに再度プッシュされます。

手順

ステップ 1 スイッチの CLI にログインします。

ステップ 2 仮想シェルに入ります。

```
leaf1# vsh
```

ステップ 3 ターミナルのセッション タイムアウトを無効化します。

```
leaf1# terminal session-timeout 0
```

タイムアウトを無効にしないと、安全な消去が完了してステータスを提示できるようになる前に、VSH セッションがタイムアウトして終了する可能性があります。

ステップ 4 スイッチを工場出荷時の設定にリセットします。これにより、スイッチからデータが安全に消去されます。

```
leaf1# factory-reset [preserve-image] [module module_number]
```

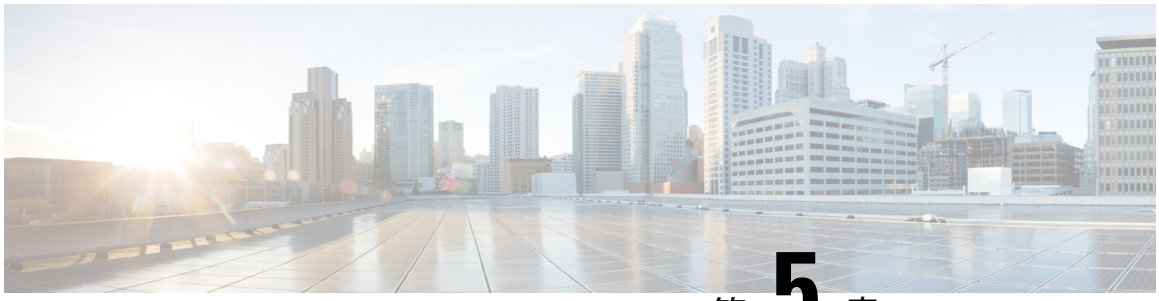
- `preserve-image`：スイッチのブートフラッシュに NX-OS イメージを保持するには、このフラグを指定します。このフラグを指定しなかった場合、NX-OS イメージも消去され、スイッチはローダー プロンプトで起動します。
- `module module_number`：モジュラ スイッチ ラインカードおよびファブリック モジュールの場合、安全な消去を実行するモジュールの番号を指定する必要があります。

非モジュラ スイッチの場合、スイッチと SSD のタイプに応じて、デコミッション プロセスには 2 ～ 8 時間かかります。このプロセスにより、スイッチが安全に消去され、スイッチ設定が Cisco Application Policy Infrastructure Controller（APIC ）から削除されます。安全な消去プロセスでは、ブートフラッシュから NX-OS イメージは削除されません。スイッチを手動で再登録するまで、スイッチはファブリックに参加できません。

安全な消去操作が完了すると、スイッチが再起動します。IP アドレスに到達できないため、スイッチに接続するには、端末コンソールを使用する必要があります。

モジュラ スイッチ ラインカードまたはファブリック モジュールの場合、デコミッション プロセスには、スイッチと SSD のタイプに応じて 30 分から 2 時間かかります。このプロセスにより、スイッチのモジュールからデータが安全に消去され、モジュールの構成が Cisco APIC から削除されます。このプロセスでは、ブートフラッシュから NX-OS イメージは削除されません。

安全な消去操作が完了すると、モジュールはパワーダウン状態になります。IP アドレスに到達できないため、スイッチに接続するには、端末コンソールを使用する必要があります。



第 5 章

Cisco APIC クラスタの管理

APIC クラスタ

Application Policy Infrastructure Controller (APIC) アプライアンスは、クラスタに配置されます。Cisco ACI ファブリックを制御するためには、クラスタ内で少なくとも3台のコントローラを設定します。コントローラ クラスタの最終的なサイズは、ACI導入のサイズに直接正比例し、トランザクション レートの要件によって決まります。クラスタ内のコントローラは、あらゆるユーザのあらゆる操作に対応できます。また、クラスタのコントローラは、透過的に追加または削除できます。

このセクションでは、APIC クラスタの拡張、契約、および回復に関連する例を示します。

Cisco APIC Cluster のクラスタの拡大

Cisco APIC のクラスタの拡大とは、正当な境界内で、クラスタ サイズを N から N+1 へサイズの不一致を増加させる動作です。オペレータが管理クラスタ サイズを設定し、適切なクラスタ ID の APIC を接続すると、クラスタが拡張を実行します。

クラスタの拡大時は、APIC コントローラを物理的に接続した順序に関係なく、APIC の ID 番号順に検出および拡大が実行されます。たとえば、APIC2 が APIC1 の後で検出され、APIC3 が APIC2 の後に検出され、以降、クラスタに追加する必要のあるすべての APIC が検出されるまで続行されます。各 APIC が順番に検出されるとともに、単一または複数のデータ パスが確立され、パスに沿ってすべてのスイッチがファブリックに参加します。拡張プロセスは稼動中のクラスタ サイズが管理クラスタ サイズと同等に達するまで続行されます。

Cisco APIC クラスタの縮小

Cisco APIC クラスタの縮小とは、正当な境界内で、クラスタ サイズ N から N -1 へサイズの不一致を軽減する動作です。縮小によってクラスタ内の残りの APIC の計算およびメモリの負荷が増大し、解放された APIC クラスタのスロットはオペレータ入力だけで使用できなくなります。

クラスタの縮小の際は、クラスタ内の最後の APIC を最初に解放し、以降逆順で連続的に行います。たとえば、APIC4 は APIC3 の前に解放し、APIC3 は APIC2 の前に解放する必要があります。

クラスタ管理の注意事項

Cisco Application Policy Infrastructure Controller (APIC) クラスタは複数の Cisco APIC コントローラで構成され、Cisco Application Centric Infrastructure（ACI）ファブリックに対する統合されたリアルタイム モニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスが得られるように、Cisco APIC クラスタを変更する場合は次のガイドラインに使用してください：

- クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の Cisco APIC のヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。また、Cisco APIC に追加されたクラスタ コントローラが Cisco APIC クラスタ内の他のコントローラと同じファームウェア バージョンを実行しているか確認してください。
- クラスタ内には少なくとも 3 つのアクティブな Cisco APIC があり、追加のスタンバイ Cisco APIC があることを推奨します。 Cisco APIC クラスタには、3 ～ 7 個のアクティブな Cisco APIC を含めることができます。展開に必要なアクティブな Cisco APIC の数を確認するには、『検証済みスケーラビリティ ガイド』を参照してください。

- 現在クラスタにない Cisco APIC からのクラスタ情報は無視します。正確なクラスタ情報ではありません。
- クラスタ スロットには Cisco APIC `ChassisID` を含みます。スロットを設定すると、割り当てられたシャーシ `ID` の Cisco APIC を解放するまでそのスロットは使用できません。
- Cisco APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが完全に適合するまでクラスタへの他の変更はしないでください。
- Cisco APIC を移動する際は、最初に正常なクラスタがあることを確認します。Cisco APIC クラスタの状態を確認するには、後にシャットダウンする Cisco APIC を選択します。Cisco APIC をシャットダウンした後、Cisco APIC に移動し、再接続して、電源を入れます。GUI から、クラスタ内のすべてのコントローラが完全に適合状態に戻すことを確認します。

（注） 一度に 1 つの Cisco APIC のみ移動します。

- 一連のリーフ スイッチに接続されている Cisco APIC を別のリーフ スイッチのセットに移動する場合、または Cisco APIC を同じリーフ スイッチ内の別のポートに移動する場合は、まずクラスタが正常であることを確認します。Cisco APIC クラスタの状態を確認したら、移動してクラスタからデコミッションする Cisco APIC を選択します。Cisco APIC がデコミッションされたら、 Cisco APIC を移動してコミッションします。
- Cisco APIC クラスタを設定する前に、すべての Cisco APIC のパフォーマンスが同じファームウェア バージョンを実行していることを確認します。異なるバージョンを実行して Cisco APIC のパフォーマンスの最初のクラスタ リングはサポートされていない動作し、クラスタ内の問題が発生する可能性があります。
- 他のオブジェクトとは異なり、ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの 1 つのシャードにのみ保存されます。これらのオブジェクトは、使用停止または Cisco APIC交換すると永久に失われます。
- Cisco APICをデコミッションすると、Cisco APIC に保存されていたすべての障害、イベント、および監査ログ履歴が失われます。すべての Cisco APIC を交換すると、すべてのログ履歴が失われます。Cisco APICを移行する前に、ログ履歴を手動でバックアップすることをお勧めします。

APIC クラスタ サイズの拡大

APIC クラスタ サイズを拡大するには、次のガイドラインに従ってください。

- クラスタの拡大がファブリックのワークロードの要求に影響しないときに、クラスタの拡大を予定します。
- クラスタ内の 1 つ以上の APIC コントローラのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。

- ハードウェア インストレーション ガイドの手順に従って、新しい APIC コントローラを準備します。PING テストでインバンド接続を確認します。
- クラスタの目標サイズを既存のクラスタ サイズ コントローラ数に新規コントローラ数を加えた数になるように増やします。たとえば、既存のクラスタ サイズ コントローラの数が 3 で、3 台のコントローラを追加する場合は、新しいクラスタの目標サイズを 6 に設定します。クラスタは、クラスタにすべての新規コントローラが含まれるまで一度にコントローラ 1 台ずつ順にサイズを増やします。

（注） 既存の APIC コントローラが利用できなくなった場合、クラスタの拡大は停止します。クラスタの拡大を進める前に、この問題を解決します。

- 各アプライアンスの追加時に APIC が同期化しなければならないデータ量によって、拡大処理を完了するために必要な時間はアプライアンスごとに 10 分を超える可能性があります。クラスタが正常に拡大すると、APIC の運用サイズと目標サイズが同じになります。

（注） APIC がクラスタの拡大を完了するまでは、クラスタに追加の変更をしないようにします。

APIC クラスタのサイズ縮小

Cisco Application Policy Infrastructure Controller（APIC）クラスタのサイズを縮小し、クラスタから削除されたCisco APICを解放するには、次のガイドラインに従います。

（注） 縮小したクラスタからCisco APICを解放し、電源オフする正しい手順を実行しないと、予期しない結果を招く可能性があります。認識されていないCisco APICをファブリックに接続されたままにしないでください。

- クラスタ サイズを縮小した場合、残りCisco APICの負荷が増加します。クラスタの同期がファブリックのワークロードの要求に影響しないときに、Cisco APICサイズの縮小を予定します。
- クラスタ内の1つ以上のCisco APIC のヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。
- クラスタの目標サイズを新たな低い値に減らします。たとえば、既存のクラスタ サイズが 6 で、3 台のコントローラを削除する場合は、クラスタの目標サイズを 3 に減らします。
- 既存のクラスタ内でコントローラ識別子の番号が最大のものから、APICを 1 台ずつ、解放、電源オフ、接続解除し、クラスタが新規の小さい目標サイズになるまで行います。

各コントローラを解放および削除するごとに、Cisco APIC はクラスタを同期します。

（注） クラスタから Cisco APICをデコミッションした後に、直ちに電源をオフにし、再発見を予防するためにファブリックから切断します。サービスを回復する前に、全消去を実行して工場出荷時の状態にリセットします。

切断が遅延し、デコミッションされたコントローラが再検出された場合は、次の手順に従って削除します：

1. Cisco APICの電源を切り、ファブリックから切断します。
2. [未承認コントローラ（Unauthorized Controllers）] のリストで、コントローラを拒否します。
3. GUI からコントローラを消去します。

- 既存のCisco APICが使用できなくなると、クラスタの同期が停止します。クラスタの同期を進める前に、この問題を解決します。
- コントローラの削除の際に Cisco APIC が同期すべきデータの量により、各コントローラの解放とクラスタの同期を完了するために要する時間は、コントローラごとに 10 分以上になる可能性があります。

（注） クラスタに追加の変更を行う前に、必要な解放手順全体を完了し、Cisco APIC がクラスタの同期を完了できるようにしてください。

クラスタでの Cisco APIC コントローラの交換

Cisco APIC コントローラを交換するには、次の注意事項に従ってください。

- クラスタの Cisco APIC コントローラのヘルス ステータスが **[十分に適合]** ではない場合、続行する前に問題を解決します。
- クラスタの同期がファブリックのワークロードの要求に影響しないときに、Cisco APIC コントローラの交換を予定します。
- Cisco APIC コントローラで使用される最初のプロビジョニング パラメータとイメージが交換されることに注意してください。同じパラメータおよびイメージは、交換コントローラで使用する必要があります。Cisco APIC はクラスタで交換コントローラの同期を続行します。

（注） 既存の Cisco APIC コントローラが使用できなくなると、クラスタの同期が停止します。クラスタの同期を進める前に、この問題を解決します。

- デコミッションされるコントローラではなく、クラスタ内にある Cisco APIC コントローラを選択する必要があります。例：Cisco APIC1 または APIC2 にログインして、APIC3 およびデコミッション APIC3 のシャットダウンを取り消します。
- CIMC ポリシー構成：スタンバイ APIC を交換する場合、スタンバイおよびアクティブ APIC の CIMC ポリシーを削除。CIMC ポリシーを削除しない場合は、スタンバイ APIC の交換が完了した後に、アクティブな APIC の CIMC ポリシーを更新してください。
- 次の順序で交換手順を実行します。
  1. APIC の設定パラメータとイメージが交換されることに注意してください。
  2. 交換する APIC をデコミッションします（GUI を使用したクラスタでの Cisco APIC のデコミッション （107 ページ） を参照）
  3. 交換される APIC と同じ設定およびイメージを使用して、交換 APIC をコミッションします（GUI を使用したクラスタの Cisco APIC のコミッショニング （103 ページ） を参照）
- ハードウェア インストレーション ガイドの手順に従って、Cisco APIC コントローラの交換を準備します。PING テストでインバンド接続を確認します。

（注） 交換する前に Cisco APIC コントローラを解放しないと、クラスタによる交換コントローラの吸収が妨げられます。さらに、解放された Cisco APIC コントローラを稼働状態に戻す前に、全消去を実行して工場出荷時の状態にリセットします。

- データ量によって Cisco APIC はコントローラの交換時に同期する必要があり、交換が完了するまでに交換コントローラごとに 10 分以上かかることがあります。交換コントローラとクラスタが正常に同期されると、Cisco APIC 動作サイズと目標サイズは未変更のままです。

（注） Cisco APIC がクラスタの同期を完了するまで、クラスタに追加の変更を加えないでください。

- UUID とファブリックのドメイン名は、リブートしても Cisco APIC コントローラに保持されます。ただし、初期状態にリブートするとこの情報は削除されます。Cisco APIC コント

ローラを1つのファブリックから別のファブリックへ移動する場合、そのコントローラを異なる Cisco ACI ファブリックに追加する前に初期状態にリブートする必要があります。

GUI を使用した APIC クラスタの拡大

この手順では、既存のクラスタに 1 つ以上の APIC を追加します。この手順は、Cisco APIC リリース 6.0(2) より前のリリースに適用されます。リリース 6.0(2) でクラスタを拡張するには、後続の手順で詳しく説明するように、**[ノードの追加（Add Node）]** オプションを使用できます。

始める前に

最初に、クラスタに追加する Cisco APIC を設定する必要があります。Cisco APIC の設定の詳細については、Cisco APIC のセットアップ （6 ページ） を参照してください。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、 **Controllers** > ***apic_name*** > **Cluster as Seen by Node** を展開します。

apic_name の場合、拡大したいクラスタ内にある Cisco APIC を選択する必要があります。

[ノード別に表示されるクラスタ（Cluster as Seen by Node）] ウィンドウに、**[APIC クラスタ（APIC Cluster）]**、および **[スタンバイ APIC（Standby APIC）]** とともに、 **[作業（Work）]** ペインに表示されます。**[APIC クラスタ (APIC Cluster)]** タブに、コントローラの詳細が表示されます。これには、現在の対象クラスタとその現在のサイズ、およびそのクラスタ内の各コントローラの管理、運用、ヘルスのステータスが含まれます。

ステップ 3 クラスタの縮小に進む前に、クラスタのヘルス ステータスが [Fully Fit] であることを確認します。

ステップ 4 [Work] ペインで、**[Actions]** > **[Change Cluster Size]** をクリックします。

ステップ 5 [Change Cluster Size] ダイアログボックスの、[Target Cluster Administrative Size] フィールドで、目的のクラスタ サイズの数字を選択します。**Submit** をクリックします。

（注）
2 つの Cisco APIC のクラスタ サイズをもつことはできません。 1 つ、3 つ、またはそれ以上の Cisco APIC のクラスタを作成できます。

ステップ 6 [Confirmation] ダイアログボックスで、[Yes] をクリックします。
Work ウィンドウの **Properties** の下の **Target Size** フィールドには、ターゲットのクラスタ サイズが表示されている必要があります。

ステップ 7 クラスタに追加するすべての Cisco APIC コントローラを物理的に接続します。

[Work] ペインの **[Cluster]** > **[Controllers]** 領域に、Cisco APIC が 1 台ずつ追加され、N + 1 から順に目的のクラスタ サイズになるまで表示されます。

ステップ 8 Cisco APIC が動作状態にあり、各コントローラのヘルス ステータスが **Fully Fit** であることを確認します。

ノード追加オプションを使用した APIC クラスタの拡大

Cisco APIC リリース 6.0(2) で導入された **[ノードの追加（Add Node）]** オプションを使用してクラスタを拡張するには、既存の Cisco Application Policy Infrastructure Controller （APIC）クラスタでこの手順に従います。6.0(2) より前の Cisco APIC リリースでクラスタを拡張するには、前の手順を参照してください。

[ノードの追加（Add Node）] オプションは、Cisco APIC をクラスタに追加するためのより簡単で直接的な方法です。

始める前に

- 追加するノードが クリーンなノードであるか、 工場出荷時の状態にリセットされていることを確認します。
- **[全般（General）]** ペインで現在の**クラスタサイズ**を確認します。*N* の場合、ノードが正常に追加されると、サイズは *N+1* になります。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。**[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）]** > **apic_controller_name** > **[ノードで表示されるクラスタ（Cluster as Seen by Node）]** を展開します。

ステップ 2 **[アクティブコントローラ（Active Controllers）]** ペインで、**[アクション（Actions）]** ボタンをクリックし、**[ノードの追加（Add Node）]** オプションを選択します。

[ノードの追加（Add Node）] 画面が表示されます。

ステップ 3 **[ノードの追加（Add Node）]** 画面で、以下の詳細を入力します：

[コントローラの種類（Controller Type）] を選択します。選択に基づいて、関連するサブステップに進みます。

IPv6 アドレスをサポートする必要がある場合は、**[有効（Enabled）]** チェックボックスをオンにします。

a) コントローラタイプが **[物理（Physical）]** の場合：

- CIMCの詳細ペイン

- [IPアドレス（IP Address）]：CIMC の IP アドレスを入力します。
- [ユーザー名（Username）]：CIMC にアクセスするためのユーザー名を入力します。
- [パスワード（Password）]：CIMC にアクセスするためのパスワードを入力します。
- [**Validate**] をクリックします。認証が成功すると、検証成功が表示されます。

