Cisco APIC スタートアップ ガイド、リリース 4.0(1)

初版：2018 年 10 月 24 日

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

Trademarks

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

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

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

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

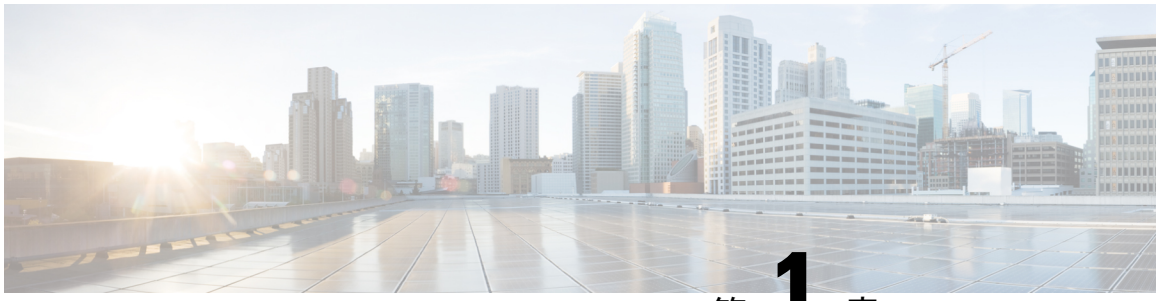
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

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

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

Trademarks

目 次



第 1 章

初期設定

この章は、次の内容で構成されています。

新機能および変更された機能に関する情報

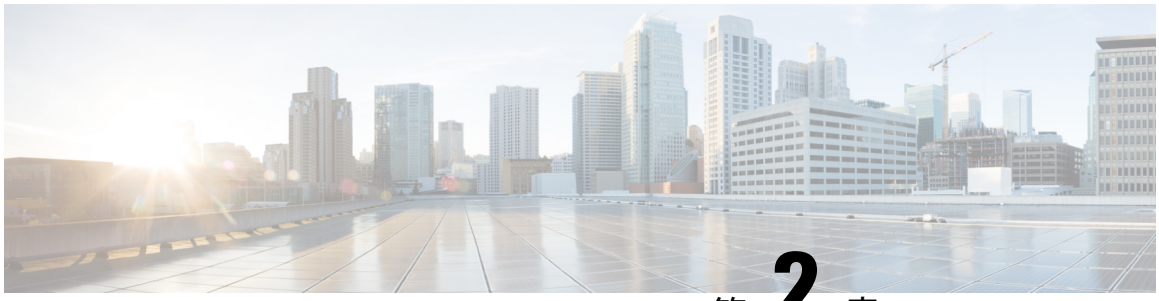
次の表に、本リリースに関するこのガイドでの重要な変更点の概要を示します。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *6.0(2)* の新機能および変更された機能に関する情報

特長	説明	参照先
APIC クラスタを呼び出すための新しい GUI	Cisco APIC リリース 6.0(2) 以降では、APIC クラスタを呼び出すための GUI 画面が追加され、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ました。**APIC クラスタの呼び出し** GUI は、仮想および物理 APIC プラットフォームをサポートします。アウトオブバンドと CIMC 間の接続は必須になりました。	Bringing up the Cisco APIC Cluster Using the GUI （16 ページ）

表 *2 : Cisco APIC* リリース *6.0(1)* の新機能および変更された機能に関する情報

特長	説明	参照先
Cisco Nexus 9000 スイッチの安全な消去	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。	Cisco Nexus 9000 スイッチの安全な消去について （71 ページ）



第 2 章

初期設定

この章は、次の内容で構成されています。

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 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 基本設定ガイド、リリース 5.2.x
Cisco APIC レイヤ 2 ネットワーク設定ガイド、リリース 5.2(x)

ドキュメント
Cisco APIC レイヤ 3 ネットワーク設定ガイド、リリース 5.2(x)
Cisco ACI 仮想化ガイド、リリース 5.2(x)
Cisco アプリケーション セントリック インフラストラクチャの基本、リリース 5.2(x)
Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド、リリース 5.2 (x)

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。

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、Bringing up the Cisco APIC Cluster Using the GUI （16 ページ） の手順を参照してください。

