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 （14 ページ） の手順を参照してください。

表 *1*: 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 *2:* 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 （14 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 （3 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。

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。