このペインは、CIMC を構成した場合にのみ表示されます。CIMC を構成していない場合は、代わりに新しいノードで手順 GUI を使用した Cisco APIC クラスタの呼び出し （16 ページ） の物理 APIC ログイン手順（ステップ 1b）を実行して、アウトオブバンド管理を設定します。

- [一般（General）] ペイン
  - [名前（Name）]：コントローラの名前を入力します。
  - [管理者パスワード（Admin Password）]：コントローラの管理者パスワードを入力します。
  - コントローラ ID：既存のクラスタサイズに基づいて自動入力されます。現在のクラスタサイズが *N*の場合、コントローラ ID は *N+1*と表示されます。
  - [シリアル番号（Serial Number）]：CIMC 検証後に自動入力されます。
  - [強制追加（Force Add）]：6.0(2) より前のリリースの Cisco APIC を追加するには、**[有効（Enabled）**] チェックボックスをオンにします。
- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4アドレス（IPv4 Address）]：アドレスは自動入力されます。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイ アドレスは自動入力されます。

（注）
前に IPv6 の **[有効（Enabled）]** チェックボックスをオンにした場合は、IPv6 アドレスとゲートウェイを入力します。

- [インフラ ネットワーク（Infra Network）] ペイン
  - [IPv4 アドレス（IPv4 Address）]：インフラ ネットワークの IP アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイのインフラ ネットワーク IP アドレスを入力します。
  - [VLAN ID]：VLAN ID を入力します。

b) コントローラタイプが **仮想（Virtual）** の場合：

- [管理 IP（Management IP）] ペイン
  - [IPアドレス（IP Address）]：管理 IP アドレスを入力します。

    （注）
    管理 IP アドレスは、ESXi/AWS を使用した仮想マシンの展開時に定義されます。

  - 仮想 APICのユーザー名を入力します。
  - 仮想 APICのパスワードを入力します。
  - [**Validate**] をクリックします。認証が成功すると、検証成功が表示されます。
- [一般（General）] ペイン
  - [名前（Name）]：コントローラのユーザー定義名。
  - コントローラ ID：既存のクラスタサイズに基づいて自動入力されます。現在のクラスタサイズが *N*の場合、コントローラ ID は *N+1*と表示されます。
  - [シリアル番号（Serial Number）]：仮想マシンのシリアル番号は自動入力されます。
  - [強制追加（Force Add）]：6.0(2) より前のリリースの Cisco APIC を追加するには、**[有効（Enabled）**] チェックボックスをオンにします。
- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4アドレス（IPv4 Address）]：IP アドレスは自動入力されます。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイ IP アドレスは自動入力されます。

（注）
前に IPv6 の **[有効（Enabled）]** チェックボックスをオンにした場合は、IPv6 アドレスとゲートウェイを入力します。

- [インフラ ネットワーク（Infra Network）] ペイン
  - [IPv4 アドレス（IPv4 Address）]：インフラ ネットワーク アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイの IP アドレスを入力します。
  - [VLAN]：（リモート接続された仮想APIC - ESXi にのみ適用）使用するインターフェイス VLAN ID を入力します。

（注）
AWS を使用して仮想 APIC を展開する場合、[インフラ L3 ネットワーク（Infra L3 Network）] ペインは表示されません。

ステップ 4 [適用（Apply）] をクリックします。

次のタスク

新しく追加されたコントローラが **[未承認のコントローラ（Unauthorized Controllers）]** ペインに表示されます。最新のコントローラがクラスタの他のコントローラとともに **[アクティブなコントローラ（Active Controllers）]** ペインに表示されるまで数分待ちます。

また、**[一般（General）]** ペインの **[現在のサイズ（Current Size）]** と **[ターゲットサイズ（Target Size）]** を確認します。表示される数は、最新のノード追加で更新されます。

GUI を使用した APIC クラスタの縮小

この手順により、クラスタ サイズが縮小されます。この手順は、Cisco APIC リリース 6.0(2) より前のリリースに適用されます。リリース 6.0(2) でクラスタを縮小するには、後続の手順で説明する **[ノードの削除（Delete Node）]** オプションを使用できます。

手順

ステップ 1 メニューバーで、**System** > **Controllers** を選択します。**Navigation** ウィンドウで、**Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。

クラスタ内にある **apic_name** で、これから解放するコントローラ以外のものを選択します。

[ノード別に表示されるクラスタ（Cluster as Seen by Node）] ウィンドウに、**[APIC クラスタ（APIC Cluster）]**、および **[スタンバイ APIC（Standby APIC）]** とともに、**[作業（Work）]** ペインに表示されます。**[APIC クラスタ (APIC Cluster)]** タブに、コントローラの詳細が表示されます。これには、現在の対象クラスタとその現在のサイズ、およびそのクラスタ内の各コントローラの管理、運用、ヘルスのステータスが含まれます。

ステップ 2 クラスタの縮小に進む前に、クラスタのヘルス ステータスが [Fully Fit] であることを確認します。

ステップ 3 [Work] ペインで、**[Actions]** > **[Change Cluster Size]** をクリックします。

ステップ 4 [Change Cluster Size] ダイアログボックスの [Target Cluster Administrative Size] フィールドで、縮小したいクラスタの目標数を選択します。**Submit** をクリックします。

（注）
クラスタ サイズを 2 つの APIC にすることはできません。 1 つ、3 つ、またはそれ以上の APIC のクラスタは許容されます。

ステップ 5 **[作業（Work）]** ペインの **[アクティブ コントローラ（Active Controller）]** 領域で、クラスタ内の最後の APIC を選択します。

例：

3 台からなるクラスタの場合、クラスタ内の最後になるのは、コントローラ ID 3 です。

ステップ 6 デコミッションするコントローラを右クリックして、**[デコミッション（Decommission）]**を右クリックします。**[確認 (Confirmation)]** ダイアログ ボックスが表示されたら、**[はい (Yes)]** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは、稼動対象外になり、[Work] ペインに表示されなくなります。

ステップ 7 コントローラ ID の番号で最大から最小に向かう正しい順序でクラスタ内のすべての APIC について、上記のコントローラを 1 つずつ解放する手順を繰り返します。

（注）
稼動クラスタのサイズが縮小するのは、最後のアプライアンスが解放されたときで、管理サイズを変更したときではありません。各コントローラを解放した後、そのコントローラの動作状態が未登録になり、すでにクラスタ内で稼動していないことを確認します。

APIC クラスタ内に必要なコントローラを残しておきます。

ノード削除オプションを使用した APIC クラスタの縮小

Cisco APIC リリース 6.0(2) で導入された **[ノードの 削除（Delete Node）]** オプションを使用してクラスタを縮小するには、次の手順に従います。6.0(2) より前の APIC リリースでクラスタを縮小するには、前の手順を参照してください。

この手順を使用すれば、APIC クラスタから 1 つ以上のノードを削除できます。

[ノードの削除（Delete Node）] オプションには、クラスタ サイズの縮小とノードのデコミッションの 2 つの操作が含まれます。

（注） 2 ノード クラスタはサポートされていません。3 ノード クラスタから 1 つのノードを削除することはできません。推奨される最小クラスタ サイズは 3 です。

（注） Cisco APIC 6.1(2) 以降では、クラスタからスタンバイ ノードを削除できます。スタンバイ ノードを削除したら、クラスタに追加する前にクリーン リブートを実行する必要があります。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。**[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）]** > **apic_controller_name** > **[ノードで表示されるクラスタ（Cluster as Seen by Node）]** を展開します。

ステップ 2 **[アクティブコントローラ（Active Controllers）]** ペインで、必要なチェックボックスをオンにして、削除するコントローラを選択します。

ステップ 3 **[アクション（Actions）]** ボタンをクリックし、**[ノードの削除（Delete Node）]** オプションを選択します。

ステップ 4 ポップアップ画面で **[OK]** をクリックして、削除を確認します。

force オプションを選択しても影響はありません。Cisco APIC リリース 6.0(2) ではサポートされていないため、無操作のオプションです。

（注）
ノードは降順で削除する必要があります。たとえば、ID 6 のノードを削除する前に ID 5 のノードを削除することはできません。

[一般（General）] ペインの **[現在のサイズ（Current Size）]** と **[ターゲットサイズ（Target Size）]** を確認します。表示されるサイズは、以前より 1 つ小さくなります。以前のクラスタサイズが *N* であった場合には、*N-1* になります。

（注）
クラスタから複数のノードを削除する場合は、クラスタの最後のノードが最初に削除し、その後に他のノードが削除してください。選択したすべてのノードが削除されるまで、**[全般（General）]** ペインの **[縮小が進行中（Shrink In Progress）]** が *[*はい（*Yes*）*]* に設定されます。

次のタスク

- クラスタから APIC をデコミッションした後に、コントローラの電源をオフにし、ファブリックから切断します。
- 数分待ってから、クラスタの残りのノードの **[正常性状態（Health State）]** が *[*完全に適合（*Fully fit*）*]* と表示されていることを確認してから、さらにアクションを実行します。

Cisco APIC コントローラのコミッションとデコミッション

GUI を使用したクラスタの Cisco APIC のコミッショニング

APIC をコミッショニングするには、次の手順を使用します。この手順は、Cisco APIC リリース 6.0(2) より前のリリースに適用されます。リリース 6.0(2) では、試運転ワークフローが変更されました。詳細については、後続のセクションを参照してください。

手順

ステップ 1 メニュー バーで、**[システム (System)]** > **[コントローラ (Controllers)]** を選択します。

ステップ 2 **Navigation** ウィンドウで、**Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。
[ノード別に表示されるクラスタ (Cluster as Seen by Node)] ウィンドウに、**[APIC クラスタ (APIC Cluster)]**、および **[スタンバイ APIC (Standby APIC)]** とともに、**[作業 (Work)]** ペインに表示されます。**[APIC クラスタ (APIC Cluster)]** タブに、コントローラの詳細が表示されます。これには、現在の対象クラスタとその現在のサイズ、およびそのクラスタ内の各コントローラの管理、運用、ヘルスのステータスが含まれます。

ステップ 3 継続する前に、**[作業 (Work)]** ウィンドウの **[APIC クラスタ (APIC Cluster)]** から、**[アクティブ コントローラ (Active Controllers)]** サマリ テーブルのクラスタの **[健全性状態 (Health State)]** が **[完全に適合 (Fully Fit)]** になっていることを確認します。

ステップ 4 **[作業 (Work)]** ウィンドウで、**[未登録 (Unregistered)]** と **[動作状態 (Operational State)]** カラムに表示されている、デコミッションされたコントローラを右クリックし、**[コミッション (Commission)]** を選択します。
コントローラはハイライト表示になります。

ステップ 5 **Confirmation** ダイアログボックスで **Yes** をクリックします。

ステップ 6 コミッションされた Cisco APIC が動作状態であり、ヘルス ステータスが、**Fully Fit** であることを確認します。

クラスタでの Cisco APIC のコミッション

既存の Cisco Application Policy Infrastructure Controller （APIC）クラスタでこの手順に従い、そのクラスタで Cisco APIC をコミッションします。この手順は、Cisco APIC リリース 6.0(2) に当てはまります。リリース 6.0(2) から、コミッション ワークフローが強化されました。これは、既存のコントローラのプロビジョニングと、RMA（返品承認）にも使用できます。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）]** > **apic_controller_name** > **ノードで表示されるクラスタ（Cluster as Seen by Node**）を展開します。

ステップ 3 **[アクティブ コントローラ（Active Controllers）]** テーブルからデコミッションされた Cisco APIC を選択します。

ステップ 4 **[アクティブ コントローラ（Active Controllers）]** テーブルで、各 Cisco APICの行の末尾に表示される **[アクション（Actions）]** アイコン（3 つのドット）をクリックします。表示されたオプションから、**[コミッション（Commission）]**をクリックします。

[コミッション（Commission）] ダイアログボックスが表示されます。

ステップ 5 **[コミッション（Commission）]** 画面に以下の詳細を入力します。

[コントローラ タイプ（Controller Type）]を選択します。選択に基づいて、関連するサブステップに進みます。

IPv6 アドレスをサポートする必要がある場合は、**[有効（Enabled）]** チェックボックスをオンにします。

a) コントローラタイプが **[物理（Physical）]** の場合：

- CIMCの詳細ペイン
  - [IPアドレス（IP Address）]：CIMC の IP アドレスを入力します。
  - [ユーザー名（Username）]：CIMC にアクセスするためのユーザー名を入力します。
  - [パスワード（Password）]：CIMC にアクセスするためのパスワードを入力します。
  - [**Validate**] をクリックします。認証が成功すると、検証成功が表示されます。

  このペインは、CIMC を構成した場合にのみ表示されます。CIMC を構成していない場合は、代わりに新しいノードで手順 GUI を使用した Cisco APIC クラスタの呼び出し （16 ページ） の物理 APIC ログイン手順（ステップ 1b）を実行して、アウトオブバンド管理を設定します。
- [一般（General）] ペイン
  - [名前（Name）]：コントローラの名前。名前は、CIMC 検証後に自動的に入力されます。
  - [管理者パスワード（Admin Password）]：コントローラの管理者パスワードを入力します。
  - [コントローラ ID（Controller ID）]：デコミッションされた Cisco APIC に基づいて自動入力されます。デコミッションされたノードの ID が割り当てられます。
  - [シリアル番号（Serial Number）]：CIMC 検証後に自動入力されます。
  - [ポッド ID（Pod ID）]： Cisco APICのポッドの ID 番号を入力します。
- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4 アドレス（IPv4 Address）]：アウトオブバンド ネットワークの IPv4 アドレスを入力します。

- [IPv4 ゲートウェイ（IPv4 Gateway）]：アウトオブバンド ネットワークの IPv4 ゲートウェイアドレスを入力します。

（注）
前に IPv6 の **[有効（Enabled）]** チェックボックスをオンにした場合は、IPv6 アドレスとゲートウェイを入力します

b) コントローラタイプが **仮想（Virtual）** の場合：

- [仮想インスタンス（Virtual Instance）]：管理 IP を入力し、 **[検証（Validate）]**をクリックします。

（注）
管理 IP アドレスは、ESXi/AWS を使用した VM の展開時に定義されます。

- [一般（General）] ペイン
  - [名前（Name）]：コントローラのユーザー定義名。
  - [コントローラ ID（Controller ID）]：デコミッションされた Cisco APIC に基づいて自動入力されます。デコミッションされたノードの ID が割り当てられます。
  - [シリアル番号（Serial Number）]：VM のシリアル番号は自動入力されます。
- [アウトオブバンド ネットワーク（Out of Band Network）] ペイン
  - [IPv4アドレス（IPv4 Address）]：IP アドレスは自動入力されます。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイ IP アドレスは自動入力されます。

（注）
前に IPv6 の **[有効（Enabled）]** チェックボックスをオンにした場合は、IPv6 アドレスとゲートウェイを入力します

- [インフラ ネットワーク（Infra Network）] ペイン
  - [IPv4 アドレス（IPv4 Address）]：インフラ ネットワーク アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイの IP アドレスを入力します。
  - [VLAN]：（リモート接続された仮想APIC - ESXi にのみ適用）使用するインターフェイス VLAN ID を入力します。

（注）
AWS を使用して仮想 APIC を展開する場合、[インフラ L3 ネットワーク（Infra L3 Network）] ペインは表示されません。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 コミッションされた Cisco APIC が動作状態であり、ヘルス ステータスが、*Fully Fit* であることを確認します。

GUI を使用したクラスタでの Cisco APIC のデコミッション

この手順では、クラスタ内の Cisco Application Policy Infrastructure Controller（APIC）をデコミッションします。この手順は、Cisco APIC リリース 6.0(2) より前の APIC リリースに適用されます。リリース 6.0(2) で APIC をデコミッションするには、次の手順を参照してください。

（注） 他のオブジェクトとは異なり、ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの 1 つのシャードにのみ保存されます。これらのオブジェクトは、使用停止または Cisco APIC交換すると永久に失われます。

手順

ステップ 1 メニューバーで、 **System** > **Controllers** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、 **Controllers** > **apic_name** > **Cluster as Seen by Node** を展開します。

クラスタ内にある **[apic_name]** で、これから解放するコントローラ以外のものを選択します。

[ノードで確認されるクラスタ (Cluster as Seen by Node)] ウィンドウは、**[作業 (Work)]** ペインにコントローラの詳細と 3 つのタブ (**[APIC クラスタ (APIC Cluster)]**、および **[スタンバイ APIC (Standby APIC)]**) が表示されます。

ステップ 3 継続する前に、**[作業 (Work)]** ウィンドウで、**[APIC クラスタ (APIC Cluster)]** (**[アクティブ コントローラ (Active Controllers)]** サマリ テーブルの **[健全性状態 (Health State)]**) が **[完全に適合 (Fully Fit)]** になっていることを確認します。

ステップ 4 **[作業 (Work)]** ペインの **[APIC クラスタ (APIC Cluster)]** タブにある **[アクティブ コントローラ (Active Controllers)]** テーブルで、デコミッションするコントローラを右クリックし、**[デコミッション (Decommission)]** を選択します。
[Confirmation] ダイアログボックスが表示されます。

ステップ 5 **Yes** をクリックします。

解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**Work** ウィンドウには表示されなくなります。

（注）
- クラスタから Cisco APIC をデコミッションした後に、コントローラの電源をオフにし、ファブリックから切断します。Cisco APIC をサービスに戻す前に、コントローラで初期設定へのリセットを実行します。

- 稼動クラスタのサイズが縮小するのは、最後のアプライアンスが解放されたときで、管理サイズを変更したときではありません。各コントローラを解放した後、そのコントローラの動作状態が未登録になり、すでにクラスタ内で稼動していないことを確認します。
- Cisco APIC をデコミッションした後に、レイヤ 7 サービスにレイヤ 4 のコントローラを再起動する必要があります。コントローラをリコミッションする前に再起動を実行する必要があります。

クラスタでの Cisco APIC のデコミッション

この手順では、クラスタ内の Cisco APIC をデコミッションします。この手順は、Cisco APIC リリース 6.0(2) に当てはまります。リリース 6.0(2) より前のリリースの Cisco APIC をデコミッションするには、前述の手順を使用します。

（注） 他のオブジェクトとは異なり、ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの 1 つのシャードにのみ保存されます。これらのオブジェクトは、使用停止または Cisco APIC交換すると永久に失われます。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[コントローラ（Controllers）]** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、 **Controllers** > **apic_name** > **Cluster as Seen by Node** を展開します。