表 *3*: 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

名前	説明	デフォルト値
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
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。

名前	説明	デフォルト値
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。	
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。	—

名前	説明	デフォルト値
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]
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 *4:* 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

名前	説明	デフォルト値
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
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。

名前	説明	デフォルト値
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、「Bringing up the Cisco APIC Cluster Using the GUI （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]:
```

Bringing up the Cisco APIC Cluster Using the GUI

Beginning with Cisco APIC release 6.0(2), the initial cluster set up and bootstrapping procedure has been simplified with the addition of GUI screen(s) for cluster bring up. The **APIC Cluster Bringup** GUI supports virtual and physical APIC platforms. The virtual APICs (deployed using ESXi or AWS), and physical APICs can be connected to the ACI fabric directly to the leaf switches or remotely attached through a Layer 3 network. The GUI supports both the scenarios. A major advantage of using the **APIC Cluster Bringup** GUI is that, you do not need to enter the parameters for every APIC in a cluster. One APIC can relay the information to the other APICs of the cluster.

Alternatively, you can perform the initial setup and cluster bringup using the REST APIs. See the *Getting Started* section of the APIC REST API Configuration Procedures guide.

Before you begin

Prerequisites:

- For virtual APIC on ESXi, ensure to complete the deployment of the Cisco APIC VM using the OVF template on the VMware vCenter GUI. For a three-node cluster, configure three VMs with management IP, gateway and admin passwords. The number of VMs is dependent on the size of the Cisco APIC cluster.
- For virtual APIC on AWS, ensure to complete the deployment of the Cisco APIC VM using the cloud formation template (CFT) on the AWS GUI. AWS allocates IP addresses dynamically from the OOB/infra/inband subnets accordingly, to correspond with the network adapters of the virtual APIC's EC2 instance.
- For virtual APICs (deployed using AWS/ ESXi), ensure that the admin password(s) are the same for all the Cisco APICs in a cluster.
- For the physical APIC cluster, configure the Out of Band (OOB) address for APIC 1. Ensure that the CIMC addresses of APICs 2 to *N* (where N is the cluster size) are reachable via the OOB address of APIC 1.
- Connectivity between out-of-band and the CIMC is mandatory.

Limitations:

- No support for IPv6 addresses on virtual APICs deployed using AWS.
- For login and cluster operations, non-default HTTPS port (default is 443) is not supported for remotely-attached Cisco APICs (physical and virtual).

ステップ 1 Log in to the APIC 1 using *https://APIC1-IP*.

If you have completed the deployment of virtual APICs using ESXi (OVF template) or remote AWS (CFT), then, you output on the VM console similar to the following example:

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

The IP address to access the bootstrapping GUI (**APIC Cluster Bringup**) is explicitly indicated, as shown in the example. You can proceed to step 2.

After deploying Cisco APIC on AWS, keep the OOBMgmt IP address handy to access the Cluster Bringup GUI. You can get the OOBMgmt IP address from the **Stacks Outputs** tab on the AWS GUI.

For physical APICs, log in to the APIC 1 KVM console using the CIMC; you will see a screen as shown below:

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

If you see only a black screen on the KVM, connect to the CIMC using SSH and use serial over LAN (SoL) ("connect host") to connect to the console.

Choose either of these options (given below) before proceeding to step 2:

- On APIC 1, click **Enter** to provide the information interactively. The IP address to access the bootstrapping GUI (**APIC Cluster Bringup**) is explicitly indicated.

  ```
  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
```

- Provide information about the cluster as a **JSON** string. Before you enter the JSON string, change to the text mode and ensure you enter the string as a single line. The following example has been expanded with line feeds, spaces, and indentations for readability, but does not represent how you should enter the string.

