初期設定

この章の内容は、次のとおりです。

Cisco APIC のドキュメンテーション ロードマップ

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。Cisco APIC のすべてのドキュメントは、APIC ドキュメント ランディング ページから入手できます。

マニュアル
『*Application Centric Infrastructure Fabric Hardware Installation Guide*』
『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』
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
Cisco APIC Layer 3 ネットワーキング設定ガイド
『*Cisco ACI Virtualization Guide*』
『*Cisco Application Centric Infrastructure Fundamentals*』

マニュアル
『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』

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

APIC コントローラには、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。

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。

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。

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

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 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 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 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。
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 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 [1]	仮想スイッチを含む APIC/スイッチ間の通信用のインフラストラクチャ VLAN （注） 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。

名前	説明	デフォルト値
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 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]
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 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 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 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 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APIC/スイッチ間の通信用のインフラストラクチャ VLAN （注） 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 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

名前	説明	デフォルト値
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例です。

```
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]: sec-ifc5
  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): 3967
  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]: 172.23.142.29/21
  Enter the IPv4 address of the default gateway [None]: 172.23.136.1
  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: sec-ifc5
  POD ID: 1
  Controller ID: 1
```

```
  TEP address pool: 10.0.0.0/16
  Infra VLAN ID: 3967
  Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
  Management IP address: 172.23.142.29/21
  Default gateway: 172.23.136.1
  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]:
```

APIC コントローラの 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、APIC コントローラが動作中になった際にポリシーによって、APIC コントローラ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。次のスニペットは、セットアップ時にアウトオブバンド管理インターフェイスのデュアル スタック（IPv6 および IPv4）アドレスを設定する方法について説明する一般的なセットアップ画面です。

```
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): 3967
  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:
```

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 （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

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。