クラスタ内にある **[apic_name]** で、これから解放するコントローラ以外のものを選択します。

[ノードから見たクラスタ（Cluster as Seen by Node）] ウィンドウでは、**[作業 （Work）]** ペインにコントローラの詳細と 3 つのタブ（[APIC クラスタ（APIC Cluster）]、および [スタンバイ APIC （Standby APIC）]）が表示されます。

ステップ 3 継続する前に、**[作業（Work）]** ウィンドウで、クラスタの **[正常性状態（Health State）]**（**[アクティブ コントローラ（Active Controllers）]** サマリ テーブルに示されているもの）が **[完全に適合（Fully Fit）]** になっていることを確認します。

ステップ 4 **[アクティブコントローラ（Active Controllers）]** テーブルで、各 APIC の行の最後に表示される **[アクション（Actions）**] アイコン（3 つのドット）をクリックします。**[デコミッション（Decommission）]** オプションを選択します。

[デコミッション（Decommission）] ダイアログ ボックスが表示されます。

ステップ 5 **[OK]** をクリックします。

Cisco APIC リリース 6.0(2) ではサポートされていないため、[強制（Force）] の **[有効（Enabled）]** チェックボックスは 操作不可 オプションです。

解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**Work** ウィンドウには表示されなくなります。

（注）
- クラスタから Cisco APIC をデコミッションした後に、コントローラの電源をオフにし、ファブリックから切断します。Cisco APIC をサービスに戻す前に、コントローラで初期設定へのリセットを実行します。
- 稼動クラスタのサイズが縮小するのは、最後のアプライアンスが解放されたときで、管理サイズを変更したときではありません。各コントローラを解放した後、そのコントローラの動作状態が未登録になり、すでにクラスタ内で稼動していないことを確認します。
- Cisco APIC をデコミッションした後に、レイヤ 7 サービスにレイヤ 4 のコントローラを再起動する必要があります。コントローラをリコミッションする前に再起動を実行する必要があります。

クラスタ内の APIC のシャットダウン

クラスタですべての APIC のパフォーマンスのシャット ダウン

クラスタですべての APIC パフォーマンスをシャットダウンする前に、APIC クラスタが健全な状態であり、すべての APIC が完全に適合していることを確認します。このプロセスを開始したら、このプロセス中に設定の変更を行わないことをお勧めします。クラスタのすべての APIC をグレースフルにシャット ダウンするには、次の手順を使用します。

手順

ステップ 1 アプライアンス ID1 で Cisco APIC にログインします。

ステップ 2 メニュー バーで、**[システム]** > **[コントローラ:** を選択します。

ステップ 3 [ナビゲーション] ペインで、**Controllers** > **apic_controller_name** を展開します。

クラスタ内の三番目のノードを選択する必要があります。

ステップ 4 コントローラを右クリックし、**[シャット ダウン]** をクリックします。

ステップ 5 クラスタの二番目の APIC をシャットダウンするには手順を繰り返します。

ステップ 6 クラスタの最初の APIC の Cisco IMC にログインし、APIC をシャットダウンします。

ステップ 7 **Server** > **Server Summary** > **Shutdown Server** を選択します。

クラスタの 3 つすべての APIC をシャットダウンしました。

クラスタ内、apic のパフォーマンスを元に戻す方法

クラスタに戻り、apic のパフォーマンスを起動するのにには、次の手順を使用します。

手順

ステップ 1 クラスタ内の最初の APIC の Cisco IMC にログインします。

ステップ 2 選択 **サーバ** > **Server Summary** > **電源オン** 最初 APIC の電源をオンにします。

ステップ 3 APIC し、クラスタ内の 3 番目の APIC の電源を 2 番目の手順を繰り返します。

Apic のパフォーマンスの電源がオンにすべての後にことを確認しますが、apic のパフォーマンスが完全に適合状態ではすべて。Apic のパフォーマンスが完全に適合状態であることを確認した後でのみ、apic 内で、設定変更を行う必要があります。

Cold Standby

Cold Standby について (Cisco APIC クラスタ用)

Cold Standby 機能 Cisco Application Policy Infrastructure Controller(APIC クラスタ用) を使用すれば、クラスタ内の Cisco APIC をアクティブ/スタンバイモードで運用できます。Cisco APIC クラスタでは、指定されたアクティブ状態の Cisco APIC は負荷を共有し、指定されたスタンバイ状態の Cisco APIC はアクティブなクラスタ内の任意の Cisco APIC の置き換えとして動作することができます。

管理者ユーザーとして、Cisco APIC が初めて起動したときに Cold Standby 機能をセット アップできます。クラスタ内には少なくとも 3 基のアクティブ状態の Cisco APIC があり、1 基以上のスタンバイ状態の Cisco APIC があるようにすることを推奨します。管理者ユーザーとして、アクティブな Cisco APIC をスタンバイ状態の Cisco APIC で置き換えるには、切り替えを開始できます。

スタンバイ Cisco APIC に対する注意事項と制限事項

スタンバイ Cisco Application Policy Infrastructure Controller（APIC）に対する注意事項と制限事項：

- Cisco APIC 6.1(3) より前では、スタンバイ APIC は、物理 APIC ノードを備えた APIC クラスタでのみサポートされていました。Cisco APIC 6.1（3）以降、仮想ノードを使用した

APIC クラスタのスタンバイ APIC もサポートされています。スタンバイ APIC は、クラスタ内のアクティブな APIC と同じフォーム ファクタ（物理またはリモート対応）である必要があります。

- スタンバイ Cisco APIC を追加するには 3 つのアクティブ Cisco APIC が必要です。
- スタンバイ Cisco APIC は、初期セットアップ中にスタンバイ Cisco APIC がクラスタに参加するときに、クラスタの同じファームウェア バージョンで実行する必要があります。
- アップグレードプロセス中に、Cisco APIC のすべてのアクティブなパフォーマンスをアップグレードすると、スタンバイ Cisco APIC もありますが自動的にアップグレードします。
- 初期設定時に、スタンバイ Cisco APIC に ID が割り当てられます。スタンバイ Cisco APIC がアクティブ Cisco APIC に切り替えられた後、スタンバイ Cisco APIC（新しくアクティブになった）は、置き換えられた（前にアクティブだった）Cisco APIC の ID の使用を開始します。
- 管理者ログインはスタンバイ Cisco APIC で有効ではありません。Cold Standby Cisco APIC をトラブルシューティングをするには、*rescue-user* として SSH を使用して、スタンバイにログインする必要があります。
- 切り替え中、置き換えられたアクティブ Cisco APIC は、置き換えられた Cisco APIC への接続を防ぐため、電源オフにする必要があります。
- 次の条件が失敗する経由でスイッチします。
  - スタンバイ Cisco APIC に接続がない場合。
  - スタンバイ Cisco APIC のファームウェアのバージョンがアクティブ クラスタと同じではない場合。
- スタンバイ Cisco APIC をアクティブに切り替えた後、必要に応じて別のスタンバイ Cisco APIC をセットアップできます。
- **スタンバイの OOB IP アドレスを保留する（新しいアクティブ）**がオンの場合、スタンバイ（新しいアクティブ）Cisco APICは元のスタンバイのアウトオブバンド管理 IP アドレスを保留します。
- **[スタンバイ（新しいアクティブ）の OOB IP アドレスを保持する（Retain OOB IP address for Standby（new active）]** がオンでない場合：
  - 1 つのアクティブな Cisco APIC がダウンした場合：スタンバイ（新しいアクティブ）Cisco APICは古いアクティブな Cisco APIC のアウトオブバンド管理 IP を使用します。
  - 複数のアクティブ Cisco APIC がダウンしている場合：スタンバイ（新しいアクティブ）Cisco APIC は、アクティブな Cisco APIC のアウトオブバンド管理 IP アドレスを使用しようとしますが、アクティブな Cisco APIC のアウトオブバンド管理 IP アドレス構成のシャードがマイノリティ状態にある場合は失敗する可能性があります。
- Cisco ACI マルチポッドについては、古いアクティブ Cisco APIC とスタンバイ Cisco APIC が異なるアウトオブバンド管理 IP サブネットを使用している場合、スタンバイ（新しい

アクティブ）では、Cisco APIC が元のスタンバイ アウトオブバンド管理 IP アドレスを保持するオプションをオンにする必要があります。そうしないと、スタンバイ（新しいアクティブ）Cisco APIC へのアウトオブバンド管理 IP 接続が失われます。この状況は、古いアクティブ Cisco APIC とスタンバイ Cisco APIC が異なるポッドにある場合に発生する可能性があります。

この理由でアウトオブバンド管理 IP 接続が失われた場合、または複数のアクティブ Cisco APIC がダウンしている場合は、新しい静的ノード管理 OOB IP アドレスを作成して、新しいアクティブ（以前はスタンバイ）Cisco APIC アウトオブバンド管理 IP アドレスを変更する必要があります。構成を変更するには、クラスタのマイノリティ状態を解除する必要があります。

- スタンバイ Cisco APIC はポリシー設定または管理で関係しません。
- 管理者クレデンシャルを持っている場合でも、スタンバイ Cisco APIC に情報が複製されることはありません。
- Cisco APIC をアクティブに昇格させても、スタンバイ Cisco APIC はインバンド管理 IP アドレスを保持しません。正しいインバンド管理 IP アドレスを持つように Cisco APIC を手動で再設定する必要があります。

GUI を使用した Cold Standby ステータスの確認

1. メニューバーで、 **System** > **Controllers** を選択します。
2. **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。
3. **[作業]**ペインで、スタンバイ コントローラが**[スタンバイ コントローラ]**で表示されます。

GUI を使用して現用系 APIC とスタンバイ APIC を切り替える

スタンバイ APIC 内で現用系 APIC 経由でスイッチするには、次の手順を使用します。

手順

ステップ 1 メニューバーで、 **System** > **Controllers** を選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）]** > **apic_controller_name** > **ノードで表示されるクラスタ（Cluster as Seen by Node）**を展開します。

Apic_controller_name 交換されているコントローラの名前以外にする必要があります。

ステップ 3 **作業** ペインで、ことを確認します、 **ヘルス状態** で、**現用系コントローラ**の要約表は、続行する前に、 **十分に適合**現用系コントローラのことを示します。

ステップ 4 をクリックする ***apic_controller_name*** スイッチ オーバーします。

ステップ 5 **[ワーク（Work）]** ペインで、置き換えるコントローラの行にある [**...**] をクリックし、**[置換（Replace）]** を選択します。
Replace ダイアログボックスが表示されます。

ステップ 6 ドロップダウンリストから **Backup Controller** を選択して、**Submit** をクリックします。

現用系 APIC をスタンバイ APIC に切り替えて、システムを現用系として登録するには、数分かかる場合があります。

ステップ 7 上で、スイッチの進行状況を確認します **フェールオーバーのステータス** フィールドで、 **アクティブ コントローラ** の要約表。

（注）
各ポッドが異なるアウトオブバンド管理IPサブネットを使用する可能性があるため、同じポッド内のスタンバイ APIC を使用して現用系 APIC を置き換えることをお勧めします。

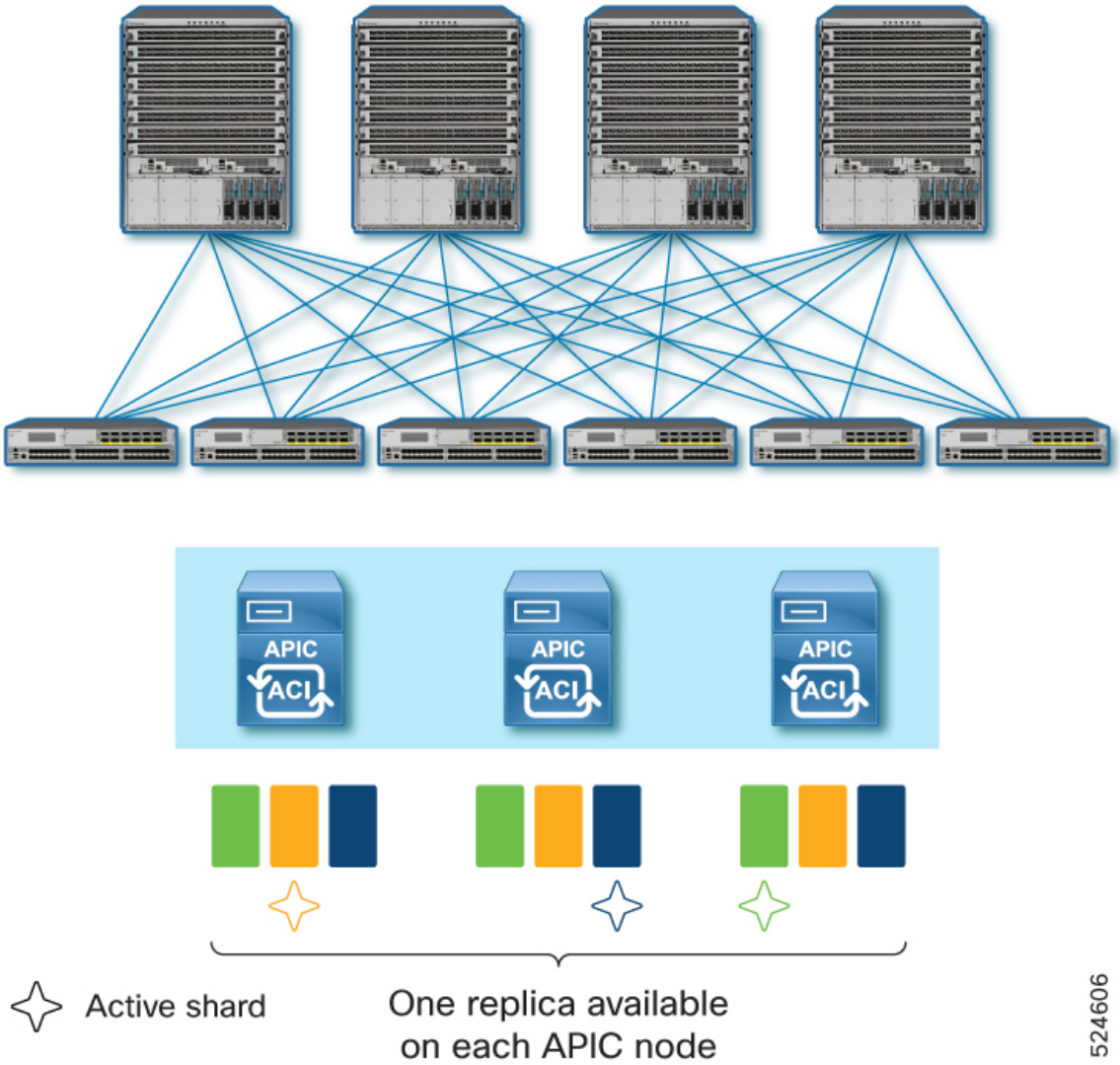
推奨されるアプローチを使用できず（たとえば、Pod1の現用系APIC（ID:2）がPod2のスタンバイ APIC（ID:21）に置き換えられた場合）、アウトオブバンド管理IPサブネットがポッド間で異なる場合、フェールオーバー後にスタンバイCisco APIC（新しい現用系）が元のアウトオブバンド管理 IP アドレスを保持するには、追加の手順が必要です。

- **[スタンバイ（新しいアクティブ）の OOB IP アドレスを保持（Retain OOB IP address for Standby（new active））]** を ステップ 6 （113 ページ） でオンにします。
- フェールオーバー後、置き換えられた（古いアクティブ）CiscoAPICの静的ノード管理アドレス構成を削除し、新しいアクティブ（以前のスタンバイ）CiscoAPICの静的ノード管理アドレス構成を読み取ります。

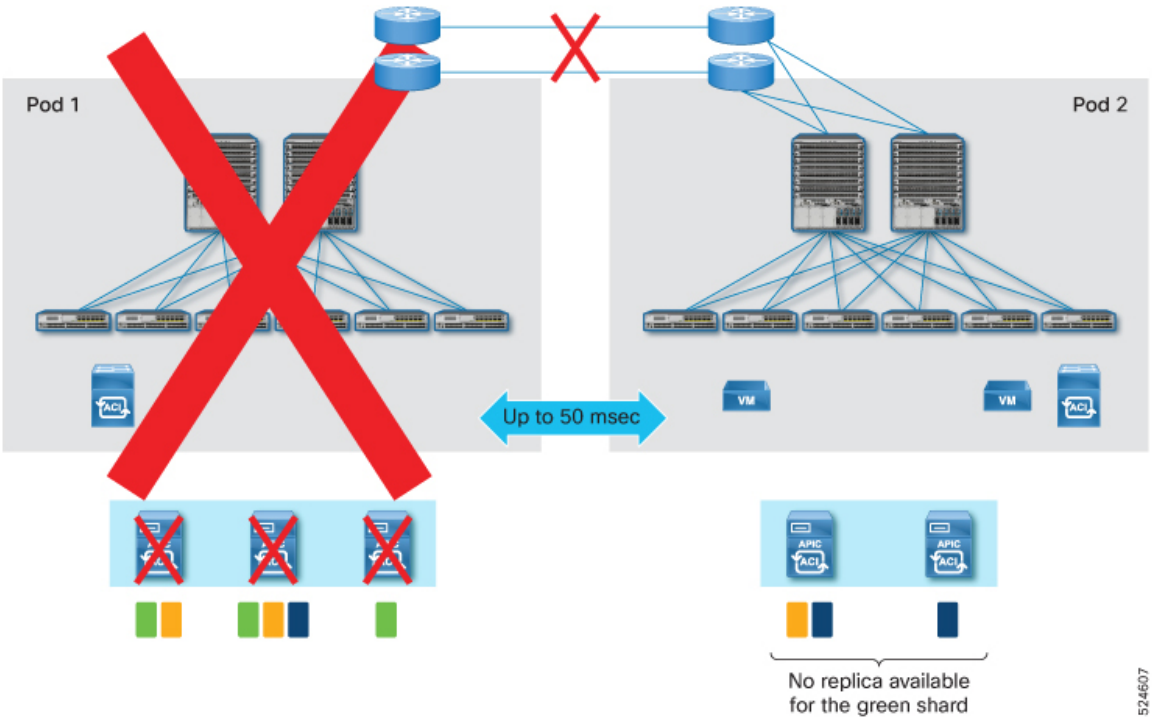
ウォーム スタンバイ

Cisco APIC クラスタのウォーム スタンバイ

Cisco APIC 6.1(2) 以降、スタンバイ APIC は、コールド スタンバイ APIC とは異なるウォーム スタンバイ APIC として設定できます。アクティブに昇格するまでデータが含まれないコールド スタンバイ APIC とは異なり、ウォーム スタンバイ APIC は、スタンバイ ロールである間、アクティブ APIC ノードからのすべてのデータを常に同期します。これにより、データベースの一部またはすべてが APIC クラスタ全体に分散されているため、ウォーム スタンバイ APIC を使用して APIC クラスタを再構築できます。このようなシナリオのいくつかを以下で説明します。