```
{
    "cluster": {
        "fabricName": "<fabric_name>",
        "fabricId": 1,
        "clusterSize": 3,
        "layer3": false,
        "gipoPool": "225.0.0.0/15",
        "adminPassword": "<password>",
        "infraVlan": 2
    },
    "nodes": [{
        "nodeName": "<node_name>",
        "controllerType": "physical",
        "serialNumber": "<serial_number>",
        "nodeId": 1,
        "podId": 1,
        "cimc": {
            "address4": "<ip_address>",
            "username": "admin",
            "password": "<password>"
        },
        "oobNetwork": {
            "address4": "<ip_address>",
            "gateway4": "<gateway_address>",
            "enableIPv4": true,
            "enableIPv6": false,
            "address6": "",
            "gateway6": ""
        }
    }, {
        "nodeName": "<node_name>",
        "controllerType": "physical",
        "serialNumber": "<serial_number>",
        "nodeId": 2,
        "podId": 1,
        "cimc": {
            "address4": "172.23.140.175",
            "username": "admin",
            "password": "<password>"
        },
        "oobNetwork": {
            "address4": "<ip_address>",
            "gateway4": "<gateway_address>",
            "enableIPv4": true,
            "enableIPv6": false,
            "address6": "",
            "gateway6": ""
        }
    }, {
        "nodeName": "<node_name>",
        "controllerType": "physical",
        "serialNumber": "<serial_number>",
```

