初期設定

この章で説明する内容は、次のとおりです。

次の手順については、以下を参照してください

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

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

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

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

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

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

Cisco APIC での設定のための簡略化されたアプローチ

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

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

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

BIOS のデフォルト パスワードの変更

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

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

デフォルトの BIOS パスワードを変更するには、次のタスクを実行します。

手順

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

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

（注）
デフォルトは、「password」です。

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

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

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

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

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

ステップ 7 **[Save & Exit]** タブを選択します。

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

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

APIC について

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

Cisco APIC のセットアップ

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

初期接続

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

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

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

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

（注） これらの方法を同時に複数使用することはできません。

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

工場出荷時のデフォルトの接続設定は次のとおりです。

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

シリアル アクセスに関するその他の注意事項を次に示します。

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

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

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

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

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

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

Cisco APIC の初期設定

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

特記事項

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

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

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

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

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

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

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

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

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

  この場合は、次のいずれかの方法を使用して問題を解決します。

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

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

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

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

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

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

Cold Standby について (Cisco APIC クラスタ用)

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

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

アクティブ APIC とスタンバイ APIC のセットアップ

Cisco Application Policy Infrastructure Controller（APIC）リリース 6.0(2) 以降では、初期設定とクラスタの呼び出し GUI を使用します詳細については、GUI を使用した Cisco APIC クラスタの呼び出し （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
コントローラ ID	アクティブな Cisco APIC インスタンスに対する一意の ID 番号です。	有効な範囲は 1 ～ 132 です。
スタンドアロン APIC クラスタ	クラスタはファブリックに直接接続されていませんが、レイヤ3ポッド間ネットワーク（IPN）によって接続されています。Cisco APICこの機能は、Cisco APIC リリース 5.2（1）以降でのみ使用できます。	いいえ 追加の設定手順については、ナレッジベースの記事 「*Deploying APIC Cluster Connectivity to the Fabric Over a Layer 3 Network*」 を参照してください。
コントローラ名	アクティブなコントローラの名前	apic1

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

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

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

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

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

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

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

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

例

次は、コンソールに表示される初期設定ダイアログの出力例です。

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

Cisco APIC リリース 6.0(2) 以降では、出力例の質問は含まれていません。Cisco APIC クラスタをブートストラップして起動するには、GUI を使用します。詳細については、「GUI を使用した Cisco APIC クラスタの呼び出し （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]:
```

GUI を使用した Cisco APIC クラスタの呼び出し

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

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

始める前に

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

制限事項

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

手順

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

a) 仮想 APICの場合：

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

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

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

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

b) 物理 APIC：

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

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

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

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

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

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

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

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

（注）
ワークフローの選択は、リリース 6.1（3）以降からのみです。

GUI 画面には 4 つの部分があります。以下の画面の詳細を入力します。

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

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

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

次のオプションがあります。

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

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

ステップ 5 [次へ（Next）] をクリックします。

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

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

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

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

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

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

ステップ 7 [次へ（Next）] をクリックします。

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

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

a) コントローラタイプが **仮想（Virtual）** の場合：

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

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

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

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

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

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

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

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

b) コントローラタイプが **[物理（Physical）]** の場合：

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

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

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

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

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

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

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

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

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

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

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

- **SSH 秘密キー ファイルの使用**

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

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

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

ステップ 9 **[次へ (Next)]** をクリックします。

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

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

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

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

APIC の IPv6 管理アドレスのプロビジョニング

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

```
Cluster configuration …

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

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

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

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

  Reenter the password for admin:
```

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

GUI へのアクセス

手順

ステップ 1 サポートされているブラウザの 1 つを開きます。

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

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

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

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

[Show Certificate] をクリックします。

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

これらの手順に従わないと、WebSockets は接続できません。

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

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

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

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

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

これは、https と http の両方を使用して Cisco APIC にログインするときに発生する既知の問題が原因です。この問題と回避策の詳細については、Cisco APIC のセットアップ （4 ページ）の「重要事項」を参照してください。

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

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

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

次のタスク

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

REST API へのアクセス

手順

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

初期設定時に設定したアウトオブバンド管理 IP アドレスを使用します。

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

NX-OS スタイル CLI へのアクセス

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

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

ガイドラインと、APIC NX-OS スタイル CLI の制限事項

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

端末から NX-OS スタイル CLI へのアクセス

手順

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

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

ステップ 2 プロンプトが表示されたら、管理者パスワードを入力します。

次のタスク

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

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

GUI から NX-OS スタイル CLI へのアクセス

手順

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

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

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

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

次のタスク

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

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

オブジェクト モデル CLI へのアクセス

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

手順

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

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

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

現在 APIC 用の NX-OS スタイル CLI です。

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

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

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

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

次のタスク

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

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

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

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。