APIC クラスタは、シャーディングおよびレプリカと呼ばれるデータベース テクノロジを使用します。ACI ファブリックのデータは、シャードと呼ばれる小さな部分に分割され、アクティブな APIC ノードに分散されます。各シャードは、クラスタのサイズに関係なく、最大 3 つのレプリカに複製されます。たとえば、5 つの APIC ノードのクラスタがある場合、1 つのシャードは APIC 1、2、および 3 で複製され、別のシャードは APIC 3、4、および 5 で複製される、などのようになります。そのため、クラスタ内の 3 つ以上の APIC ノードが失われると、アクティブな APIC ノードが残っていても、一部のシャードのデータが完全に失われます。このような場合を考えると、コールド スタンバイ APIC は失われた APIC ノードの代わりになることはできません。それ自体にデータを含まず、残りのアクティブな APIC ノードから失われたシャードを復元できないからです。同様に、クラスタ内のすべての APIC ノードが失われた場合も、失われた APIC ノードの数に関係なく、コールド スタンバイ APIC はそれらを置き換えることができません。



これらのシナリオでは、ウォーム スタンバイ APIC を使用できます。このようなデータ損失シナリオの現実的な例を次に示します。

データ損失のシナリオ 1：

ポッド 1 に APIC 1、2、3 があり、ポッド 2 に APIC 4 と 5 があるマルチポッド展開では、ポッド 1 が災害（洪水、火災、地震など）のためにダウンした場合、 3 つの APIC ノードが失われます。これは、一部のデータベース シャードが完全に失われることを意味します。

データ損失のシナリオ 2：

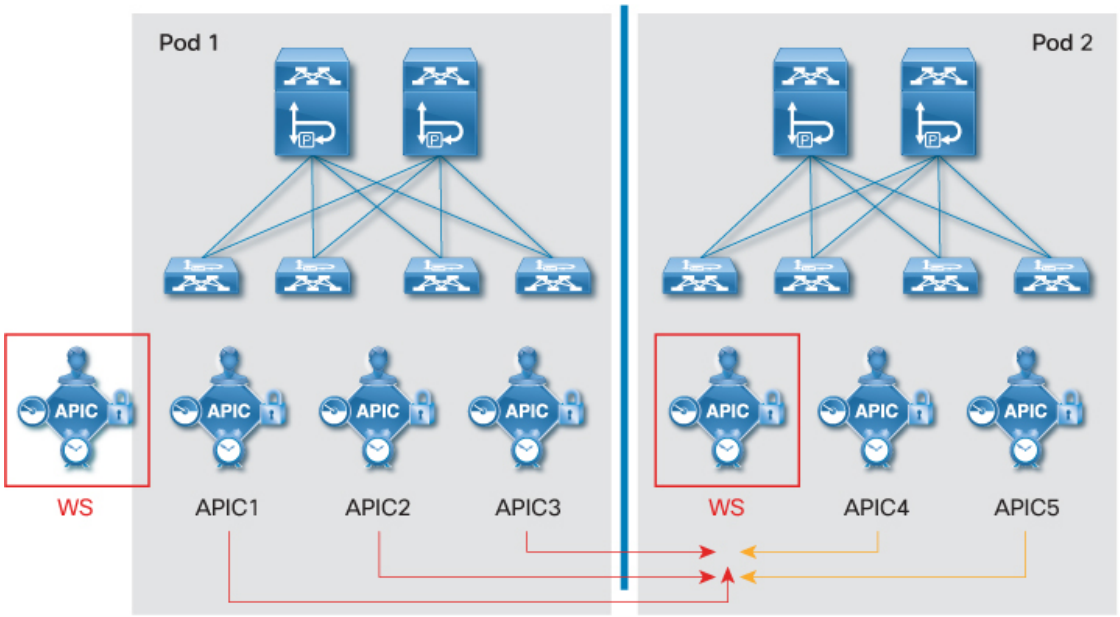
ポッド 1 と 2 が同じ場所にあり、ポッド 3 と 4 が別の場所にあるマルチポッド展開で、ポッド 1 に APIC 1 と 2、ポッド 2 に APIC 3 と 4、ポッド 3 に APIC 5 と 6、ポッド 4 の APIC 7 があるとします。ポッド 1 と 2 がある場所で障害が発生すると、4 つの APIC（APIC 1、2、3、4）が失われます。これは、一部のデータベースシャードが完全に失われることを意味します。

データ損失のシナリオ 3：

ポッド 1 に APIC 1 と 2 があり、ポッド 2 に APIC 3 があり、ポッド 3 にアクティブな APIC がないマルチポッド展開では、ポッド 1 と 2 が災害のためにダウンすると、ファブリックのすべてのデータが失われます。すべてのアクティブな APIC ノードが失われると、クラスタが削除されるからです。

これらのシナリオで、正常なポッド/サイトにウォーム スタンバイ APIC がある場合には、ウォーム スタンバイ APIC は、すべてのアクティブ APIC ノードからすべてのシャードを同期していたため、失われたデータ シャードを復元し、ファブリックを復元できます。これは、コールド スタンバイ APIC では不可能です。

これらの例は、すべてマルチポッド展開です。これは、単一のポッド展開で、スタンバイ APIC ノードが失われても、クラスタ内の 3 つ以上の APIC ノードまたはすべての APIC ノードが失われる可能性は低いためです。それとは反対に、ウォーム スタンバイ APIC は、マルチポッドとシングル ポット展開の両方で、同様にサポートされ、機能します。



これらの例に示すように、ウォーム スタンバイ APIC で導入された新機能は、特別な障害リカバリです。データベース シャードの一部またはすべてが失われ、APIC クラスタを再構築する必要がありますが、アクティブな APIC ノードの交換が短時間で容易に行えます。これはウォーム APIC とコールド スタンバイ APIC の両方でサポートされています。

1 つのアクティブ APIC ノードをウォームまたはコールド スタンバイ APIC ノードに置き換える必要がある場合、残りの正常なアクティブ APIC ノードの 1 つから置換操作がトリガされます。ただし、データ損失の場合にクラスタを再構築するためのウォーム スタンバイ APIC の昇格は、アクティブな APIC ノードが残っていない可能性があるため、残りの正常なアクティブ APIC ノードを介して実行されません。実際には、ウォーム スタンバイ APIC ノードの 1 つで GUI または REST API を介して実行できます。これにより、ウォーム スタンバイ APIC が常に APIC 1 に昇格され、障害リカバリの開始点になることができます。詳細はGUI を使用したウォーム スタンバイ APIC によるディザスタ リカバリ （121 ページ）を参照してください。

ウォーム スタンバイ APIC が壊滅的なイベントからファブリックを復元できるようにするため、ポッドまたは地理的サイトなどの各障害ドメインに少なくとも 1 つのウォーム スタンバイ APIC ノードを配置することをお勧めします。

スタンバイ Cisco APIC に対するガイドラインと制限事項

ウォーム スタンバイ APIC に対するガイドラインと制限事項を以下に示します。

- Cisco APIC 6.1(2) では、ウォームスタンバイ APIC は、物理 APIC ノードでのみ APIC クラスタをサポートしていました。Cisco APIC 6.1（3）以降、仮想ノードを使用した APIC クラスタのスタンバイ APIC もサポートされています。スタンバイ APIC は、クラスタ内の

アクティブな APIC と同じフォーム ファクタ（物理またはリモート対応）である必要があります。

- ウォーム スタンバイ APIC は、直接接続と L3 ネットワーク経由でリモート接続の両方のタイプの APIC 接続でサポートされます。
- APIC クラスタは、1 つのタイプのスタンバイ APIC（コールドまたはウォーム）のみをサポートできます。コールド スタンバイ APIC とウォーム スタンバイ APIC は、同じ APIC クラスタに共存できません。デフォルトはコールド スタンバイ APIC に設定されています。スタンバイ APIC ノードがクラスタに追加される前後に、スタンバイ APIC のタイプを変更できます。
- APIC クラスタごとに最大 3 つのウォーム スタンバイ APIC ノードがサポートされます。
- 4 つ以上のコールドスタンバイ APIC ノードがある場合、クラスタのスタンバイ APIC タイプをウォームに変更することはできません。
- クラスタ全体を再構築するためのウォーム スタンバイ APIC を使用したディザスタ リカバリは、クラスタにデータ損失がある場合、つまり 3 つ以上のアクティブな APIC ノードが失われ、その結果、一部のシャードの 3 つのレプリカがすべて永久に失われた場合にのみ許可されます。
- ポッド間ネットワーク（IPN）のネットワークの問題が原因で 3 つ以上のアクティブな APIC が一時的に失われた場合は、ウォーム スタンバイ APIC ノードを APIC 1 に昇格しないでください。これを行うと、APIC ノードが各ポッドで正常であっても、他のすべての APIC を初期化してクラスタを再構築せざるを得なくなるからです。
- ウォーム スタンバイ APIC をサポートしていない 6.1(2) よりも古いバージョンにダウングレードする前に、クラスタのスタンバイ APIC タイプをコールドに変更する必要があります。
- コールド スタンバイ APIC のみを備えた Cisco APIC 6.1(2) より前では、スタンバイ APIC ノードのアップグレード（またはダウングレード）は表示されませんでした。スイッチのアップグレードを続行する前に待機する必要はありませんでした。アクティブノードの APIC アップグレードが完了した後、スタンバイ APIC ノードが初期化され、新しいバージョンで起動されました。

  Cisco APIC 6.1(2) 以降、スタンバイ APIC ノードがある場合、APIC のアップグレードプロセスは以前よりも少し長くかかることがあります。アップグレードプロセスには、ウォーム スタンバイ APIC とコールド スタンバイ APIC の両方のスタンバイ APIC ノードが明示的に含まれます。これは、データベースがウォーム スタンバイ APIC でバックアップされ、新しいバージョン モデルに一致するように更新されるようにするためです。コールド スタンバイ APIC には更新されるデータは含まれていませんが、同じプロセスがコールド スタンバイ APIC に適用されます。このプロセスはウォーム スタンバイ APIC よりもはるかに高速に完了します。
- スタンバイ ノードはクラスタから削除できます。詳細については、クラスタからスタンバイを削除する （120 ページ）を参照してください。

- Cisco APIC 6.1（2）以降で **厳格** モードで実行されている Cisco APIC クラスタがあり、スイッチが Cisco APIC 6.1（1）より前の古いバージョンである場合、ディザスタ リカバリ操作は失敗します。ディザスタ リカバリ操作を実行する前に、**検出** モードに切り替える必要があります。

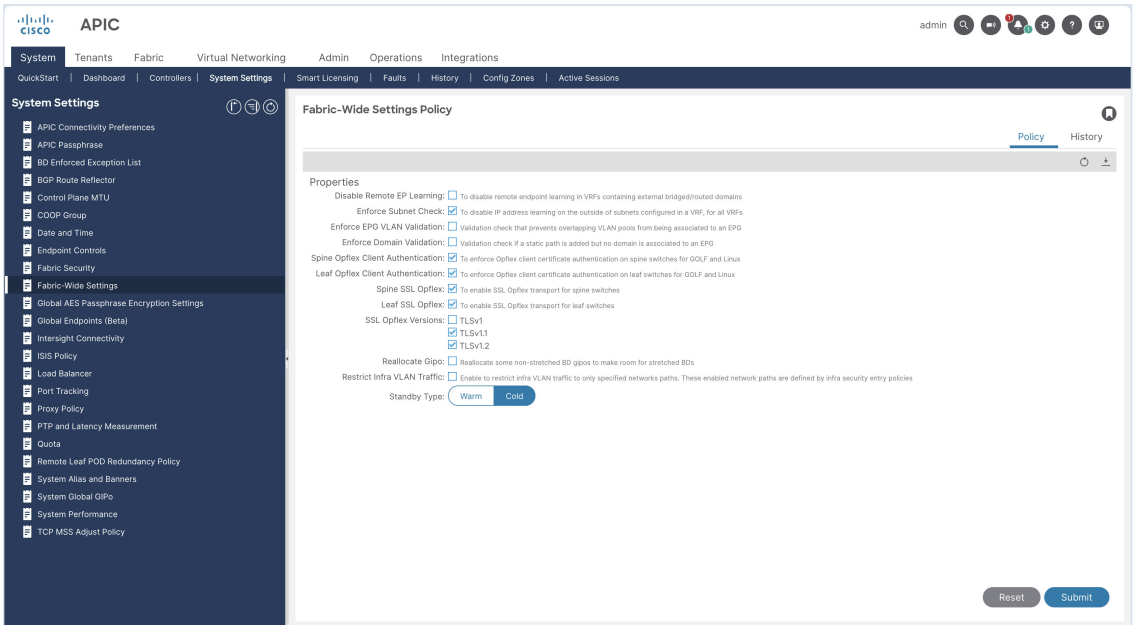
GUI を使用したスタンバイ APIC タイプの変更

Cisco APIC のスタンバイタイプを変更するには、次の手順を実行します。

手順

ステップ 1 **[システム（System）] > [システムの設定（System Settings）]** サブメニューに移動します。

ステップ 2 **[ファブリック全体の設定ポリシー（Fabric Wide Settings Policy）]** ページで、スタンバイタイプとして **[ウォーム（Warm）]** または **[コールド（Cold）]** を選択します。



524471

ステップ 3 [送信（Submit）] をクリックします。

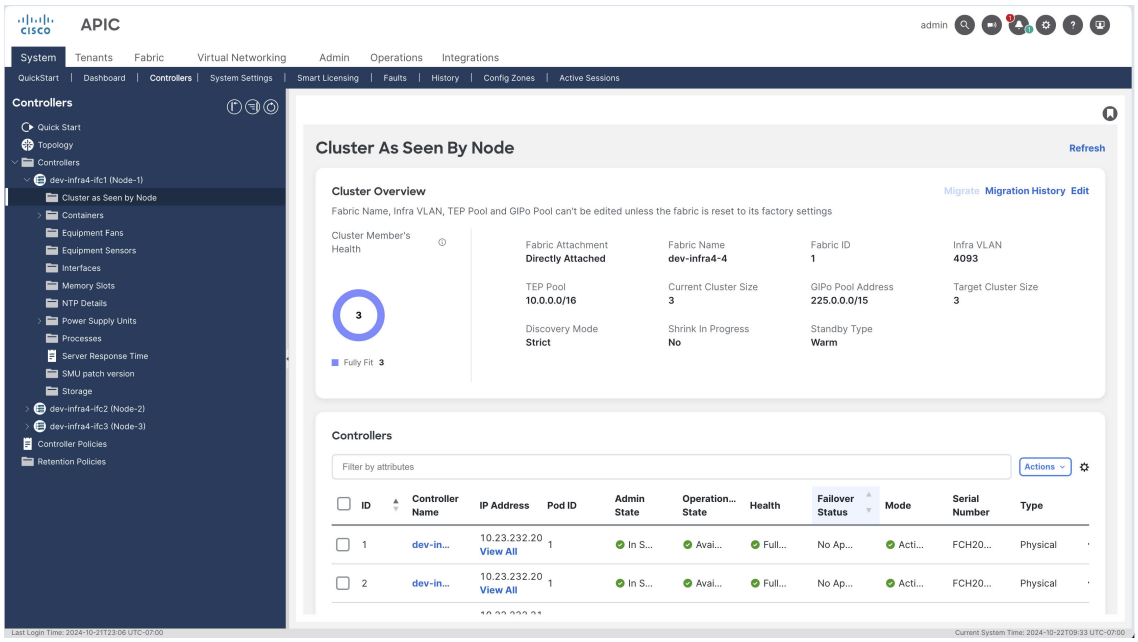
ステップ 4 ウォーム スタンバイのステータスを確認するには、次の手順を実行します。

a) メニュー バーで、**[システム（System）][コントローラ（Controllers）]** を選択します。

b) **[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）] > [apic_controller_name] > [ノードで表示されるクラスタ（Cluster as Seen by Node）]** を展開します。

c) **[作業（Work）]** ペインで、スタンバイ コントローラが **[スタンバイ コントローラ（Standby Controllers）]** に表示されます。

d) [スタンバイ タイプ（Standby Type）] が **[ノードで表示されるクラスタ（Cluster As Seen by Node）]** ペインに表示されます。



524470

スタンバイ APIC の追加

スタンバイ APIC を追加するには、次の手順に従います。

手順

ステップ 1 メニュー バーで、[System] > [Controllers] の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、[コントローラ（Controllers）] > apic_name > [ノードから見たクラスタ（Cluster as Seen by Node）] を展開します。

[ノードから見たクラスタ（Cluster as Seen by Node）] ウィンドウが **[作業（Work）]** ペインに表示されます。

ステップ 3 **[作業（Work）]** ペインで、**[アクション（Actions）]** > **[スタンバイ ノードの追加（Add Standby Node）]** をクリックします。

ステップ 4 **[コントローラタイプ（Controller Type）]** フィールドでは、クラスタ内のアクティブなコントローラと同じタイプとして **[物理（Physical）]** または **[仮想** （Virtual）] が事前に選択されています。

ステップ 5 **[接続タイプ（Connectivity Type）]** フィールドで、**[CMIC]** または **[OOB]** を選択します。仮想 APIC の場合、OOB は唯一のオプションとして事前に選択されています。

ステップ 6 **[CMICの詳細（CMIC Details）]** ペインまたは **[管理 IP（Management IP）]** ペインで、次の詳細を入力します。

a) **[IPアドレス（IP Address）]**：CIMC の IP アドレスを入力します。

b) **[ユーザー名（Username）]**：CIMC にアクセスするためのユーザー名。
c) **[パスワード（Password）]**：CIMC にアクセスするためのパスワードを入力します。

ステップ 7 **[全般（General）]** ペインで、次の詳細を入力します。

a) **[名前（Name）]**：コントローラの名前を入力します。
b) **[コントローラ ID（Controller ID）]**：コントローラ ID の値を入力します。この ID には 21 ～ 29 の範囲の値を追加することを推奨します。
c) **[Pod ID]**：APIC のポッド ID を入力します。有効な範囲は 1 ～ 128 です。
d) **[シリアル番号（Serial Number）]**：シリアル番号は、CIMC 検証後に自動入力されます（1 ～ N、N はクラスタ サイズ）。