```
            "nodeId": 3,
            "podId": 1,
            "cimc": {
                "address4": "<ip_address>",
                "username": "admin",
                "password": "<password>"
            },
            "oobNetwork": {
                "address4": "<ip_address>",
                "gateway4": "<gateway_address>",
                "enableIPv4": true,
                "enableIPv6": false,
                "address6": "",
                "gateway6": ""
            }
        }],
        "pods": [{
            "podId": 1,
            "tepPool": "10.0.0.0/16"
        }]
    }
```

The IP addresses displayed above are samples. The IP address(es), based on your deployment, may vary.

ステップ 2 Using the OOB address, log in to the **APIC Cluster Bringup** GUI. The GUI screen has four parts. Enter the details in the following screens:

- Connection Type
- Cluster Details
- Controller Registration
- Summary

Each of the above screens are discussed in detail in the subsequent steps. The screens are marked as steps with sequential numbers, 1,2,3,4; after you have entered and saved the required details in each of these screens, the number is replaced with a tick-mark.

ステップ 3 The first step is entering the **Connection Type** information. In the **Connection Type** screen, select the type of connection between the APIC and the fabric.

The options are:

- Directly connected to leaf switches (ACI fabric)
- Remotely attached through an L3 network

If it is virtual APIC using AWS, the system detects that the APIC is remotely-attached through a Layer 3 network and proceeds directly to the **Cluster Details** screen.

ステップ 4 Click **Next**.

ステップ 5 The second step is entering the **Cluster Details**. Enter the fabric-level details in the **Cluster Details** screen.

- Fabric Name—Enter a name for the fabric.
- Cluster Size—The default cluster size displayed is "3", which is the recommended minimum cluster size. You can modify this value, based on your cluster size. The supported values are 1,3,4,5,6,7,8,9.

- GiPo Pool—Enter the IP address used for fabric multicast. The default address is 225.0.0.0/15. Valid range is, 225.0.0.0/15 to 231.254.0.0/15, prefixlen must be 15 (128k IPs).

  You can not change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.

- Pod ID—(applicable only for directly connected APICs (virtual and physical)) the pod ID is displayed. If this is your first APIC, "1" is auto-populated. Subsequent APICs of the cluster can be associated with any pod number.

  For a remotely-attached APICs, pod is 0.

- TEP Pool—(applicable only for directly connected APICs (ESXi virtual APIC and physical APIC)) enter the subnet of addresses used for internal fabric communication. The size of the subnet used will impact the scale of your pod.

  You can not change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.

- Infrastructure VLAN—Enter the VLAN ID for fabric connectivity (infra VLAN). This VLAN ID should be allocated solely to ACI, and not used by any other legacy device(s) in your network. Default value is 3914. Supported range is from 0 to 4093.

  You can not change this value after you have completed the configuration. Having to modify this value requires a wipe of the fabric.

- Enable IPv6 on APICs (not applicable for virtual APIC on AWS)—select this check-box if you want to enable IPv6 addresses for out of band management.

ステップ 6 Click **Next**.

ステップ 7 The third step is entering the **Controller Registration** details. Click **Add Controller** to add the first APIC (of the cluster). Enter the following details:

- Controller Type—The bootstrapping procedure auto-detects the deployment for which the configuration is being carried out. Based on that, either **Virtual** or **Physical** is selected. The options displayed for the virtual and physical controller types are discussed in substeps (a) and (b), respectively. Follow either of these substeps based on the controller type.

a) When the Controller Type is **Virtual**:

- Virtual Instance—The management IP used to access the APIC cluster bringup GUI. Only for the first APIC, this IP address is auto-populated. For the nodes that you subsequently add to the cluster, you will need to enter the management IP address and click **Validate**.

  The management IP addresses are defined during the deployment of the VMs using ESXi/AWS. As mentioned in the prerequisites, keep all the required IP addresses handy while bringing up the cluster.

- General pane
  - Name—User-defined name for the controller.
  - Controller ID—The ID is auto-populated. If this is the first APIC of the cluster, the ID is "1". If you are adding the second controller of the cluster, "2" is auto-populated (and so on).
  - Pod ID—(Applicable only for *directly connected* virtual APIC on ESXi) The pod ID is auto-populated for APIC 1 of the cluster. For subsequent controllers of the cluster, enter a value. Range is from 1 to 128.
  - Serial Number—The serial number of the VM is auto-populated.

- Out of Band Network pane
  - IPv4 Address—The IP address is displayed (as defined during the deployment).
  - IPv4 Gateway—The IP address is displayed (as defined during the deployment).

  If you have enabled IPv6 addresses for OOB management earlier (Step 5), enter the IPv6 address and gateway.
- Infra L3 Network pane (this pane is displayed only if the **Connection Type** earlier selected is- *Remotely attached through an L3 network*.
  - IPv4 Address—Enter the infra network address.
  - IPv4 Gateway—Enter the IP address of the gateway.