APIC 1 は、CIMC IP アドレスの到達可能性を確認し、新しい APIC のシリアル番号もキャプチャします。

ステップ 8 **[アウトオブバンドネットワーク（Out of Band Network）]** ペインで、次の詳細を入力します。

a) **[IPv4アドレス（IPv4 Address）]**：IPv4 アドレスを入力します。
b) **[IPv4 ゲートウェイ（IPv4 Gateway）]**：ゲートウェイの IPv4 アドレスを入力します。

OOB 管理用に IPv6 アドレスを有効にしている場合は、IPv6 アドレスとゲートウェイを入力します。

a) **[IPv6 アドレス（IPv6 Address）]**：IPv6 アドレスを入力します。
b) **[IPv6ゲートウェイ（IPv6 Gateway）]**：IPv6 ゲートウェイアドレスを入力します。

ステップ 9 [適用（Apply）] をクリックします。

クラスタからスタンバイを削除する

Cisco APIC からウォーム スタンバイを選択して削除するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[System] > [Controllers] の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ウィンドウで、**[コントローラ（Controllers）] > apic_controller_name < [ノードから見たクラスタ（Cluster as Seen by Node）]** を展開します。

ステップ 3 **[コントローラ（Controllers）]** ペインで、ノードを選択し、**[アクション（Actions）] > [ノードの削除（Delete Nodes）] をクリックします。**

（注）
削除する必要があるノードをシャットダウンから、ノードを削除します。ノードを削除したら、ファブリックから切断する必要があります。このノードを工場出荷時設定にリセットするまで、削除したスタンバイノードをクラスターに再度追加することはできません。

GUI を使用したウォーム スタンバイ APIC によるディザスタ リカバリ

「ウォーム スタンバイ」セクションで説明したように、ウォーム スタンバイ APIC の使用例の 1 つは、アクティブな APIC ノードとともに一部またはすべてのデータベース情報（シャード）が失われた場合に、APIC クラスタを再構築することです。ウォーム スタンバイ APIC を使用したリカバリが必要なデータ損失シナリオの詳細については、Cisco APIC クラスタのウォーム スタンバイ （113 ページ） セクションを参照してください。

APIC クラスタを再構築して、APIC クラスタのデータ損失を引き起こした壊滅的なイベントからファブリックを復元するには、ウォーム スタンバイ APIC ノードの 1 つの GUI または REST API にアクセスし、以下の手順に従います。

このセクションの手順では、スタンバイ ノード自体のデータベース情報を使用して、ウォーム スタンバイ APIC ノードを APIC 1 に昇格させます。ウォーム スタンバイ APIC ノードが APIC 1 に正常に昇格されたら、残りのアクティブおよびスタンバイ（あるいはその両方の）APIC ノードを初期化し、新しいアクティブ APIC 2、APIC 3 などとして検出します。新しい APIC ノードが検出されると、以前はウォーム スタンバイ APIC ノードであった APIC 1 に保存されたデータが、各シャードの新しいレプリカとしてそれらの新しいノードに配布されます。

（注） ウォーム スタンバイ APIC ノードが APIC 1 に昇格されると、スタンバイ APIC ノードは、ACI スイッチがスタンバイ ノード（間もなく新しい APIC 1 になる）のみを確認できるように、まだ到達可能な残りのアクティブまたはスタンバイ APIC のインフラ インターフェイスをシャットダウンします。残りのアクティブな APIC ノードとの競合を回避するためです。

Cisco APIC の Cisco APIC ディザスタ リカバリを構成するには、次の手順を実行します。

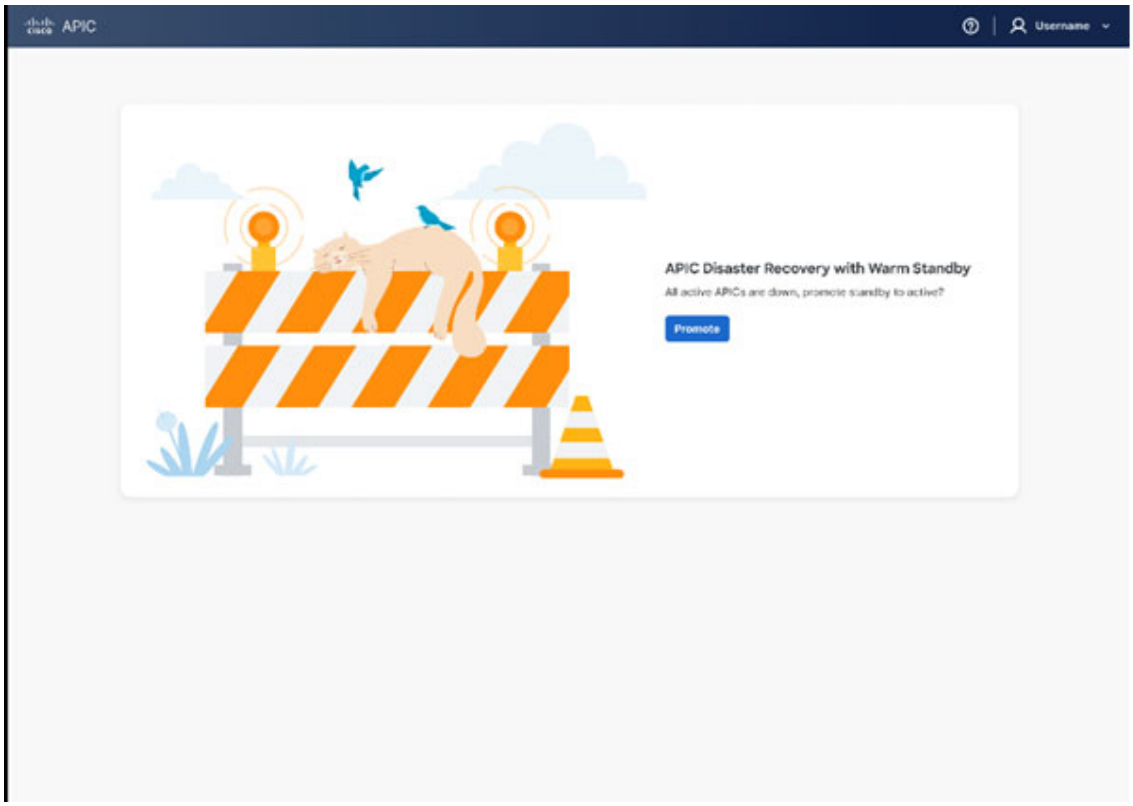
手順

ステップ 1 `https://<standby APIC OoB IP>` にアクセスして、ウォームスタンバイ APIC のいずれかにログインします。管理者ユーザーのパスワードは必須です。

ステップ 2 **[昇格（Promote）]** をクリックして、ウォーム スタンバイ APIC を APIC 1 に昇格させ、APIC クラスタの再構築を開始します。

（注）
Cisco APIC クラスタにディザスタ リカバリが必要ない場合は、アクティブな APIC UI にリダイレクトされます。

ステップ 3 [イニシエーションの進行状況（Initiation Progress）] ステータスが表示されます。成功すると、アクティブな Cisco APIC が表示されます。GUI は、以前のスタンバイ ノードを新しい APIC 1 として使用する通常の APIC GUI に移行します。この GUI を使用して、次の手順で新しい APIC 2、APIC 3 などを追加します。



ステップ 4 各ノードの CLI で、**acidiag touch setup** を使用して残りの APIC ノードを初期化し、**acidiag reboot** を実行します。

ステップ 5 新しい APIC 1 の APIC GUI を使用して、初期化された APIC ノードを新しい APIC 2、APIC 3 などとして追加します。詳細については、ノード追加オプションを使用した APIC クラスタの拡大 （98 ページ）を参照してください。

APIC の移行

Cisco APIC リリース 6.1(1) 以降では、物理 APIC クラスタから ESXi ホストに展開された仮想 APIC クラスタへの移行がサポートされています（VMware vCenter を使用）。（ESXi ホスト上の）仮想 APIC クラスタから物理 APIC クラスタへの移行もサポートされています。

注意事項と制約事項

次に、物理 APIC を仮想 APIC に移行する（およびその逆）ための注意事項と制限事項を示します。

ガイドライン

- レイヤ 2 の物理 APIC（ファブリックに直接接続）はレイヤ 2 仮想 APIC に移行でき、レイヤ 2 仮想 APIC はレイヤ 2 物理 APIC に移行できます。レイヤ 3（ファブリックにリモー

ト接続されている）の物理 APIC は、レイヤ 3 仮想 APIC に移行できます。レイヤ 3 の仮想 APIC は、レイヤ 3 の物理 APIC に移行できます。レイヤ 2 APIC からレイヤ 3 APIC への移行（またはその逆）はサポートされていません。

- アップグレードが進行中の場合は、移行プロセスを開始しないでください。
- 移行が進行中の場合は、アップグレードを開始しないでください。
- APIC OOB を使用する構成は、移行プロセスの完了後に更新する必要があります。
- NDO が設定されている場合は、移行によって OOB IP アドレスとサブネットアドレスが変更されるため、NDO の接続の詳細を更新する必要があります。
- SMU が物理 APIC にインストールされている場合、Cisco APIC リリース 6.1(1) の移行（物理 APIC から仮想 APIC へ）は推奨されません。移行を続行する前に、SMU の修正が適用されたイメージにクラスタをアップグレードする必要があります。
- app-infra の場合、移行前に ELAM/FTRIAGE の実行中のジョブを停止し、移行が完了した後に再起動します。

制限事項

- スタンバイ ノードの移行はサポートされていません。移行の前に、クラスタからスタンバイ ノードを削除してから移行します。
- ミニ ACI ファブリックの移行はサポートされていません。

移行プロセス

このセクションでは、移行プロセスの概要について説明します。詳細な手順については、後続のセクションの物理 APIC から仮想 APIC への移行の手順を参照してください。

3 ノードクラスタを考えてみます。 つまり、3 つのソースノードがあり、移行の後には 3 つのターゲットノードになります。コントローラ ID 1 の APIC は APIC 1 と見なされます。APIC 1（IP アドレス 172.16.1.1）にログインし、移行プロセスを開始します。

表 *12*：サンプル *APIC* ノード

APIC	ソース ノード	ターゲットノード
APIC 1	172.16.1.1	172.16.1.11
APIC 2	172.16.1.2	172.16.1.12
APIC 3	17.16.1.3	172.16.1.13

移行プロセスの段階

1. ソース APIC 1（172.16.1.1）にログインし、移行プロセスを開始します。
2. ソース ノード APIC 3（172.16.1.3）の移行が開始されます。
3. APIC 3 の移行が完了しました（ターゲット ノード 172.16.1.13 へ）。
4. ソース ノード APIC 2（172.16.1.2）の移行が開始されます。
5. APIC 2 の移行が完了しました（ターゲット ノード 172.16.1.12 へ）。
6. ターゲット APIC 2 が制御を行い、APIC 1 の移行を有効にします。これはハンドオーバープロセスと呼ばれ、制御がソース APIC 1（172.16.1.1）からターゲット APIC 2（172.16.1.12）に渡されます。この段階で、新しいウィンドウが表示されます（URL がターゲット APIC 2 にリダイレクトされます）。これは、移行が成功すると、ソース APIC 1 が（移行されたターゲット APIC を持つ）クラスタの一部ではなくなるためです。

移行は逆順で完了されます。つまり、APIC *N*（例では APIC 3）が最初に移行され、次に APIC *N-1*（例では APIC 2）、最後に APIC 1 が移行されます。

物理 APIC クラスタを仮想 APIC クラスタに移行する（または仮想 APIC クラスタを物理 APIC クラスタに移行する）

この手順に従って、物理 APIC クラスタのノードを仮想 APIC クラスタに移行します（またはその逆）。

始める前に

移行プロセスを開始する前に必要な前提条件は次のとおりです。

クラスタの正常性

現在の APIC クラスタが 完全に適合していることを確認します。

全般

- 送信元と宛先の APIC の日付と時刻が同期されていることを確認します。
- すべてのコントローラが Cisco APIC リリース 6.1(1) 上にあり、すべてのスイッチがコントローラと同じバージョンを実行していることを確認します。

送信元ノードとターゲット ノード

- 直接接続された APIC の移行では、ソースノードとターゲットノードの両方が同じレイヤ 2 ネットワーク上にあることを確認します。
- リモート接続された APIC の移行では、送信元ノードとターゲット ノードの両方にインフラ ネットワーク接続があることを確認します。つまり、新しいターゲット APIC には、ファブリックのインフラ ネットワークと対話できるように、正しい IPN 構成が必要です。
- ターゲット ノードの管理者パスワードは、送信元クラスタと同じです。

- ターゲット ノードの OOB IP アドレスは異なる必要がありますが、他のすべてのフィールドは送信元ノードと同じでも異なっていてもかまいません。インフラアドレスは、レイヤ 2（直接接続）でも同じままです。レイヤ3（リモート接続）クラスタの場合、展開に基づいて同じにすることも、異なるものにすることもできます。
- 送信元クラスタとターゲット クラスタの OOB ネットワーキング スタックが一致している必要があります。たとえば、送信元クラスタが OOB にデュアル スタック（IPv4 および IPv6）を使用している場合、ターゲット ノードにもデュアル スタック（IPv4 および IPv6）アドレスの詳細を指定する必要があります。
- 送信元 APIC と宛先 APIC 間の OOB 接続を確認します。
- 新しい APIC の OOB コントラクトと到達可能性が正しく設定されていることを確認します。移行プロセスでは、OOB IP アドレスを使用して APIC 間の通信を行います。

仮想 APIC から物理 APIC への移行の場合

- 物理 APIC ノードが初期設定にリセットされていることを確認します。 **acidiag touch setup** および **acidiag reboot** コマンドを使用します。
- CIMC の有無にかかわらず移行する場合（物理 APIC に適用）：

次の場合....	手順 ...
CIMC 使用	物理 APIC CIMC アドレスが仮想 APIC の OOB ネットワークから到達可能であることを確認します。
CIMC 不使用	工場出荷時のリセット後に物理 APIC で OOB IP アドレスが手動で設定されていることを確認し、接続に OOB オプションを使用します。

物理から仮想への移行の場合

- VMware vCenter を使用したCisco 仮想 APIC の展開ガイドの手順に従って仮想 APIC ノードを展開したことを確認します。
- VMM ドメインの一部である vCenter に仮想 APIC が展開されている場合は、仮想 APIC が展開されている ESXi ホストに接続されているインターフェイスで設定されている AEP でインフラストラクチャ VLAN が有効になっていることを確認します。

手順

ステップ 1 **[ノードから見たクラスタ（Cluster as Seen by Node）]** 画面で、**[移行（Migrate）]** をクリックします（**[クラスタの概要（Cluster Overview）]** 領域に表示されます）。

クラスタ内の使用可能なすべてのコントローラが表示されます。

（注）
[移行（Migrate）] ボタンは、（クラスタの）APIC 1 にのみ表示されます。

ステップ 2 [検証（Validate）] 列の横にある鉛筆アイコンをクリックして、選択したコントローラの移行プロセスを開始します。

[ノードの追加（Add Node）] 画面が表示されます。

ステップ 3 **[ノードの追加（Add Node）]** 画面で、以下の詳細を入力します：

a) **[コントローラタイプ（Controller Type）] では、**場合に応じて [仮想（Virtual）] または [物理（Physical）] を選択します（物理 APIC から仮想 APIC への移行、およびその逆の移行がサポートされています）。

b) 物理 APIC を仮想 APIC に移行する場合は、**[接続タイプ（Connectivity Type）]** で [OOB] を選択します。仮想 APIC を物理 APIC に移行する場合は、[OOB] オプションまたは [CIMC] オプションのいずれかを選択できます。

仮想から物理への移行には、[CIMC] オプションを選択することをお勧めします。[OOB] オプションを使用するには、移行プロセスを開始する前に、物理 APIC の CIMC アドレスに接続し、OOB IP アドレスを手動で設定します。

[コントローラタイプ（Controller Type）] と **[接続タイプ（Connectivity Type）]** は、 送信元コントローラ タイプに基づいて自動的に選択されます。必要であれば、値を変更できます。

c) [管理 IP（Management IP）] ペインで、ターゲット APIC の詳細として [管理 IP アドレス（Management IP address）]、[ユーザー名（Username,）]、[パスワード（Password）]を入力します。

または

（仮想 APIC から物理 APIC への移行にのみ適用可能）[CIMCの詳細（CIMC Details）] ペインで、物理 APIC の次の詳細（[CIMC IP アドレス（CIMC IP address）]、ノードの [ユーザー名（username）]、およびパスワード[password]）を入力します。

d) [**Validate**] をクリックします。

[検証（Validate）] をクリックすると、[一般（General）] および [アウトオブバンド（Out of Band）] 管理ペインに表示されている詳細が、コントローラの詳細と一致するように変更されます。編集可能なフィールドは [名前（Name）] と [ポッド ID（Pod ID）]（レイヤ 2 にのみ適用）のみで、他のフィールドは変更できません。仮想 APIC から物理 APIC への移行の場合は、管理者パスワードも確認します。

（注）
デュアルスタックがサポートされている場合は、IPv4 および IPv6 アドレスを入力します。

e) [インフラストラクチャ ネットワーク（Infra Network）] ペイン（レイヤ 3 にのみ適用され、APIC はリモートでファブリックに接続されます）で、次のように入力します。

- [IPv4 アドレス（IPv4 Address）]：インフラ ネットワーク アドレス。
- [IPv4 ゲートウェイ（IPv4 Gateway）]：ゲートウェイの IP アドレス。
- [VLAN]：使用するインターフェイス VLAN ID。

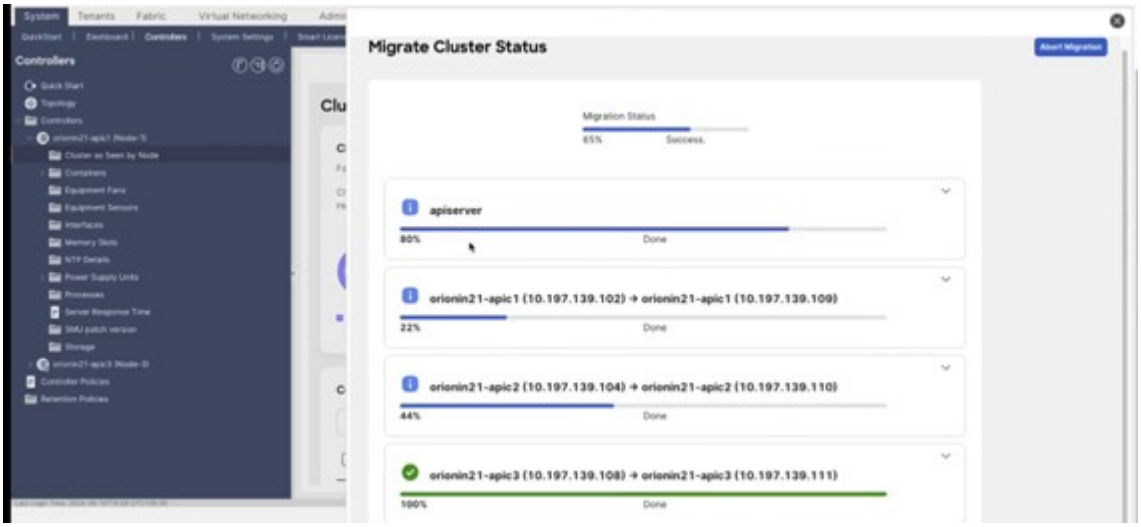
OOB ゲートウェイと IP アドレスは、（検証に基づいて）テーブルに自動的に入力されます。**[適用（Apply）]**をクリックします。検証ステータスは、[ノードの移行（Migrate Nodes）] 画面に [完了（Complete）] と表示されます。