  - VLAN—(Applicable only for *remotely attached* virtual APIC- ESXi) Enter the interface VLAN ID to be used.

  The Infra L3 Network pane is not displayed when you deploy the virtual APIC using AWS.

After you have entered and saved the first APIC details, click **Add Controller** on the **Controller Registration** screen to add another APIC to the cluster.

b) When the Controller Type is **Physical**:

- CIMC Details pane
  - IP Address—The CIMC IP address. Only for the first Cisco APIC, this IP address is auto-populated. When you add more controllers to the cluster, you need to enter the CIMC IP addresses.
  - Username—The username to access the CIMC. The username is auto-populated (for the first controller and subsequent controllers).
  - Password—Enter the password to access CIMC. For the first controller, the password is auto-populated. For the subsequent controllers, enter the password.
  - Click **Validate**. *Validation success* is displayed on successful authentication.

    If the CIMC is unreachable from the Cisco APIC out of band management IP address due to the CIMC NIC mode settings, change the NIC mode or enter JSON strings to perform the bootstrap.
- General pane
  - Name—Enter a name for the controller.
  - Controller ID—If it is the first controller of the cluster, "1" is auto-populated. If it is the second controller, "2" is auto-populated, and so on (increasing order).
  - Pod ID—(applicable only for a directly-connected APIC) the pod ID is auto-populated for APIC 1 of the cluster. For subsequent controllers of the cluster, enter a value. Range is from 1 to 128.
  - Serial Number—The serial number is auto-populated (for APICs 1 to N, where N is the cluster size) after CIMC validation.

    APIC 1 verifies the reachability of the CIMC IP addreses and also captures the serial number of the new APICs.
- Out of Band Network pane

- IPv4 Address—For APIC 1, the address is auto-populated. For subsequent APICs, enter the IP address (as defined during the deployment).
- IPv4 Gateway—For APIC 1, the gateway address is auto-populated. For subsequent APICs, enter the IP address (as defined during the deployment).

If you have enabled IPv6 addresses for OOB management earlier (Step 5), enter the IPv6 address and gateway.

- Infra L3 Network pane (this pane is displayed only if the **Connection Type** earlier selected is remotely attached through a Layer 3 network).
  - IPv4 Address—Enter the infra network IP address.
  - IPv4 Gateway—Enter the infra network IP address of the gateway.
  - VLAN—Enter a VLAN ID.

On the **Controller Registration** screen, after you have entered and saved the first APIC details, click **Add Controller** to add another APIC to the cluster.

(Optional, applicable only for virtual APICs) On the **Controller Registration** screen, select the **Import existing security certificates** check-box to import existing security certificates for fabric recovery in virtual APICs. After selecting the check-box, enter the required details in the following fields:

- The **Remote Server IP Address** which contains the configuration file.
- The **Remote Path** which contains the configuration file.
- The configuration **File Name**.
- The **AES Encryption Passphrase** which was earlier used while backing up the configuration. The backup configuration file is linked to this key (passphrase).
- Select the **Protocol**. The options are— FTP, SFTP, SCP.
- **Remote Port**
- (applicable only for SFTP and SCP **Protocols**) Select the **Authentication Type**. The options are— Use Password, Use SSH Private Key Files.
- The **Username** to access the remote server.
- The **Password** to authenticate access to the remote server.
- (applicable only for Use SSH Private Key Files **Authentication Type**) Enter the **SSH Key Contents** here.
- (applicable only for Use SSH Private Key Files **Authentication Type**) Specify the **SSH Key Passphrase** used for encrypting the private key.

  For details about the Import/Export procedure, see the Cisco ACI Configuration Files: Import and Export document.

The **Import existing security certificates** is applicable only for virtual APICs (deployed using AWS/ ESXi). Physical APICs have in-built certificates. However, in case of virtual APICs, when you are restoring using backup configuration to recover the fabric, the existing security certificates can be re-used.

ステップ 8 Click **Next**.

The **Next** button is disabled until all the controllers for a cluster are added. This is defined by the value you have entered for **Cluster Size** in the **Cluster Details** screen.

You can use the **Back** button to navigate to an earlier screen. After adding an APIC, click **Edit Details** to edit the information for an APIC. Except the first APIC, you can delete the other controllers, if required, by clicking the delete icon.

ステップ 9 In the **Summary** screen, review the updates, and click **Deploy**.

ステップ 10 The **Cluster Status** page is displayed which shows the current status of the cluster formation. Wait for a few minutes after which you will be automatically redirected to the standard Cisco APIC GUI.

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

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 （5 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

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

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

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。

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#
```

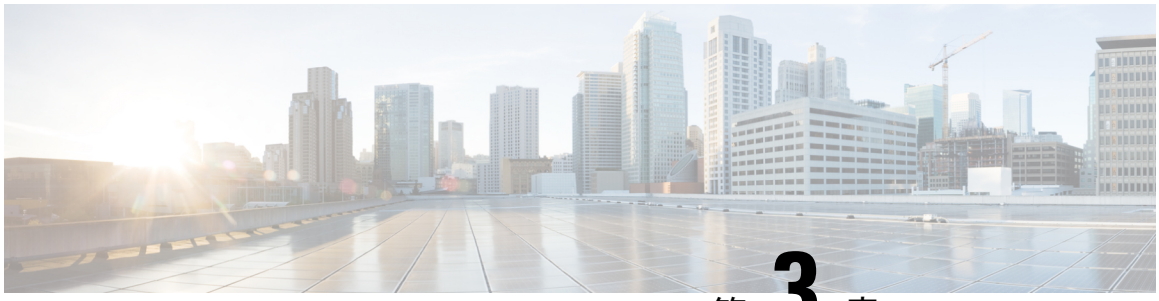
次のタスク

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

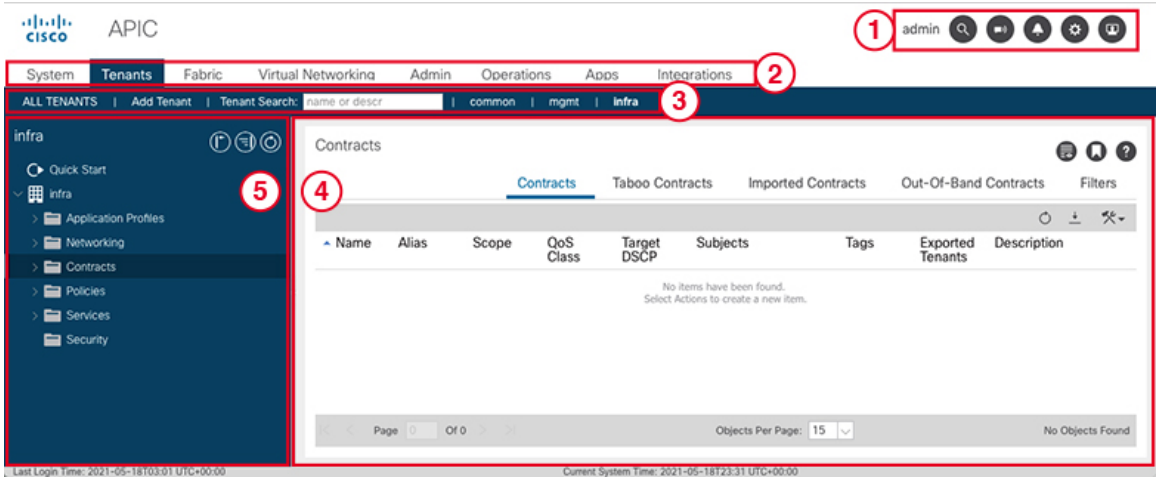
APIC GUI の概要

この章は、次の内容で構成されています。

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 （30 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 （30 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 （30 ページ）
4. 作業ウィンドウ: [Work] ペイン （39 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 （38 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 （43 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 （35 ページ）
	Multi-Site Manager の起動 （35 ページ）
	フィードバック （35 ページ）
	アラート （35 ページ）
	ツール （36 ページ）
	ヘルプ （36 ページ）
	マイ プロファイルの管理 （37 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。

[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 （43 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まます。
  - **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 （41 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 （41 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 （41 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。

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。

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 [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。

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。

名前	説明
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。
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 *5 : APIC GUI* に頻繁に表示されるアイコン

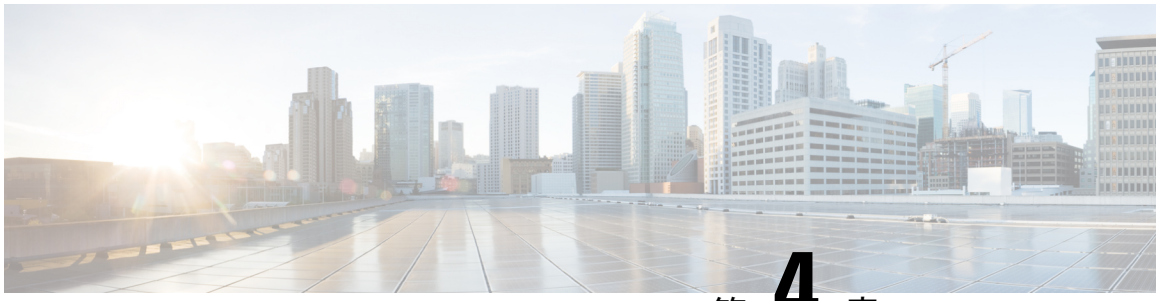
アイコン	説明
	検索 （35 ページ）
	アラート （35 ページ）
	マイ プロファイルの管理 （37 ページ）
	ツール （36 ページ）
	このページをブックマーク
	現在のメニュー ページに関連したコンセプトの情報を表示
	クイック スタート
	クイック スタートのビデオを再生
	クイック スタートの手順を表示
	関連するセクションへのリンク
	トポロジ
	ポッド

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 *6 : 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。