鉛筆アイコン（[検証（Validation）] 列の横）をクリックして、クラスタ内の他の APIC に対して同じプロセスを繰り返します。すべてのコントローラの詳細を入力したら、[移行（Migrate）] 画面の下部にある **[移行（Migrate）]** ボタンをクリックします。

移行ステータス

移行プロセスには一連のアクティビティが含まれ、段階的に表示されます。各段階は、色分けされたバーで示されます。

図 *14 :* 移行ステータス



[クラスタ ステータスの移行（Migrate Cluster Status）] 画面には、全体的な移行ステータスが表示され、その後に apisever のステータスが表示されます。apiserver は、移行プロセス全体を調整するプロセスです。apiserver ステータスの下に、コントローラ単位の移行ステータスが表示されます。ノードのソース IP アドレスとターゲット IP アドレスも示されます。

APIC 2 へのハンドオーバーが完了すると、apiserver のステータスは 100% 完了（緑色のバー）と表示されます。この段階で、新しいウィンドウが表示されます（URL がターゲット APIC 2 にリダイレクトされます）。ターゲット APIC 2 にログインします。移行が完了するまで、 移行が進行中であることを示すバナーが GUI の上部に表示されます。ハンドオーバー プロセスの後、ソース APIC 1 に表示されていたバナーがターゲット APIC 2 に表示されます。バナーの **[ステータスの表示（View Status）]** リンクをクリックして、移行ステータスを確認します。

[クラスタステータスの移行（Migrate Cluster Status）] 画面にある **[中止（Abort）]** ボタンをクリックして、送信元 APIC 1 からの移行プロセスを中止することもできます。**[中止（Abort）]** ボタンは、移行を開始してから一定期間が経過した後にのみ表示されます。

移行が正常に終了すると、次のようになります：

- 移行ステータスは表示されなくなります。移行が失敗した場合は、明示的に失敗メッセージが表示されます。
- ターゲット クラスタが正常であり、完全に適合しているかどうかを確認するには、**[システム（System）] > [コントローラ（Controllers）] > [コントローラの展開（Expand Controllers）]**に移動します。**[コントローラ 1 （Controller 1）] > Cluster as seen by Node** page.
- すべてのファブリック ノードがアクティブ状態であるかどうかを確認します。**[ファブリック（Fabric）]**、**[ファブリック メンバーシップ（Fabric Membership）]** の順に選択します。
- ターゲット APIC のポッド ID が変更された場合は、[テナント管理（Tenant Management）] 画面でノードのインバンド アドレスを再構成する必要があります。**[テナント（Tenants）] > [管理（Mgmt）]> [ノード管理アドレス（Node Management Addresses）]** ページに移動します。

移行が失敗した場合の操作

移行プロセスは、障害が原因で中断されることもありますし、ユーザーが移行の中止を選択することもあります。移行が成功しなかった場合は、ソースまたはターゲットのいずれかのコントローラタイプに移行を元に戻すか、移行を再開することをお勧めします。物理コントローラと仮想コントローラが混在する状態で APIC クラスタを移行が失敗した状態にすることは推奨されません。復元または再開を試みる前に、次のセクション基本的なトラブルシューティングの手順に従って、クラスタを正常な状態にします。

[再開（resume）] を選択した場合、移行プロセスは続行されます。**[ノードの移行（Migrate Node）]** 画面（ソース APIC 1）で、次の手順を実行します。

1. 移行するコントローラタイプに基づいて、すべてのターゲットノードの詳細を入力します。
2. **[移行（Migrate）]** をクリックします。

元に戻すことを選択した場合：移行プロセスは再起動されます。クラスタのコントローラを初期（送信元）IPアドレスに取得した後、移行プロセスを再起動する必要があります。

1. **acidiag touch setup** および **acidiag reboot** コマンドを使用して、移行の途中だった各ソース APIC ノードを初期設定にリセットします。
2. 移行プロセスによって以前に移行された APIC がソース コントローラ タイプに戻るため、**[ノードの移行（Migrate Node）]** 画面で、すべてのノードのソース APIC の詳細を入力します。
3. **[移行（Migrate）]** をクリックします。

（注） ハンドオーバー プロセス（ソース APIC 1 からターゲット APIC 2 に制御が渡される）後に移行プロセスが失敗した場合、移行を再開または元に戻すことはできません。

前述のように、移行のさまざまなサブステージとその完了の進行状況は、コントローラごとにバーで示されます。いずれかの段階で障害が発生した場合は、関連するテクニカルサポートの詳細を収集し、Cisco TAC にお問い合わせください。テクニカル サポートのログを収集するには、**[管理（Admin）]** > **[インポート/エクスポート（Import/Export ）]** > **[エクスポート ポリシー（Export Policies）]** > **[オンデマンド テクニカル サポート（On-demand Tech Support）]** > **migration_techsuppport** に移動します。

基本的なトラブルシューティング

2 つのノードが正常に移行され、3 番目のノードの移行中に障害が検出された 3 ノードクラスタについて考えます。障害が発生したノードのステータスを確認します。コントローラが完全に適合した 状態でない場合、移行は失敗する可能性があります。

クラスタを正常な状態にする手順：

手順

ステップ 1 （APIC 1 での移行の失敗した場合） **[システム（System）]** > **[コントローラ（Controllers）]**に移動して、ターゲット APIC 2 からクラスタの正常性を確認します。**[コントローラ 2（Controller 2）]** > **[ノードから見たクラスタ（Cluster as seen by Node）]** を選択します。

または

（APIC 2 から *N* への移行が失敗した場合） **[システム（System）]**> **[コントローラ（Controllers）]** に移動して、ソース APIC 1 からクラスタの正常性を確認します。**[コントローラ 1（Controller 1）]** > **[ノードから見たクラスタ（Cluster as seen by Node）]** を選択します。

ステップ 2 APIC 1（またはクラスタの他のノード）が *[*完全に適合（*Fully Fit*）*]*でない場合は、コントローラのシリアル番号の横にある 3 つのドットをクリックします。**[メンテナンス（Maintenance）]** > **[デコミッション（Decommission）]**を選択します。ノードが *[*完全に適合（*Fully Fit*）*]* 状態ではないため、**[強制デコミッション（Force Decommission）]** をクリックします。SSH を使用して送信元 APIC ノード *N* に接続し、次のコマンド **acidiag touch setup**、 **acidiag reboot**を使用してノードを工場出荷時の状態にリセットします。

ステップ 3 ソース APIC 1 から、**[システム（System）]**> **[コントローラ（Controllers）]**に移動します。**[コントローラ（Controllers）]** > **[コントローラ 1（Controller 1 ）]** > **[ノードから見たクラスタ（Cluster as seen by Node）]** をクリックします。

または

ターゲット APIC 2 から、**[システム（System）]** > **[コントローラ（Controllers）]**に移動します。**[コントローラ（Controllers）]** > **[コントローラ 2（Controller 2）]** > **[ノード別クラスタ（Cluster）]** をクリックします。

ステップ 4 コントローラのコミッションを行うには、コントローラのシリアル番号の横にある 3 つのドットをクリックします。**[メンテナンス（Maintenance）]** > **[コミッション（Commission）]** を選択します。必要に応じて、詳細を入力します。「ノードのコミッショニング」の手順（この章で前述）を参照してください。ここでの唯一の違いは、コントローラ ID には、クラスタ内のコントローラの ID に対応する番号が事前に入力されていることです。

コントローラのコミッションが行われると、クラスタは *[*完全に適合（*Fully Fit*）*]*と表示されます。

ステップ 5 障害が発生したノードのコミッションを行った後、クラスタのステータスを確認します。クラスタが正常な状態の場合は、**[ノードから見たクラスタ（Cluster as seen by Node）]** 画面で **[移行（Migrate）]** をクリックして移行を再開します。移行が再び失敗した場合には、シスコの TAC に連絡してください。

GUI を使用して起動時の APIC クラスタを管理する

GUI を使用して、新しいクラスタを構築し、既存のクラスタにノードを追加し、既存のクラスタ内のノードの 1 つを起動時に新しいノードに置き換えるには、次の手順に従います。

手順

ステップ 1 *https://APIC-IP* を使用して APIC にログインし、パスワードを入力します。

a) 仮想 APIC の場合：

ESXi（OVF テンプレート）またはリモート AWS（CFT）を使用した仮想の展開が完了している場合は、この例のような出力が VM コンソールに表示されます。

```
System pre-configured successfully.
Use: https://172.31.1.2 to complete the bootstrapping.
```

ブートストラップ GUI にアクセスするための IP アドレス（**[APIC Cluster Bringup]**）は、例に示すように明示的に示されます。ステップ 2 に進むことができます。

AWS に Cisco APIC を展開した後、OOBMgmt IP アドレスを手元に置いて、**クラスタの起動** GUI にアクセスします。OOB 管理 IP アドレスは、AWS GUI の **[スタック出力（Stacks Outputs）]** タブから取得できます。

b) 物理 APIC の場合：

CIMC を使用して APIC KVM コンソールにログインします。次のような画面が表示されます。

```
APIC Version: 6.0(2a)
Welcome to Cisco APIC Setup Utility
Press Enter Or Input JSON string to bootstrap your APIC node.
```

KVM に黒い画面しか表示されない場合は、SSH を使用して CIMC に接続し、Serial over LAN（SoL）（「connect host」）を使用してコンソールに接続します。

APIC で**Enter**を押し、要求された情報を入力します。ブートストラップ GUI（**APIC Cluster Bringup**）にアクセスするための IP アドレスが明示的に示されます。

```
admin user configuration ...
  Enter the password for admin [None]:
  Reenter the password for admin [None]:
Out-of-band management configuration ...
  Enter the IP Address [192.168.10.1/24]: 172.20.7.79/23
  Enter the IP Address of default gateway [192.168.10.254]: 172.20.6.1
Would you like to edit the configuration? (y/n) [n]:
System pre-configured successfully.
Use: https://172.20.7.79 to complete the bootstrapping
```

（注）
管理者パスワードは、既存のクラスタのパスワードと同じである必要があります。

上記の IP アドレスは例です。IP アドレスは、展開環境によって異なる場合があります。

ステップ 2 **APIC Cluster Bringup** ウィザードの **[ワークフローの選択（Select Workflow）]** 画面で、これらのワークフローのいずれかを選択します。

- **[新規クラスタ（New cluster）]**：新しいクラスタを開始するには、このオプションを使用します。
- **クラスタ拡張**: このオプションを使用して、既存のクラスタにノードを追加します。
- **[APIC の交換（APIC replace）]**：このオプションを使用して、既存のクラスタ内のノードの 1 つを新しいノードに置き換えます。

a) 新規クラスタを開始する方法は、「GUI を使用した Cisco APIC クラスタの呼び出し」を参照してください。

b) 既存のクラスタにノードを追加するには、次の手順を実行します。

- **[ワークフローの選択（Select Workflow）]** 画面で、**[クラスタ拡張（Cluster extension）]** を選択し、**[次へ（Next）]**をクリックします。
- **[Cluster Verification (クラスタの検証)**] 画面で、アクティブな APIC ノードの OOB IP アドレスを入力し、**[Validate (検証)]**をクリックします。

  ファブリックとコントローラの情報が表示されます。

  情報を確認したら **[次へ（Next）]** をクリックします。
- **[ノード詳細の入力（Enter Node Details）]** 画面で、**[コントローラ名（Controller Name）]** フィールドと **[ポッド ID（Pod ID）]** フィールドにそれぞれコントローラの名前とポッド ID を入力します。

  （注）
  レイヤ 3 APIC にはポッド ID は必要ありません。

- （オプション）**[スタンバイ（Standby）]** チェックボックスをオンにして、**[コントローラ ID（Controller ID）]** フィールドに値を入力します。

  スタンバイ コントローラ ID の範囲は 21 ～ 29 です。

  [コントローラ ID（Controller ID）] フィールドには値が自動的に入力され、デフォルトでは無効になっています。

- （オプション）この構成を強制するには、**[強制（Force）]** チェックボックスをオンにします。

- （オプション）アウトオブバンド管理用に IPv6 アドレスを有効にする場合は **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにして、IPv6 アドレスとゲートウェイを入力します。

  IPv4 アドレスと IPv4 ゲートウェイが **[アウトオブバンド ネットワーク (Out-of-band Network)]** ペインの下に自動入力されます。

- （レイヤ 3 APIC の場合） **[インフラ L3 ネットワーク（Infra L3 Network）]** ペインでこれらの詳細を入力します。

  - [IPv4 アドレス（IPv4 Address）] : インフラ ネットワーク アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）] : ゲートウェイの IP アドレスを入力します。
  - [VLAN] : 使用するインターフェイス VLAN ID を入力します。

  [次へ（Next）] をクリックします。

- **[概要（Summary）]** 画面で更新を確認し、**[展開（Deploy）]** をクリックします。

  進行状況が画面に表示されます。

c) 既存のクラスタ内のノードの 1 つを新しいノードに置き換えるには、次の手順を実行します。

- **[ワークフローの選択（Select Workflow）]** 画面で、**[APIC] の交換** を選択し、**[次へ（Next）]**をクリックします。
- **[Cluster Verification (クラスタの検証)**] 画面で、アクティブな APIC ノードの OOB IP アドレスを入力し、**[Validate (検証)]**をクリックします。

  ファブリックとコントローラの情報が表示されます。

  情報を確認したら **[次へ（Next）]** をクリックします。

- **[ノード詳細の入力（Enter Node Details）]** 画面で、**[コントローラ ID（Controller ID）]** ドロップダウン リストからコントローラ ID を選択します。

  [コントローラ ID（Controller ID）] ドロップダウン リストには、解放されたコントローラの ID のみが表示されます。

  コントローラ名は、選択したコントローラ ID に基づいて自動的に入力されます。

- **[ポッド ID（Pod ID）]** フィールドにポッド ID を入力します。

（注）
レイヤ 3 APIC にはポッド ID は必要ありません。

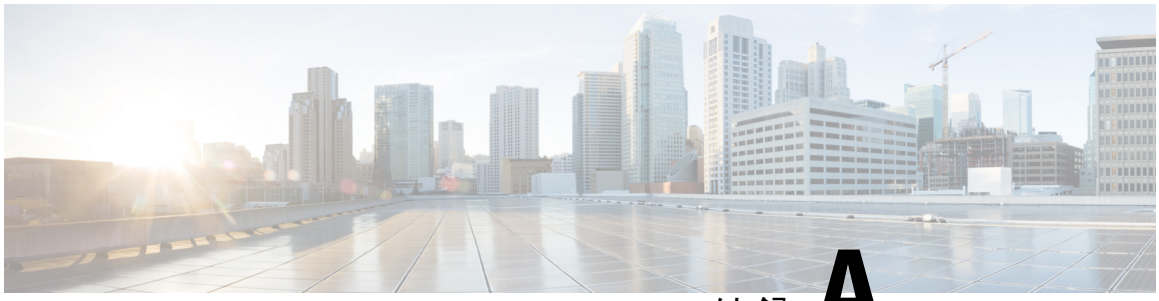
- （オプション）この構成を強制するには、**[強制（Force）]** チェックボックスをオンにします。
- （オプション）アウトオブバンド管理用に IPv6 アドレスを有効にする場合は **[IPv6 の有効化（Enable IPv6）]** チェックボックスをオンにして、IPv6 アドレスとゲートウェイを入力します。

  IPv4 アドレスと IPv4 ゲートウェイが **[アウトオブバンド ネットワーク (Out-of-band Network)]** ペインの下に自動入力されます。
- （レイヤ 3 APIC の場合） **[インフラ L3 ネットワーク（Infra L3 Network）]** ペインでこれらの詳細を入力します。
  - [IPv4 アドレス（IPv4 Address）] : インフラ ネットワーク アドレスを入力します。
  - [IPv4 ゲートウェイ（IPv4 Gateway）] : ゲートウェイの IP アドレスを入力します。
  - [VLAN] : 使用するインターフェイス VLAN ID を入力します。

  [次へ（Next）] をクリックします。
- **[概要（Summary）]** 画面で更新を確認し、**[展開（Deploy）]** をクリックします。

  進行状況が画面に表示されます。

（注）
この手順の後、メインの APIC UI に移動するには、ユーザーは手動で UI をリロードする必要があります。



付録 A

CLI を使用している Cisco APIC の設定

クラスタ管理の注意事項

Cisco Application Policy Infrastructure Controller (APIC) クラスタは複数の Cisco APIC コントローラで構成され、Cisco Application Centric Infrastructure（ACI）ファブリックに対する統合されたリアルタイム モニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスが得られるように、Cisco APIC クラスタを変更する場合は次のガイドラインに使用してください：

- クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の Cisco APIC のヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。また、Cisco APIC に追加されたクラスタ コントローラが Cisco APIC クラスタ内の他のコントローラと同じファームウェア バージョンを実行しているか確認してください。

- クラスタ内には少なくとも 3 つのアクティブな Cisco APIC があり、追加のスタンバイ Cisco APIC があることを推奨します。 Cisco APIC クラスタには、3 ～ 7 個のアクティブな Cisco

CLI を使用している Cisco APIC の設定

APICを含めることができます。展開に必要なアクティブな Cisco APIC の数を確認するには、『検証済みスケーラビリティ ガイド』を参照してください。

- 現在クラスタにない Cisco APIC からのクラスタ情報は無視します。正確なクラスタ情報ではありません。
- クラスタ スロットには Cisco APIC `ChassisID` を含みます。スロットを設定すると、割り当てられたシャーシ `ID` の Cisco APIC を解放するまでそのスロットは使用できません。
- Cisco APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが完全に適合するまでクラスタへの他の変更はしないでください。
- Cisco APIC を移動する際は、最初に正常なクラスタがあることを確認します。Cisco APIC クラスタの状態を確認するには、後にシャットダウンする Cisco APIC を選択します。Cisco APIC をシャットダウンした後、Cisco APIC に移動し、再接続して、電源を入れます。GUI から、クラスタ内のすべてのコントローラが完全に適合状態に戻すことを確認します。

（注） 一度に 1 つの Cisco APIC のみ移動します。

- 一連のリーフ スイッチに接続されている Cisco APIC を別のリーフ スイッチのセットに移動する場合、または Cisco APIC を同じリーフ スイッチ内の別のポートに移動する場合は、まずクラスタが正常であることを確認します。Cisco APIC クラスタの状態を確認したら、移動してクラスタからデコミッションする Cisco APIC を選択します。Cisco APIC がデコミッションされたら、 Cisco APIC を移動してコミッションします。
- Cisco APIC クラスタを設定する前に、すべての Cisco APIC のパフォーマンスが同じファームウェア バージョンを実行していることを確認します。異なるバージョンを実行して Cisco APIC のパフォーマンスの最初のクラスタ リングはサポートされていない動作し、クラスタ内の問題が発生する可能性があります。
- 他のオブジェクトとは異なり、ログ レコード オブジェクトは、いずれかの Cisco APIC のデータベースの 1 つのシャードにのみ保存されます。これらのオブジェクトは、使用停止または Cisco APIC交換すると永久に失われます。
- Cisco APICをデコミッションすると、Cisco APIC に保存されていたすべての障害、イベント、および監査ログ履歴が失われます。すべての Cisco APIC を交換すると、すべてのログ履歴が失われます。Cisco APICを移行する前に、ログ履歴を手動でバックアップすることをお勧めします。

CLI を使用した、クラスタ内の Cisco APIC の交換

（注）
- クラスタの管理の詳細については、「クラスタ管理の注意事項 （92 ページ）」を参照してください。
- Cisco APIC を交換すると、パスワードは必ずクラスタから同期されます。APIC 1 を交換するときには、パスワードの入力を求められますが、そのパスワードはクラスタ内の既存のパスワードを優先して無視されます。Cisco APIC 2 または 3 を交換するときには、パスワードの入力は求められません。

始める前に

Cisco Application Policy Infrastructure Controller (APIC)を交換する前に、交換用 Cisco APIC が、交換する Cisco APIC と同じファームウェアバージョンを実行していることを確認します。バージョンが同じでない場合は、開始する前に代替 Cisco APICのファームウェアを更新する必要があります。異なるバージョンを実行して Cisco APIC のパフォーマンスの最初のクラスタ リングはサポートされていない動作し、クラスタ内の問題が発生する可能性があります。

手順

ステップ 1 交換する Cisco APIC を特定します。

ステップ 2 **acidiag avread** コマンドを使用して、交換するCisco APICの設定の詳細を確認します。

ステップ 3 **decommission controller** *controller-id* コマンドを使用して Cisco APIC をデコミッションします。

Cisco APIC を解放すると、APIC ID とシャーシ ID のマッピングが削除されます。通常、新しい Cisco APIC には、異なる APIC ID があるので、クラスタに新しい Cisco APIC を追加するにはこのマップを削除する必要があります。

Cisco APICリリース 6.0（2）以降、廃止操作を強制できるようにするために、オプションの引数（`force`）が **decommission** コマンドに追加されました。改訂されたコマンドは **decommission controller** *controller-id* [**force**] で、次のように動作します。

- `force` を宣言しないと、クラスタが異常またはアップグレード状態の場合には廃止が適切でない可能性があるので、それ以外の場合にのみ廃止が続行されます。
- `force` を宣言すると、クラスタの状態に関係なく、廃止が続行されます。

たとえば、`decommission controller 3 force` は、クラスタの状態に関係なく、APIC3 を強制的にデコミッションします。

ステップ 4 新しい Cisco APIC をコミッションする手順は、次のとおりです。

a) ファブリックから古い Cisco APIC を切断します。

b) ファブリックに交換 Cisco APIC を接続します。

新しいCisco APIC **[未認可コントローラ (Unauthorized Controllers)]** リストの Cisco APIC GUI メニュー **[システム (System)]** > **[コントローラ (Controllers)]** > ***[apic_controller_name]*** > **[ノードで確認するクラスタ (Cluster as Seen by Node)]**に表示されます。

c) **controller** *controller-id* **commission** コマンドを使用して新しい Cisco APIC をコミッションします。

d) 新しい Cisco APIC を起動します。

e) クラスタの残りの部分に新しい Cisco APIC 情報が伝播するまでに数分かかります。

新しいCisco APIC **[現用系コントローラ (Active Controllers)]** リストの Cisco APIC GUI メニュー **[システム (System)]** > **[コントローラ (Controllers)]** > ***[apic_controller_name]*** > **[ノードで確認するクラスタ (Cluster as Seen by Node)]**に表示されます。

次のタスク

解放した各コントローラにつき、そのコントローラの動作状態が未登録になり、すでにクラスタ内で稼動していないことを確認します。

（注） デコミッションされたCisco APICがファブリックからすぐに削除されない場合、再検出される可能性があり、問題が発生する可能性があります。その場合、コントローラを削除するためにAPIC クラスタのサイズ縮小 （94 ページ） の説明に従います。

APIC クラスタのサイズ縮小

Cisco Application Policy Infrastructure Controller（APIC）クラスタのサイズを縮小し、クラスタから削除されたCisco APICを解放するには、次のガイドラインに従います。

（注） 縮小したクラスタからCisco APICを解放し、電源オフする正しい手順を実行しないと、予期しない結果を招く可能性があります。認識されていないCisco APICをファブリックに接続されたままにしないでください。

- クラスタサイズを縮小した場合、残りCisco APICの負荷が増加します。クラスタの同期がファブリックのワークロードの要求に影響しないときに、Cisco APICサイズの縮小を予定します。
- クラスタ内の1つ以上のCisco APICのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。

- クラスタの目標サイズを新たな低い値に減らします。たとえば、既存のクラスタ サイズが 6 で、3 台のコントローラを削除する場合は、クラスタの目標サイズを 3 に減らします。
- 既存のクラスタ内でコントローラ識別子の番号が最大のものから、APICを 1 台ずつ、解放、電源オフ、接続解除し、クラスタが新規の小さい目標サイズになるまで行います。

  各コントローラを解放および削除するごとに、Cisco APIC はクラスタを同期します。

（注） クラスタから Cisco APICをデコミッションした後に、直ちに電源をオフにし、再発見を予防するためにファブリックから切断します。サービスを回復する前に、全消去を実行して工場出荷時の状態にリセットします。

切断が遅延し、デコミッションされたコントローラが再検出された場合は、次の手順に従って削除します：

1. Cisco APICの電源を切り、ファブリックから切断します。
2. [未承認コントローラ（Unauthorized Controllers）] のリストで、コントローラを拒否します。
3. GUI からコントローラを消去します。

- 既存のCisco APICが使用できなくなると、クラスタの同期が停止します。クラスタの同期を進める前に、この問題を解決します。
- コントローラの削除の際に Cisco APIC が同期すべきデータの量により、各コントローラの解放とクラスタの同期を完了するために要する時間は、コントローラごとに 10 分以上になる可能性があります。

（注） クラスタに追加の変更を行う前に、必要な解放手順全体を完了し、Cisco APIC がクラスタの同期を完了できるようにしてください。

Cisco APIC クラスタの縮小

Cisco APIC クラスタの縮小とは、正当な境界内で、クラスタ サイズ N から N -1 へサイズの不一致を軽減する動作です。縮小によってクラスタ内の残りの APIC の計算およびメモリの負荷が増大し、解放された APIC クラスタのスロットはオペレータ入力だけで使用できなくなります。

クラスタの縮小の際は、クラスタ内の最後の APIC を最初に解放し、以降逆順で連続的に行います。たとえば、APIC4 は APIC3 の前に解放し、APIC3 は APIC2 の前に解放する必要があります。

CLI を使用してスタンバイ apic 内でアクティブな APIC 経由でスイッチング

スタンバイ apic 内でアクティブな APIC 経由でスイッチするには、次の手順を使用します。

手順

ステップ 1 **replace-controller replace** *ID* 番号 バックアップ シリアル番号

スタンバイ APIC でアクティブな APIC に置き換えられます。

例：

```
apic1#replace-controller replace 2 FCH1804V27L
Do you want to replace APIC 2 with a backup? (Y/n): Y
```

ステップ 2 **replace-controller reset** *ID* 番号

アクティブなコントローラのステータスをリセットが失敗します。

例：

```
apic1# replace-controller reset 2
Do you want to reset failover status of APIC 2? (Y/n): Y
```

CLI を使用して Cold Standby ステータスを確認する

手順

APIC の **show controller** ステータスを確認するには、管理者として APIC にログインして、Cold Standbyshow controllerCold Standby コマンドを入力します。

```
apic1# show controller
Fabric Name          : vegas
Operational Size     : 3
Cluster Size         : 3
Time Difference      : 496
Fabric Security Mode : strict

 ID    Pod   Address          In-Band IPv4     In-Band IPv6               OOB IPv4
    OOB IPv6                   Version             Flags  Serial Number     Health
 ----  ----  ---------------  ---------------  -------------------------  ---------------
  -------------------------  ------------------  -----  ----------------
------------------
 1*    1     10.0.0.1         0.0.0.0          fc00::1                   172.23.142.4
    fe80::26e9:b3ff:fe91:c4e0  2.2(0.172)          crva-  FCH1748V0DF       fully-fit
```

```
 2     1     10.0.0.2         0.0.0.0          fc00::1                    172.23.142.6
    fe80::26e9:bf8f:fe91:f37c  2.2(0.172)          crva-  FCH1747V0YF       fully-fit
 3     1     10.0.0.3         0.0.0.0          fc00::1                    172.23.142.8
    fe80::4e00:82ff:fead:bc66  2.2(0.172)          crva-  FCH1725V2DK       fully-fit
 21~         10.0.0.21
                                                 -----  FCH1734V2DG

Flags - c:Commissioned | r:Registered | v:Valid Certificate | a:Approved | f/s:Failover
 fail/success
(*)Current (~)Standby
```

CLI を使用した未登録スイッチの登録

この手順を使用して、CLI を使用して **[ファブリック メンバーシップ (Fabric Membership)]** 作業ウィンドウの **[保留中ノードの登録 (Nodes Pending Registration)]** タブからスイッチを登録します。

（注） この手順は、「CLI を使用したディスカバリ前のスイッチの追加」と同じです。コマンドを実行すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在する場合、システムにより登録されます。

手順

	コマンドまたはアクション	目的
ステップ 1	[**no**] **system switch-id** *serial-number switch-id name* **pod** *id* **role leaf node-type tier-2-leaf**	スイッチを保留中の登録リストに追加します。

CLI を使用したディスカバリ前のスイッチの追加

この手順を使用して、CLI を使用して **[ファブリック メンバーシップ (Fabric Membership)]** 作業ウィンドウの **[保留中ノードの登録 (Nodes Pending Registration)]** タブにスイッチを追加します。

（注） この手順は、「CLI を使用した未登録スイッチの登録」と同じです。コマンドを実行すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

手順

[**no**] **system switch-id** *serial-number switch-id name* **pod** *id* **role leaf node-type tier-2-leaf**

スイッチを保留中の登録リストに追加します。

CLI を使用してメンテナンス モードにスイッチを移行する

CLI を使用してメンテナンス モードにスイッチを移行するには、次の手順を使用します。

（注） スイッチがメンテナンスモード中の場合、スイッチのCLI「show」コマンドでは、前面パネルポートがアップ状態であり、BGPプロトコルがアップ状態かつ実行中であることを示します。インターフェイスは実際にシャットダウンされ、BGPのその他すべての隣接関係がダウンしますが、表示されているアクティブ状態でデバッグが可能です。

手順

[**no**]**debug-switch** *node_id or node_name*

メンテナンス モードにスイッチを移行します。

CLI を使用して操作モードにスイッチを挿入する

この手順を使って、スイッチを CLI を使用している動作モードに挿入します。

手順

[**no**]**no debug-switch** *node_id or node_name*

動作モードにスイッチを挿入します。

NX-OS スタイルの CLI を使用したリモート ロケーションの設定

ACI ファブリックでは、techsupport またはコンフィギュレーション ファイルをエクスポートする 1 つ以上のリモート宛先を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **remote path** *remote-path-name* 例： `apic1(config)# remote path myFiles`	リモート パスのコンフィギュレーション モードを開始します。
ステップ 3	**user** *username* 例： `apic1(config-remote)# user admin5`	リモート サーバにログインするユーザ名を設定します。パスワードを入力するように求められます。
ステップ 4	**path** {**ftp** | **scp** | **sftp**} *host*[*:port*] [**remote-directory**] 例： `apic1(config-remote)# path sftp filehost.example.com:21 remote-directory /reports/apic`	リモート サーバへのパスとプロトコルを設定します。パスワードを入力するように求められます。

例

次に、ファイルをエクスポートするためにリモート パスを設定する例を示します。

```
apic1# configure
apic1(config)# remote path myFiles
apic1(config-remote)# user admin5
You must reset the password when modifying the path:
Password:
Retype password:
apic1(config-remote)# path sftp filehost.example.com:21 remote-directory /reports/apic
You must reset the password when modifying the path:
Password:
Retype password:
```

NX-OS CLI を使用したスイッチ インベントリの検索

このセクションでは、NX-OS CLI を使用してスイッチのモデルとシリアル番号を見つける方法について説明します。

手順

次のようにスイッチ インベントリを見つけます。

例：

```
switch# show hardware
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Documents: http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html
Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 07.56
  kickstart: version 12.1(1h) [build 12.1(1h)]
  system:    version 12.1(1h) [build 12.1(1h)]
  PE:        version 2.1(1h)
  BIOS compile time:       06/08/2016
  kickstart image file is: /bootflash/aci-n9000-dk9.12.1.1h.bin
  kickstart compile time:  10/01/2016 20:10:40 [10/01/2016 20:10:40]
  system image file is:    /bootflash/auto-s
  system compile time:     10/01/2016 20:10:40 [10/01/2016 20:10:40]


Hardware
  cisco N9K-C93180YC-EX ("supervisor")
   Intel(R) Xeon(R) CPU  @ 1.80GHz with 16400384 kB of memory.
  Processor Board ID FDO20101H1W

  Device name: ifav41-leaf204
  bootflash:    62522368 kB

Kernel uptime is 02 day(s), 21 hour(s), 42 minute(s), 31 second(s)

Last reset at 241000 usecs after Sun Oct 02 01:27:25 2016
  Reason: reset-by-installer
  System version: 12.1(1e)
  Service: Upgrade

plugin
  Core Plugin, Ethernet Plugin
--------------------------------
Switch hardware ID information
--------------------------------
```

```
Switch is booted up
Switch type is : Nexus C93180YC-EX Chassis
Model number is N9K-C93180YC-EX
H/W version is 0.2010
Part Number is 73-15298-01
Part Revision is 1
Manufacture Date is Year 20 Week 10
Serial number is FDO20101H1W
CLEI code is 73-15298-01

--------------------------------
Chassis has one slot
--------------------------------

Module1 ok
  Module type is : 48x10/25G
  1 submodules are present
  Model number is N9K-C93180YC-EX
  H/W version is 0.2110
  Part Number is 73-17776-02
  Part Revision is 11
  Manufacture Date is Year 20 Week 10
  Serial number is FDO20101H1W
  CLEI code is 73-17776-02

GEM ok
  Module type is : 6x40/100G Switch
  1 submodules are present
  Model number is N9K-C93180YC-EX
  H/W version is 0.2110
  Part Number is 73-17776-02
  Part Revision is 11
  Manufacture Date is Year 20 Week 10
  Serial number is FDO20101H1W
  CLEI code is 73-17776-02

---------------------------------------
Chassis has  2 PowerSupply Slots
---------------------------------------

PS1 shut
  Power supply type is : 54.000000W 220v AC
  Model number is NXA-PAC-650W-PE
  H/W version is 0.0
  Part Number is 341-0729-01
  Part Revision is A0
  Manufacture Date is Year 19 Week 50
  Serial number is LIT19500ZEK
  CLEI code is 341-0729-01

PS2 ok
  Power supply type is : 54.000000W 220v AC
  Model number is NXA-PAC-650W-PE
  H/W version is 0.0
  Part Number is 341-0729-01
  Part Revision is A0
  Manufacture Date is Year 19 Week 50
  Serial number is LIT19500ZEA
  CLEI code is 341-0729-01

---------------------------------------
Chassis has  4 Fans
---------------------------------------
```

```
FT1 ok

 Fan1(sys_fan1)(fan_model:NXA-FAN-30CFM-F)                                    is inserted
 but info is not available

FT2 ok

 Fan2(sys_fan2)(fan_model:NXA-FAN-30CFM-F)                                    is inserted
 but info is not available

FT3 ok

 Fan3(sys_fan3)(fan_model:NXA-FAN-30CFM-F)                                    is inserted
 but info is not available

FT4 ok

 Fan4(sys_fan4)(fan_model:NXA-FAN-30CFM-F)                                    is inserted
 but info is not available


================================================================================
```

CLI を使用した Cisco APIC クラスターの確認

Cisco Application Policy Infrastructure Controller（APIC）リリース 4.2.(1) では、Cisco APIC クラスタのステータスを段階的に確認できる **cluster_health** コマンドが導入されています。次の出力例は、非アクティブな 1 つのノード（ID 1002）を除いてすべてが問題ないシナリオを示しています。

（注） **cluster_health** コマンドを使用するには、管理者としてログインする必要があります。

手順

クラスタ ステータスを確認する方法：

```
F1-APIC1# cluster_health
Password:

Running...

Checking Wiring and UUID: OK
Checking AD Processes: Running
Checking All Apics in Commission State: OK
Checking All Apics in Active State: OK
Checking Fabric Nodes: Inactive switches: ID=1002(IP=10.1.176.66/32)
Checking Apic Fully-Fit: OK
Checking Shard Convergence: OK
Checking Leadership Degration: Optimal leader for all shards
Ping OOB IPs:
```

CLI を使用している Cisco APIC の設定

```
APIC-1: 172.31.184.12 - OK
APIC-2: 172.31.184.13 - OK
APIC-3: 172.31.184.14 - OK
Ping Infra IPs:
APIC-1: 10.1.0.1 - OK
APIC-2: 10.1.0.2 - OK
APIC-3: 10.1.0.3 - OK
Checking APIC Versions: Same (4.2(0.261a))
Checking SSL: OK

Done!
```