第 4 章

ファブリックの初期化とスイッチの検出

この章は、次の内容で構成されています。

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。

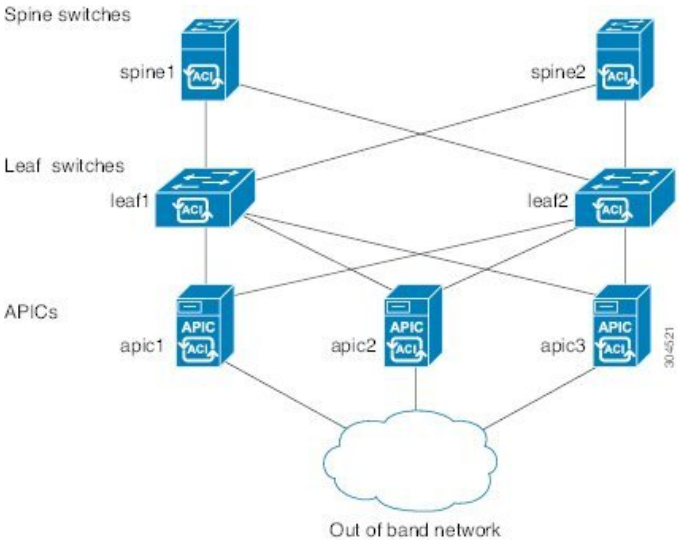
ファブリック トポロジ (例)

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 *9:* 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)

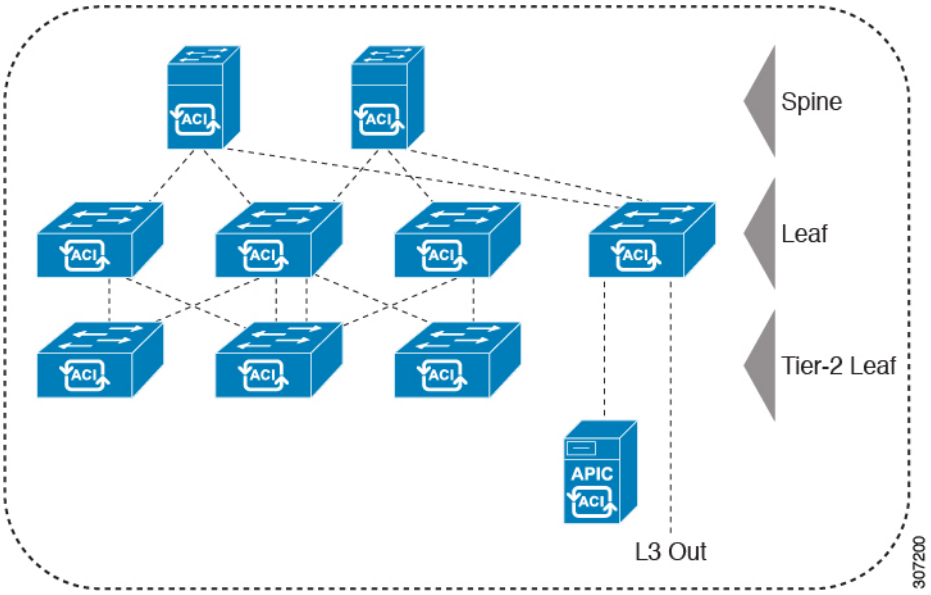
3 階層コア集約アクセス アーキテクチャは、データ センター ネットワーク トポロジで共通です。Cisco APIC リリース 4.1(1) 時点で、コア集約アクセス アーキテクチャに対応するマルチ階層 ACI ファブリック トポロジを作成するため、ラックスペースや配線などコストが高いコンポーネントのアップグレードの必要性を軽減できます。階層 2 リーフ レイヤーを追加することで、このトポロジが可能になります。階層 2 リーフ レイヤーは、ダウンリンク ポート上のホストまたはサーバへの接続、およびアップリンク ポート上のリーフ レイヤー (集約) への接続をサポートします。

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 *10* : 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 7: 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。

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

（注） 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、http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/products-installation-guides-list.htmlを参照してください。

スイッチが APIC で登録されると、そのスイッチは 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。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（ACIファブリック）を使用すると、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。

（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。

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。
- 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

次の表に、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 *8:* 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-C9364C-GX	リーフ	5.1(3)
N9K-C9316D-GX	スパイン	5.1(4)

[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指定します。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。

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。

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。
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。

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 （56 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

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

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。

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。

- **グレースフル挿入と削除（GIR）**：ユーザー トラフィックからスイッチを分離するために使用される操作。
- **メンテナンス モード**：デバッグ目的でユーザー トラフィックからスイッチを分離するために使用されます。**ファブリック**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。したがって、この状態にあるスイッチのファームウェア アップグレードを実行しようとすると、障害が発生したり、不完全なステータスで無限にスタックしたりする可能性があるため、この状態のスイッチに対するファームウェア アップグレードの実行はサポートされていません。