表 *13 : Cluster_Health* 検証手順

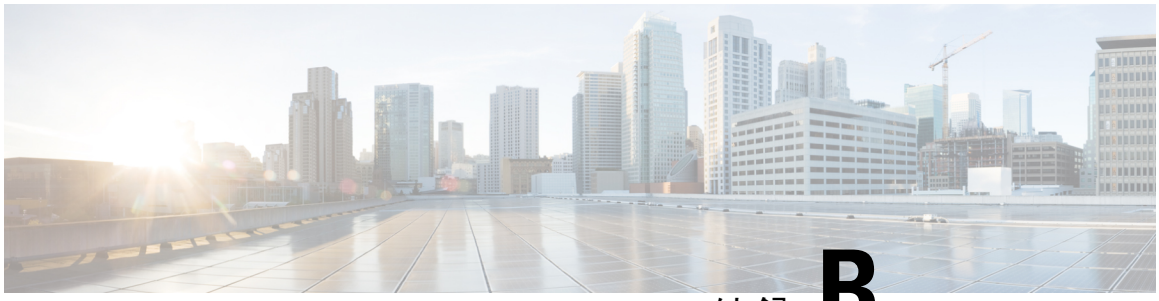
ステップ	説明
配線と UUID の確認	リーフ スイッチは、Cisco APIC の LLDP を使用して を検出することにより、Cisco APIC 相互間のインフラ接続を提供します。この手順では、LLDP検出中に検出されたリーフとCisco APIC の間の配線の問題をチェックします。 ここでの問題は、有効な情報がないため、リーフ スイッチがCisco APICにインフラ接続を提供できないことを意味します。たとえば、Cisco APIC の UUID の不一致は、新しい APIC2 の UUID が以前の既知の APIC2 とは異なることを意味します。 UUID：Universally Unique ID、または一部の出力のシャーシ ID
AD プロセスの確認	Cisco APIC クラスタリングは、Cisco APIC のそれぞれの Appliance Director プロセスによって処理されます。このステップでは、プロセスが正しく実行されているかどうかを確認します。
コミッション状態のすべての APIC のチェック	Cisco APIC クラスタリングを完了するには、すべての Cisco APIC を試運転する必要があります。
アクティブ状態のすべての APIC のチェック	Cisco APIC クラスタリングを完了するには、コミッションされたすべての Cisco APIC がアクティブである必要があります。アクティブになっていない場合は、Cisco APIC がまだ起動していない可能性があります。

CLI を使用している Cisco APIC の設定

ステップ	説明
ファブリック ノードの確認: 非アクティブ スイッチ	Cisco APIC の通信は、リーフ スイッチとスパイン スイッチによって提供されるインフラ接続を介して行われます。この手順では、非アクティブなスイッチをチェックして、スイッチがインフラ接続を提供していることを確認します。
APIC の完全フィットの確認	Cisco APIC は、インフラ ネットワークを介して相互に IP 到達可能性を確立すると、データベースを相互に同期します。同期が完了すると、すべて Cisco APIC のステータスが「Fully-Fit」になります。それ以外の場合、ステータスは「Data Layer Partially Diverged」などになります。
シャード収束の確認	Cisco APIC が完全に「Fully-Fit」でない場合、データベース シャードをチェックして、完全に同期されていないサービスを確認する必要があります。同期に問題のあるサービスがある場合は、Cisco TAC に連絡して、さらにトラブルシューティングを行ってください。
リーダーシップのデグレーションの確認	ACI では、各データベース シャードに 1 つのリーダー シャードがあり、クラスタ内の Cisco APIC それぞれに分散されます。このステップは、すべてのシャードに最適なリーダーがあるかどうかを示します。すべての Cisco APIC が稼働しているときにここで問題が発生した場合は、Cisco TAC に連絡して、さらにトラブルシューティングを行ってください。
Ping OOB IP	この手順では、クラスタリングとは別に構成されている OOB IP に ping を実行して、すべての Cisco APIC が稼働しているかどうかを確認します。
Ping インフラ IP	この手順では、それぞれの Cisco APIC 間にインフラ接続があるかどうかを確認します。Cisco APIC クラスタリングは、OOB ではなくインフラ接続を介して実行されます。
APIC バージョンを確認する	クラスタリングを完了するには、すべての Cisco APIC が同じバージョンである必要があります。

ステップ	説明
SSL の確認	Cisco APIC をアプライアンスとして購入する場合、すべての Cisco APIC に有効な SSL を組み込む必要があります。有効な SSL がないと、サーバは Cisco APIC OS を正しく動作させることができません。

CLI を使用している Cisco APIC の設定



付録 B

REST API を使用した Cisco APIC の設定

REST API を使用した APIC クラスタの拡大

クラスタは、実際のサイズを目標サイズに合わせます。目標サイズが実際のサイズよりも大きい場合、クラスタ サイズが拡大します。

手順

ステップ 1 APIC クラスタのサイズを拡大するために目標のクラスタ サイズを設定します。

例：

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=3/>
```

ステップ 2 クラスタに追加する APIC コントローラを物理的に接続します。

REST API を使用した APIC クラスタの縮小

コントローラを削除してクラスタサイズを縮小するには、次の手順を使用します。クラスタ サイズの縮小の詳細については、Cisco APIC クラスタの縮小 （92 ページ） を参照してください。

（注） Cisco APIC リリース 6.0(2) 以降、デコミッション操作を強制できるようにするために、API コマンドに2つの追加プロパティが追加されました。新しいオブジェクトプロパティは次のとおりです。

- `infraClusterPol:shrink`
  - `false`：（デフォルト）ターゲット クラスタ サイズ（`infraClusterPol:size`）が現在の運用クラスタ サイズより小さい場合、以前のリリースと同様に、削除する APIC を手動で廃止する必要があります。
  - `true`：ターゲット クラスタ サイズが現在の運用クラスタ サイズよりも小さい場合、クラスタ縮小デコミッションがトリガーされます。削除される APIC については、コントローラ ID 番号が最も大きい APIC から自動的にデコミッションされます。
- `infraWiNode:force`
  - `false`：（デフォルト）クラスタが異常な場合、またはアップグレード状態である場合には、デコミッションが適切でない可能性があるため、それ以外の場合にのみデコミッションを続行します。
  - `true`：クラスタの状態に関係なく、デコミッションを続行します。

次に、クラスタを 3 つの APIC コントローラから 1 つのコントローラに縮小する例を示します。ターゲット サイズを 1 にするには、APIC3 と APIC2 をこの順序で廃止する必要があります。

手順

ステップ 1 APIC クラスタのサイズを縮小するため、目標のクラスタ サイズを設定します。

`shrink='true'` を使用してクラスタ サイズを縮小すると、削除される APIC は自動的にデコミッションされます。それ以外の場合は、手動でデコミッションする必要があります。

例：

Cisco APIC リリース 6.0(1) 以前：

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=1 />
```

REST API を使用した Cisco APIC の設定

次の手順に示すように、削除する APIC を手動でデコミッションする必要があります。

例：

Cisco APIC リリース 6.0(2) 以降で「shrink」プロパティを使用する場合：

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=1 shrink='true' />
```

`shrink='true'` を使用すると、次の手順をスキップできます。削除する APIC は自動的にデコミッションされます。

```
POST
https://<IP address>/api/node/mo/uni/controller.xml
<infraClusterPol name='default' size=1 shrink='false' />
```

`shrink='false'` を使用する場合には、次の手順に示すように、削除する APIC を手動でデコミッションする必要があります。

ステップ 2 クラスタ縮小のための APIC1 上の APIC3 の解放

例：

Cisco APIC リリース 6.0(1) 以前：

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=3 adminSt='out-of-service'/>
```

デコミッションは、クラスターが正常な状態にある場合にのみ続行されます。

例：

Cisco APIC リリース 6.0(2) 以降で「force」プロパティを使用する場合：

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=3 adminSt='out-of-service' force='true' />
```

`force='true'` の場合、クラスタの状態に関係なくデコミッションが進行します。

ステップ 3 クラスタ縮小のための APIC1 上の APIC2 の解放

例：

Cisco APIC リリース 6.0(1) 以前：

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 adminSt='out-of-service'/>
```

デコミッションは、クラスターが正常な状態にある場合にのみ続行されます。

例：

Cisco APIC リリース 6.0(2) 以降で「force」プロパティを使用する場合：

```
POST
https://<IP address>/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 adminSt='out-of-service' force='false' />
```

`force='false'` の場合、クラスターが正常な状態にある場合にのみデコミッションが続行されます。

稼動クラスタのサイズが縮小するのは、最後のアプライアンスが解放されたときで、管理サイズを変更したときではありません。各コントローラを解放した後、そのコントローラの動作状態が未登録になり、すでにクラスタ内で稼動していないことを確認します。

（注） デコミッションされた APIC コントローラがファブリックからすぐに削除されない場合、再検出される可能性があり、問題が発生する可能性があります。その場合、コントローラを削除するために APIC クラスタのサイズ縮小 （94 ページ） の説明に従います。

APIC クラスタのサイズ縮小

Cisco Application Policy Infrastructure Controller（APIC）クラスタのサイズを縮小し、クラスタから削除されたCisco APICを解放するには、次のガイドラインに従います。

（注） 縮小したクラスタからCisco APICを解放し、電源オフする正しい手順を実行しないと、予期しない結果を招く可能性があります。認識されていないCisco APICをファブリックに接続されたままにしないでください。

- クラスタサイズを縮小した場合、残りCisco APICの負荷が増加します。クラスタの同期がファブリックのワークロードの要求に影響しないときに、Cisco APICサイズの縮小を予定します。
- クラスタ内の1つ以上のCisco APICのヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。
- クラスタの目標サイズを新たな低い値に減らします。たとえば、既存のクラスタ サイズが 6 で、3 台のコントローラを削除する場合は、クラスタの目標サイズを 3 に減らします。
- 既存のクラスタ内でコントローラ識別子の番号が最大のものから、APICを 1 台ずつ、解放、電源オフ、接続解除し、クラスタが新規の小さい目標サイズになるまで行います。

  各コントローラを解放および削除するごとに、Cisco APIC はクラスタを同期します。

（注） クラスタから Cisco APICをデコミッションした後に、直ちに電源をオフにし、再発見を予防するためにファブリックから切断します。サービスを回復する前に、全消去を実行して工場出荷時の状態にリセットします。

切断が遅延し、デコミッションされたコントローラが再検出された場合は、次の手順に従って削除します：

1. Cisco APICの電源を切り、ファブリックから切断します。
2. [未承認コントローラ（Unauthorized Controllers）]のリストで、コントローラを拒否します。
3. GUI からコントローラを消去します。

- 既存のCisco APICが使用できなくなると、クラスタの同期が停止します。クラスタの同期を進める前に、この問題を解決します。
- コントローラの削除の際に Cisco APIC が同期すべきデータの量により、各コントローラの解放とクラスタの同期を完了するために要する時間は、コントローラごとに 10 分以上になる可能性があります。

（注） クラスタに追加の変更を行う前に、必要な解放手順全体を完了し、Cisco APIC がクラスタの同期を完了できるようにしてください。

REST API を使用してアクティブ APIC とスタンバイ APIC を切り替える

REST API を使用してアクティブな APIC とスタンバイ APIC を切り替えるには、この手順を使用します。

手順

アクティブ APIC とスタンバイ APIC を切り替えます。

```
URL for POST: https://ip
address/api/node/mo/topology/pod-initiator_pod_id/node-initiator_id/av.xml
Body: <infraWiNode id=outgoing_apic_id targetMbSn=backup-serial-number/>
where initiator_id = id of an active APIC other than the APIC being replaced.
pod-initiator_pod_id = pod ID of the active APIC
backup-serial-number = serial number of standby APIC
```

例：

```
https://ip address/api/node/mo/topology/pod-1/node-1/av.xml
<infraWiNode id=2 targetMbSn=FCH1750V00Q/>
```

REST API を使用した未登録スイッチの登録

この手順を使用して、REST API を使用して **[ファブリック メンバーシップ (Fabric Membership)]** 作業ウィンドウの **[保留中ノードの登録 (Nodes Pending Registration)]** タブからスイッチを登録します。

（注） この手順は、「REST API を使用したディスカバリ前のスイッチの追加」と同じです。コードを適用すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

手順

スイッチ説明を追加します。

例：

```
POST
https://<IP address>/api/policymgr/mo/uni.xml

<!-- /api/policymgr/mo/uni.xml -->
<polUni>
<ctrlrInst>
    <fabricNodeIdentPol>
        <fabricNodeIdentP  nodeType="tier-2-leaf" podId="1" serial="XXXXXXXXX"
        name="tier-2-leaf-leaf1" nodeId="101"/>

    </fabricNodeIdentPol>
</ctrlrInst>
</polUni>
```

REST API を使用したディスカバリ前のスイッチの追加

この手順を使用して、REST API を使用して **[ファブリック メンバーシップ (Fabric Membership)]** 作業ウィンドウの **[保留中ノードの登録 (Nodes Pending Registration)]** タブにスイッチを追加します。

（注） この手順は、「REST API を使用した未登録スイッチの登録」と同じです。コードを適用すると、システムはノードが存在するかどうかを判断し、存在しない場合はそのノードを追加します。ノードが存在しない場合、システムにより登録されます。

手順

スイッチ説明を追加します。

例：

```
POST
https://<IP address>/api/policymgr/mo/uni.xml

<!-- /api/policymgr/mo/uni.xml -->
<polUni>
<ctrlrInst>
    <fabricNodeIdentPol>
        <fabricNodeIdentP  nodeType="tier-2-leaf" podId="1" serial="XXXXXXXXX"
        name="tier-2-leaf1" nodeId="101"/>

    </fabricNodeIdentPol>
</ctrlrInst>
</polUni>
```

REST API を使用して、メンテナンス モードにスイッチを削除

REST API を使用して、メンテナンス モードにスイッチを削除するのにには、次の手順を使用します。

手順

メンテナンス モードにスイッチを削除します。

例：

```
POST
https://<IP address>/api/node/mo/uni/fabric/outofsvc.xml

<fabricOOServicePol
    descr=""
    dn=""
    name="default"
    nameAlias=""
```

```
    ownerKey=""
    ownerTag="">
  <fabricRsDecommissionNode
      debug="yes"
      dn=""
      removeFromController="no"
      tDn="topology/pod-1/node-102"/>
</fabricOOServicePol>
```

REST API を使用した操作モードへのスイッチの挿入

REST API を使用して操作モードにスイッチを挿入するには、次の手順を使用します。

手順

操作モードにスイッチを挿入します。

例：

```
POST
https://<IP address>/api/node/mo/uni/fabric/outofsvc.xml

<fabricOOServicePol
    descr=""
    dn=""
    name="default"
    nameAlias=""
    ownerKey=""
    ownerTag="">
  <fabricRsDecommissionNode
      debug="yes"
      dn=""
      removeFromController="no"
      tDn="topology/pod-1/node-102"
      status="deleted"/>
</fabricOOServicePol>
```

REST API を使用したリモート ロケーションの設定

この手順では、REST API を使用してリモート ロケーションを作成する方法について説明します。

```
<fileRemotePath name="local" host="host or ip" protocol="ftp|scp|sftp" remotePath="path
 to folder" userName="uname" userPasswd="pwd" />
```

REST API を使用したオンデマンド テクニカル サポート ファイルの送信

手順

ステップ 1 REST API を使用して次の例のような XML を POST 送信し、テクニカル サポート ファイルのリモート宛先を設定します。

例：

```
<fileRemotePath userName="" remotePort="22" remotePath="" protocol="sftp" name="ToSupport"
 host="192.168.200.2"
dn="uni/fabric/path-ToSupport" descr="">

<fileRsARemoteHostToEpg tDn="uni/tn-mgmt/mgmtp-default/oob-default"/>

</fileRemotePath>
```

ステップ 2 REST API を使用して次のような XML を POST 送信し、オンデマンドのテクニカル サポート ファイルを生成します。

例：

```
<dbgexpTechSupOnD upgradeLogs="no" startTime="unspecified" name="Tech_Support_9-20-16"
  exportToController="no" endTime="unspecified" dn="uni/fabric/tsod-Tech_Support_9-20-16"
 descr=""
  compression="gzip" category="forwarding" adminSt="untriggered">
    <dbgexpRsExportDest tDn="uni/fabric/path-ToSupport"/>
    <dbgexpRsTsSrc tDn="topology/pod-1/node-102/sys"/>
    <dbgexpRsTsSrc tDn="topology/pod-1/node-103/sys"/>
    <dbgexpRsTsSrc tDn="topology/pod-1/node-101/sys"/>
    <dbgexpRsData tDn="uni/fabric/tscont"/>
</dbgexpTechSupOnD>
<fabricFuncP>
    <fabricCtrlrPGrp name="default">
        <fabricRsApplTechSupOnDemand tnDbgexpTechSupOnDName=" Tech_Support_9-20-16"/>
    </fabricCtrlrPGrp>
</fabricFuncP>
```

REST API を使用したスイッチ インベントリの検索

このセクションでは、REST API を使用してスイッチのモデルとシリアル番号を見つける方法について説明します

REST API を使用した Cisco APIC の設定

手順

次のようにスイッチ インベントリを見つけます。

例：

```
GET
https://192.0.20.123/api/node/mo/topology/pod-1.json?query-target=children&target-subtree-class=fabricNode
```

次の応答が返されます：

```
response:
  {
     "totalCount":"8",
     "imdata":
     [{
         "fabricNode":{
           "attributes":{
              "adSt":"on",
              "childAction":"",
              "delayedHeartbeat":"no",
              "dn":"topology/pod-1/node-103",
              "fabricSt":"active",
              "id":"103",
              "lcOwn":"local",
              "modTs":"2016-10-08T14:49:35.665+00:00",
              "model":"N9K-C9396PX",
              "monPolDn":"uni/fabric/monfab-default",
              "name":"leaf3",
              "nameAlias":"",
              "role":"leaf",
              "serial":"TEP-1-103",
              "status":"","uid":"0",
              "vendor":"Cisco Systems, Inc",
              "version":""}
            }
     },{
         "fabricNode":{
           "attributes":{
             "adSt":"on",
             "childAction":"",
             "delayedHeartbeat":"no",
             "dn":"topology/pod-1/node-105",
             "fabricSt":"active",
             "id":"105",
             "lcOwn":"local",
             "modTs":"2016-10-08T14:47:52.011+00:00",
             "model":"N9K-C9508",
             "monPolDn":"uni/fabric/monfab-default",
             "name":"spine2",
             "nameAlias":"",
             "role":"spine",
             "serial":"TEP-1-105","status":"",
             "uid":"0",
             "vendor":"Cisco Systems, Inc",
             "version":""
           ...
       [TRUNCATED]
```

REST API を使用した Cisco APIC の設定

```
            ...
    }
```

REST API を使用した Cisco APIC の設定

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