メンテナンス モードでは、最小限のサービスの中断でネットワークからのスイッチを分離できます。メンテナンス モードでトラフィックに影響を与えることなくリアルタイムのデバッグを実行することができます。

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

- アップグレードまたはダウン グレード メンテナンス モードでスイッチがサポートされていません。
- 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。

- 複数のポッドの **再配布されたルートのメトリックを IS-IS** 63 未満に設定する必要があります。設定を **再配布されたルートのメトリックを IS-IS** 、選択 **ファブリック** > **ファブリック ポリシー** > **ポッド ポリシー** > **IS-IS ポリシー** 。
- 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。

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。

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。

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。

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。

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。

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。

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。

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。

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]
```

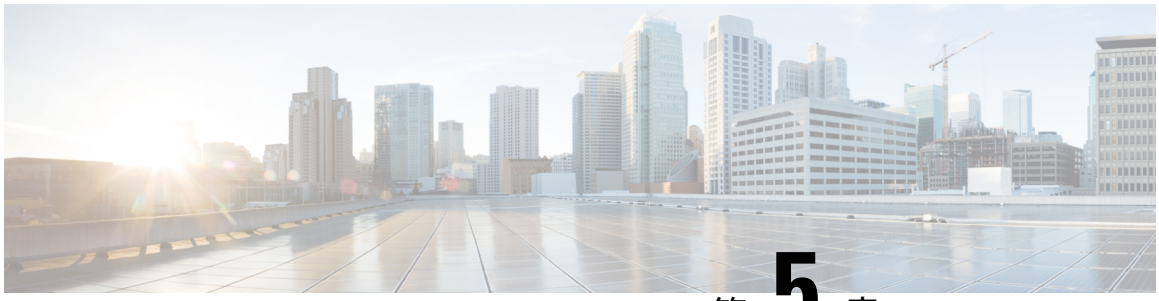
- `preserve-image`：スイッチのブートフラッシュに NX-OS イメージを保持するには、このフラグを指定します。このフラグを指定しなかった場合、NX-OS イメージも消去され、スイッチはローダープロンプトで起動します。
- `module` *`module_number`*：モジュラ スイッチ ラインカードおよびファブリック モジュールの場合、安全な消去を実行するモジュールの番号を指定する必要があります。

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 クラスタの概要

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 を追加のスタンバイ Cisco APIC とともに使用することを推奨します。ほとんどの場合、3、5、または 7 の Cisco APIC のクラスタ サイズにすることをお勧めします。80 ~ 200 のリーフ スイッチの 2 つのサイトのマルチポッド ファブリックには 4 つの Cisco APIC を推奨します。
- 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。

- Cisco APIC クラスタが 2 つ以上のグループに分割されると、ノードの ID が変更され、その変更はすべての Cisco APIC で同期されません。これにより、Cisco APIC との間のノード ID で不整合が発生する可能性があります。また、影響を受けるリーフ ノードも Cisco APIC GUI のインベントリに表示されないことがあります。Cisco APIC クラスタを分割すると、Cisco APIC からの影響を受けるリーフ ノードの使用停止し、ここでもに登録するため、ノード Id での矛盾が解決されると、クラスタ内の APIC のヘルス ステータスが完全に適合状態ではします。
- 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。
- 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 （83 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 （83 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 （5 ページ） を参照してください。

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。

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。

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。

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。

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。

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。

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。

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。

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：

- 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。

始める前に

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 **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **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、 **アクティブ コントローラ** の要約表は、アクティブ コントローラことを示します **十分に適合** 続行する前にします。

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 **作業**] ペインで、をクリックして **アクション** > **交換** 。
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。

スイッチ オーバー アクティブ APIC スタンバイ APIC とは、システムのアクティブとして登録するの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 を使用してアクティブな 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 のアクティブ 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（新しいアクティブ）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 （88 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）Cisco APIC 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）Cisco APIC の静的ノード管理アドレス構成を読み取ります。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。